LIVRE BLEU

Tome V

Octobre 2008

Sécurité globale et gestion des risques IT

réalisé par

hapsis education

pour

08 Les Assises

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

Prenez de l'altitude avec Le cercle

Le Cercle Européen de la Sécurité et des Systèmes d'Information rassemble les utilisateurs et décideurs en sécurité informatique

Parce que cybercriminalité 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, d'Experts en sécurité ainsi que de personnalités reconnues, le Cercle compte déjà plus de 500 membres 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, voici le programme du Cercle Européen de la Sécurité et des Systèmes d'Information.

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

un événement

Pour plus d'informations contactez-nous au **01 41 93 09 12**
par courriel **contact@lecercle.biz** ou sur notre site web **www.lecercle.biz**

09 Les Assises
L'Evénement Européen de la Sécurité et des Systèmes d'Information

SOMMAIRE

1- Introduction

Depuis 2004, les enquêtes du Cercle Européen de la Sécurité et des Systèmes d'Information analysent l'évolution des rôles et des activités des professionnels de la Sécurité des Systèmes d'Information (SSI).

Elles ont aussi tracé des perspectives :
- Sur l'importance d'un management stratégique des cyber-risques (2004)
- Sur l'usage d'indicateurs et de tableaux de bord en SSI (2005)
- Sur les grands défis qui attendent les professionnels de la SSI (2006)
- Sur les pouvoirs attachés aux questions de sécurité / sûreté (2007)

Nous avons eu au fil des années, de nombreuses confirmations statistiques qui font apparaître clairement deux « profils types » de RSSI, qu'il convient plus que jamais de distinguer au titre de la séparation des pouvoirs :
- Le pilote centré sur la gestion de risques
- L'opérationnel centré sur la mise en œuvre des moyens

Nous avons aussi constaté que la Sécurité des SI « historique », née il y a une vingtaine d'années, a profondément évolué sous un double effet :
- La dématérialisation des processus et de la société (e-business, e-commerce, e-administration)
- La valorisation et la protection des actifs immatériels (informations stratégiques, personnelles, mais aussi innovations, marques, savoirs, savoir-faire, etc.)

Par ailleurs, la chute du Mur de Berlin, la mondialisation, l'avènement d'Internet, le terrorisme et le crime organisé créent un monde plus dangereux, plus instable, plus « incertain » dont les impacts se font sentir aussi dans le domaine des systèmes d'information.

Ainsi, d'un mal nécessaire associé à toutes sortes de contraintes, la sécurité est bien devenue un service, une valeur ajoutée, sans laquelle la confiance des acteurs et la préservation des intérêts vitaux des organisations ne sont plus garanties.

Explicitant et renforçant cette tendance, le début du XXI^{ème} siècle a vu apparaître le concept de « Sécurité globale ». Il apporte un nouveau regard sur les enjeux contemporains (compréhension, évaluation, protection) de la gestion des risques en relation avec une vision élargie de la sécurité/ sûreté (défense des actifs corporels et incorporels). L'enjeu est de mener, de front, une lutte avant tout préventive et sur un large spectre d'activités.

Car la Société n'accepte plus le moindre petit incident, immédiatement récupéré et amplifié, par les médias et les marchands, ou certains lobbys. Le mythe du « risque zéro » a la vie dure !

L'enjeu est donc d'intégrer globalement :
- Les agressions physiques (enlèvements, pédophilie, violences, etc).
- Les trafics organisés (produits dangereux, contrefaçons, etc.)
- Les fraudes financières (délits d'initiés, malversations, manipulations de cours, etc.)
- Les actes cybercriminels (sabotages, intrusions, fraudes, vols de données, etc.)
- Les actes terroristes (dérives idéologiques, nationalistes ou régionalistes, etc.)
- Les accidents industriels (fuites toxiques, explosions, etc.)
- Les catastrophes naturelles (ouragans, inondations, tremblements de terre, etc.)
- Les pandémies (grippe aviaire, etc.)

Ainsi, se forge une solidarité entre nations, entreprises, associations et citoyens où qu'ils soient localisés sur la planète. La gestion de ces risques, de nature stratégique, implique certes les pouvoirs publics (concentrés sur la protection des populations et le développement durable), mais aussi et surtout les entreprises (préoccupées par la croissance de l'activité économique et de leur valeur financière).

Le thème de l'année **« Sécurité globale et gestion des risques informatiques »** est encore une fois ambitieux et nous l'aborderons avec humilité. Trois axes pourraient être abordés :

- Les infrastructures informatiques, les réseaux et les données comme cibles des menaces et des attaques,
- Les outils informatiques comme moyens de la malveillance, voire véritables armes de guerre,
- Les systèmes d'information comme moyens de protection, de surveillance, de renseignement.

Le propos du Livre Bleu 2008 ne sera pas d'analyser ces trois dimensions. Il mesure les évolutions de la fonction SSI face au développement de la Sécurité globale en s'appuyant sur les résultats de l'enquête du Cercle Européen de la Sécurité et des Systèmes d'Information.

Les chiffres produits n'ont de valeur que par la qualité d'un panel qui s'est progressivement élargi passant de 40 personnes en 2004 à 174 en 2008 contre 107 en 2007 (soit +60%). Cette évolution n'est pas sans influence sur certains résultats. Des variations assez importantes sont apparues (baisses statistiques significatives). Elles trouvent leur explication à la fois dans l'évolution structurelle de la fonction SSI et dans l'élargissement voulu du panel.

Nous avons aussi pu effectuer des « zooms », toujours instructifs, pour 4 secteurs d'activité : Banque/Finance/Assurance, Administration/Services publics, Industrie, High Tech/Médias.

Les 4 secteurs d'activité analysés

Banque/Finance Assurance | Administration Services publics | Industrie | High Tech Médias

L'analyse des chiffres est aussi renforcée par les avis de 3 professionnels reconnus qui doivent être remerciés :

- Isabelle Tisserand (Coordinatrice du Cercle)
- Eric A. Caprioli (Avocat à la Cour - Caprioli & Associés)
- Hervé Schmidt (Président - Cercle Gaspar)

Enfin, nous remercions chaleureusement tous ceux qui oeuvrent à cette démarche, chez DG Consultants, au Cercle, mais aussi tous les participants anciens et nouveaux à cette enquête.

Nous espérons vivement que ce 5ème volet des Livres Bleus des Assises vous éclairera dans vos activités quotidiennes, présentes et futures.

Pierre-Luc REFALO, Hapsis Education

2 - PRÉAMBULE : CONCEPT DE SÉCURITÉ GLOBALE

2.1. Définitions

En 2005, la revue « La Pensée et les hommes » (N°57 – Editions Espaces de Libertés) a tenté d' « imaginer la Sécurité globale », sous la houlette de Patrick Laclémence. Parmi les thématiques abordées, nous pouvions remarquer entre autres :

- Vivre ensemble sans nos peurs
- Entre second souffle démocratique et autoritarisme de la précaution
- On veille sur vous, on vous surveille
- Sport et violence
- Etc.

A l'époque, on constatait l'aspect fragmentaire et encore très conceptuel de la Sécurité globale. Pourtant, peu à peu, les travaux ont conduit à se focaliser sur des menaces stratégiques dont les origines et les conséquences :

- Remettent en cause les équilibres fragiles de la démocratie et de l'économie libérale
- Ne distinguent pas les victimes (populations, entreprises, ONG, Etats)
- Ne connaissent pas les frontières

« Le concept de Sécurité globale correspond « au-delà d'un Etat, à la capacité d'assurer à une collectivité quelconque et à ses membres, un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture dommageable de la vie et des activités collectives et individuelles. »

Définition de la Sécurité globale pour l'INHES
(Institut National des Haute Etudes de la Sécurité)

Dans une note de la Fondation pour la Recherche Stratégique (J-F. Daguzan– Avril 2007), l'accent est mis sur le besoin de « Sécurité individuelle » ou de « Sécurité humaine » à laquelle répond la Sécurité globale, en opposition avec la Défense « classique » qui vise avant tout une « Sécurité collective » et qui répond à des menaces agressives et malveillantes. L'enjeu est donc de garantir à chacun ses besoins (eau, énergie, alimentation) et les services essentiels (transports, banque, télécoms, santé, information).

C'est peu dit, mais la Sécurité globale, si elle est garantie pour tous, sera synonyme de paix.

Dans le 1er numéro de la revue « Sécurité Globale » créée à l'automne 2007 (Editions Choiseul), L'ingénieur Général de l'Armement, Jacques Roujansky, propose un bilan des travaux dans le domaine et une « stratégie pour piloter la Sécurité globale ». On y découvre que dès 2004, les experts préconisaient de développer cinq fonctions principales :

- Identification des personnes
- Sécurité des Systèmes d'Information
- Traitement automatisé de la cybercriminalité
- Renseignement
- Gestion des crises

Les Systèmes d'Information et leur sécurité sont ainsi placés au cœur du management de la Sécurité globale, en amont et en aval.

C'est aussi ce que confirme une étude réalisée par Thales en 2007 dont certains résultats sont frappants.

- Trois quarts des entreprises interrogées seraient déjà engagées dans une approche globale de la Sécurité.
- Les 3 risques majeurs devant être traités par la Sécurité globale sont :
  - les atteintes à l'image,
  - les violations de la loi,
  - les attaques contre le système d'information.
- 70% des entreprises considèrent la Sécurité globale comme une réponse pour « assurer un développement à long terme de l'entreprise ».

Dès lors, la mise en œuvre effective d'une Politique de Sécurité globale est un enjeu majeur et nécessaire au développement de l'économie.

2.2. La démarche engagée en France

L'Etat a pris conscience du concept de Sécurité globale dans le cadre du décret n° 2006-212 du 23 février 2006 relatif à la Sécurité des Activités d'Importance Vitale (SAIV), complété par l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs : activités civiles de l'État ; activités judiciaires ; activités militaires de l'État ; alimentation ; communications électroniques, audiovisuel et information ; énergie ; espace et recherche ; finances ; gestion de l'eau ; industrie ; santé ; transports.

Le décret SAIV a été pris en application des articles L.1332-1 et suivants du code de la Défense. Il réforme le régime de vigilance et de protection des installations les plus sensibles pour la défense de la Nation et la sécurité de l'État et s'inscrit dans une démarche de Sécurité globale.

Il désigne également **les principaux acteurs au sein de ces secteurs, permettant la protection des populations et le maintien de l'activité économique, ces derniers étant nommés « opérateurs d'importance vitale » (OIV).**

Sous la responsabilité d'un ministre coordinateur, une Directive Nationale de Sécurité (DNS) est rédigée par l'Etat afin :

- D'identifier les types de menaces (terrorisme, organisations criminelles,...)
- D'en définir les scénarios potentiels (attentats, cybercriminalité,...)

Cette approche est applicable au sein de chaque secteur. Ainsi, il est clair que les transports sont particulièrement impliqués en matière de risque terroriste (détournement, attentat à l'explosif,...). Le secteur des télécommunications pourra être plus spécifiquement menacé par des attaques informatiques, terroristes ou criminelles.

Cette démarche « classique » et « institutionnelle » se heurtera structurellement à plusieurs difficultés majeures.

1-En termes de gouvernance : L'Etat ne doit pas se contenter de Directives imposées mais doit plutôt favoriser la mise en place d'un dialogue régulier entre les parties (publiques, privées, associatives). Chacun devra disposer des interlocuteurs adéquats.

2- Au plan économique : des distorsions de concurrence peuvent apparaître entre les OIV, soumis à des obligations (avec un coût), et les autres entreprises dégagées de telles obligations. Les solutions à ce niveau ne sont évidemment pas simples.

3- Enfin, il est probable que de nombreux opérateurs ne connaissent pas le concept de « Sécurité globale » et une véritable action de pédagogie et de formation semble désormais nécessaire.

2.3. Sécurité vs Sûreté

Alors que le concept de « Sécurité globale » se développe et tend à remodeler les stratégies, la gouvernance et les plans d'action, les questions de « Sûreté » tendraient-elle à disparaître ou à s'intégrer ?

Les deux termes étant régulièrement confondus et aussi de plus en plus utilisés, il semble important de les repositionner.

La **sûreté** est, de façon générale, **un état de protection contre des dangers ou des menaces**. Elle se focalise essentiellement sur la protection contre des menaces externes.

La **sécurité** est **l'état d'esprit d'une personne qui se sent tranquille et confiante** (en anglais = security). C'est aussi le sentiment, bien ou mal fondé, d'être à l'abri de tout danger ou risque (en anglais = safety).

Si la Sécurité et la Sûreté poursuivent des objectifs communs et aboutissent, en final, à des situations similaires, leurs approches diffèrent (l'une, la sécurité, sera plus impliquée de l'aval à l'amont, la sûreté se concentrant sur des mesures de protection).

2.4. Quelques bases philosophiques

Au fil des âges, penseurs, philosophes, politiques et scientifiques se sont préoccupés du risque et de la sécurité / sûreté. Ils font incontestablement partie des bases de la construction de toute société. Bref aperçu, chronologique et non exhaustif.

Sun Tzu

« Celui qui excelle à vaincre ses ennemis triomphe avant que les menaces de ceux-ci ne se concrétisent. »

Jean de la Fontaine

« La méfiance est mère de sûreté. »
« Deux sûretés valent mieux qu'une. »

Pierre Dupont de Nemours

« Point de propriété sans liberté ; point de liberté sans sûreté. »

Thomas Jefferson

« Si tu es prêt à sacrifier un peu de ta liberté pour te sentir en sécurité, tu ne mérites ni l'une ni l'autre. »

Déclaration des droits de l'homme et du citoyen

« Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression. »

Rudyard Kipling

« Il faut toujours prendre le maximum de risques, avec le maximum de précautions. »

Albert Einstein

« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique. »

Alexandre Minkowski

« Accepter les risques inévitables de la vie, c'est ce qui fait la noblesse de la condition humaine. »

Kofi Annan

« Une attaque terroriste contre un pays est une attaque contre l'humanité tout entière. »

Michèle Alliot-Marie

« La Sécurité est la première obligation d'un Etat. »

2.5. Sécurité globale et Sécurité du SI

Comment aborder alors, les questions de Sécurité SI dans le vaste champ de la Sécurité globale ?

Tous les travaux en la matière mettent l'accent sur trois enjeux directement liés aux systèmes d'information :

- **L'identification** : protéger l'individu des usurpations d'identité et des malveillances qui y sont liées.
- **La surveillance** : prévenir les actes (cyber) criminels voire les crises majeures, par des actions de renseignement et de contrôles renforcés.
- **Les infrastructures critiques** : protéger les systèmes d'information et de communication pour les rendre le moins vulnérable possible et garantir leur fonctionnement en cas de crise.

Ces trois aspects seront mis en exergue dans les chapitres suivants.

2.5.1. Cybercriminalité : quelques faits d'actualité 2007 / 2008

La cybercriminalité doit être perçue comme tous les actes sanctionnés pénalement qui portent atteinte aux systèmes d'information (sabotages, intrusions) ou les exploitent à des fins frauduleuses (escroqueries, détournements, etc.), d'atteintes à la vie privée, d'espionnages, de diffusion de contenus illégaux, de contrefaçons, etc.

Peu importe la potentialité de menaces colportées par les vendeurs. Rien ne compte plus que les leçons à retenir de faits réels qui démontrent non seulement la faiblesse des Systèmes d'Information, les limites des mesures de protection mais aussi la puissance des techniques de fraude et de malveillance, sans oublier les forces / faiblesses organisationnelles et managériales.

Affaire « Kerviel » : manipulations financières sur des marchés créant un préjudice de 4,9 milliards d'euros pour la Société Générale. Fraude, complaisance ou faiblesse du contrôle interne ?

L'Estonie « bombardée » : attaques informatiques massives sur les sites gouvernementaux et bancaires du pays balte. Représailles russes suite au retrait de monuments à la gloire de l'Armée Rouge ?

Un Cheval de Troie à Sumitomo Bank : des détournements de fonds, opérés via l'installation d'un cheval de Troie (par une femme de ménage) sur un ordinateur placé à Londres. Acte isolé ou organisé ? A distance ou local ?

Des CDs « disparaissent » : sont concernées des données personnelles de plusieurs millions de retraités de l'armée américaine. CDs égarés, vendus ou volés ?

Blocage à la Mairie de San Francisco : chantage d'un administrateur du réseau, voulant dénoncer les faiblesses de la sécurité interne et menaçant de bloquer les services municipaux. Psychose ou réalité ?

Cybercriminels en Roumanie et en France : démantèlement de réseaux organisés dans des actions de phishing à grande échelle.

Manipulations en ligne : suicide d'une adolescente américaine après une rupture « virtuelle ». Elle était en fait manipulée sur MySpace par une adulte se faisant passer pour son fils.

2.5.2. Exploitation des résultats de l'enquête 2008

Le Livre Bleu des Assises 2008 présente l'analyse de l'enquête du Cercle, orientée selon la thématique de la Sécurité globale.

Il est structuré en 3 volets :

1-La perception de la Sécurité globale et ses impacts sur la SSI
2-La gouvernance de la SSI dans le cadre de la Sécurité globale
3-3 avis d'experts
- Le dilemme sécurité / liberté : gérer les intrusions dans la vie privée (Eric A. Caprioli)
- L'équilibre prévention / réaction : anticiper la gestion des crises (Hervé Schmidt)
- Le facteur humain : comprendre la crise (Isabelle Tisserand)

Avertissement : Nous analysons les résultats de l'enquête (la réalité du terrain) en rapport avec le concept de « Sécurité globale ». Nous ne cherchons pas à le redéfinir ou le préciser, et en aucun cas, nous ne pouvons être exhaustifs sur le sujet.

3- Perception de la Sécurité globale

3.1. Préambule

Dans son enquête de 2006, Thales avait identifié trois axes de progrès pour que la « Sécurité globale » devienne une réalité intégrée dans le management :

- Installer la fonction en définissant le champ d'action, en établissant une reconnaissance stratégique et en conduisant le **changement organisationnel**,
- Mettre en place des outils, avec comme priorité des indicateurs « temps réel », en construisant la **mesure du retour sur investissement**, en capitalisant sur les points forts des secteurs d'activités les plus avancés,
- Construire sur le **facteur humain**, en mobilisant le management, trouvant de nouveaux modes de sensibilisation et surtout en communiquant mieux.

En clair, tout reste à faire !

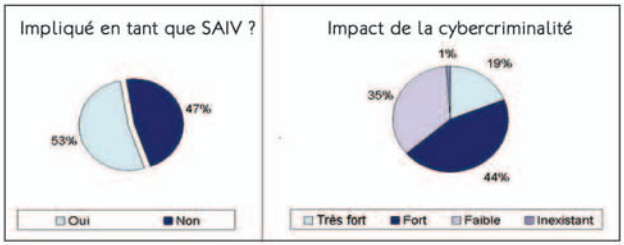
Ce chapitre se propose d'analyser comment est perçue la Sécurité globale au regard de tendances fortes ayant un lien avec la Sécurité des SI (Secteurs d'Activités à Infrastructures Vitales (SAIV) et Cybercriminalité) en précisant les impacts en termes de « veille et contrôle ».

Sont ensuite abordées les questions de « synergies organisationnelles » qui sont la clé de la mise en œuvre progressive d'un management global de la sécurité.

Dans la suite du document, les statistiques des schémas doivent être considérées en % de réponses des membres du panel sur une base de 174 participants (sauf indication spécifique).

3.2. Cybercriminalité et Secteurs d'Activité à Infrastructure Vitale

Ces deux paramètres sont des bras de levier importants dans la gestion des risques qui visent ou exploitent les systèmes d'information. Une majorité des répondants est concernée et par voie de conséquence « mûre » pour l'intégration d'un management de la sécurité globale.



Sans surprise, la gestion de la cybercriminalité est plus intégrée que la notion de Secteur d'activité d'Infrastructure Vitale.

Seulement 1/3 du panel est peu ou pas impacté par la cybercriminalité. On peut imaginer que ces professionnels interviennent d'abord sur des menaces et vulnérabilités internes dans une approche « qualité » plus que « sécurité / sûreté ».

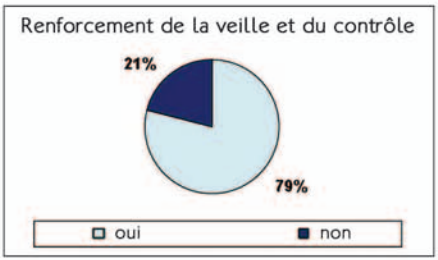
Zoom par secteur d'activité

				
Impliqué en tant que SAIV	55%	57%	73%	47%
Impact fort ou très fort de la cybercriminalité	64%	68%	73%	40%

Les divergences par secteurs d'activité sont très importantes et aussi surprenantes. Alors que l'Industrie est fortement concernée, le secteur des Médias / High Tech se situe très en retrait. Les maturités de la Banque/Finance et de l'Administration/Services publics sont similaires.

3.3. Impacts sur la veille et le contrôle

La prise en compte d'enjeux et de menaces qui peuvent compromettre gravement l'atteinte des objectifs d'une organisation (avec impacts majeurs médiatiques, économiques ou juridiques) implique nécessairement des conséquences opérationnelles. C'est notamment le cas en termes de prévention ou d'anticipation (veille, renseignement, contrôle, surveillance).



Le rapprochement des fonctions « Sécurité SI» et du contrôle interne s'est opéré depuis plusieurs années là où le management des risques s'est instauré et s'est séparé de la sécurité opérationnelle (Banque/Finance notamment). Quoiqu'il en soit, la tendance devrait et doit se poursuivre voire se renforcer (à l'instar des faiblesses constatées dans une affaire comme celle de la Société Générale fin 2007).

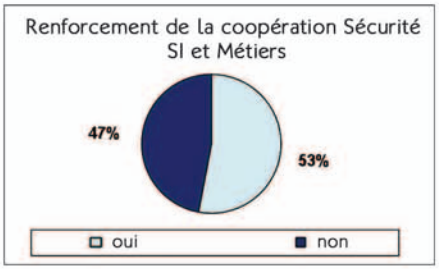
La Sécurité globale doit avoir des impacts significatifs en termes de gouvernance pour faciliter la séparation des pouvoirs et renforcer des actions opérationnelles à caractère stratégique.
Sinon, la sécurité se contente de « jouer » aux « boucheurs de trous » et aux « pompiers ».

3.4. Synergies organisationnelles

La mise en place d'une Politique de Sécurité globale ne peut s'opérer que dans la durée, petit à petit, avec un véritable accompagnement du changement. Dans l'intermède, des synergies anciennes ou en cours doivent se renforcer et d'autres se créer. Nous insistons ici sur trois d'entre elles.

3.4.1. Avec les métiers

C'est sans doute le plus important. On ne cesse de le dire depuis 20 ans mais la clé du succès des pratiques de sécurité (prévention et protection, voire réaction) réside dans leur capacité d'intégration et de prise en compte dans tous les métiers et à tous les niveaux de management.

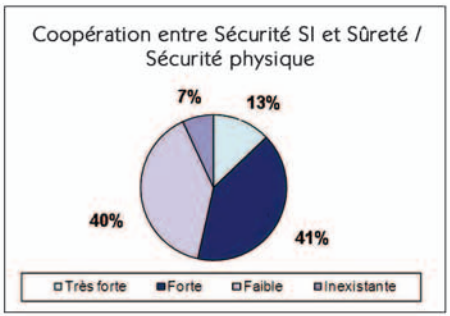


Le développement de la cybercriminalité fait peser des risques croissants sur le « business » et dans tous les secteurs d'activité comme au niveau des Etats. Il n'est donc pas surprenant que les professionnels du panel constatent que leur collaboration avec les métiers se renforcent. C'est encourageant !

Aucune différence n'apparaît entre les secteurs d'activité.

3.4.2. Physique et Logique

La Sécurité globale implique aussi des recouvrements dans la gestion des failles techniques, informatiques et comportementales, comme des menaces internes et externes. La sécurité des SI et la sécurité physique se sont longtemps « observées » sans réellement coopérer.



Cette situation perdure malheureusement, car près de la moitié du panel avoue une coopération insuffisante.

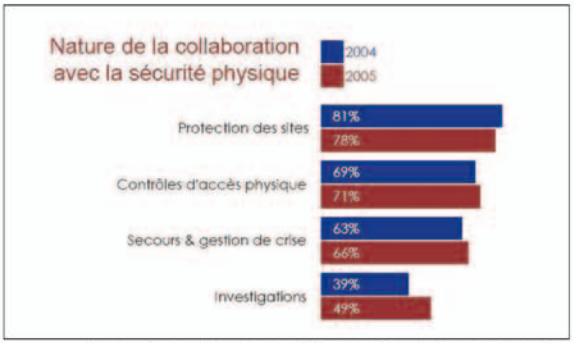
Zoom par secteur d'activité

Sécurité SI et Sûreté / Sécurité physique				
Coopération forte ou très forte	51%	63%	53%	27%

Les divergences sont ici très fortes entre les secteurs d'activité. L'Administration/Services publics semblent les plus avancés alors que les Médias / High Tech sont très en retrait.

Globalement, le bilan reste très mitigé et il demeure une grande marge de progrès à ce niveau.

En 2004 et 2005, nous avions déjà abordé cette dimension qui prend une importance plus forte dans le cadre de la Sécurité globale.

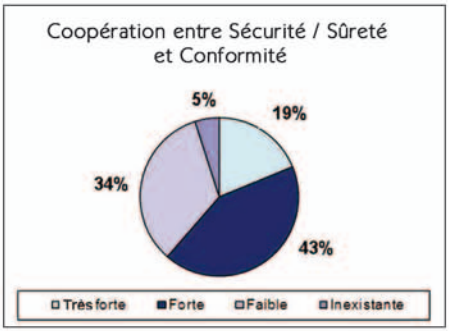


Source : Cercle Européen de la Sécurité et des Systèmes d'Information

La gestion des crises et les investigations apparaissaient à l'époque en retrait, pour ceux qui ont noué des relations avec les Services généraux ou les directions de la Sécurité / Sûreté.

3.4.3. Avec la conformité

Cet aspect ne concerne pas tout le panel (128 réponses sur les 174 potentielles). Les deux fonctions se regardent souvent en « chiens de faïence » !



Beaucoup d'aspects de sécurité (des SI et des informations) ont des connotations juridiques ou réglementaires que les équipes « conformité » ont d'abord souvent abordé du bout des doigts (CNIL par exemple). Mais progressivement, elles s'approprient ces domaines tout en devant nouer des relations fortes avec les équipes Sécurité.

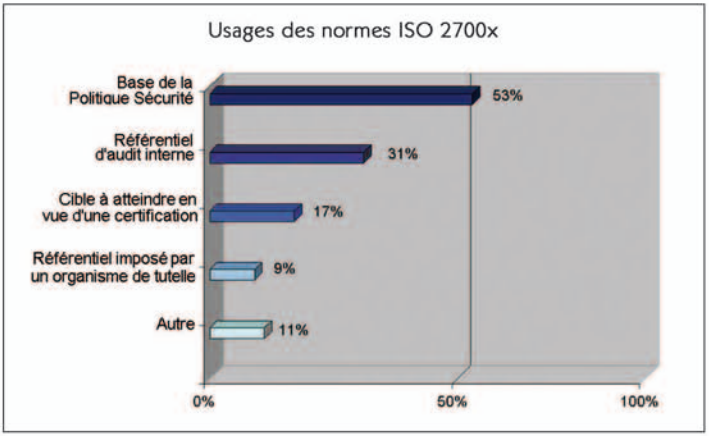
Zoom par secteur d'activité

Sécurité SI et Conformité				
Coopération forte ou très forte	61%	71%	53%	64%

L'Administration/Services publics est en tête de ces questions tandis que l'Industrie se situe en retrait.

Globalement, la situation dans ce domaine est encourageante et des progrès sont sans doute en cours.

Par ailleurs, la prise en compte des normes ISO 2700x dans le management de la sécurité de l'information peut apporter des points de convergence et de coopération plus que des oppositions ou rivalités.



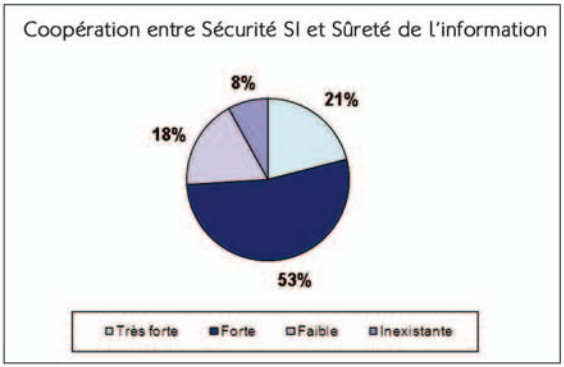
A ce jour, les fonctions SSI se sont emparées de ces normes mais pas nécessairement dans une logique de « conformité » voire de « certification ». On constate qu'elles sont avant tout considérées comme une aide à l'élaboration d'une politique (53%) puis comme un référentiel d'audit interne (31%).

3.4.4. Avec la sûreté de l'information

On entend par Sûreté de l'Information la mise en place de processus de protection de l'information confidentielle face à des menaces malveillantes et d'origine supposée externe (même si les collusions ou attaques internes sont possibles).

Comme nous le verrons plus loin, la distinction entre Sécurité des SI et Sûreté de l'information est de plus en plus forte. Aussi, la répartition des rôles et les synergies doivent se préciser entre ce qui touche aux contenants (infrastructures) et aux contenus (informations).

L'ensemble du panel a répondu à la question, ce qui présuppose que la notion est, sinon en place, au moins appréhendée.



C'est à ce niveau que la synergie est la plus forte avec environ les ¾ du panel pour qui la coopération est forte ou très forte.

Zoom par secteur d'activité

Sécurité SI et Sûreté de l'information				
Coopération forte ou très forte	74%	81%	71%	54%

Le secteur des médias / High Tech se situe ici encore très en retrait par rapport aux autres secteurs d'activités tandis que l'Administration/Services publics se place en tête avec 81%.

3.5. Bilan

La Sécurité globale n'est pas encore suffisamment prise en compte par les membres du panel mais de nombreux aspects qui la composent sont déjà appréhendés.

La protection des infrastructures est d'évidence le domaine le plus simple à aborder. Que ce soit au plan des SAIV (malgré de grandes divergences par secteurs d'activité) ou de la montée de la cybercriminalité, la Sécurité des SI ne peut pas être absente des enjeux et des processus à mettre en œuvre. Les atouts de la SSI sont indéniables aux plans méthodologique et technologique comme en termes opérationnels dans le domaine du « contrôle » et de la « surveillance ».

Néanmoins, une « guerre sans fin » est à prévoir où agissent :
- Les offreurs de technologies emplies de vulnérabilités, parfois critiques,
- Les « experts » avides de dénoncer ces failles « potentielles » et alimentant un marketing de la peur toujours un peu facile,
- Les marchands disposés à proposer (le plus rapidement possible) des « correctifs » ou des « solutions palliatives » (les « anti-truc »),
- Et enfin les « attaquants » qui restent à l'affût de toute opportunité, en tout lieu, à tout moment, et sans scrupule envers les victimes potentielles.

La gestion des identités demeure un domaine éminemment complexe et la sécurité des SI n'a toujours pas démontré sa capacité à proposer des solutions et des processus simples et efficaces. La biométrie et les cartes à puce s'inscrivent dans ce vaste champ de l'identification / authentification et semblent devoir, à terme, offrir une solution globale qu'il conviendra encore de faire accepter à tous.

Enfin, la gestion des crises reste un domaine encore insuffisamment exploré. La SSI agissant quasi-uniquement en termes de prévention, elle reste éloignée de cet enjeu majeur pour la Sécurité globale.

4- Gouvernance de la Sécurité des SI

Ce volet est consacré à une analyse des résultats de l'enquête 2008 en mettant en évidence les évolutions majeures depuis 3 ans et les enseignements pertinents en termes de Sécurité globale.

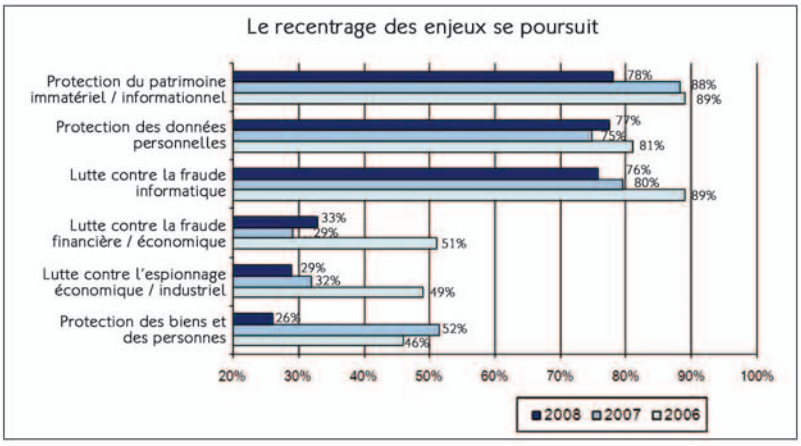
4.1. Quel périmètre ?

Depuis 2004, nous avons défini 6 grands enjeux (voir schéma ci-dessous) directement liés ou non à la Sécurité des SI. Ce périmètre s'inscrit complètement dans le champ de la Sécurité globale. Certes, les pandémies et le terrorisme n'apparaissent pas explicitement (ce sont des menaces et non des enjeux) mais on conçoit qu'ils s'intègrent totalement dans la protection des biens et des personnes.

En 2008, nous constatons que le recentrage se poursuit autour de 3 enjeux directement liés à la SSI. On peut penser que les années précédentes, faute de référentiels précis et d'un management global, les membres du panel agissaient parfois au-delà de leur cadre naturel.

Désormais, face à la complexité et à l'importance de chaque enjeu, les professionnels se doivent d'agir « à fond » dans leur domaine de prédilection, et ce, en relation avec d'autres acteurs internes et externes.

Enfin, il est remarquable de noter que c'est vraiment de Protection de l'Information (stratégique, personnelle) dont s'occupent prioritairement les membres du panel. La fraude informatique, qu'on assimilera aux actes intrusifs et de sabotages, n'est pas en tête, sans doute sous l'effet d'une prise en compte par des acteurs opérationnels (internes ou externes).



La Sécurité des SI poursuit son recentrage sur la protection du patrimoine et de l'information, véritable actif des organisations, sans sortir de son champ naturel de prévention des attaques informatiques.

Zoom par secteur d'activité

« Top 3 des enjeux »				
Protection du patrimoine immatériel	82%	73%	85%	83%
Protection des données personnelles	89%	70%	80%	78%
Lutte contre la Fraude informatique	81%	88%	70%	61%

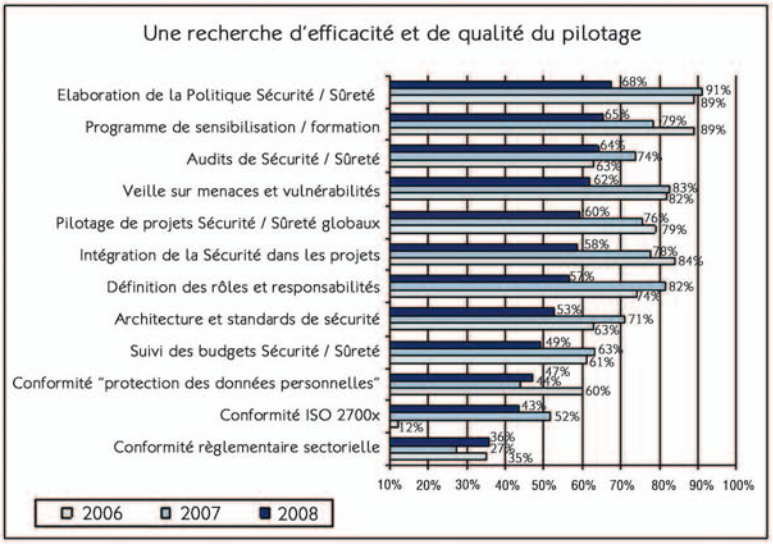
Un filtre effectué sur les 120 Directeurs / Responsables Sécurité SI ou Sûreté de l'Information montre des différences significatives pour les 3 enjeux de type « protection ».

- Protection du patrimoine informationnel : 84% contre 78% pour l'ensemble du panel
- Protection des données personnelles : 83% contre 77% pour l'ensemble du panel
- Protection des biens et des personnes : 22% contre 26% pour l'ensemble du panel

On retrouve ici les valeurs des enquêtes précédentes où le panel était constitué exclusivement de professionnels de la SSI.

4.2. Quelles actions de pilotage ?

La mise en place d'un management stratégique des risques est devenue une réalité dans de nombreuses entreprises. En garantissant la séparation des pouvoirs et en renforçant les capacités de contrôle et d'audit (indépendants), les entreprises constatent aussi l'ampleur des mesures à mettre en place. Douze actions « types » ont été proposées au panel.



Le constat est frappant :
- Toutes les actions baissent parfois significativement.
- Après la définition de la Politique Sécurité, ce sont la formation / sensibilisation et les audits qui se placent en tête (pour environ 2/3 du panel).
- Les activités liées à la Conformité résistent voire se développent.

L'élargissement du panel explique ici aussi certaines baisses mais on constate un recentrage des actions vers un véritable pilotage « amont » sans toutefois se dissocier de « l'aval » (démarche projet, veille, architecture).

Les questions de gouvernance restent logiquement majoritaires (compte-tenu du panel de l'enquête) tandis que la conformité « sécurité » se développe lentement.

Zoom par secteur d'activité

Conformité				
Protection des données personnelles	52%	50%	65%	53%
ISO 2700x	45%	40%	56%	29%
Réglementaire sectorielle	34%	30%	28%	47%

Le secteur de l'Industrie se distingue dans le domaine de la Conformité sans doute par manque de fonction dédiée ou insiffisamment développée en la matière. Les professionnels de la Sécurité intègrent donc plus ces aspects dans leurs missions. C'est aussi le cas du secteur High Tech/Médias pour les règlementations plus « sectorielles » (propriété intellectuelle ou secret des correspondances par exemple).

4.3. Quels rôles au quotidien ?

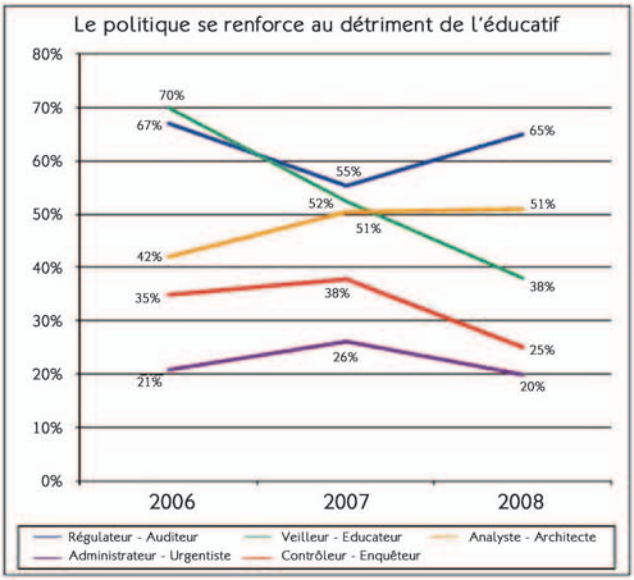
Le panel 2008 s'inscrit encore plus fortement au plan de la stratégie ou de la politique. Néanmoins, celui-ci s'étant élargi au-delà de la SSI, on distingue plus difficilement qu'en 2007, les 2 profils de RSSI :
- Le Pilote : Régulateur-Auditeur + Veilleur-Educateur
- L'Opérationnel : Analyste-Architecte + Administrateur-Urgentiste

La baisse des statistiques brutes démontre ici encore un recentrage et une focalisation des rôles tenus au quotidien par les professionnels : on ne peut pas tout faire !

Il n'en demeure pas moins que l'évolution majeure concerne la diminution continue de leur implication directe dans la « veille » et la « sensibilisation ». Celles-ci sont sans doute désormais très largement sous-traitées (les membres du panel ne s'impliquent pas ou plus directement dans ces activités). Les RSSI qui ont assumé ce rôle au lancement de leur mission doivent aujourd'hui renouveler leurs approches et font appel à des structures spécialisées voire à des agences de communication.

C'est aussi certainement le cas dans le domaine du contrôle et des investigations. Les membres du panel se détachent d'activités qu'ils ont assurées par défaut au profit d'experts internes ou externes.

Les deux tiers du panel se positionnent dans une position « régalienne » démontrant l'importance de la séparation des pouvoirs, essentielle en termes de Sécurité globale.



L'évolution des rôles des professionnels est encourageante sous l'influence d'une meilleure gouvernance et du marché qui propose les services requis.

4.4. Confidentialité vs disponibilité ?

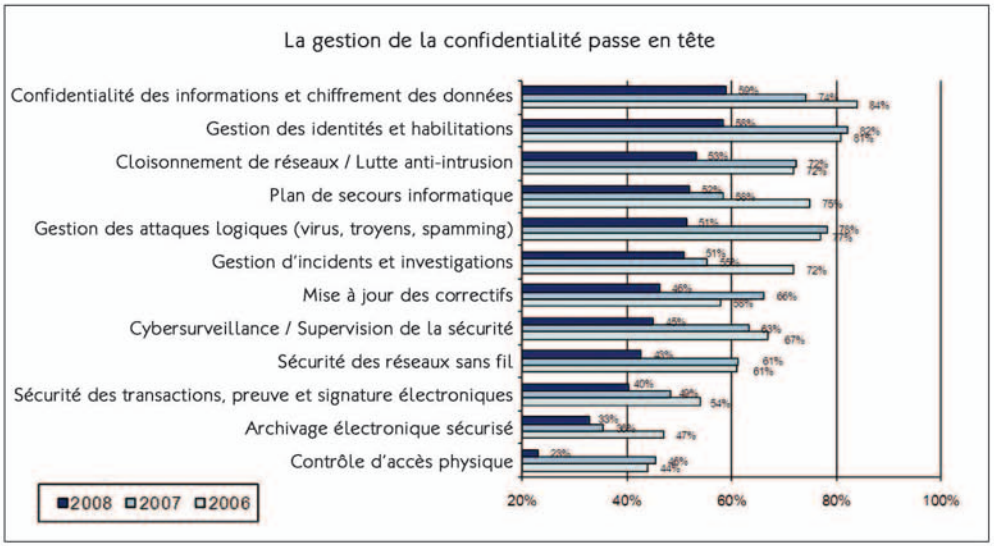
L'analyse des processus opérationnels dans lesquels s'implique le panel est encore une fois significative des évolutions suivies ces dernières années. La tendance au « 50% » pour les questions purement informatiques (sécurité réseau, plan de secours) tend aussi à montrer que la moitié du panel conserve une orientation « opérationnelle », l'autre moitié étant plus de nature « pilotage » ou « maîtrise d'ouvrage ».

La gestion de la confidentialité (re) passe en tête et au même niveau que la gestion des identités. Ce sont des préoccupations, anciennes qui ne sont toujours pas correctement garanties, notamment au regard des 2 enjeux :

- la protection de la vie privée (intrusions dans la vie privée et le vol d'identités)
- le développement de l'espionnage économique et industriel (atteintes au savoir et au savoir faire)

Il convient néanmoins de bien lier ce constat avec deux points majeurs :

1. Le chiffrement des données doit se développer, certes, mais l'outil n'est pertinent qu'avec un accompagnement éducatif et des processus allant jusqu'à la destruction des données.
2. La détection des vols, divulgations, intrusions ne peut s'effectuer sans un contrôle et une surveillance des flux et des accès comme des utilisateurs (authentification forte et fiable).



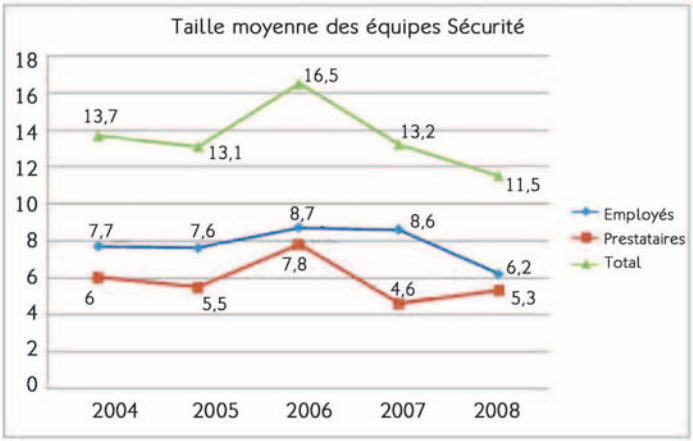
La protection des infrastructures (comme la cyber-surveillance) se situe un peu en retrait et intègre environ la moitié des processus proposés (approche informatique de la Sécurité SI). La moitié du panel est d'évidence de nature « opérationnelle » au sein des DSI.

L'ensemble des processus de la SSI couvre les 3 aspects visés dans le cadre de la Sécurité globale (gestion des identités, veille - surveillance et protection des infrastructures critiques). La cyber-surveillance apparaît néanmoins en retrait à ce jour.

4.5. Un poids relatif toujours significatif des prestataires

Nous abordons ici un des indicateurs clés des enquêtes du Cercle. Une part significative mais en forte baisse du panel reste sans équipe interne (26% de « solitaires ») alors que 21% d'entre eux n'ont qu'un collaborateur (binômes). Mais ils s'appuient alors plus ou moins fortement sur des consultants.

Le panel a aussi évolué et certainement vers des professionnels aux équipes plus réduites (quelques personnes) et fortement aidées par des prestataires.



L'élargissement du panel réduit mécaniquement la taille moyenne des équipes « Sécurité ». Dans les grands comptes, il est fréquent de constater une proportion de 50 à 60% de prestataires SSI, ce que confirment nos résultats.

L'analyse des équipes par secteur d'activité apporte un éclairage intéressant où l'Administration/ Services Publics disposent d'équipes avec environ 20% de collaborateurs de plus que les banques.

Zoom par secteur d'activité

Taille des équipes Sécurité				
Employés	6	7,4	5,9	6,1
Prestataires	5	5,8	3,8	5,1
Total	11	13,2	9,7	11,2

4.6. Bilan

La gouvernance de la Sécurité des SI possède incontestablement de nombreux atouts pour s'intégrer à un management global de la sécurité et des risques.

1. La séparation des pouvoirs avec 2 profils de RSSI (pilote et opérationnel) est une tendance de fond désormais bien ancrée dans de nombreuses entreprises. Le RSSI Pilote doit désormais s'intégrer à une Direction (si possible de la Sécurité globale, voire des Risques) indépendante de la DSI.
2. Le déploiement des normes ISO 2700x facilite la prise en compte des meilleures pratiques de management et offre un cadre pertinent pour les démarches de conformité.
3. La Sécurité des SI tend à se re-concentrer sur la protection des infrastructures tandis que la Protection du Patrimoine Informationnel (sous entendu « Sûreté de l'information »), bien engagée dans certains secteurs (Industrie, Assurance), se développe dans d'autres (Banque).
4. La Sécurité des SI a beaucoup investi dans des plans de secours dont l'efficacité n'est pas toujours garantie tandis que la continuité des activités et la gestion des crises ont souvent été négligées.

Désormais, il conviendra de se concentrer sur certains points :

1- Le RSSI-Pilote doit être clairement désigné et nommé car il ne peut pas être Responsable de la Sécurité du SI. C'est impossible, d'autant plus qu'il n'appartient pas toujours à la DSI.

2- L'externalisation (voire l'offshore) pose des problèmes de fond, notamment au niveau des équipes de développement et d'exploitation de systèmes ou de réseaux. Et les solutions ne sont pas simples dès lors que l'économie prime sur le reste.

3- Transformer les nombreux essais dans le domaine de la gestion des identités, de l'authentification forte, etc. Si la biométrie apporte un plus, elle ne règle pas tous les problèmes.

4- Les pratiques d'audits se sont industrialisées mais ne sont pas toujours indépendantes et professionnalisées. La certification individuelle dans ce domaine devra se développer.

5- Avis d'experts

5.1. Préambule

Comme indiqué en introduction, la définition de la Sécurité globale pose des problématiques de fond dans plusieurs domaines. La gouvernance, bien sûr, que les chapitres précédents tentent d'éclairer.

Mais des points très sensibles méritent aussi d'être appréhendés. Et trois experts reconnus nous apportent aussi leur éclairage sur :

- Le dilemme Sécurité / Liberté et l'enjeu du respect de la vie privée à l'heure de la surveillance et du contrôle généralisés : Eric A. Caprioli
- Le dilemme « prévention – réaction » et l'enjeu d'une gestion de crise efficace face à l'incertitude de menaces de nature stratégique : Hervé Schmidt
- Le facteur humain et la conscience de la crise : Isabelle Tisserand

5.2. Le dilemme « Sécurité - Liberté » par Eric A. CAPRIOLI

La réduction du périmètre de la vie privée au profit du développement des normes sécuritaires est un débat de société, intéressant tant les citoyens que les entreprises depuis déjà plusieurs années. La rapidité de développement des techniques de fraude et d'atteintes aux droits des citoyens a conduit au contrôle des activités des individus (biométrie, géolocalisation, RFID..., v. Eric Caprioli et Pascal Agosti, L'identification par Radio fréquence et le droit, Confidentiel Sécurité, n°128, décembre 2005, p. 2 et s). Or, face à la cybersurveillance, la protection juridique de la vie privée a eu parfois du mal à s'adapter voire à perdurer.

C'est justement ce thème que la CNIL a choisi de mettre en avant dans son 27ème rapport d'activité pour l'année 2006, publié le 13 juillet 2007, en choisissant d'intituler son sujet principal « Alerte à la société de surveillance ». Elle met ainsi en avant le risque pour la population de voir restreindre ses libertés sans même s'en rendre compte, avec l'incessante évolution des technologies de surveillance et l'augmentation des textes législatifs et réglementaires permettant leur utilisation. Ce risque ne concerne pas que la France, mais tous les pays occidentaux et, selon la CNIL, il est souvent issu des exigences des autorités américaines. Par exemple, les Etats-Unis ont récemment proposé aux Etats de l'Union européenne de signer des accords bilatéraux (Protocoles d'accord appelés Memorandum of Understanding et faisant suite à l'accord PNR Etats Unis- Europe signé en juillet 2007) concernant la sécurité, dans le but de moderniser leur programme d'exemption de visa. La mise en place de ce dispositif ayant soulevé quelques questions quant à la protection des données à caractère personnel des citoyens, la CNIL veille à ce que certaines garanties (droits d'accès, de rectification aux données collectées visant les personnes et proportionnalité des traitements de données à caractère personnel) soient respectées.

Les domaines dans lesquels la liberté des personnes peut être atteinte sont nombreux. La CNIL a tenté d'encadrer le développement de la géolocalisation des véhicules des employés par GPS dans une recommandation du 16 mars 2006 (disponible sur le site www.cnil.fr), leur mise en œuvre ne pouvant être justifiée que par un nombre limité de finalités. Encore plus commun, le passe Navigo de la RATP est un moyen de ficher les personnes et de répertorier leurs trajets. C'est pour cela que la CNIL a exigé que les informations soient cryptées afin d'éviter leur exploitation à des fins commerciales. L'utilisation croissante de la biométrie nécessite également de contrôler l'utilisation qui est faite de ces données à caractère personnel particulièrement sensibles et soumises à autorisation (par exemple, TGI Paris du 19 avril 2005, disponible sur le site : www.legalis.net). En revanche, la CNIL a parfois eu plus de mal à se faire entendre, comme au sujet de la vidéosurveillance. La loi du 23 janvier 2006 relative à la lutte contre le terrorisme en a étendu l'utilisation et a autorisé la police à avoir accès aux images hors d'une enquête judiciaire. La CNIL avait émis un avis le 10 octobre 2005 visant à offrir plus de garanties par rapport à la vie privée mais il n'a pas été retenu pour des raisons de sécurité publique.

Le monde du travail est également un secteur privilégié pour évoquer ce problème. En effet, les employés ont droit au respect de leur vie privée sur leur lieu de travail, mais ce droit est limité pour des raisons de sécurité propres à l'entreprise (v. la jurisprudence découlant de l'arrêt Nikon (Cass. soc., 2 octobre 2001, Nikon c/ F. Ono, Bull. civ. V, n°291 et où l'on voit bien la prise en compte de plus en plus marquée des intérêts de l'entreprise confrontée à des employés peu scrupuleux utilisant les données de l'entreprise ou les outils mis à leur disposition : Cass. soc.

17 mai 2005, Philippe X c/ Cathnet-Science, Bull. civ. V, n°1089 ; Cass. soc., 21 décembre 2006, P. c/ Sté Ad 2 One : R.D.B.F,. 2007, comm.125, note Éric. A Caprioli ; Cass. soc. 30 mai 2007, commentaire E. A. Caprioli, R.D.B.F Novembre-Décembre 2007, n°233, p. 59 et s ; Cass. soc. 29 janvier 2008, R.D.B.F. Mai-Juin 2008, comm. n°87, p. 43 et s). Récemment, dans un arrêt du 9 juillet 2008, la Chambre sociale de la Cour de cassation a énoncé que des connexions Internet effectuées par un salarié sur son lieu et pendant son temps de travail étaient présumées professionnelles, ce qui permettait à l'employeur de les rechercher et de les identifier en l'absence du salarié, sauf s'ils sont marqués comme étant personnels. En l'espèce, le salarié a ensuite été licencié pour faute grave car il avait utilisé l'ordinateur pour des connexions Internet personnelles et abusives. Cet arrêt montre bien que même si la jurisprudence a tendance à protéger la vie privée du salarié en refusant, entre autres, que l'employeur ouvre des fichiers identifiés comme personnels en son absence, le droit à l'intimité de sa vie privée ne sera jamais absolu, et ceci se comprend parfaitement dès lors que les moyens de contrôle et de surveillance sont limités et justifiés par le bon fonctionnement de l'entreprise et la sécurité des systèmes d'information.

Ainsi, les principes relatifs aux contrôles de sécurité et à la vie privée doivent être établis dans la PSSI et dans la charte d'utilisation des Systèmes d'information. Une veille juridique est essentielle. Mais l'opposabilité de ces règles aux salariés dépendra également du respect des obligations d'information qui incombent à l'entreprise ou à l'autorité administrative.

Sécurité intérieure et/ou extérieure, des biens et des personnes vont servir de fondements pour légitimer les atteintes aux libertés fondamentales. Pour protéger de façon pragmatique les individus contre les intrusions dans leur sphère privée, il faut d'abord admettre la légitimité de la lutte contre les crimes et délits par la prévention, et donc la surveillance (et la traçabilité), pour ensuite trouver les moyens appropriés, à savoir les plus respectueux possible des libertés fondamentales, et les meilleures garanties pour les citoyens. Il est en effet délicat, comme souvent, de concilier les intérêts en présence, mais c'est pourtant bien vers cet équilibre qu'il faut tendre pour éviter tout débordement liberticide ou libertaire... D'ailleurs, n'est-ce pas le fragile équilibre résultant du rapport entre le droit au respect de la vie privée et la nécessité de sécurité qui doit être préservé ?

Eric A. CAPRIOLI
Avocat à la Cour
Docteur en droit

www.caprioli-avocats.com

5.3. Le dilemme « prévention - réaction » par Hervé SCHMIDT

La gestion des risques est indissociable de la prévention. Ce fait est, dans l'esprit de chacun comme dans la pratique, indiscutable.

Cependant, est-il envisageable de la limiter à cela ? Le terme « prévention » recouvre l'ensemble des mesures mises en place afin de diminuer la fréquence d'apparition d'un accident. Mais qu'en est-il lorsque le risque se réalise, lorsqu'on se retrouve confronté à une situation critique ? C'est à ce moment là qu'il faut réagir, à ce moment là que, par définition, la prévention a atteint ses limites.

Gérer une crise, c'est réagir face à un incident, quel qu'il soit, et quelques soient les mesures de prévention existantes. Comprendre ce processus est un cheminement intellectuel parfois difficile à accepter, lorsque, en tant que Directeur de la sécurité par exemple, l'objectif est de protéger l'entreprise pour éviter, autant que faire se peut, la réalisation d'un sinistre. Comment ces deux démarches, en apparence contradictoires, doivent être perçues et que faut-il en penser ?

Positionnons-nous, tout d'abord, dans une échelle de temps. Il faut bien comprendre que prévention et réaction ne se situent pas au même niveau.

La prévention est une démarche longue à mettre en place. Sa difficulté majeure réside dans le fait qu'il faut choisir les menaces à traiter en particulier, les vulnérabilités contre lesquelles il faut se protéger en priorité. Comment les hiérarchiser, « comment être certain que tel risque ne va pas se réaliser alors que je traite tel autre... » ?

La réaction, quant à elle, et quel que soit l'événement qui la provoque, doit être immédiate. S'organiser à cet effet nécessite d'établir des procédures simples à mettre en œuvre, mais surtout à mémoriser, de telle sorte que chacun sache que faire au plus vite le jour où...

Mettre en place un tel dispositif est une priorité évidente. Se préparer « un minimum », face à n'importe quel type de crise et à n'importe quel moment, est un enjeu majeur pour l'entreprise, indépendamment des mesures de prévention puisqu'une crise est, par définition, une défaillance de mesure de sécurité non ou mal prévenue.

D'autre part, le choix entre prévention et réaction peut être cornélien d'un point de vue financier. Chacun sait qu'obtenir des budgets n'est pas chose facile et que ce qui semble prioritaire pour les uns, ne l'est pas forcément pour les autres. Cette difficulté, en matière de prévention, est quotidienne : choisir une mesure, et non une autre, est totalement subjectif et dépend des sensibilités de chacun.

En revanche, tout le monde s'accordera à dire que savoir réagir rapidement et efficacement est indispensable, afin de préserver, quoi qu'il arrive l'atteinte permanente des objectifs. La réaction passe avant la prévention.

Il ne faut cependant pas tomber dans un piège évident : réagir ne veut pas dire improviser. Savoir anticiper est essentiel. Une organisation structurée permet d'adapter les « réactions » des acteurs

principaux et ne doit pas laisser libre cours à des actions subites, peu réfléchies, et dont les conséquences pourraient être désastreuses. Sous l'effet du stress, la panique est compréhensible et seules les procédures claires, connues de tous, et testées régulièrement permettent de réagir correctement.

Le dilemme prévention - réaction apparait lorsqu'un incident survient : à quel moment réagit-on ? Jusqu'où fait-on confiance aux mesures de prévention ? Il faut trouver un juste milieu et toute l'efficacité du système de gestion des risques réside dans une bonne communication entre les acteurs.

Aucune de ces deux composantes n'est à négliger et elles sont complémentaires : la prévention ne suffit pas car un risque peut se réaliser quelles que soient les mesures en place ; la réaction, quant à elle, doit être organisée pour être efficace.

Et certains diront qu'établir des procédures de gestion de crise relève de la prévention...

Hervé SCHMIDT
Président du Cercle GASPAR

www.gaspar.fr

5.4. Sommes-nous criso-formés ? par Isabelle TISSERAND

Pari gagné : les membres du Cercle Européen de la Sécurité et des Systèmes d'Information projettent désormais et définitivement la sécurité des patrimoines de façons interdisciplinaire et transversale (1).

Avantages : nos audits et analyses de risques sont plus complets et renforcent la puissance des technologies en stimulant nos partenaires toujours plus créatifs.

Nouveau challenge pour tous les professionnels de la sécurité : tous les systèmes doivent pouvoir fonctionner en cas de situations extrêmes. Par conséquent nous n'avons jamais autant parlé de la crise -des crises, des liaisons de crises et de ses modes de gestion- ; des types de communication à adopter pour les contrer - contenir, maîtriser, étouffer, sublimer (2)- ; ceci pour aboutir, comme bien souvent, au questionnement relatif au facteur humain : mécanisme fondamental dans la phase de résilience psychologique, économique et sociale d'une entreprise.

Sommes-nous équipés ?

On nous demande d'être prêts à savoir réagir en cas de crise sectorielle, nationale, européenne, internationale, planétaire (3). On nous renseigne plus précisément et de plus en plus vite sur les rouages d'un dispositif global permettant à tout organisme produisant une économie sociale de travailler avec l'Etat et les Etats. Mais les organisations relais, les cellules de gestion de crises sont-elles en place dans les entreprises ?, les équipes sont-elles en formation ?, les outils de veille, les technologies et les réseaux sociaux permettent-ils en effet de disposer du maximum d'outils ou s'agit-il d'un nouveau programme accéléré à lancer pour modifier nos lignes de codes, de conduites et de performances ? (4).

Pouvons-nous communiquer ?

Moult a priori intellectuels ont volé en éclat ces derniers mois. Un : la communication en situation de crise n'est pas uniquement réservée aux managers mais peut leur être attribuée, non par obligation politique mais par choix et pour ce qui concerne un type de message en particulier. Deux : tous les gestionnaires de crises doivent par conséquent être instruits car il existe un véritable vocabulaire de crise, une psychologie des impacts de la parole sur les actions. Trois : il existe des techniques de gestion de la communication en situation de crises, basiques et préventives, qu'il faut impérativement acquérir et enrichir par la formation continue (5).

Savons-nous nous former ?

Les écoles françaises et européennes proposant ce type de formations sont mal identifiées, peu promues et semblent assez rares. Des prestataires privés et habilités font timidement leurs apparitions en France. Les professionnels de l'Etat communiquent généreusement dès que nous les contactons et il est à souhaiter qu'ils participent de plus en plus activement à la formation des personnels de tous types d'entreprises.

La littérature qui traite le sujet de la crise sur le net est assez abondante mais plutôt descriptive, rarement analytique et peu formatrice car les interrogations portent plus sur les conséquences que sur les causes à traiter.
La presse sécurité « people » a en outre pour effet de limiter les explorations intellectuelles à la lecture des acteurs les plus prolixes (sorte de spécialistes idolâtrés car plutôt rares), aux dépens d'auteurs scientifiques plus discrets mais rentables sur les plans méthodologiques.

Or, les modes structurels et opératoires relatifs aux crises sont d'une extrême complexité. Ils focalisent sur l'activation des mécanismes les plus actifs du système cérébral humain pour la survie de l'espèce et de ses productions. Il est donc indispensable d'enrichir nos bases de connaissances et de nous rendre encyclopédiques sur le sujet.

Enfin, en plus de nous former en tant que technicien de la crise, il importera de savoir, à un moment donné de sa propre expérience, transmettre les connaissances théoriques et les savoirs faire à ceux qui décident de participer : question pédagogique.

Pouvons-nous nous coordonner ?

Tous les techniciens de crise interrogés s'accordent à penser que tout existe -mais de façon éparse et peut-être insuffisamment partagé- pour que puissent se constituer des équipes efficaces en mesure d'améliorer les pratiques pour construire les plus solides défenses. Les connaissances, les personnels, les lieux, les outils, les questionnements, les critères psychologiques et les nécessaires vertus sont inventoriés. Reste à les cultiver, les associer, les partager.

Comme nous le disait un expert du centre de gestion des crises du Ministère des Affaires Etrangères et Européennes : « il faut être criso-formé ». Comme l'ajoutait un autre expert en protection des patrimoines dans le journal Le Monde cet été, « la coordination est un concept clef sur lequel il faut s'interroger, travailler, insister » (6) et nous approuvons car il faut effectivement coordonner de nombreux paramètres immatériels et matériels pour atteindre un niveau de performance correct.

Selon l'avis du Commandant Patrice Eoche-Duval, « il est nécessaire d'être formé intellectuellement et mécaniquement à la gestion de crise. Dans le mot formation, il faut comprendre deux sens : tout d'abord celui de l'apprentissage, de l'acquisition de connaissances et, deuxièmement, celui de la malléabilité et de la forme qu'on lui donne. Concernant cet aspect, il s'agit de réflexes dans la vie de chaque jour ; on parle souvent de psychose ou d'état paranoïaque pour ces professionnels qui voit du danger partout. En réalité, il ne s'agit que de l'inscription, y compris dans leurs vies privées, de réflexes comportementaux: anticipation, identification des risques et des menaces, stratégie des scénarios. La réflexion doit donc également porter sur les conséquences individuelles de la gestion de crises. Les dangers pour la sphère privée, la famille, les amis existent. En décortiquant les rubriques faits divers dans la presse, on découvre combien de drames auraient pu être évités si tous ces aspects étaient pris en compte ».

Constat :

La criso-formation est en soi une résilience à gérer car elle interroge à perpétuité les efficacités individuelles et collectives dépouillées de facteurs humains contraignants, bloquants, non constructifs. Il y va, au fond, et à chaque fois qu'une cellule de gestion de crise s'anime dans le monde, de survie. Cet exercice exige un imbroglio de performances à sans cesse entraîner.

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

(1) Liste des domaines explorés dans le cadre des travaux du Cercle Européen de la Sécurité & des Systèmes d'Information : ingénierie informatique, économie, sociologie, psychologie, pédagogie.

(2) Daniel Goleman (docteur en psychologie, professeur à Harvard, journaliste au New York Times) : « l'intelligence émotionnelle », Edition J'ai lu, Paris 1995 ; Edition Robert Laffont, Paris 1997.

(3) Le livre blanc de la sécurité nationale, Edition Odile Jacob, Paris, 2008.

(4) Cette exigence situationnelle est à l'origine de la méthode de sécurité globale des patrimoines NINAH : Normes d'Intégration Nécessaires à l'Adaption Humaine en environnements sensibles, (auteurs : Jullian Barthélémy, Alexandra Besnard, Izabelle Pinto, Isabelle Tisserand) INPI 2001.

(5) 1- On liste les cibles à informer lors des différentes phases de la gestion de crises, 2- on vérifie le DICP de chaque information relative à la crise, on rédige les messages en prenant en compte, au minimum, les questions suivantes : quelle information donner ?, pourquoi la donner ?, à qui la donner ?, quand la donner ?, comment la donner? (In NINAH), INPI 2003, page 5)

(6) Il s'agit de nos confrères Patrice Eoche-Duval et Denis Langlois.

6- Conclusion

6.1. Bilan

Depuis 2004, nous avons mis en évidence que la Sécurité des SI n'était qu'un sous-ensemble de ce que beaucoup ont appelé dès la fin des années 90, la Sécurité de l'Information. Dix ans plus tard, à l'aube d'une dématérialisation de plus en plus poussée de la société et d'une forte croissance des exigences de sécurité, la SSI existe-t-elle encore en tant que telle ?

Dans certains secteurs, on voit la SSI se recentrer vers la protection des infrastructures, la disponibilité et la qualité, dans d'autres s'élargir aux questions de sécurité voire de sûreté de l'information.

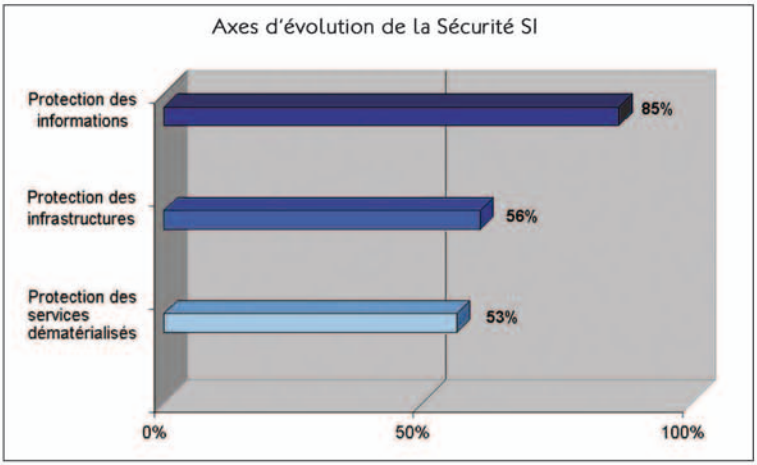
Certes, il n'existe toujours pas de modèle et même si la norme ISO27001 concerne le *management de la sécurité de l'information*, force est de constater que l'approche reste très « informatique ».

Comment les professionnels perçoivent-ils aujourd'hui l'évolution de la fonction Sécurité SI ?

6.2. L'information avant tout le reste ?

Comme l'atteste le schéma ci-dessous, l'évolution majeure concerne la protection des informations (sous entendues confidentielles, stratégiques, personnelles, etc.).

Le plus marquant réside dans cette moitié du panel qui place la « confiance numérique » autour des services en ligne, au même niveau que les infrastructures critiques elles-mêmes. Que ce soit dans le e-commerce, le e-business et la e-administration, la sécurité doit ou devra être synonyme de confiance notamment au regard de la fraude en ligne et des cyber-attaques. (cf. Définitions du chapitre 2.3).



La Sécurité globale se doit d'intégrer la Sécurité des SI dans son acceptation la plus large (Infrastructures, Services, Informations) en visant tous les types de menaces. Malgré ses 56%, la protection des infrastructures est sans doute la plus mûre tandis que les évolutions et les progrès

en cours concernent la sûreté des informations et dans une moindre mesure la confiance numérique.

Une analyse par secteur d'activité apporte un éclairage intéressant sur cette perception avec de grandes divergences.

Zoom par secteur d'activité

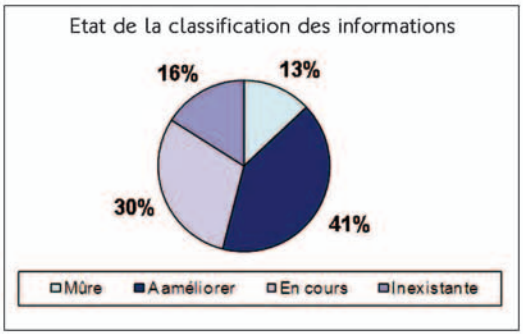
Axes d'évolution de la Sécurité SI				
Protection des infrastructures	63%	70%	12%	38%
Protection des informations	91%	77%	85%	88%
Protection des services dématérialisés	52%	50%	18%	56%

A ce jour, il n'existe pas de cohérence dans l'évolution de la fonction SSI (l'Industrie notamment se focalisant vraiment sur l'information) mais les Banques/Assurances et l'Administration/Services publics semblent les mieux armées pour intégrer, à plus ou moins long terme) les 3 dimensions dans leur ensemble.

6.3. La classification : défi permanent ou peine perdue ?

Nous terminerons sur un des aspects majeurs de toute démarche de sécurité. Classifier les actifs et ne protéger que ce qui a de la valeur. Si l'immatériel est devenu le patrimoine majeur des organisations, on constate que sa classification (en termes de disponibilité ou de confidentialité, voire d'intégrité ou d'imputabilité) reste un défi à relever.

Très peu d'entreprises peuvent revendiquer (13% du panel) une classification de qualité. Plus des 2/3 du panel sont sur la voie mais encore 16% ne se sont pas lancés.



6.4. L'éducation encore et toujours ?

Comme cela a été dit en introduction et comme le souligne Isabelle Tisserand, il existe une très forte exigence en termes d'éducation à tous les niveaux.

En amont, sur l'ampleur de la problématique et des moyens adaptés à mettre en œuvre en termes de prévention et de protection. Les professionnels de la sécurité et les membres du Cercle en particulier, savent qu'il existe un marketing très efficace de la sécurité (ou de l'insécurité !). Tous les professionnels, pour se considérer comme tel, doivent être conscient que la sécurité c'est toujours un compromis, un équilibre. Et qu'ils doivent le rappeler sans cesse.

En termes de menaces surtout, car tout le monde est-il conscient que nous sommes en guerre (s) ? Que ses formes sont multiples et que les ennemis sont nombreux, à la fois très proches et lointains ? Sans tomber, bien sûr, dans le marketing de la peur.

En termes de mesures pertinentes, sur les apports des nouvelles technologies comme la biométrie ou la cybersurveillance qui posent des questions sociétales complexes. Protéger les libertés individuelles ne doit pas faire le lit du crime et du terrorisme, malgré toute la sagesse de Thomas Jefferson.

En aval, sur la prise de conscience que malgré toutes les précautions, la crise surviendra un jour et que l'individu doit être préparé à l'affronter, autant psychologiquement que matériellement. Et ce n'est pas simple de toujours suivre la pensée d'Eugène Minkovsky.

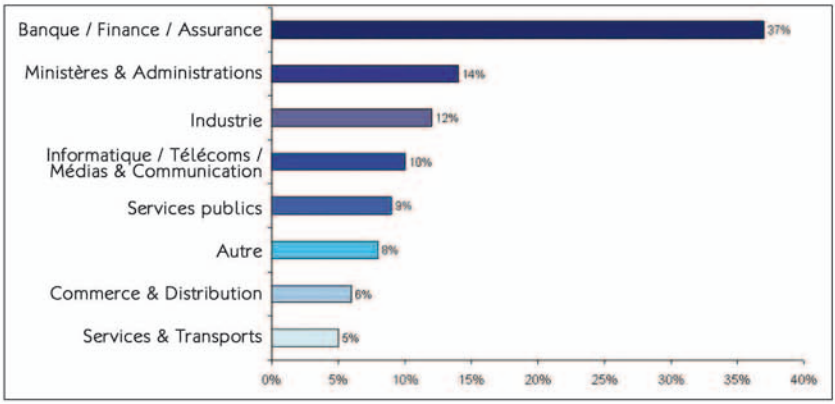
Par contre, au regard de notre société moderne, dite de l'information, nous ne pouvons pas avancer sans garder à l'esprit le génie d'Einstein :

> « L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique. »

7- Le panel de l'enquête 2008

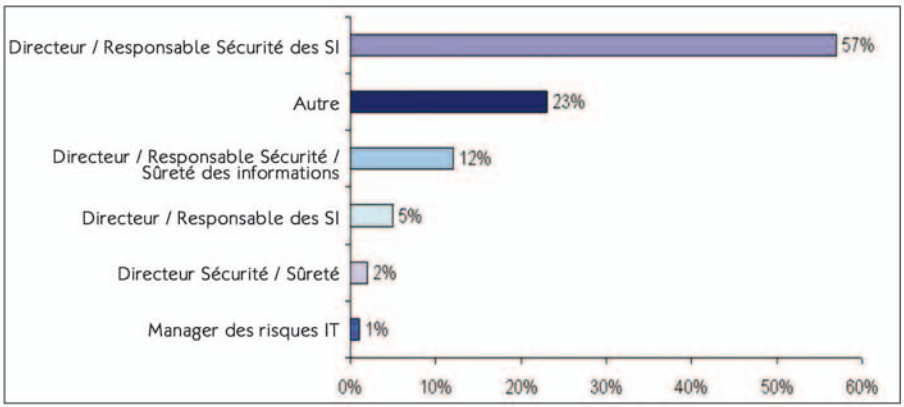
Le panel de l'enquête est constitué de 174 professionnels dont les principales caractéristiques sont présentées ci-dessous.

7.1. Secteurs d'activité du panel



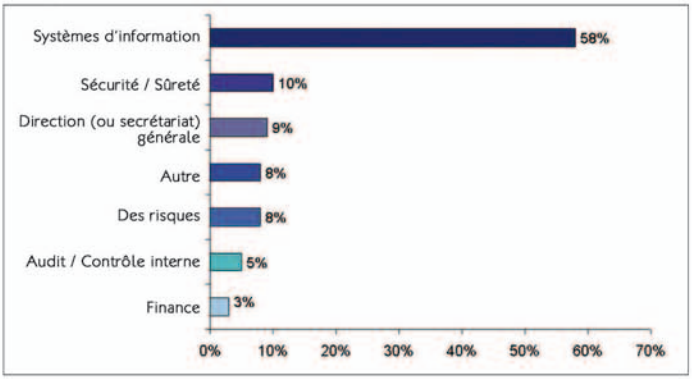
Une forte représentation de la Banque/Finance/Assurance devant l'Administration/Services publics

7.2. Fonctions du panel



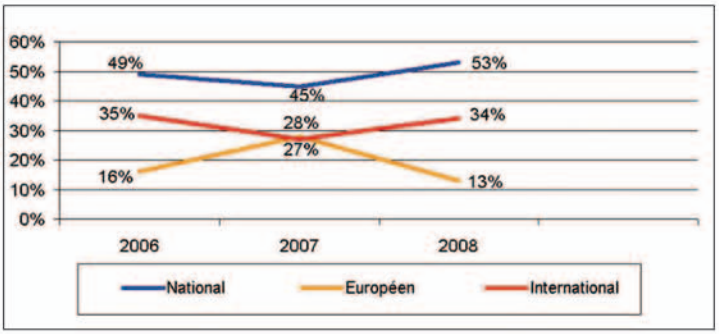
Un quart du panel assume des fonctions de sécurité à un niveau plus opérationnel que décisionnel.

7.3. Entités organisationnelles de rattachement



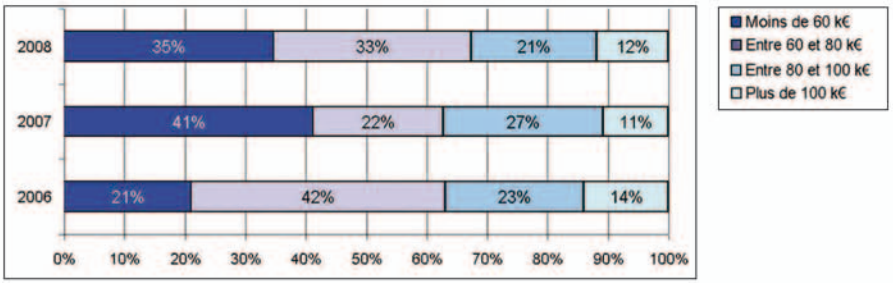
Une répartition classique et conforme aux enquêtes précédentes.

7.4. Couverture géographique de l'activité



Un panel plus centré sur la France mais près de la moitié oeuvre à l'international.

7.5. Rémunération



Une répartition des salaires assez cohérente.
Une rémunération annuelle moyenne de 73,4 k€ contre 71,6 k€ en 2007.

Monaco
15-16-17-18 octobre 2008

8ème édition

08 Les Assises
L'Evénement Européen de la Sécurité et des Systèmes d'Information

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

- **Un outil stratégique unique**
- **Un temps fort d'échanges et de rencontres**
- **Un lieu de réflexions et de détection d'innovations**
- **Un exceptionnel potentiel de business**
- **Le rendez-vous de tous les acteurs, décideurs et experts de la sécurité**

Un événement

Pour plus d'information, contactez-nous au 01 41 93 07 07

www.lesassisesdelasecurite.com

Prix de l'Innovation des Assises 08
L'Evénement Européen de la Sécurité et des Systèmes d'Information

Le cercle



Nos Partenaires

accenture · Alcatel·Lucent · ARUBA networks · AXIS COMMUNICATIONS · Actividentity · ARKOON NETWORK SECURITY · Avocent · BeeWare · BlueCoat · ca Transforming IT Management · CROSSBEAM SYSTEMS · BlackBerry · BT · Check Point SOFTWARE TECHNOLOGIES LTD · denyall SECURITY SOLUTIONS · enterasys Secure Networks · EXAPROBE · f5 · DICTAO · EVIDIAN · exaprotect · FORTINET · Google · IBM · INTEGRALIS SECURING BUSINESS · Global Knowledge · ProCurve Networking by HP · ilex · IRONPORT · KEYNECTIS · LINAGORA GROUPE · McAfee · Juniper NETWORKS · LANDesk An Avocent Company · logica management consulting · Microsoft · mobiquant · nexTHINK · Novell · mobilEGOV · NETASQ we secure IT · NOKIA · OPENTRUST · POLYCOM · QUALYS · RICOH · ORACLE · Prim'X TECHNOLOGIES · radware availability | performance | security · RITTAL · SecurActive · SkyRecon · SOPHOS · RSA The Security Division of EMC · secure · solucom group · SPIE · Sun microsystems · telindus · TREND MICRO · STONESOFT · symantec. · THALES · VeriSign · verizon business Security Solutions powered by Cybertrust · webroot · WEBSENSE ESSENTIAL INFORMATION PROTECTION

Partenaires Presse

CIO · Global Security Mag · lesnouvelles.net · Qualité références · SECURITY VIBES · SOLUTIONS & LOGICIELS · cnis mag · it-expert · MAG SECURS · REGARDS.IE · siliconfr

Prochain rendez-vous

9ème édition des Assises

Monaco
7-8-9-10 octobre 2009

09 Les Assises

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

Pour plus d'information, contactez-nous au 01 41 93 07 07
ou sur www.lesassisesdelasecurite.com

Un événement