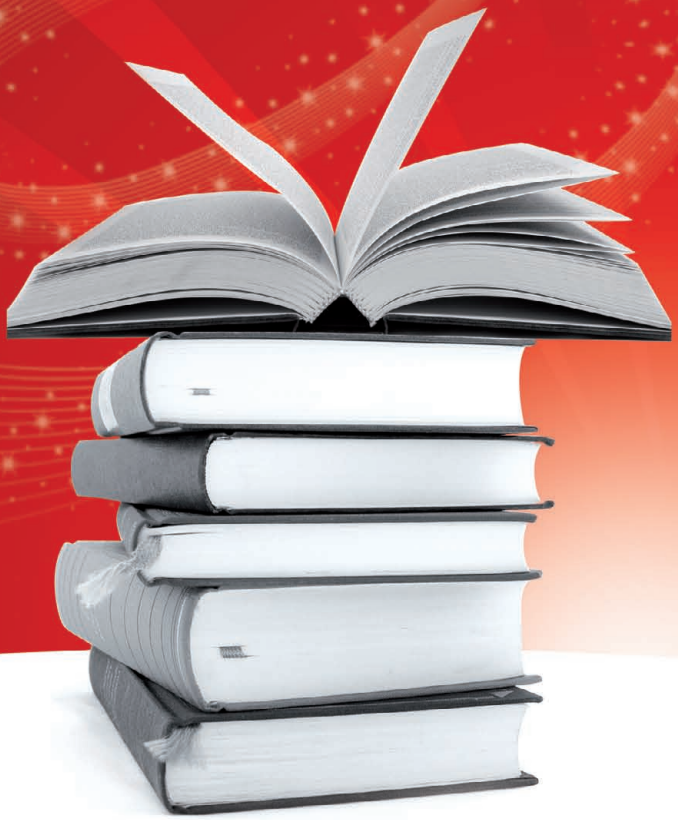
tome VII
Octobre 2010



Le Livre Bleu

Dimension économique de la Sécurité des Systèmes d'Information

Bilan 2001-2010

réalisé par

hapsis

10 ans

pour

les assises de la sécurité et des systèmes d'information

we protect your digital worlds*
*nous protégeons votre monde numérique.

Notre Business est de sécuriser votre Business

ESET NOD32 Antivirus 4
Business Edition

Antivirus I Antispyware I Anti-rootkits
Facile à déployer et à administrer

Protégez efficacement votre réseau contre les virus connus et inconnus, chevaux de Troie, vers, adware, spyware, rootkits et autres menaces évolutives sans en affecter les performances.

Rendez-vous sur www.eset-nod32.fr/assises

- Version d'évaluation gratuite 30 jours
- Analyse et nettoyage gratuits en ligne de votre PC

Monaco du 6 au 9 octobre 2010
lesassises
de la sécurité et des systèmes d'information
Participez à l'Atelier ESET
Mercredi 6 octobre 2010
www.lesassisesdelasecurite.com

RECORD DE RECOMPENSES 62VB100

Produit Bronze de l'année 2009
Solution Business recommandée en 2009
Meilleures Performances en 2008
Antivirus de l'année 2006 et 2007

Sources : www.virusbtn.com et www.av-comparatives.org.

© 2010 ESET, LLC. Tous droits réservés.

SOMMAIRE

1- Introduction **2**

2- Cadrer la problématique **4**

2.1. L'environnement général 4
2.2. Quelques rappels historiques 6
2.3. Des travaux universitaires 9
2.4. Des travaux récents de l'ENISA 10
2.5. Exploitation des résultats de l'enquête 2010 11

3 - Le bilan de la décennie 2001-2010 ..... **12**

3.1. Les menaces et les risques : l'essor de la cybercriminalité 12
3.2. Les outils et les services : un marché « hors crise » ? 17
3.3 Échanges sur l'évolution du cadre légal 24
3.4 La fonction Sécurité des SI : de « Docteur No » à « Yes we can ! » 30

4 - Considérations économiques sur la sécurité des SI **41**

4.1. Introduction 41
4.2. Impacts économiques des incidents 41
4.3. Dépenses et approches budgétaires 46
4.4. Approche pénaliste : des sanctions dissuasives ? 57
4.5. La cybercriminalité : entre naïveté et cyber-guerre ? 58
4.6. Synthèse 60

5 - Conclusion **62**

6 - Annexe : le panel **64**

6.1. Secteurs d'activités 64
6.2. Titres et fonctions 64
6.3. Entités d'appartenance 65
6.4. Couverture géographique 65
6.5. Rémunération 66

1- INTRODUCTION

Depuis 2004, les enquêtes du Cercle Européen de la Sécurité analysent l'évolution des rôles et des activités des professionnels de la Sécurité des Systèmes d'Information (SSI). Véritable observatoire d'une fonction clé des entreprises et des administrations, elles alimentent surtout la réflexion autour de thématiques majeures sélectionnées par le Comité de Pilotage du Cercle.

Nous avons ainsi abordé :

- le management stratégique des cyber-risques (2004)
- les indicateurs et tableaux de bord en SSI (2005)
- les grands défis des professionnels de la SSI (2006)
- les pouvoirs en sécurité / sûreté (2007)
- la sécurité globale (2008)
- la culture des risques informatiques / informationnels (2009)

L'an dernier, nous avions souhaité sortir du cadre technico-juridique de la sécurité où face à un risque, les réponses « techniques » du marché et « juridiques » des États tentent de satisfaire l'ensemble des parties. Complémentaires sans doute, elles sont surtout insuffisantes. C'est ce que nous avions voulu montrer en engageant **une réflexion sur le facteur humain et la culture des risques liés aux technologies de l'information**.

A cet égard, le rôle des organismes internationaux (Conseil de l'Europe, ISO, etc.), européens (ENISA) ou nationaux (ANSSI) avait été abordé. Leurs normes et règlements, conventions, études ou directives participent-ils réellement au renforcement de cette culture ? Ou est-ce au marché de s'emparer du sujet, notamment via les banques et les opérateurs télécoms / internet ?

Par ailleurs, au-delà du renforcement des connaissances, de l'adoption des comportements, attitudes, réflexes utiles, quel peut être l'impact sur le marché « sécurité » de normes comme ISO 27001 ou 27002, d'une Directive européenne sur la Signature électronique, d'une loi sur la Confiance dans l'Économie Numérique, d'un Règlement Général de Sécurité récemment publié en France ? La question mérite d'être posée sachant que les réponses peuvent toucher l'industrie et les services, mais aussi l'enseignement. **La culture et l'économie ne peuvent être dissociées dans de nombreux domaines et il en est de même en matière de risque / sécurité**.

Synthétisant superbement ce lien ténu, Rudyard Kipling et sa fameuse boutade *« Il faut toujours prendre le maximum de risques avec le maximum de précautions. »* reste d'actualité. Comme le Livre bleu des Assises 2009 l'a mis en évidence, on serait aussi plus enclin aujourd'hui, à revisiter et moderniser Molière et son Tartuffe avec un savoureux *« Cachez ce risque que je ne saurais voir ! »*.

Politiques et décideurs sont en effet sous la **pression de la société** qui ne veut plus comprendre qu'une catastrophe ou le moindre incident puisse survenir et encore moins en assumer les conséquences, toujours en quête d'un bouc émissaire. Mais ils sont aussi sous la **pression économique** qui fait qu'on ne peut pas dépenser sans compter pour satisfaire la moindre peur, crainte, envie, exigence en matière de sécurité. Cruel dilemme !

Gérard RIO
Fondateur des Assises de la Sécurité

« L'économie sécuritaire »

Le titre de ce 7ème volet du Livre Bleu des Assises peut paraître incongru voire surréaliste pour beaucoup, mais il regroupe pourtant les grands défis des trois prochaines années !
Le Comité de Pilotage des Assises 2010 a souhaité que la problématique économique des risques relatifs aux Systèmes d'Information soit abordée cette année, et qu'un Groupe de Travail soit créé afin d'apporter des réponses pragmatiques.
Les résultats seront présentés dès les premières réunions du Cercle en 2011.

Le Livre Bleu des Assises 2010 va tenter d'apporter un premier éclairage sur cette problématique majeure en partant de deux éléments :

- Quel bilan pouvons-nous tirer de la décennie 2001-2010 afin d'alimenter la réflexion sur ces aspects économiques ?
- Quels enseignements apporte l'analyse de l'enquête annuelle du Cercle Européen de la Sécurité consacrée à ce sujet cette année ?

Nous nous appuierons autant que possible sur des éléments factuels, des rapports et des études indépendants et également sur des avis d'experts impliqués de longue date, reconnus pour leur professionnalisme. En ce qui concerne le bilan de la décennie, nous aborderons 4 thèmes d'analyse :

- **L'évolution de la menace** est basée sur une analyse des faits marquants des10 dernières années.
- **Les réponses du marché** sont analysées à partir d'un profond travail de veille et d'entretiens avec des experts du Cercle.
- **Les nouveautés du cadre légal** sont traitées sous la forme d'un entretien avec Maître Christiane Féral-Schuhl et Maître Éric A. Caprioli.
- **La mutation de la fonction Sécurité SI** est étudiée au travers d'entretiens avec des RSSI reconnus de tous secteurs d'activité : Pascal BASSET (PMU), Antoine BELIGNE (Groupe PSA), Alain BOUILLÉ (Groupe Caisse des Dépôts et Consignations), Didier GRAS (BNP Paribas), Mylène JAROSSAY (Institut CURIE), Jean-François LOUAPRE (AG2R La Mondiale), Lazaro PESJACHOWICZ (CNAM-TS).

Pierre-Luc REFALO
Directeur associé
HAPSIS

« Nous remercions le panel de RSSI, comme l'ensemble des participants, anciens et nouveaux à notre enquête annuelle, pour la pertinence de leurs apports et, au-delà du bilan, pour l'éclairage apporté à un domaine stratégique du management des entreprises.

Nous espérons surtout que ce travail vous éclairera dans vos activités quotidiennes, présentes et futures, et aussi, que vous ne manquerez pas d'alimenter cette réflexion initiale au sein du Cercle Européen de la Sécurité. »

Bonne lecture !

2- CADRER LA PROBLÉMATIQUE...

La dimension économique de la Sécurité du SI ne peut pas être abordée en tant que telle, de manière « nombriliste ». Elle touche un domaine vaste et complexe, lui-même lié au développement de la société dans son ensemble, et dans un contexte technologique, juridique et politique en perpétuelle évolution.

Aussi, il nous a paru utile, d'une part de positionner le sujet dans un environnement général, et d'autre part, d'exprimer quelques hypothèses pour ne pas nous égarer dans des considérations trop théoriques, détachées des réalités.

2.1. L'environnement général

> ***Le marché et la démocratie sont aujourd'hui en pleine opposition dans leurs finalités et dans leurs modes de fonctionnement.***

Ceci ne date certainement pas d'aujourd'hui, mais ce point fondamental ne doit pas être ignoré avant d'engager cette réflexion sur la dimension économique de la Sécurité des Systèmes d'Information. La « Une » du numéro de septembre du magazine l'Expansion titrait : *« Les marchés plus forts que les États »*. Ce titre accrocheur et d'actualité s'avère pertinent mais fait aussi référence à un contexte plus général et parfois ancien.

- Le **court-termisme** – comme la quête de profit et de rentabilité – de l'un (le marché) est visiblement incompatible avec les problématiques de **long terme** de l'autre (l'État) – financement de la dette et des systèmes sociaux, sécurité intérieure, etc.
- Le **nomadisme** et l'absence de frontière de l'économie – s'oppose à la **sédentarité** de l'autre – l'espace vital de la Nation ou de l'État et de ses populations.
- La **prise de risque** « génétique » de l'un – au cœur du fonctionnement de l'entreprise – s'oppose au **principe de précaution** de l'autre.
- L'**innovation technologique** permanente de l'un se heurte aux **ajustements juridiques** longs et fastidieux de l'autre.
- L'**esprit libéral** de l'un est régulièrement en guerre contre les **tendances et réflexes protectionnistes** de l'autre.

Cette vision macroscopique s'adresse à des réalités bien concrètes et est parfois éclairée par des évènements qui l'illustrent de manière on ne peut plus explicite, notamment dans le domaine de la gestion des risques.

Exemple 1 : la santé.

En 2009, le risque de pandémie grippale A H1N1 a défrayé la chronique sur fond de principe de précaution et de crise économique planétaire. Il a donc fallu répondre aux angoisses et aux questions de la population par des mesures sans doute trop onéreuses et complexes à mettre en œuvre (du point de vue de leur technicité et des processus nécessaires).
Puis, une fois les choix – difficiles – effectués, chacun a pu apprécier et constater que la menace avait été plus ou moins bien évaluée par les soi-disant experts. Remarquer aussi que tous les pays n'ont pas eu la même approche. Et enfin, remettre en cause des achats de vaccins devenus inutiles. Trop cher principe de précaution ? Pourtant, ne doit-on pas garder à l'esprit André Malraux et son célèbre *« La vie ne vaut rien, mais rien ne vaut une vie. »* ?

Exemple 2 : les transports.

La vie, justement ! La mise en place des radars (fixes et mobiles) répond à une exigence forte qui est de réduire le nombre de morts sur les routes. Si la méthode semble donner des résultats, elle s'inscrit certainement aussi dans un « cadre économique » qui touche le système de santé (coûts d'hospitalisation), les revenus des garagistes (coûts de réparation), l'assurance (montant des polices) autrement plus importants que les frais d'équipement et de gestion des radars et que les amendes payées par les contrevenants.

Exemple 3 : les loisirs.

Passons aux loisirs. Le modèle économique du secteur de la musique et du cinéma a été sérieusement remis en cause avec la multiplication des sites de partage en ligne « pirates ». Les solutions techniques complexes liées aux DRM (Digital Right Management) et juridiques contraintes par la territorialité des lois, n'ont jamais réellement endigué le phénomène. L'État français a élaboré une loi (HADOPI 2) - qui semble intéresser finalement les anglo-saxons - intégrant une riposte graduée cherchant à sanctionner les vrais professionnels du piratage et non les copieurs occasionnels qui n'auraient peut-être jamais acheté CDs et DVDs. Les acteurs économiques (producteurs, artistes, distributeurs et consommateurs) doivent aussi revoir leurs pratiques (offres payantes légales et attractives) tandis que les mesures de surveillance ont sans doute pris le pas sur les droits d'usage.

Ces trois exemples démontrent que pour des questions essentielles de la société moderne, les réponses apportées par le marché et par les États ne satisfont réellement personne. Pourtant :

- Il a fallu agir dans une certaine urgence pour la Grippe A H1N1 et sans doute dépenser sans trop compter, à l'inverse d'autres pays.
- Les « majors » de la musique et du cinéma ont tout fait pour ralentir le développement d'offres légales (et maintenir leurs rentes) en promouvant à la fois des solutions techniques impossibles et des sanctions pénales hasardeuses voire extrémistes.
- Entre les deux, la mise en place des radars a, souhaitons le, reposé sur une analyse préalable de l'accidentologie routière et des zones aux meilleurs « gains » pour mettre en place le contrôle et une surveillance pertinente, socialement et économiquement.

Désormais, les États, les entreprises et les individus évoluent au quotidien en considérant les questions de risques et de sécurité de façon prioritaire, avec des réponses technologiques et juridiques complexes et délicates à mettre en œuvre, souvent dans des délais très courts, et dans un contexte de crise économique planétaire.

> ***La Société du XXIe siècle est celle de l'Information et la Sécurité des Systèmes d'Information est devenue un secteur d'activité essentiel dont l'essence technico-juridique doit être complétée par des considérations économiques essentielles.***

2.2. Quelques rappels historiques

Alexis de Tocqueville
(1805-1859)

> *« Lorsque le passé n'éclaire plus l'avenir, l'esprit marche dans les ténèbres. »*

Si nous partons de l'hypothèse que la Sécurité des SI a débuté au milieu des années 80 avec l'avènement de l'ordinateur personnel, nous ne devons pas perdre de vue que les États ont initié dès les années 50 une réflexion et mis au point des technologies de pointe autour de la cryptographie. Autrement dit, avant le PC, on a dépensé « sans trop compter » pour les intérêts stratégiques de l'État.

Depuis, nous pouvons distinguer 4 grandes phases qui se superposent et au cours desquelles les questions économiques des risques SI ont été abordées de manière variée du fait de l'évolution des technologies (TIC), du management des entreprises et des risques eux-mêmes.

Essayons d'éclairer ces différentes phases autour de quelques exemples et de questions clés.

Tout d'abord, et historiquement parlant, la Sécurité des SI des années 80 jusqu'au milieu des années 90 a essentiellement consisté à dérouler des méthodes dites d'analyse de risques telles que MARION (1983) MELISA (1985), EBIOS (1995) et MEHARI (1996) en France, CRAMM (1987) et COBRA (2001) en Angleterre, SPRINT de l'ISF (1995), OCTAVE (1999) aux USA, avec une question majeure :

> ***Quels seraient les impacts (notamment économiques) de divers scénarios de risque particulièrement redoutés ?***

Et au-delà de cette question : quels sont les moyens mis en œuvre pour en limiter l'occurrence ou les conséquences, dans une démarche de prévention et de protection ? Pour, *in fine*, décider de ce qu'il faut faire pour encore réduire le risque ou le cas échéant, le transférer à l'assurance ou... pourquoi pas, ne rien faire. Sont particulièrement impliqués dans cette approche, les secteurs de la banque et de l'assurance, disposant des plus gros « data centers » de l'époque, et dont la dépendance à leur SI est la plus stratégique. Les questions de la continuité et des accès logiques sont ici primordiales.

Au cours de cette même période, une deuxième question est apparue avec le développement de l'informatique distribuée et en réseau.

> ***Quelles économies réaliser en mettant en place une authentification unique et renforcée ? Peut-on concilier qualité et sécurité dans la gestion des accès logiques distribués ?***

Le risque importe sans doute moins ici. Ce sont les fameux projets de « Single Sign On », qui cherchent des réponses à la complexification des modes d'accès et à la multiplication des mots de passe. La Sécurité SI passe de l'Assurance à la Qualité voire à l'ergonomie ! Mais le RSSI est souvent en charge de ces projets et il doit en justifier les coûts par une recherche d'économies au niveau des temps de connexion et des frais de gestion (mot de passe oublié, compte bloqué, etc.).

Mais ce sont surtout les premiers développements du marché autour des menaces « Internet » (anti-virus, pare-feu, détection d'intrusion). Un marché qui attend le passage à l'an 2000 pour exploser.

2000 ou l'année de tous les dangers ! Les menaces venues d'Internet s'imposent à la face des États et des entreprises. Les médias, avides de sensationnel, s'en font des relais efficaces. L'ouverture inéluctable sur un monde dangereux ne peut pas s'effectuer sans un « maximum » de précaution. Les préjudices des attaques (notamment virales) sont évalués avec des modèles plus que tendancieux. On calcule en effet des pertes de productivité économique sur la base du PIB des États-Unis ! On n'est plus dans le risque potentiel, mais dans l'impact « réel » ou supposé comme tel !

> ***Quel est l'impact économique des attaques « Internet » ? Que faire pour ne pas en être victime ?***

On change de paradigme et le « marketing de la peur », surtout américain, bat son plein. Le marché explose. On dépense donc sans compter et les États multiplient les textes renforçant le sentiment d'insécurité ou l'exigence sécuritaire. Des règlements sectoriels (SoX, Bâle II, LSF, etc.) multiplient les projets et surtout les pratiques d'audits. Ainsi, leurs recommandations exigent encore plus la mise en place d'outils et de processus de sécurité...

Parallèlement, une thématique apparaît de manière connexe aux questions de Sécurité du SI : l'Intelligence économique. Elle est définie comme *« la maîtrise et la protection de l'information stratégique »*. C'est le retour du secret et de la confidentialité, chers au secteur de la Défense.

On vise clairement ici les atteintes aux intérêts vitaux des organisations et à leur survie économique. Depuis peu, on a d'ailleurs tendance à entendre parler de « Sécurité économique » qui concerne les *« moyens garantissant la sauvegarde du patrimoine informationnel »*.

> ***Quelle est la valeur du patrimoine informationnel ?***
> ***Comment gérer les menaces externes et internes notamment sur le plan « humain » ?***

Mais tout a une fin, et depuis 2008, face à une crise économique qui n'épargne personne, le retour à des fondamentaux s'avère nécessaire.

> ***Quelles sont les dépenses de sécurité, au regard des attaques, incidents, vols et fraudes réellement constatés ?***
> ***Sont-elles pertinentes et efficaces ?***

De manière corollaire, on pourrait alors se poser une question majeure qui ramène finalement le propos à ses origines et à l'assurance.

> ***Quel est le risque de ne pas ou de mieux dépenser en Sécurité du SI ?***
> ***De ne pas couvrir tel ou tel risque ? Et ce, pendant combien de temps ?***

Enfin, alors que certains professionnels de la Sécurité sont parfois remis en cause sur la pertinence de leurs actions - car ils se focalisent sur des menaces externes, virtuelles et peu visibles finalement, en négligeant la menace interne (une sorte d'assurance inadaptée) -, a contrario, d'autres ambitionnent de faire de leur activité une *« valeur ajoutée »* pour les métiers et les activités de leur organisation. L'ère de la confiance numérique bâtie autour du triptyque preuve / signature / archivage a-t-elle sonné ?

> ***Qu'apportent les mesures de sécurité en termes de confiance des services dématérialisés proposés par les entreprises et administrations ?***
> ***Sont-elles une condition, voire des leviers, pour la croissance de leur business ou pour leur performance économique / opérationnelle ?***

Les questions posées dans ce chapitre restent d'actualité et aucune n'est, *a priori*, plus importante que les autres. Il convient de se les poser, au bon moment, et d'y apporter des réponses argumentées dans son contexte. L'exercice n'est évidemment pas aisé !

2.3. Des travaux universitaires

En guise de préambule, il nous a aussi semblé utile de rechercher des travaux universitaires menés dans le domaine afin de confronter notre approche avec d'autres plus anciennes et surtout différentes.

C'est au sein du Laboratoire informatique de l'Université de Cambridge que l'on trouve les travaux les plus avancés et intéressants, notamment au travers des publications de Ross Anderson dont les premières datent de 2001. Les papiers et les liens les plus importants sont disponibles sur :

- Economics and Security Resource Page : http://www.cl.cam.ac.uk/~rja14/econsec.html

Les publications (plus de 100 références depuis 2001) représentent plusieurs milliers de pages de littérature, souvent répétitives et desquelles quelques thèmes clés émergent :

- **La fraude aux moyens de paiement** est historiquement le premier domaine d'étude des questions économiques en termes de sécurité informatique où la régulation, l'innovation technologique et la gestion de la fraude agissent de concert.
- **La gestion des vulnérabilités** pose des questions économiques complexes de l'amont (qualité des codes applicatifs et coût du développement) à l'aval (publication rapide des failles et processus raisonné d'application de correctifs).
- **La vie privée** nécessite des réflexions d'ordre économique avec d'une part l'obligation de protection des données personnelles qui génère de l'activité économique mais aussi du fait des trafics d'information qui se sont mis en place avec des modèles économiques efficaces. Et côté citoyen : que valent les données que je « cède » ou « confie » à un marchand en ligne ?
- **Les Digital Right Management (et autres techniques similaires)** ont été et demeurent au cœur de questions de concurrence dans l'industrie informatique, des télécoms, des médias et des loisirs.
- **Le rôle des acteurs de l'Internet** doit être précisé au regard de leur implication dans les botnets, le piratage de contenu et dans la fraude « au clic » pour la publicité en ligne.
- **Le poids de la régulation** même lorsqu'elle est incitative et surtout lorsqu'elle ne s'applique pas de manière uniforme (SoX, HIPAA, SAIV) pose des problèmes de distorsion économique entre les grandes entreprises et les plus petites structures.
- **La gouvernance de la Sécurité de l'Information** mérite d'intégrer les questions économiques à plusieurs niveaux : l'externalisation de la sécurité, la gestion des accès logiques, les conséquences économiques de la publication d'une attaque / fraude et bien sûr la question de l'assurance.
- **Le rôle des gouvernements** ne doit pas être ignoré que ce soit dans le domaine de la cryptographie ou de la certification des produits.

> ***Ces travaux montrent que la problématique économique de la Sécurité des Systèmes d'Information est vaste et complexe.***
> ***Elle est avant tout considérée sous l'angle du « marché ».***
> ***Les questions de régulation ou de gouvernance des risques semblent perçues comme des variables reliées aux considérations « business », selon un schéma anglo-saxon très classique.***

Indiquons pour conclure qu'une conférence annuelle a lieu depuis 2002 sur le sujet « Workshop on the Economics of Information Security ». On notera une approche universitaire purement anglo-américaine avec une très faible participation d'intervenants étrangers (Pays Bas, Autriche, Écosse et Israël).

Le programme 2010, les présentations et notes des intervenants sont disponibles sur :
http://weis2010.econinfosec.org/cfp.html

2.4. Des travaux récents de l'ENISA

En 2007, l'ENISA a mené un travail important sur les questions économiques de la Sécurité de l'Information et a notamment fait appel à Ross Anderson associé à Richard Clayton, Tyler Moore et Rainer Böhme (Université de Duisbourg). Un rapport a été publié à la suite d'une réunion d'experts organisée en décembre 2007 où 15 recommandations clés ont été avancées pour de futures actions de l'ENISA et de la Commission Européenne. Parmi celles-ci, certaines méritent d'être mentionnées :

- Élaboration d'une Directive obligeant à la publication des failles de sécurité et des attaques subies (atteintes aux systèmes d'information comme aux données).
- Publication des statistiques de la cybercriminalité dans les banques, au niveau européen (via la Commission ou la Banque Centrale).
- Collecte et publication par l'ENISA des trafics Internet malveillants comme le spam (via les ISP).
- Niveaux de sanction contre les ISPs qui ne réagissent pas rapidement à une requête de déconnexion d'ordinateurs infectés / compromis et associés à une possibilité de reconnexion si le client assume son entière responsabilité.
- Développement et renforcement de standards visant à promouvoir une configuration de sécurité par défaut des équipements connectés à Internet.
- Combinaison de publications rapides des vulnérabilités avec une responsabilité du fournisseur pour ses logiciels non corrigés, afin d'accélérer le cycle de développement des correctifs.
- Gratuité des correctifs dont la fourniture doit être indépendante des changements de version logicielle.
- Conseil de l'ENISA auprès de l'Autorité de la concurrence lorsque des positions dominantes d'offreurs ont des implications sécuritaires.

Les conclusions et recommandations des travaux de l'ENISA, fortement influencés par les travaux de l'Université de Cambridge, privilégient les problématiques du « marché » plaçant les banques, les opérateurs Internet et le commerce en ligne au cœur de la réflexion.

2.5. Exploitation des résultats de l'enquête 2010

S'appuyant sur le rappel historique et les éléments instructifs des travaux universitaires et de l'étude de l'ENISA, le Livre Bleu des Assises 2010 cherche avant tout à initier une réflexion au sein de la profession, en aucun cas à délivrer des vérités et encore moins des tendances prospectives incertaines.

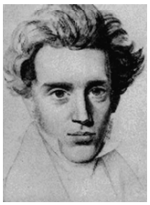
Souhaitant aussi perpétuer sa forme et sa vocation pédagogique, nous avons structuré le document en deux parties :

1. Le bilan de la décennie 2001-2010 met en lumière quelques enseignements factuels en termes « économiques » : *d'où venons-nous ?*
2. L'analyse de l'enquête annuelle du Cercle traduit la position du moment d'un panel de 250 professionnels autour de 26 questions ciblées : *où en sommes-nous ?*

Chaque partie a été structurée selon 4 axes :

1. Les menaces et les risques : réalités et impacts (sous entendus économiques)
2. Le marché : solutions et dépenses associées
3. Le cadre légal : réponses législatives et sanctions liées à la cybercriminalité
4. La fonction SSI : gouvernance de la sécurité et approche économique

Cependant, à la différence des Livres Bleus des années précédentes, le travail n'a pas de vocation « prospective ». Nous avons souhaité rester dans les leçons et le constat, tant l'incertitude règne en maître sur le monde.



Sören Kierkegaard
(1813-1855)

> ***« La vie ne se comprend que par un retour en arrière, mais on ne la vit qu'en avant. »***

3. LE BILAN DE LA DÉCENNIE 2001-2010

Effectuer le bilan de la décennie 2001-2010 dans le domaine de la Sécurité des Systèmes d'Information peut sembler une gageure. D'autant plus que l'objectif est de proposer une synthèse de 30 pages en guise de préambule du Livre Bleu des Assises 2010. C'est à dire en tirant de ce constat des leçons à caractère économique.

Pourtant, si l'exercice est périlleux et sera nécessairement incomplet et superficiel, il est aussi fort utile. Il oblige à aller à l'essentiel et à faire émerger des conclusions et des orientations ciblées.

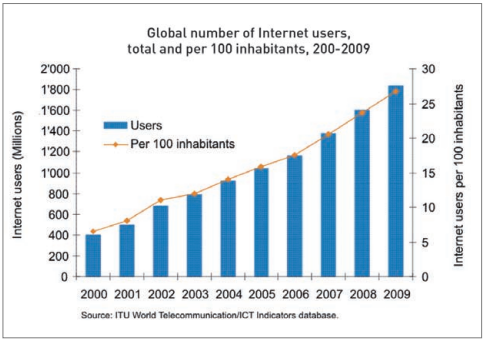
Nous avons donc retenu quatre axes d'analyse s'inscrivant dans une dialectique d'ensemble :

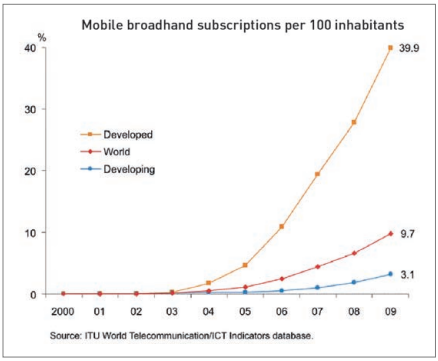
1. Comment ont évolué les menaces et les risques ?
2. Quels solutions et services ont été apportés par le marché ?
3. Quelles ont aussi été les réponses législatives ?
4. Et comment s'est adaptée la fonction sécurité des SI au sein des entreprises et des administrations ?

3.1. Les menaces et les risques : l'essor de la cybercriminalité

Le passage à l'an 2000 a représenté une véritable psychose collective du monde de l'informatique et des télécoms. La peur du grand bug a mobilisé des énergies et des sommes phénoménales pour éviter l'arrêt de l'économie mondiale. Et Bill Clinton, apeuré lui aussi, alors président de l'hyper-puissance américaine demandait aux pirates informatiques « la trêve du 31 décembre » afin qu'ils ne profitent pas des possibles dysfonctionnements et de la mobilisation des équipes informatiques mondiales !

Il y a déjà 10 ans, les entreprises et l'économie mondialisée étaient fortement dépendantes de leurs systèmes d'information et d'Internet. Aujourd'hui, elles le sont évidemment toujours voire encore plus. Mais les technologies ont totalement changé (mobilité, web 2.0) et se sont surtout démocratisées. (cf. schémas ci-dessous).





Et les dangers ne sont plus les mêmes. Certains n'hésitent pas à parler de cyber-terrorisme, de cyber-guerre. Courrier International n'hésite pas dans son numéro de septembre 2010 à faire sa « Une » sur : *« Cyber-Guerre : la menace qui vient du Net »*. Réalité profonde ou nouveau « marketing de la peur » ?

Qu'en est-il réellement au regard des faits d'actualité ? Conscients que nous ne disposons pas de la partie immergée de l'iceberg, nous pouvons néanmoins dresser une évolution des menaces et des risques en quatre grandes tendances.

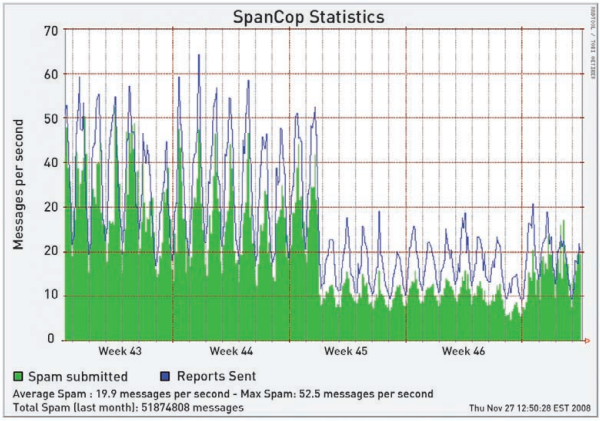
3.1.1. De Mafiaboy à Zeus ou l'essor des botnets

Le **8 février 2000**, un adolescent canadien, Michael « Mafiaboy » Calce active un ancêtre de botnet et lance une série d'attaques en « déni de service distribué » (DDoS) contre les sites web des acteurs clés du e-commerce et des médias : CNN, Yahoo, Amazon, eBay, Dell et d'autres sites connus ont plié sous le déluge.

En pleine bulle Internet, on imagine les impacts économiques et médiatiques d'une telle attaque. Pourtant, Mafiaboy alimentera plutôt la discussion sur le besoin de sécuriser les réseaux et sur les moyens législatifs de lutte contre la cybercriminalité. Un G8 « cybercrime » sera organisé à Paris en mai 2000...

Le jeune pirate, héritier des premiers hackers des années 70 et 80 (comme Kevin Mitnick alias le condor), sera arrêté à Montréal, quelques jours plus tard par le FBI. Il sera condamné à des peines symboliques (interdiction d'ordinateur et travaux d'intérêt général).

En novembre 2008,
l'arrêt d'un opérateur Internet (McColo) permet de réduire les activités de spam d'un botnet du nom de Srizbi.
Plus de 450 000 ordinateurs étaient sous son contrôle !



Impact de la fermeture de McColo
(source Spam Cop)

Aujourd'hui, l'archétype de ces réseaux d'ordinateurs infectés (zombis) et sous le contrôle de serveurs dûment hébergés est incontestablement le **botnet Zeus**. Véritable machine de guerre, Zeus serait un réseau de 200 serveurs contrôlant des millions d'ordinateurs d'entreprises et de particuliers. Apparu en 2007, il fonctionne comme un cheval de Troie voleur de mots de passe, et est spécialisé dans l'enregistrement d'informations d'identification bancaires. Le botnet Zeus est capable de voler 70 000 identifiants de connexion par mois !

> ***Le jeune étudiant en mal de reconnaissance a fait place à des organisations obscures, internationales et parfaitement organisées.***
> ***La quête de gloire éphémère est submergée par des activités commerciales avec une recherche de gains rapides et sans danger.***
> ***Les quelques victimes isolées sont potentiellement, aujourd'hui et demain, les milliards d'internautes fixes et mobiles aussi crédules qu'inconscients.***

3.1.2. De I Love You à Conficker ou l'industrialisation du malware

Le 2 mai 2000, un ouragan planétaire venu des Philippines se propage sous la forme d'un courriel à l'objet bien attractif **« Je vous aime ! »**. Incitant à ouvrir une pièce jointe, le message contient un virus (plus précisément un ver) dont la principale fonctionnalité est de renvoyer le message d'origine à tout le carnet d'adresses du destinataire. Un effet boule de neige impressionnant saturant les serveurs et les boîtes aux lettres.

Exploitant une faille d'Outlook, il infectera plus de 3 millions d'ordinateurs en seulement 4 jours. L'enquête remontera jusqu'à un jeune étudiant en informatique philippin. Il restera impuni car les Philippines n'ont pas de loi contre le piratage informatique.

Certains y ont vu l'influence des éditeurs d'anti-virus. L'attaque étant partie d'Asie, l'infection s'est propagée en pleine nuit américaine. Ceci a permis de mettre à jour les systèmes de messagerie avant le début de la journée, en appliquant les fameux « correctifs ».

Le 21 novembre 2008, une forme évoluée de programme malveillant voit le jour. Finis les Melissa, CodeRed ou Slammer avec leurs variantes régulières s'adaptant aux mises à jour de correctifs et des anti-virus.

Avec **Conficker**, place aux outils préconfigurés de création automatique de malware. Fruit du travail d'une équipe organisée de programmeurs, probablement originaires d'Ukraine, ce ver marque la fin de la décennie par ses usages multiples et son efficacité impressionnante.

Conficker a pour particularité d'utiliser un ensemble de techniques pour contaminer le plus de machines possible sans pour autant avoir systématiquement de « charge utile » bien déterminée (serait-elle en préparation ?). Chaque poste infecté démarre un serveur web local et tente d'infecter toutes les machines possibles, situées sur le réseau local ou Internet, en envoyant des requêtes RPC exploitant le débordement de tampon. Sur la machine cible, un code malveillant tente alors de télécharger une copie complète du ver stocké sur le serveur web de la première machine infectée.

Une lutte classique s'avère aléatoire et insuffisante, lorsque l'on sait que Conficker a essentiellement été introduit par des clés USB sur des machines non mises à jour et mal protégées.

> ***De pratiques isolées voire universitaires, nous sommes passés à des approches industrielles de la fabrication des logiciels malveillants où la rapidité compte autant que l'ingéniosité. Des logiciels à courte durée de vie, voire furtifs voient le jour et intéressent tout autant les organisations criminelles que les États à des fins stratégiques et parfois militaires.***

3.1.3. De l'infrastructure à l'information ou le ciblage de l'attaque

26-28 décembre 1999 : Lothar et Martin, deux tempêtes extratropicales dévastent l'Europe et créent des dégâts sans précédent. Selon les assureurs et les autorités des différents pays, on dénombrera 91 morts dont une quarantaine en France, plus de 200 pylônes haute tension renversés en France privant de courant plus de trois millions de foyers durant plusieurs jours. Les pertes économiques assurées sont évaluées à 6,5 milliards d'euros (record absolu en France) dont 55% pris en charge par les ré-assureurs.

Alors qu'on a « célébré » le 15 juillet 2010, le centenaire de la crue de la Seine, les experts persistent à dire qu'un scénario catastrophe reste plausible malgré les bassins de rétention mis en œuvre

depuis 1936. Et les conséquences économiques seront autrement plus importantes qu'en 1910 (absence de transports et d'électricité, cessation d'activité des entreprises). C'est en PIB que seront évaluées les conséquences d'une nouvelle crue centennale en Région Parisienne.

La sécurité des systèmes d'information a toujours consisté à garantir le bon fonctionnement des moyens mis en œuvre pour que les entreprises et administrations fonctionnent correctement. De la lutte anti-virus des années 90 aux plans de secours informatiques et de continuité des activités, les RSSI doivent permettre aux dirigeants, employés, clients, usagers de vivre et de travailler sans souci « informatique ».

Tout ceci reste d'actualité mais les menaces à prendre en compte, désormais au quotidien, sont de nature très différente et surtout beaucoup plus ciblées. Si l'infrastructure reste sous la menace, l'information, nerf de la guerre moderne, particulièrement vulnérable, devient une cible privilégiée.

7 août 2008 : L'invasion de la Géorgie par la Russie a été précédée d'une **cyber-attaque** sur ses infrastructures Internet.

27 avril 2009 : L'Estonie subit une série de cyber-attaques de ses sites gouvernementaux et bancaires, suite à la décision de démonter un monument à la mémoire de l'Armée Rouge.

Plus que jamais, les infrastructures critiques permettant un fonctionnement normal et serein de la société sont dans l'œil du cyclone. Dès le G8 « cybercriminalité » de mai 2000, une liste de secteurs d'activités aux infrastructures critiques a été établie : télécommunications, énergie, finance, transports. Aujourd'hui, on y retrouve aussi la santé, l'agroalimentaire, l'industrie pharmaceutique, etc. (voir le Livre bleu des Assises 2008 sur la Sécurité globale).

Mais depuis la chute du mur de Berlin (1989), l'avènement d'Internet (1995) et la globalisation (2000), nuire à ses ennemis dans la « guerre économique globale » passe aussi par une atteinte à un autre patrimoine : l'information. Et l'informatique comme Internet deviennent des armes de guerre.

18 décembre 2007 : Une **stagiaire chinoise** d'un équipementier automobile est condamnée et fera 2 mois de prison pour avoir copié des données sortant visiblement du cadre de ses activités.

Mars 2009 : Une **société d'intelligence économique**, sous-traitante d'EDF est soupçonnée d'intrusion informatique dans les ordinateurs de l'ONG Greenpeace. Deux responsables de l'entreprise publique, soupçonnés de «complicité d'intrusion informatique» sont mis en examen.

Mars 2009 : Quatre ordinateurs portables sont dérobés au sein d'une filiale de la société de BTP Eiffage. Ceux-ci auraient contenu les plans et des codes de la future prison de Nancy, dont l'ouverture était toute proche.

Les menaces naturelles et accidentelles, toujours présentes mais mieux anticipées et surtout extrêmement rares, sont aujourd'hui devancées, et ce quotidiennement, par des attaques malveillantes (sabotages, intrusions, vols). Elles ciblent tout autant les infrastructures que les informations dans une sorte de guerre généralisée qu'elle soit stratégique ou économique.

Ce qui était anecdotique hier semble devenu une pratique ordinaire !
Quel est l'impact réel d'un « vol » d'information ?
L'humain n'est-il pas plus au cœur de la solution que les moyens techniques, en termes de prévention et de réaction, comme de gestion de la crise ?

3.1.4. De Serge Humpisch à Albert « Segvec » Gonzales ou comment l'économie de la cybercriminalité impose sa loi

Fin 1999 : Un jeune ingénieur français, au chômage, affirme avoir « cassé la carte à puce bancaire ». **L'affaire Humpisch** crée la panique dans les banques. Elle aura comme effet salvateur une triple prise de conscience : sur le pouvoir des médias peu au fait des enjeux de la cybercriminalité, sur la nécessaire adaptation des mesures de protection (notamment cryptographiques) face à l'augmentation exponentielle de la puissance informatique, et enfin, sur la délicate réponse juridique aux actes cybercriminels.

Comble de l'histoire, le malheureux un peu naïf, ne sera pas seulement condamné pour contrefaçon de la carte bancaire mais pour son usage (accès frauduleux pour acheter des tickets de métro) sur la demande de la justice !

Ce qui importe ici c'est que la menace touche au nerf de la guerre, à l'argent. Quelle confiance accorder à des systèmes de paiement non sécurisés, mais réputés comme tel ? Alors qu'on cherche surtout à les déployer pour des transactions en ligne, sur Internet.

En 10 ans, de nouvelles grandes étapes vont être franchies dans ce domaine.

Depuis 2005 et avec une belle régularité, les actes de **phishing** se sont développés. Attaquant les clients des banques américaines en 2005, ce sont désormais tous les inscrits sur des services « en ligne » qui sont visés (adsl, TV numérique, allocations familiales, impôts, réseaux sociaux).

Fin 2007, Albert « Segvec » Gonzales capte 130 millions de détails CB via une attaque du **système de paiement** de la banque Heartland. Lui et ses complices ont piraté les systèmes informatiques de dizaines de sociétés pendant plusieurs années en utilisant notamment des techniques d'injection de codes SQL.

Avril 2010, un pirate nommé Kirlos propose à la vente plus de 1,5 millions de **données personnelles volées**, issues de Facebook, pour un prix de 25 à 45 dollars pour 1000 contacts. Une bonne opportunité pour d'autres pirates d'étendre leurs bases de données en préparation de leur prochaine campagne de spam ou de scam !

La dématérialisation de la société, le développement de l'e-commerce, de l'e-business, de l'e-administration voire de l'e-santé créent un monde « virtuel » où le réel ne disparait pas pour autant.

> ***Les activités frauduleuses à des fins lucratives se sont développées de façon exponentielle.***
> ***Les données personnelles et notamment sociales ou bancaires sont la cible privilégiée.***
> ***Quelle est la valeur des données personnelles des individus ?***
> ***Quel est le business de la cybercriminalité ?***

3.1.5. Synthèse et leçons

Sans surprise mais de façon très méthodique et spectaculaire, les risques et les menaces ont évolué sur les 4 paramètres :

- Les acteurs : l'étudiant-hacker a fait place au groupe organisé – cybercriminel et aux États.
- Les cibles : l'infrastructure reste critique mais l'information est devenue un patrimoine clé pour les États, les entreprises et les individus.
- Les motivations : le ludico-cupide a de toute évidence fait place au stratégico-économique.
- Les moyens : l'attaque à propagation large avec des outils simples et évolutifs est remplacée par des outils industriels et des logiciels à durée de vie courte voire « furtifs ».

Face à de tels défis, souvent obscurs, mais aussi régulièrement mis en lumière par une actualité sans complaisance, comment se sont adaptées les réponses apportées par le marché en termes de solutions et services, par les États en termes de réglementation, par les entreprises / organisations en termes de management ?

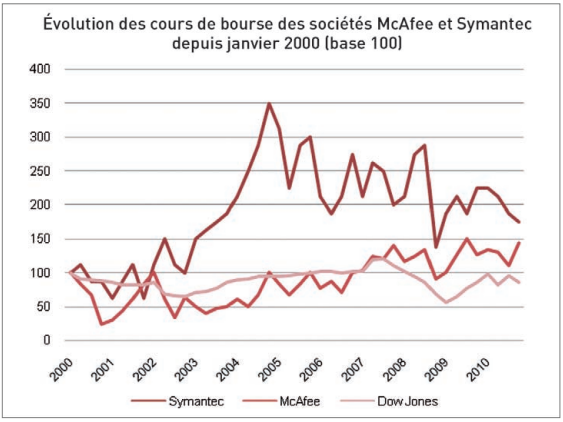
Les trois chapitres suivants vont tenter d'apporter quelques éléments de réponses à ces questions.

3.2. Les outils et les services : un marché « hors crise » ?

Loin de nous l'idée de proposer en quelques pages une analyse du marché de la Sécurité des SI ! Les cabinets spécialisés en la matière disposent de ressources, de méthodes, de temps que nous n'avons pas. Leurs segmentations, leurs analyses et les chiffres qu'ils publient se situent autant dans le présent que dans la prospective. Nous regardons ici dans le rétroviseur !

Un regard quantitatif nous montre d'entrée de jeu que le marché de la sécurité ne connaît sans doute pas la crise. Bien sûr, il y a des périodes délicates pour tous, mais globalement, que ce soit dans la technologie ou dans les services, la croissance, au pire la stagnation est la règle depuis 10 ans.

A titre d'exemple, nous avons positionné l'évolution des cours de bourse pour deux des leaders depuis 2000 (cf. schéma ci-dessous. Base 100 au 1er janvier 2000). Sans commentaire !



Le nombre d'acteurs a aussi considérablement augmenté. Il était fréquent de remarquer, lors des salons professionnels du début des années 2000, plusieurs dizaines de nouveaux entrants à chaque édition. La profusion et la complexité de l'offre devront s'accompagner, à terme, d'une indispensable rationalisation du marché, aujourd'hui totalement atomisé.

Il est indiscutable que le marketing américain a été et reste d'une efficacité redoutable. Il y a un danger, une menace, une faille, une attaque : pas de problème, nous avons l'outil qui convient ! Ainsi, des rentes se sont mises en place, des positions ont été solidement établies. Des opérations de fusions-acquisitions se sont multipliées. Des géants de l'Industrie dominent le marché, parfois au risque d'être juges et partis.

Mais l'innovation remet en cause les acquis. Des structures comme Kaspersky (Russie), Qualys (d'origine française), Dictao, Opentrust et Sagem Morpho (Fra), Nexthink (Suisse), Sophos (UK) se sont parfaitement développées. Et l'Asie ne manquera pas de promouvoir une offre à vocation internationale…

L'emploi, élément majeur de la problématique, s'est aussi développé. Des formations et certifications de qualité ont émergé, garantes à terme, souhaitons-le, d'une véritable professionnalisation.

Enfin, il ne faut pas oublier que certains offreurs n'existent plus ou presque (cabinets de conseil historiques, intégrateurs, industriels, français très souvent). Inadaptation aux attentes des clients, discours trop « technique », modèles économiques inadaptés, support insuffisant voire inexistant.

Au-delà de la maîtrise technique et des outils, le poids du service n'a heureusement cessé d'augmenter. Selon les différents chiffres produits par les analystes, le marché des « services » a supplanté au début des années 2000 celui du « matériel-logiciel » ; mais la proportion demeure proche du 50/50. La question clé demeure évidemment : *« qu'inclut-on dans les produits et dans les services de sécurité ? »*.

Le bilan que nous proposons dans ce chapitre est structuré en 4 thèmes :

- De l'anti-virus à l'anti-tout… A l'anti-rien ?
- De l'application des correctifs à la gestion des vulnérabilités : une quête sans fin ?
- De la défense périmétrique à la défense en profondeur : les leçons de l'histoire !
- De la détection/prévention d'intrusion au SIM / SIEM : pour boucler la boucle…

Évidemment, nous ne prétendons pas à l'exhaustivité mais tentons simplement d'apporter un éclairage sur quelques éléments clés du marché.

3.2.1. De l'anti-virus à l'anti-tout… A l'anti-rien ?

L'anti-virus est-il devenu le « mammouth » de la Sécurité du SI ? Omniprésent, coûteux, ingérable, inefficace… De tout temps, les menaces se sont adaptées aux mesures de prévention / protection. Il en va de même pour les virus informatiques. Les virus « système » sont devenus « macro », puis « réseau » ou « vers », « troyens », spywares, adwares, etc. Mais plus important encore, ils sont évolutifs (variantes multiples) et désormais furtifs ou à usage unique.

Les anti-virus se sont aussi intégrés à des « anti-tout » incluant pare-feu, contrôle parental et anti-phishing. Ont-ils finalement atteint leur limite ou ne tendraient-ils pas à une simple disparition ?

Beaucoup d'experts disent depuis plusieurs années qu'un anti-virus sur les postes fixes, sédentaires au sein des entreprises, n'est plus vraiment utile. Mais qu'il faut aussi accompagner une telle évolution avec d'autres mesures (filtrage sur passerelles, station de décontamination, blocage de ports USB, etc.) évitant les mises à jour de bases de signature lourdes et parfois incomplètes.

Selon Kaspersky Lab, on dénombre aujourd'hui 30 000 nouvelles menaces par jour, soit 1 toutes les 2 secondes. Ce rythme terrifiant va-t-il se poursuivre au fil du temps ?

D'autres experts ont clairement martelé que si on applique les correctifs, on ne risque rien puisque les logiciels malveillants exploitent les fameuses vulnérabilités pour attaquer et se propager (voir le chapitre suivant).

Bien qu'il faille distinguer les problématiques spécifiques aux entreprises et celles des internautes individuels, une chose semble quasi certaine : l'anti-malware ne sert plus à rien ou presque. La gratuité n'est-elle pas la marque de cette tendance de fond ? Pour le Gartner Group, *« la capacité de ces outils pour protéger les organisations est en déclin. »* (Gartner : Magic Quadrant for Endpoint Protection Platforms ; May 4, 2009). *« En 2010, les moyens de défense contre les malwares restent limités : les anti-virus ne sont pas une protection suffisante, il n'y a pas de protection technique infaillible face à un attaquant motivé, la solution ne peut pas être que technique. »* (Forum 2010 du Cert-IST).

Comme les mammouths il y a 10 000 ans, les anti-virus / anti-malware disparaîtront-ils « naturellement », de leur belle mort ou à l'issue d'une catastrophe qui les aura eux-mêmes surpassés ?

Pour Pierre-Marc BUREAU (chercheur sénior chez ESET), *« La prévention des risques informatiques est un combat permanent dont chacun est responsable. Or, il est devenu de plus en plus difficile d'en percevoir les dangers, tant les technologies utilisées par les cyber-attaquants ont évolué. Il convient donc de bien sensibiliser les dirigeants à cette situation afin, notamment, que la solution anti-virus appliquée à chaque poste ou serveur, soit considérée comme un pré-requis, qu'elle soit accompagnée de conseils et de bonnes pratiques et qu'elle s'intègre dans une politique globale de sécurité. »*

Mais finalement, n'est-ce pas de l'innovation technologique associée à de nouveaux modèles économiques qu'émergera la solution ? Avec des questions clés :

- Où s'installe le filtrage adapté ? Sur les postes ou sur des plates-formes de « protection sanitaire » sectorielles, d'opérateurs ou, pourquoi pas, étatiques ?
- Avec quelle technologie ? Nationale, européenne ou via un standard international ?
- Avec quel modèle économique pour un service global ? Un coût au poste ou à l'usage ?

> ***S'adressant difficilement, hier et encore aujourd'hui, aux entreprises et à quelques 2 milliards d'internautes, comment la lutte anti-malware pourra-t-elle protéger les 5 milliards d'utilisateurs « mobiles » et les déjà 500 millions de membres de réseaux sociaux comme Facebook ?***
> ***Quel crédit accorder à des solutions gratuites qui se généralisent sur le marché ?***

3.2.2. De l'application des correctifs à la gestion des vulnérabilités : une quête sans fin ?

La gestion des correctifs a complété la mise en place des anti-malware, dès lors que les attaques se sont mises à exploiter toute faille logicielle. Melissa en 99 s'attaquait à la messagerie Outlook. Slammer aux serveurs SQL, Sasser une faille du service LSASS (Local Security Authority Subsystem Service) de Windows et ce, seulement 2 semaines après la publication de ladite faille. Des failles « zero day », exploitables voire exploitées dès leur publication sont apparues dès 2005-2006 notamment pour IE7 et Firefox.

Nessus, le pionnier de ce marché (créé en 2002) s'est très bien maintenu malgré les difficultés inhérentes à ce type d'approche, quelque peu empirique. Car les processus de gestion des correctifs se sont avérés, à la longue complexes et fastidieux, mais aussi onéreux. Il faut en effet :

- Détecter les failles et les correctifs manquants
- Évaluer la nécessité d'appliquer un correctif
- Obtenir le correctif d'une source sûre
- Tester le correctif en veillant aux effets collatéraux voire indésirables
- Déployer le correctif
- Maintenir la surveillance des systèmes critiques nécessitant de nouveaux correctifs

Désormais, sous l'effet de l'évolution du marché de l'informatique (cloud computing, outsourcing, SaaS, data centers, web services, etc.) la gestion des correctifs s'apparente à une quête sans fin où la riposte aura toujours un temps de retard.

L'offre s'est déplacée de l'outil vers le service, de l'approche « interne » vers le SaaS. Les MSSPs du début des années 2000, (Managed Security Services Providers), comme Ubizen ont quasiment tous rejoint la sphère des opérateurs télécoms pour l'administration des infrastructures réseaux sécurisées (dans une optique de défense qui reste cependant « périmétrique »).

La gestion des correctifs a donc évolué vers des offres de gestion des vulnérabilités proposées notamment par un leader comme Qualys ou un acteur plus récent comme VUPEN Security. Une approche plus proactive, plus économique aussi a vu le jour et répond sans doute aux attentes du marché des grandes entreprises et peut-être demain des PME.

Pour Chaouki Bekrar, PDG de VUPEN Security, « *Les clients font face à une recrudescence spectaculaire du nombre de vulnérabilités informatiques. En 2000, les professionnels de la sécurité devaient gérer quelques dizaines de vulnérabilités par mois, alors qu'aujourd'hui les failles révélées chaque mois se comptent en centaines. L'évolution et la complexité des parcs et infrastructures informatiques rendent le travail de gestion des vulnérabilités fastidieux, et l'externalisation de cette tâche devient incontournable. Les solutions de gestion des vulnérabilités ne se concentraient que sur l'aspect système alors que la première menace aujourd'hui est celle qui concerne les applications, qu'elles soient web ou logicielles. Les vulnérabilités web étaient quasi-inexistantes et leur danger méconnu, alors qu'elles représentent aujourd'hui plus de 80% des failles découvertes et sont devenues la première source d'attaque sur Internet.* »

De son côté, pour libérer les entreprises de la « charge » de la sécurité, Qualys ambitionne de « *devenir les "contrôleurs" d'Internet grâce à nos milliards de sondes disposées dans le monde et l'ensemble de nos partenariats avec les acteurs du monde de la sécurité ...* »
Philippe COURTOT (CEO – Qualys)

Les outils informatiques, qu'ils soient systèmes d'exploitation, navigateurs, messageries électroniques, protocoles, bases de données, applications ne seront jamais conçus ni programmés sans faille.
Si la certification des technologies (ISO15408) propose une alternative utile pour les systèmes sensibles, les services de gestion de vulnérabilités en mode Saas n'ont-ils pas un bel avenir devant eux ?

3.2.3. De la défense périmétrique à la défense en profondeur : les leçons de l'histoire !

Comment ne pas rendre hommage ici à Hervé Schauer, qui a conceptualisé dès 1991 les relais applicatifs, conscient que les pare-feu « couche basse » étaient insuffisants ! Depuis le milieu des années 90, routeurs, pare-feux, proxys, VPN se sont multipliés afin de rejeter les intrus indésirables. On peut d'ailleurs se poser la question si ces outils font encore partie du marché de la sécurité informatique. Ne sont-ils pas des composants indispensables à toute infrastructure « réseau » sans que l'on parle nécessairement de risque ou de menace ? A l'image d'une porte ou d'une fenêtre dans un bâtiment (qui délimitent l'intérieur de l'extérieur en protégeant du bruit et du froid avant tout !).

Le concept de « défense périmétrique » repose sur des zones ou des espaces à protéger d'un monde hostile et où règnent la confiance, le sentiment de sécurité. Cependant l'ouverture des entreprises sur l'Internet mais plus précisément à des tierces parties (clients, partenaires, fournisseurs, administrations, etc.) oblige de définir des zones « grises », de partage, d'échange et d'autres « noires » où règnent le chaos, le mal, la violence, la guerre.

Les infrastructures ont ainsi évolué en proposant des VLAN, des VPN, des DMZ. Toujours dans une optique de périmètres et de frontières. Sans être totalement submergée, cette approche a montré ses limites. Parce qu'une clé USB de quelques grammes, une puce RFID, voire demain, une nano-technologie, se jouent des pare-feux et de tout cloisonnement de réseau. Aussi parce que les logiciels malveillants devenus furtifs et à usage unique, agiront via un flux applicatif ou un protocole piégé avant que la parade ne soit disponible, si elle l'est un jour. Enfin et surtout parce que ce n'est pas uniquement par la technologie et des outillages sophistiqués que l'on protège réellement ce qui a de la valeur. L'homme a aussi son rôle à jouer.

Le concept de défense en profondeur, d'origine militaire, a donc été remis au goût du jour. Ses grands principes sont les suivants :

- Le **renseignement** est la première ligne de défense : depuis l'information sur les menaces effectives, la détection d'agissements souvent précurseurs d'attaques, jusqu'à toute détection non seulement d'attaques avérées et identifiées, mais encore de tout comportement « anormal » et donc suspect.
- Plusieurs lignes de défenses **coordonnées et ordonnées** sont nécessaires. L'infrastructure en propose une mais elle doit être a minima complétée par le code applicatif et les points d'accès, incluant l'utilisateur.
- La perte d'une ligne de défense doit **affaiblir l'attaque** (au moins indirectement en recueillant un maximum d'information sur ses origines, sa nature, sur les prochaines étapes possibles ou probables), ne pas entraîner la perte des autres lignes de défense mais au contraire permettre de les **renforcer**.
- Une ligne de défense doit comporter les parades (même si cela se limite à la détection d'anomalies et au traçage dans le cas d'attaques de type non identifiable) à toutes les attaques possibles (**complétude** d'une ligne en elle-même).
- Enfin, la défense n'exclut pas des actions offensives.

La **défense en profondeur pour un système d'information** est une défense **globale et dynamique**. Il s'agit alors de permettre des actions de neutralisation des atteintes contre la sécurité, ***à moindre coût***, grâce à une gestion des risques, un système de renseignement, une planification des réactions et l'enrichissement permanent grâce au retour d'expérience.

> ***Appliquer les principes des normes ISO 2700x ne traduit-elle pas une approche raisonnée de la défense en profondeur sans pour autant entrer dans le diktat de la certification ?***

3.2.4. De la détection / prévention d'intrusion au SIM / SIEM : boucler la boucle !

Le SIM (Security Information Management) et le SIEM (Security Information and Event Management) font partie d'une longue suite d'acronymes dont les professionnels de la Sécurité du SI semblent friands. VPN (Virtual Private Network), IDS (Intrusion Detection System), IPS (Intrusion Prevention System), SSO (Single Sign On), IAM (Identity and Access Management) ou encore PKI (Public Key Infrastructure), voire DLP (Data Loss Prevention) font partie du quotidien des RSSI. Malheureusement, pas toujours pour des projets couronnés de succès.

Le SIEM fait désormais partie de cet ensemble de projets, concepts, produits, méthodes ou processus - on ne sait plus très bien – qui monopolisent beaucoup d'énergie pour des résultats qui restent incertains, souvent faute de définition d'un objectif clair sortant du piège classique du choix d'un outil.

Dès 2006, le SANS Institute publiait un article de 41 pages orientant résolument la question en termes de technologies et énumérant les 4 fonctionnalités du SIEM :

- consolidation des traces,
- corrélation des menaces,
- gestion d'incident,
- reporting.

D'une certaine façon, le SIEM prolonge des pratiques anciennes dans une démarche globale : gestion de vulnérabilités, de traces, détection d'intrusion ou pourquoi pas de code malveillant, etc.

En mai dernier, lors d'une réunion du Groupe de travail Netfocus consacré au SIEM, la majeure partie des RSSI présents concentrait leur démarche sur l'analyse et la corrélation de traces en avouant avant tout chercher un outil, en omettant les autres dimensions (la méthode, les processus, les ressources humaines).

Pour Didier GRAS (Responsable Sécurité des SI du Groupe BNP Paribas), *« le SIEM répond à deux exigences fortes. Il faut, d'une part, tenir compte du contexte spécifique des entreprises qui fonctionnent comme des « hubs » de gestion de flux d'information ouverts sur l'extérieur (comme un aéroport), et d'autre part, introduire une approche plus tactique de la Sécurité SI entre la vision stratégique des enjeux et la gestion purement opérationnelle. »*

Finalement, l'approche « SIEM » répond à une question de fond du pilotage de la sécurité : **la mise en place d'une « tour de contrôle » qui supervise certains « évènements »**. La difficulté est de définir lesquels ! Une association loi 1901 dédiée au sujet (R2JS : Club de Réflexion et de Recherche en Gestion Opérationnelle de la Sécurité) a été créée et en a identifié environ 300. L'association regroupe des représentants de grands groupes, des pouvoirs publics et du monde de la recherche.

Cette gestion d'évènements doit alors répondre à des enjeux différents mais étroitement liés entre eux :

- **Le risque** : en fonction des systèmes « sous contrôle » et de leur sensibilité pour les métiers ou l'entreprise
- **La sécurité** : en termes de gestion des vulnérabilités et d'évaluation des menaces / attaques
- **La conformité** : notamment au regard d'obligations de conservation de données ou d'archivage légal
- **La performance** : dès lors qu'un évènement de sécurité impacte le fonctionnement du SI
- **Le juridique** : notamment en termes de protection des données personnelles, de conditions d'accès aux traces

Nul doute que le SIEM représente une démarche de fond de la Sécurité du SI mais qui demeure encore trop artisanale ou restrictive pour beaucoup. Son industrialisation passe par une responsabilisation d'acteurs clés qui font et feront partie de la sphère « Internet ». Car se pose indubitablement la question des équipes et du mode de fonctionnement en 24/7 : Internes ou externes ou mixtes ? Quelle formation ? Quelle déontologie ? Quelle rémunération ? Quelle localisation ?

> ***La question économique (comme le facteur humain) est donc au cœur de l'approche SIEM qui dépasse largement le cadre d'un outil et d'une analyse de traces.***
> ***Si le recentrage sur son cœur de métier est la clé du management des entreprises, une offre de service économiquement acceptable (avec des volumes suffisants pour être attractive) avec un cadre contractuel adapté pour être acceptée, ne devrait-elle pas être encouragée ?***

3.2.5. Synthèse et leçons

Globalement, le marché de la sécurité semble ne pas véritablement connaître la crise bien que des tensions existent ici ou là, sur les budgets des entreprises et sur des offres anciennes (IDS, anti-virus, PKI) ou en devenir (IAM, DLP, SIEM).

Pourtant, au terme d'une décennie riche en innovations et en adaptations aux menaces comme aux enjeux et aux besoins spécifiques des entreprises et administrations, plusieurs questions structurantes méritent d'être posées :

- Comment mettre fin au marketing de la peur « Internet » ?
  - Sortie définitive de la défense périmétrique avec l'avènement du Cloud computing ?
  - Gestion plus économique des vulnérabilités et des correctifs ?
- L'achat de services va-t-il réellement supplanter les outils ?
  - Lutte anti-malware « dans le réseau » et rôle des ISP et des États ?
  - Tours de contrôle « mutualisées », bien au-delà des CERT ou CSIRT ?
- Comment les donneurs d'ordre peuvent-ils reprendre le contrôle face aux offreurs ?
  - Abonnements à des services selon des volumes variables dans le temps ?
  - Consolidation du marché selon une orientation « service » et réduisant le nombre de « juges et partis » ?

Éric Domage
IDC Security Software & Services Research Manager

> ***« Le cloud computing ouvre une nouvelle ère de l'informatique en banalisant la technicité du réseau, des infrastructures et des applications. Désormais, tout le monde peut acheter de la puissance de calcul ou du temps d'application sans avoir besoin d'être informaticien. Tout est dans le nuage, plus besoin de savoir comment cela marche.***
>
> ***Voilà un défi majeur pour les experts de la sécurité : comment sécuriser cette informatique sans serveur, sans data center et sans Direction Informatique ? Comment protéger les données alors que l'accès au Nuage (et à la puissance de calcul) est aussi simple que de recharger une carte de cantine ?***
>
> ***Si les fondamentaux bougent, il va falloir apprendre à bouger avec ! »***

3.3. Échanges sur l'évolution du cadre légal

Troisième aspect du bilan de la décennie, la dimension juridique n'est sans doute pas la plus simple à aborder. L'exigence sécuritaire et la frénésie législative ne sont plus à démontrer et le domaine de la Sécurité des SI est touché de plein fouet. Quelle profusion de textes en 10 ans !

Pour aborder le sujet, nous avons sollicité les deux avocats spécialisés du Cercle Européen de la Sécurité pour effectuer un bilan des textes et de leur application, depuis le début des années 2000.

En dix questions, nous abordons ainsi les problématiques de la protection des données personnelles, du piratage, de la cybercriminalité et de la confiance numérique. Des sujets complexes mais passionnants, et intéressant au plus haut point l'ensemble des acteurs de la Sécurité SI.

Question n°1 **Quel est selon vous l'évènement le plus marquant dans le domaine juridique de la Sécurité des SI depuis 2000 ? Pourquoi ?**

Christiane FERAL-SCHUHL : Je considère que l'évènement de la décennie est la loi du 13 mars 2000 qui a consacré l'écrit sous forme électronique par l'apposition d'une signature électronique. C'est une incroyable révolution qui consacre, au plan juridique, l'égalité de traitement entre l'écrit électronique et l'écrit « traditionnel » revêtu de la signature manuscrite.

En marge de cette révolution, il faut également signaler le Référentiel général de sécurité (RGS) créé par une ordonnance de 2005 dont la version 1.0 a été publiée par arrêté du 18 mai 2010. Ce référentiel concerne toutes les administrations susceptibles d'échanger des données avec les usagers ou entre elles. L'objectif du RGS n'est pas d'imposer une technologie, une architecture ou une solution technique. En revanche, une administration doit s'y référer et respecter les règles édictées lorsqu'elle juge nécessaire de mettre en œuvre des fonctions de sécurité prévues dans le RGS.

Éric CAPRIOLI : Selon moi, ce sont plusieurs événements qui pourraient être analysés séparément mais qui convergent vers un même objectif :

- prise en compte des notifications des failles de sécurité au niveau européen par le biais de 2 directives (Directives 2009/140/CE et 2009/136/CE), suivies d'une proposition de loi votée au Sénat ;
- création de l'ENISA (Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information) et de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) – créée par le décret n° 2009-834 du 7 juillet 2009.

La sécurité des systèmes d'information est reconnue comme étant une priorité de l'Union Européenne. En outre, l'intégration des notifications de failles de sécurité envoyées aux instances nationales (CNIL, ANSSI ou autres) en charge des données à caractère personnel et de la sécurité doit permettre d'établir des statistiques concernant le niveau de sécurité des entreprises françaises et européennes. Cela permettra de mieux gérer les risques (notamment juridiques) liés aux incidents de sécurité (ex : approche SIEM).

D'autres référentiels comme le Référentiel Général de Sécurité (authentification, signature, confidentialité et horodatage) et le Référentiel Général d'Interopérabilité (plus axé sur l'archivage) permettront d'assurer une meilleure sécurité des échanges électroniques.

Question n°2 **Allons plus loin. C'est un fait, le Code Civil a été modifié le 13 mars 2000 pour y introduire la preuve électronique. Texte extrêmement simple ! Mais, pour paraphraser Napoléon, est-ce un « enfer à l'application » ?**

CFS : Un « enfer » ? C'est excessif. Mais la France n'a pas choisi la formule la plus simple ! Elle a opté pour la « signature électronique avancée » qui exige, conformément à la directive européenne de 1999, quatre conditions cumulatives : (I) être liée uniquement au signataire, (II) permettre de l'identifier, (III) être créée par des moyens que celui-ci puisse garder sous son contrôle exclusif, et (IV) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure de ces données soit détectable (dir. 1999/93/CE, art. 2.2).

Ces exigences ont été précisées par le décret n°2001-272 du 30 mars 2001 qui fixe trois conditions à la reconnaissance de fiabilité d'un procédé de signature électronique, à savoir : (I) l'usage d'une signature électronique sécurisée (1ère condition) ; (II) l'utilisation d'un dispositif sécurisé de création de signature électronique (2ème condition) ; (III) l'utilisation d'un certificat électronique qualifié (3ème condition).

On mesure tout de suite la difficulté d'intégration et de prise en compte de l'ensemble de ces contraintes. Le résultat est que si le principe de la signature électronique marque une formidable avancée, dans la pratique, elle est, à ce jour, très peu utilisée.

EC : L'application de la loi de 2000 n'est pas vraiment un enfer. En fait, les écrits signés électroniquement n'ont pas encore été portés devant les tribunaux français. A ce jour, il n'existe qu'une seule décision aux Etats Unis au cours de l'été 2009 à l'occasion de la signature d'un contrat d'assurance.

L'utilisation croissante du recours à des signatures électroniques (sans certificat qualifié au sens du décret du 30 mars 2001) se passe pour l'instant sans recours au juge (par exemple : les certificats éphémères dans certaines applications bancaires et de crédit à la consommation ou les certificats TéléTVA). Je pense que les certificats qualifiés ne doivent être utilisés que pour les actes authentiques (notaires, huissiers de justice, jugements et Etat civil), voire pour les transactions particulièrement sensibles ou d'une valeur économique importante. Pour les autres actes courants et du commerce, la signature électronique dite « simple » (sans certificat qualifié) est suffisante et parfaitement valable.

Au niveau du conseil lors de la mise en place de solutions, il faut une bonne connaissance des éléments techniques, organisationnels, pour appréhender les fonctionnalités que le droit détermine. Il est arrivé que les règles relatives à la copie numérisée d'un document papier signé, soit confondues avec celles relatives à l'original (original électronique). Or, ces règles sont différentes. En outre, certains manques ont vu le jour comme la possibilité de détruire les originaux « papier » dès le moment où la copie numérisée du document papier est reconnue comme suffisamment fiable.

Question n°3 **Autre sujet majeur, la Convention « cybercriminalité » du Conseil de l'Europe a été ratifiée le 23 novembre 2001 par plus de 30 pays. Quel bilan peut-on faire de ses impacts réels ?**

EC : Les impacts réels se positionnent, d'une part, dans le cadre de l'harmonisation des législations des États signataires (au nombre de 30 ratifications/adhésions et de 16 signatures à ce jour) et, d'autre part, dans la prise de conscience des États des infractions commises via le recours aux

réseaux numériques (attaques, contrefaçon, ...). En outre, les autorités judiciaires coopèrent avec notamment la création de points de contact dans les États.

CFS : En effet, sur les mesures visant à faciliter les moyens d'enquêtes et de poursuites pénales adaptés à la mondialisation des réseaux ou encore à favoriser la coopération internationale, plusieurs mesures ont été prises et sont d'ores et déjà opérationnelles.

Ainsi, la France a créé l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC). En effet, l'article 35 de la Convention demande à chaque État de créer un « point de contact joignable 24 heures sur 24, sept jours sur sept », afin de fournir une assistance immédiate aux fins d'investigations concernant les infractions pénales liées à des systèmes et données informatiques ou afin de recueillir des preuves électroniques se rapportant à une infraction pénale. Nous disposons donc d'un tel organisme. Il s'agit, pour la France, du point de contact pour la coopération policière internationale avec Europol, Interpol et le G8.

La Commission européenne a, quant à elle, pris l'initiative de confier à une équipe de recherche la mise au point d'une procédure standard de perquisition et de saisie en temps réel d'informations relatives à une infraction liée à l'utilisation de l'informatique. Elle vise à permettre d'identifier les preuves afin qu'elles soient recevables devant un juge. Il s'agit de la méthode « cybertools online search evidence » (CTOSE) qui inclut la mise à disposition d'un logiciel, baptisé « outil de conseil en cybercriminalité ».

Sur l'harmonisation des législations, l'exercice est plus délicat en raison des divergences que soulève l'élaboration de standards internationaux en la matière. Pour autant, le protocole additionnel du 7 novembre 2002 portant sur l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques a pu être négocié. Ce texte vise également à prévenir les menaces et insultes racistes, le négationnisme, le révisionnisme ou la justification des crimes contre l'humanité. Son objectif est d'harmoniser le droit pénal en vigueur dans les différents États parties. Il a été ouvert à la signature le 28 janvier 2003, date à laquelle il a été signé par la France.

Question n°4 **En relation avec le point précédent, les textes liberticides se multiplient depuis les attentats du 11 septembre 2001 (LSQ, LSI, terrorisme, LOPPSI). Avez-vous constaté de réels impacts au sein des entreprises ? A quels niveaux ?**

Christiane Féral-Schuhl
Avocat à la Cour

La responsabilité de l'entreprise du fait de ses salariés

« Les entreprises ont conscience aujourd'hui que leur responsabilité peut être engagée en raison de l'usage que les employés peuvent faire des outils technologiques mis à leur disposition ou encore à cause d'une défaillance dans le système de sécurité informatique de l'entreprise. »

Elles cherchent donc à mieux contrôler les employés en mettant en place des dispositifs de filtrage visant à interdire l'accès à certains sites, ou encore en interdisant le téléchargement de logiciels, la connexion à des forums ou à des chats, voire l'accès aux réseaux sociaux personnels. La plupart des entreprises encadre, via une charte ou un règlement intérieur, les conditions d'utilisation des outils technologiques.

Par ailleurs, elles mettent en place une véritable politique de sécurité, en définissant une procédure de gestion des habilitations ou des accès.

Enfin, pour certains organismes publics ou privés (visés par le décret du 26 octobre 2007, relatif aux demandes de mise à disposition de données par voie électronique), il existe une obligation de communication des données de connexion sur demande d'un officier de police judiciaire. On observe également sur ce terrain une préoccupation concernant la conservation de ces données conformément aux exigences de la loi.

EC : En effet, on peut constater que les usages de la sécurité dans les entreprises se sont modifiés, par exemple avec l'encadrement juridique des mesures de surveillance et de protection des personnes (salariés) et des biens avec notamment les différentes chartes d'utilisation des ressources informatiques et des communications électroniques (utilisateurs, prestataires externes et administrateurs) ou par des dispositifs de filtrage. Mais dans le domaine de la sécurité de l'information, d'autres aspects juridiques sont pris en compte à propos de la gestion des logs techniques et de sécurité, des courriels ou encore des identités et des accès (IAM). A côté des audits juridiques de la sécurité des SI, qui visent à la conformité (ex : ISO 27001), les entreprises se préoccupent de l'utilisation de leurs traces dans le cadre de plaintes pénales ou de litiges civils.

Question n°5 **Allons plus loin : Comment expliquez-vous le peu de publicité / transparence sur les attaques et fraudes (souvent internes) subies par les entreprises ?**

CFS : Pour une entreprise, révéler une attaque de son système informatique ou une fraude en son sein n'est pas anodin. Tout d'abord, cela révèle qu'il y a une faille dans son système. Comme vous le soulignez, ces attaques sont souvent le fait d'employés ou d'anciens employés pour lesquels des mesures de sécurité de base n'ont pas été prises (changement de codes d'accès tout simplement !).

Il est donc facile d'en déduire que faire de la publicité sur de telles défaillances nuirait à la réputation de l'entreprise.

EC : C'est certain, s'il y a peu de publicité, c'est que le préjudice d'image pourrait coûter très cher. Imaginez une grande entreprise (banques, télécoms) ou administration indiquer qu'une de ses bases de données (clients ou usagers) a été piratée : outre la responsabilité à laquelle elle s'exposerait, les clients concernés pourraient être tentés de changer de professionnel, et que dire de la confiance auprès des futurs clients. Avec l'obligation de notification des failles de sécurité qui va bientôt être adoptée en France (et dans l'UE en 2011), le sujet va considérablement évoluer ; les entreprises doivent s'y préparer dès à présent étant donné son ampleur et sa complexité.

Question n°6 **Autre sujet : Le Correspondant Informatique et Libertés est obligatoire dans plusieurs pays européens (1977 pour l'Allemagne). Doit-il l'être en France ? Les RSSI sont-ils légitimes pour endosser aussi cette fonction ?**

CFS : C'est une question d'actualité soulevée par la CNIL et qui sera tranchée par le Parlement lors des débats sur la loi visant à mieux garantir le droit à la vie privée à l'heure du numérique.

Pour ma part, je pense que ce serait une bonne chose de prévoir une fonction CIL, étant précisé que je suis favorable à l'externalisation de cette mission. Le CIL salarié me semble dans une situation

de dépendance difficilement compatible avec la mission qui lui est confiée. A ce titre, il me semble que l'avocat offre à la fois les garanties de confidentialité et d'expertise requises pour mener à bien une telle mission. S'y ajoute l'obligation de non-dénonciation de son client qui doit le conduire à démissionner en cas de désaccord persistant avec le responsable des traitements et non, comme pour tout autre CIL, à alerter la CNIL.

Le RSSI, présent par hypothèse dans des entreprises importantes, peut bien sûr endosser la fonction et dispose des compétences pour cela, mais, pour autant, il me paraît préférable de bien dissocier les fonctions CIL et RSSI.

EC : On peut estimer que l'obligation de désignation d'un CIL est opportune dans les grandes entreprises et collectivités publiques dans la mesure où la protection des données à caractère personnel s'inscrit dans un cadre légal et réglementaire complexe et en mouvance qui requiert en interne la présence de compétences spécifiques.

En outre, il n'est pas inutile de rappeler que le patrimoine informationnel de l'entreprise doit être protégé, d'une part, et que lesdites structures se sont déjà dotées de correspondants en interne, voire de responsables « Informatique et libertés », d'autre part. A toutes fins utiles, il convient de préciser que le CIL aura un rôle important à jouer sur les notifications des failles de sécurité ayant un impact sur les données personnelles traitées. Le RSSI, ou plus exactement une personne au sein de la direction ou du service, me semble légitime pour remplir ce rôle. Mais un CIL nécessite des compétences techniques, organisationnelles, métiers et juridiques. Ainsi, le CIL pourrait également appartenir aux directions juridiques, RH ou conformité/risques. Le choix dépendra des organisations et des ressources internes.

Éric CAPRIOLI
Avocat à la Cour

> ***Culture et sécurité globale***
>
> ***« Les comportements et la culture sécurité de chacun contribuent à la sécurité globale de l'information de l'entreprise ».***

Question n°7 **Quels ont été, selon vous, les freins majeurs au déploiement des projets de « signature électronique » au sein des entreprises et des administrations ?**

EC : L'un des freins majeurs au déploiement des projets de signature électronique est sans aucun doute l'attente du serpent de mer qu'est la signature électronique sécurisée bénéficiant de la présomption de fiabilité (art. 1316-4 al. 2 du code civil et art. 2 du décret du 30 mars 2001).

Or, seuls 5 % du marché sont réellement concernés par ce type de signature : les actes authentiques électroniques des huissiers de justice, des notaires, les jugements et les actes de l'état civil, ou des actes particulièrement sensibles. Pour le reste, une signature électronique « simple » – c'est-à-dire dont la fiabilité doit être rapportée par le demandeur devant les tribunaux – est juridiquement suffisante.

En outre, pour le déploiement à grande échelle, on a besoin de la Carte d'identité électronique (avec certificat d'identification et signature), à moins que le projet IDéNum du Secrétariat d'État à l'économie numérique ne remplisse ce rôle dans l'attente de son déploiement.

CFS : C'est à l'évidence la complexité des textes comme évoqué précédemment.

Question n°8 **Depuis l'affaire Napster (plainte de la RIAA – Recording Industry Association of America – en décembre 1999) aucun texte n'a vraiment enrayé le phénomène du piratage alors qu'aucune solution technique fiable et pérenne n'est apparue. Est-ce que l'Hadopi 2 représente une approche pertinente (dissuasion, notification, conciliation, sanction) et utilisable dans d'autres domaines ?**

EC : Il faut souligner que la riposte graduée instaurée par l'HADOPI 2 vient d'être adoptée au Royaume-Uni, et que la tendance est à la généralisation de ce dispositif dans l'UE qui mélange à la fois une phase de dissuasion et une phase de sanction judiciaire. On peut penser que ce système perdurera en attendant de nouveaux business modèles pour les contenus (musique, film, jeux...).

CFS : On sait que le dispositif de riposte graduée n'est pas parfait. Il sera toujours possible à un « téléchargeur fraudeur » de contourner l'interdiction, notamment en usurpant d'autres identités numériques ou en détournant des connexions Internet... Par ailleurs, le regroupement des services de téléphone, de télévision et d'Internet complique forcément le dispositif.

Pour autant, comme toujours, cette mesure peut avoir un effet dissuasif sur un certain nombre de personnes. La notification d'un avertissement permettra sans aucun doute de remettre dans le droit chemin un certain nombre de téléchargeurs occasionnels. HADOPI n'est donc pas la panacée annoncée, mais est néanmoins un élément positif.

Question n°9 **Quelle est votre expérience la plus frappante, au cours de la décennie (dans le cadre d'un projet ou d'une affaire) ?**

EC : C'est le conservatisme de certaines juridictions qui tendent à forger une jurisprudence constante, alors que les modèles économiques des entreprises ont considérablement changé avec le Web 2.0. Par exemple, la directive du 8 juin 2000 qui a donné la LCEN, se fonde sur des modèles techniques de la fin des années 90 alors que les sites comme Google, YouTube, E-Bay, FaceBook ou ceux effectuant du parking des noms de domaine n'existaient pas ou commençaient leurs activités.

CFS : L'attrait de l'offshore ! Et le développement spectaculaire du problème soulevé par le transfert des données à caractère personnel en dehors de l'Union européenne. Et pour autant, l'inconscience ou le peu de sensibilité juridique des responsables de tels projets ! Il est vrai que le dispositif peut paraître complexe, mais l'on touche souvent à des applications sensibles de l'entreprise.

Question n°10 **Au plan prospectif, quel message souhaitez-vous faire passer aux participants des Assises de la Sécurité 2010 ?**

CFS : L'approche sécuritaire par les risques est la manière la plus sûre et la plus efficace pour anticiper les dérapages d'un projet. Savoir prendre le temps d'identifier les zones de risques dans l'entreprise, c'est l'étape incontournable pour définir les mesures opérationnelles et/ou juridiques efficaces pour maîtriser la sécurité !

EC : Le droit n'est pas seulement une série de contraintes relevant notamment de la conformité, il est aussi un instrument stratégique au service des entreprises et des projets, avec de nombreuses opportunités à traduire en termes « technico-juridiques » !

3.4. La fonction Sécurité des SI : de « Docteur No » à « Yes we can ! »

Risques, solutions, droit. C'est sur ces trois piliers que le RSSI bâtit son activité, sans oublier évidemment, son contexte. Son organisation est son champ d'intervention, le « pré-carré », ouvert sur l'extérieur, où il met en place sa démarche, sa stratégie et ses projets.

Si hier, il faisait souvent figure d' « empêcheur de tourner en rond », il tend désormais à incarner une certaine valeur ajoutée au sein de son organisation.

JF. LOUAPRE
Resp Sécurité SI
AG2R La Mondiale

> *« Le « RSSI qui dit non » est définitivement révolu.*
>
> *Nous nous positionnons comme les facilitateurs des évolutions des métiers de l'entreprise et des outils qui les supportent.*
> *Nous accompagnons nos directions métiers dans l'identification des risques induits par ces évolutions, et définissons, avec eux, les moyens de maitrise des risques réellement impactant pour l'activité. »*

Essayons d'analyser comment cette fonction a évolué depuis 10 ans.

3.4.1. Quelques rappels

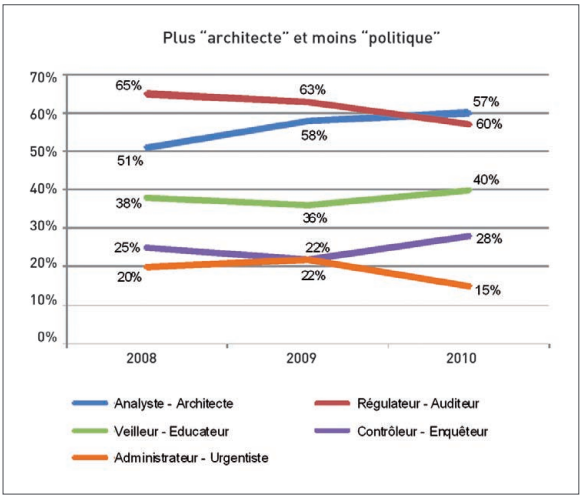
Que d'articles, de témoignages, d'études sur cette fonction qu'est le RSSI. Apparue dans les années 80 et fortement mise en valeur à la fin des années 90, elle vient de vivre une décennie des plus animées. Le moment était donc opportun d'en effectuer un bilan en affirmant d'entrée qu'il est définitivement illusoire de la définir. De tous les qualificatifs qui ont été proposés pour caractériser un RSSI, quelques uns peuvent cependant être retenus et ils montrent qu'on a plus affaire à un caméléon qu'à un chien de garde : stratège, pilote, chef d'orchestre, architecte, mécanicien, expert. Faites votre choix...

Depuis que nous menons les enquêtes du Cercle Européen, dont l'objectif est justement de « radiographier » les RSSI (qui sont-ils ? que font-ils ? où vont-ils ?), nous avons positionné dix rôles et 5 fonctions clés qui peuvent être plus ou moins assumés par les RSSI, selon leur formation, leur contexte et leur expérience.

Lorsque l'on questionne le panel de l'enquête sur les deux fonctions clés qui les **caractérisent le mieux au quotidien**, on remarque :

- Que la fonction d'analyste-architecte (principalement liée aux projets) devient prépondérante au sein du panel (qui ne comporte pas que des RSSI)...

• ... tandis que le régulateur-auditeur (rôle plus « politique ») et l'administrateur-urgentiste (rôle le plus opérationnel) régressent.
• Que les 2 fonctions clés de « support » (« contrôleur-enquêteur » et dans une moindre mesure « veilleur éducateur ») progressent légèrement.



Nous avons aussi mis en évidence deux grands profils de RSSI : le « manager » tourné vers les risques et l' « opérationnel » axé sur la mise en œuvre des solutions. Sans être parfait, ce modèle possède des vertus pédagogiques indéniables, notamment au titre de la séparation des pouvoirs. Et comme l'affirmait aussi Platon : *« A pratiquer plusieurs métiers, on ne réussit dans aucun. »*

Quant au titre et à la dangerosité d'être ou de se sentir « responsable » de la Sécurité du SI, nous laissons à chaque professionnel le soin de se déterminer et de l'apprécier par lui-même ! Sachant qu'un des leitmotivs de la fonction est le classique *« la sécurité, c'est l'affaire de chacun »*, qui dépasse le cadre de la responsabilité et qui renvoie à la question des moyens et donc de son budget.

Ce dernier chapitre du bilan introductif, reprend quelques résultats de l'enquête du Cercle et approfondit 4 thématiques qui ont pu avoir des impacts significatifs sur la fonction au cours de la décennie 2001-2010 :

- Le développement des activités d'Intelligence économique
- L'émergence du Correspondant Informatique et Libertés
- Les normes et notamment l'ISO 2700x
- La dématérialisation et les services de confiance numérique

De manière évidente, il y a ici un parti pris car on ne saurait être exhaustif en la matière. Il nous a simplement semblé utile de concentrer l'analyse pour ne pas nous disperser.

Pascal BASSET
Resp Conformité SI PMU

« Le développement de l'Internet reste le fait marquant de la décennie.

Facteur de développement et de croissance, Internet a également apporté son lot de nouvelles menaces obligeant le RSSI à redéfinir sa stratégie et ses priorités pour adresser les nouveaux risques liés à l'entreprise éclatée, l'hyper mobilité et l'avènement des réseaux sociaux. »

3.4.2. Les enjeux couverts par les professionnels

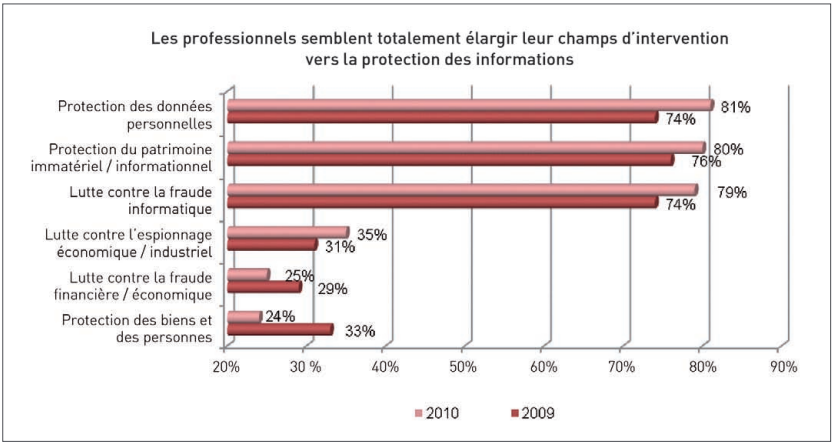
Qu'elle est loin la sécurité informatique des années 80 ! Les professionnels sont désormais passés à l'ère de la sécurité et de la sûreté des informations. C'est bien sûr une réalité pour beaucoup depuis 10 ans voire plus, mais on ne doit plus en douter. Les questions historiques de sécurité informatique, puis du Système d'information, se concentrent sur la gestion des attaques logiques, le secours et la continuité d'activité ainsi que sur la prise en compte de la sécurité dans les projets (voire dans les développements). C'est en soi une activité « ancienne » et qui doit s'industrialiser, notamment dans le cadre de l'émergence de « l'entreprise sans DSI » et du Cloud Computing.

Alain BOUILLÉ
Dir Sécurité SI
Groupe CDC

> ***« Grâce aux solutions de mobilité de plus en plus efficaces, vous ne savez déjà plus où sont vos utilisateurs. Avec le Cloud Computing, vous ne saurez plus où sont vos données.***
>
> ***Il va falloir nous concentrer sur l'essentiel à savoir la protection de deux actifs principaux : l'identité des utilisateurs et les données stratégiques. »***

Ces évolutions impliquent une prise en compte plus stratégique des risques liés au SI (que nous avions discutée dès le Livre Bleu des Assises 2004) en se concentrant autant, si ce n'est plus, sur les données et les informations, que sur l'infrastructure.

Ainsi, depuis 2004, nous avons mis en évidence que les professionnels de la Sécurité s'impliquent dans 6 enjeux dont 3 sont désormais incontournables (80% du panel en 2010) et surtout liés entre eux. Les 3 autres enjeux sont plus spécifiques à certains secteurs d'activité (cf. Analyse détaillée en ligne sur www.lecercle.biz). On notera une baisse significative pour la protection des biens et des personnes et une progression intéressante des questions d'espionnage économique / industriel.



Nous avons interrogé un panel de professionnels sur 2 enjeux particuliers :

- Le développement des activités d'intelligence économique
- La mise en place de la fonction « Correspondant Informatique et Libertés »

Les principaux avis sont résumés ci-dessous.

Les impacts de l'Intelligence économique sur la fonction Sécurité du SI
Ce qu'en pensent les professionnels...

Attention, risque de polémique ! Disons le d'entrée, pour beaucoup, le RSSI n'est pas concerné par les questions d'Intelligence Économique (vue sous l'angle de la gestion de l'information stratégique, et de la veille au sens large) mais 80% du panel se disent impliqués par la protection du patrimoine informationnel et 35% dans la lutte contre l'espionnage économique / industriel. Quelques avis tranchés :

« Un faux sujet monté en mayonnaise ! »
« L'IE défensive, ça ne veut rien dire ! »
« On évolue dans un monde ouvert, le partage est la règle et il faut juste trouver la limite. »

Clairement, le monde de l'Assurance, de la gestion des risques « SI » se heurte frontalement au secteur de la Défense pour qui la Patrie et ses entreprises sont en danger. Classique divergence entre la liberté et le protectionniste, entre le marché et l'État ?

Alors que de nombreux RSSI cherchent à sortir du modèle « Dr No », véritable empêcheur de tourner en rond pour les métiers et les utilisateurs, les contraintes défensives de la protection du patrimoine se heurtent à une dimension incontournable de nature psychologique voire sociologique, parfaitement symbolisée par l'essor des réseaux sociaux et la quasi disparition des frontières entre les sphères professionnelle et personnelle.

Pourtant, quelques points de convergence apparaissent :

- L'IE concerne avant tout des questions de « renseignement » et s'adresse, dans son volet défensif, à la menace malveillante dans une approche « sûreté ».
- La Sécurité du SI s'adresse naturellement à l'infrastructure et aux projets SI en s'attachant d'abord aux failles et vulnérabilités.
- La prise en compte du facteur humain et la sensibilisation permettent des synergies intelligentes entre protection des contenants et des contenus (cf. Évolution de la menace)
- Des projets ou activités « communs » peuvent se développer conjointement notamment autour de la « fuite d'information » et de la « cyber-surveillance ».
- Et enfin, la protection de l'information stratégique offre aussi une évolution « par le haut » à certains RSSI, hors de la DSI et proche des Comités de Direction.

En résumé, alors que le RSSI cherche à promouvoir une logique d'arbitrage raisonné par les métiers, au regard des risques liés au SI, le secteur de l'IE est perçu comme cherchant à « imposer » des mesures de protection de type « militaire » peu en phase avec leur démarche.

Cette vision doit évidemment être modérée en fonction des secteurs d'activités, mais pas nécessairement des tailles d'entreprise. Et de toute évidence, chaque professionnel se doit de déterminer, par lui-même, dans son contexte, la fonction la mieux adaptée et la place où il est le plus efficace !

Les impacts du Correspondant Informatique et Libertés sur la fonction Sécurité du SI
Ce qu'en pensent les professionnels...

Le CIL (peut-être obligatoire prochainement dans le cadre de la proposition de loi des sénateurs Détraigne et Escoffier) agit pour garantir la protection des données personnelles au sein de son organisation. En synergie ou en opposition avec le RSSI ?

Les RSSI sollicités mettent en évidence des écarts voire des divergences remarquables, plus ou moins fortes, entre les deux fonctions, et qui rendent délicat, mais pas impossible, le cumul des 2 fonctions :

- Le CIL a une approche par traitement (de données) alors que le RSSI s'adresse aux infrastructures, aux flux et aux informations.
- Le CIL permet à l'organisation de gérer un risque juridique (conformité) alors que le RSSI s'adresse à des risques opérationnels et quotidiens.
- Le CIL joue d'abord un rôle d' « avocat » (de défenseur de l'individu), le RSSI défend surtout son entreprise (et son patrimoine).
- Autant le CIL et son activité sont définis par décret, autant le RSSI est un caméléon à profil variable d'une entreprise / organisation à l'autre, et souvent positionné au sein d'une DSI.

Par ailleurs, s'il existe une genèse et une histoire des RSSI (certains ont 20 ans d'expérience), les CIL ont encore peu de recul sur leur mission. Et elle se complexifie énormément dès lors qu'on touche à des technologies innovantes (biométrie, nanotechnologies) et des processus « grand public » (santé, transports, jeux, etc.)

Enfin, alors que la question de l'externalisation du CIL est posée et sans doute pertinente, celle du RSSI apparaît délicate, voire souvent impossible. Un RSSI – CIL semble bien hasardeux sans une analyse approfondie, au cas par cas. Ou alors, éventuellement, dans une phase transitoire.

Mais des RSSI ne peuvent-ils pas pertinemment devenir CIL en abandonnant leurs anciennes fonctions ?

La question de la formation est alors essentielle. Si les fonctions seront globalement peu cumulables, des cursus « croisés » devront se développer pour permettre aux RSSI (plus largement aux professionnels de la SSI) et aux CIL de comprendre les pratiques des uns et des autres et envisager des cumuls de fonction, des répartitions de rôle voire des synergies (notamment dans la sensibilisation ou l'accompagnement des projets SI).

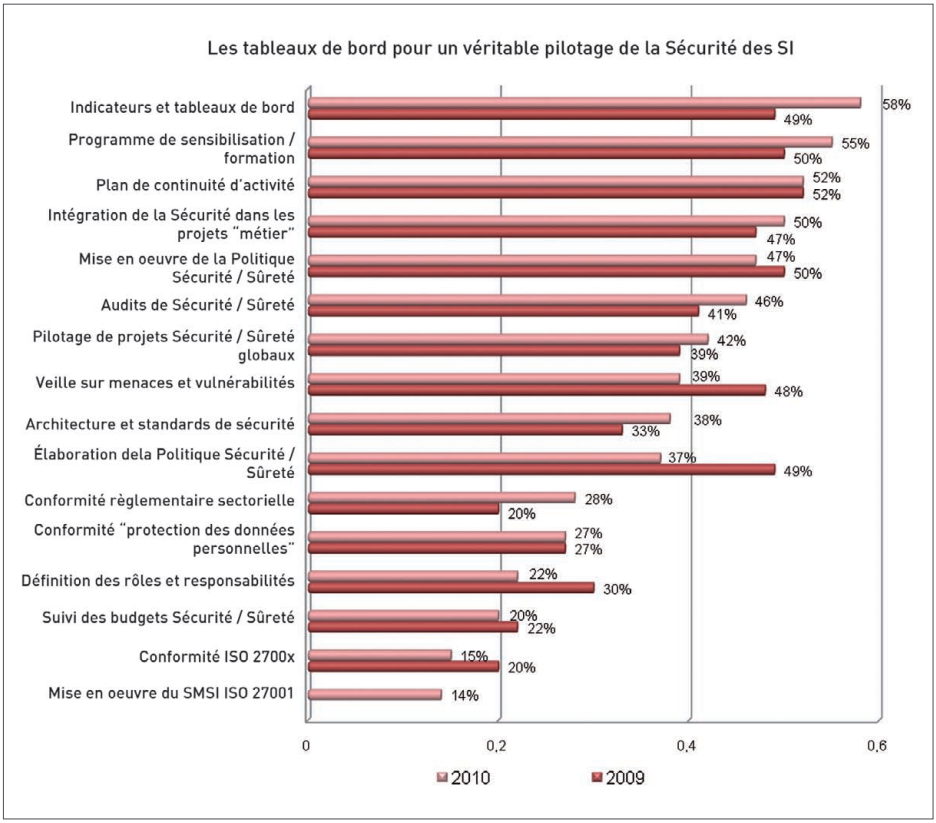
En conclusion, les enjeux couverts par les professionnels de la SSI confrontés au développement des activités « IE » et « I&L » mettent en perspective des évolutions intéressantes qui peuvent en concerner certains :

- Plus stratégique et en prise avec la protection du patrimoine
- Plus proche des décideurs et hors de la DSI
- Plus « arbitre » et moins « responsable »
- Autant « veilleur-éducateur » qu' « analyste-architecte »

3.4.3. Les activités transverses prioritaires

Observé depuis 2004, le pilotage d'activités transverses est une exigence majeure pour les RSSI de sorte que certains, les plus « managers », n'interviennent plus ou pas trop sur les projets et actions purement techniques et opérationnels.

Le schéma ci-dessous présente les résultats comparés sur les 2 dernières années.



A quelques exceptions près, les statistiques sont globalement stables et on remarque autant de baisses que de progressions.

Les questions classiques liées à la « politique » et aux « projets » sont supplantées en 2010 par deux activités dont la caractéristique commune est de « démontrer » en quoi la politique est comprise et réellement mise en œuvre : les indicateurs et tableaux de bord et la classique sensibilisation / formation. On se situe ici clairement dans la phase « check » du modèle PDCA de l'ISO 27001.

Les principaux enseignements à retenir sont :

- Des progressions importantes pour les tableaux de bord et la conformité sectorielle (santé, finance, opérateurs d'infrastructures vitales, etc.).
- Des baisses significatives sur l'élaboration de la Politique SSI, la gouvernance et sur la veille (qui démontrent une maturité croissante).
- Une faiblesse sur les normes ISO 2700x qui est corrélée avec les statistiques publiées par l'ISO et l'avis des RSSI.

En juillet 2010, 6573 certificats ISO/CEI 27001:2005 avaient été délivrés dans 81 pays, dont plus de 90 % concernent des prestataires de services. En France, les certifications ISO 27001 restent peu nombreuses (18) à égalité avec des pays comme la Slovénie ou la Slovaquie mais loin derrière le Royaume Uni avec ses 448 entreprises certifiées ou l'Allemagne avec 138 certificats délivrés, sans parler du Japon avec 3572 certificats délivrés ! (source ISO - 2010)

Les impacts des normes ISO 2700x sur la Sécurité du SI
Ce qu'en pensent les professionnels...

Comme l'attestent les résultats de l'enquête, l'utilisation des normes ISO en tant qu'outil de management et de conformité reste assez marginale. Tout au moins, elles ne se sont pas encore imposées comme une véritable priorité. C'est le principal enseignement tiré des discussions avec notre panel de RSSI pour qui, dans un large consensus, les normes ISO représentent avant tout :

- Une aide au pilotage réduisant la complexité croissante du domaine
- Un référentiel commun (vocabulaire, définitions et principes par exemple dans la relation avec les métiers et la DSI)
- Une base de référence pour les politiques de Sécurité SI, schémas directeurs et plans d'action (ce que l'on doit ou peut mettre en œuvre)

Elles ne sont absolument pas une finalité en soi notamment pour détenir un quelconque avantage concurrentiel. Mais elles permettent de réduire certaines disparités au sein de la Sécurité SI, notamment en facilitant la compréhension et la visibilité du domaine auprès d'une Direction Générale ou des métiers, sans oublier aussi l'opportunité de développement du business de la sécurité (conseil et audit essentiellement).

D'un point de vue plus stratégique, certains n'oublient pas le « pouvoir » des normes où tout part du processus d'élaboration avec des considérations géopolitiques majeures. L'importance de l'ISO 2700x sur le marché ne doit pas être négligée d'autant plus qu'elle tend à renforcer ou compléter d'autres textes ITIL, CNIL, SoX, LSF, ARJEL, etc.

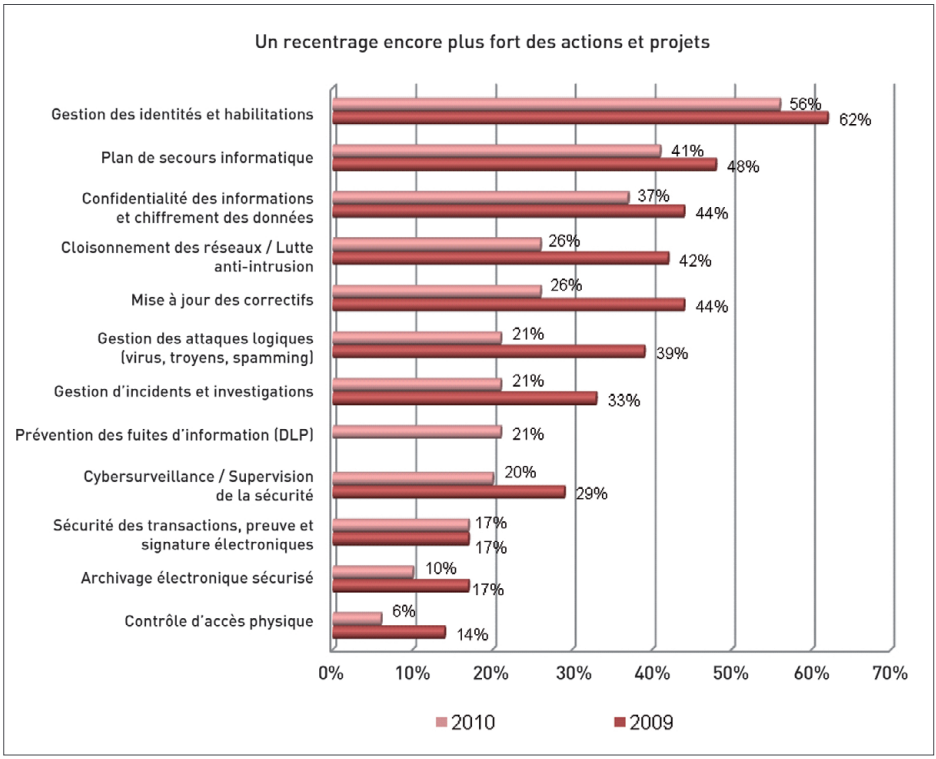
En résonance avec les relations « CIL-RSSI », ici aussi la conformité et la sécurité doivent être clairement distinguées. Etre conforme ne signifie pas sécurisé ! Pour le panel de RSSI, un des effets pervers de la certification individuelle (Implementor ou Auditor ISO27001) réside dans la baisse du niveau général de consultants qui appliquent des normes sans recul ni prise en compte réelle du contexte du client.

Ainsi, bien qu'elles deviennent incontournables, l'impact des normes ISO sur la décennie 2001-2010 semble finalement bien limité en France.

3.4.4. Les actions opérationnelles prioritaires

Observée depuis 2004, la participation des RSSI à des actions opérationnelles démontre la nécessité de ne pas être « déconnecté » à la fois de la mise en œuvre effective de la Politique, des préoccupations des métiers et, *in fine*, de la couverture réelle des risques identifiés et évalués.

En 2009, nous avions déjà mis en évidence un recentrage des priorités d'action. Effet de la crise sans doute, le panel indique clairement cette année encore, que si leur domaine s'est complexifié et devient plus stratégique, ils ne doivent pas oublier de s'impliquer au plan des « solutions » mais de manière toujours plus raisonnée et ciblée.



Le classement des priorités fait ressortir clairement 4 grandes familles d'actions.

- On retrouve en tête les trois sujets historiques (gestion des accès, plan de secours, confidentialité) qui touchent des problématiques « métier ». Mais seule la gestion des accès concerne une majorité de professionnels.
- Les trois actions suivantes (20 à 25% du panel environ) s'adressent à la protection des infrastructures dans une optique plus « informatique ».
- Les trois actions suivantes (20% su panel environ) s'adressent à la gestion d'évènements et d'incidents au sens large (cf. chapitre sur le SIM/SIEM).
- Enfin, les questions liées à la preuve, la signature et l'archivage demeurent marginales et ne progressent pas, de façon sans doute un peu surprenante (voir page suivante).

Les impacts de la dématérialisation et de la confiance numérique
Ce qu'en pensent les professionnels ?

Au-delà des considérations juridiques liées à la preuve et à la signature électronique (vues au chapitre précédent), nous avons plutôt abordé l'émergence de la confiance numérique à l'heure de la dématérialisation de pans entiers de notre société (commerce, santé, information, loisirs, jeux, etc.).

De l'avis de tous, le changement est réel mais les impacts pour la fonction SSI demeurent mesurés. Les questions de fond restent invariablement les mêmes :

- c'est d'abord au métier d'évoluer et la SSI doit apporter les solutions adaptées aux évaluations de risques
- la prise en compte de la sécurité dans les projets informatiques est globalement acquise mais c'est au niveau du processus de développement que se situent les vraies problématiques
- et *in fine*, c'est toujours le métier qui assume le risque !

A l'inverse, toute anomalie, incident, attaque, fraude est difficilement « dissimulable » et c'est alors que la Sécurité peut être mise en cause. Les dirigeants répugnant fondamentalement à être confrontés à ce type de problème, la fonction SSI se doit d'intervenir en amont dans un rôle d'arbitre et non de décideur sur les mesures à mettre en œuvre avec l'accord des responsables « métier ».

En synthèse, une des questions clés concerne l'évolution de la fonction SSI qui doit élargir son champ d'action aux processus dématérialisés, bien au-delà de la protection du SI de l'entreprise (au sens des outils de travail de ses employés).

Dans les grandes structures et pour certains secteurs (banque, assurance, industrie, médias, télécoms), c'est un acquis déjà ancien, mais pour beaucoup, ce sera peut-être la clé de la réussite à terme. Pour cela, il sera nécessaire, comme hier pour la Continuité d'activité ou l'IAM, d'être fortement en prise avec les problématiques « métiers », comprendre les opportunités et les enjeux, identifier et analyser des risques « business » (et non techniques) et proposer des solutions économiquement acceptables.

Lazaro PESJACHOWICZ
RSSI – CNAM TS

« Pour que le rôle d'un RSSI ne soit pas celui du Dr No, il doit impulser la mise en place des dispositifs qui seront nécessaires pour protéger les nouveaux services et applications qu'implique la stratégie de son entreprise, et ceci dès que celle-ci est annoncée. C'est la condition nécessaire pour pouvoir dire « Oui, mais avec cette protection ! » quand les demandes des métiers arriveront.

Le niveau d'implication du RSSI, dans la mise en place des dispositifs, sera différent selon qu'il se situe dans un service « risques », au sein d'une Maîtrise d'ouvrage ou de la DSI.
Mais il doit toujours être le moteur de cette anticipation. »

3.4.5. Synthèse

Loin de chercher à imaginer un avenir à la fonction SSI, ce bilan de la décennie 2001-2010 permet de dégager quelques convictions fortes. Elles sont de quatre natures. Tout d'abord, la fonction apparaît désormais **incontournable** et elle a gagné peu à peu, souvent dans la difficulté, ses lettres de noblesse. Les normes ISO 2700x au plan international ou le rapport du Député Pierre Lasbordes (« La Sécurité des Systèmes d'Information – Un enjeu majeur pour la France ») remis au premier Ministre en 2006, témoignent d'un intérêt stratégique du sujet.

Pierre LASBORDES
Député de l'Essonne

> ***« Les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises et du mode de vie des citoyens. Les services qu'ils assurent nous sont tout aussi indispensables que l'approvisionnement en eau ou en électricité. L'explosion mondiale d'Internet a considérablement modifié la donne et conféré aux systèmes d'information une dimension incontournable au développement même de l'économie et de la société. C'est dire si la sécurité des systèmes d'information (SSI) est un enjeu à l'échelle de la Nation toute entière. »***
>
> ***Livre blanc « La sécurité des SI, un enjeu majeur pour la France » - 2006***

Désormais bien identifiée voire reconnue, elle entre cependant dans des **zones de turbulence** qu'on ne saurait ignorer. La fonction semble notamment prise en étau entre les questions :

- de gouvernance des SI (« cloud computing » voire « entreprise sans DSI »),
- de conformité (« vie privée » et mise en place du CIL),
- de protection du patrimoine (« sécurité économique » et « sûreté de l'information »).

Plus que des conflits ou des luttes de pouvoir (cf. Livre bleu des Assises 2008 sur les « pouvoirs en sécurité du SI »), ce sont de véritables synergies et travaux communs qui doivent se mettre en place.

Force est aussi de reconnaître que la **professionnalisation** du domaine, en net progrès depuis 10 ans, reste sans doute insuffisante. Est-ce une certification « Lead implementor ISO27001 » ou CISSP qui fait un RSSI ou un architecte digne de ce nom ? A ce titre, des connaissances et compétences en finance et économie, en droit, en psychologie ou sociologie s'avèrent indispensables à terme mais certainement aussi dès aujourd'hui pour certains.

Enfin, si l'on se concentre sur le RSSI, qui incarne le plus souvent la fonction au quotidien, nous pouvons mettre en lumière **quelques qualités fondamentales** et indispensables pour réussir et que chacun pourra appréhender selon son profil, son parcours et son environnement :

- Accepter de faire **un choix clair sur son « métier »** : être un Pilote, un Architecte ou un Contrôleur / Surveillant
- Savoir se faire accepter et travailler en réseau : **avoir l'esprit d'équipe ... sans équipe**
- Sortir de l'image « Docteur No » : **incarner le « pouvoir de dire Oui... »**
- Se positionner comme un « arbitre », un « médiateur » : être **force de propositions et de solutions à l'attention des métiers**
- Améliorer ses pratiques de communication : ne pas hésiter à **sensibiliser par le jeu** et à **manier l'humour !**

Rien ne nous permet d'imaginer un avenir pour la fonction SSI à 3, 5, 7 voire 10 ans. La mise en valeur des acquis, la capitalisation des ressources disponibles, le bon sens au quotidien, l'amélioration des pratiques existantes peuvent servir de viatique fort utile et approprié en période de pénurie et d'incertitude extrêmes.

4- CONSIDÉRATIONS ÉCONOMIQUES SUR LA SÉCURITÉ DES SI

4.1. Introduction

Ce chapitre aborde spécifiquement la dimension économique de la Sécurité des SI, à la lumière de l'analyse des résultats de l'enquête annuelle du Cercle Européen de la Sécurité.

A la différence des travaux publiés par l'Université de Cambridge et de ceux de l'ENISA mentionnés au début du document, lesquels possèdent une approche très « marché », notre démarche s'appuie sur 3 principes :

Principe N°1 : Construire la réflexion sur la base des réponses à 26 questions proposées à un panel de 250 professionnels de la Sécurité des SI (cf. annexe).

Principe N°2 : Couvrir 4 axes d'analyse centrés sur le monde de l'entreprise.
- Menaces, risques, incidents, attaques et impacts économiques
- Dépenses « Sécurité SI » et approche budgétaire
- Sanctions pénales et facteur dissuasif
- Cybercriminalité et moyens de lutte

Principe N°3 : Soulever, en synthèse, des questions en vue de travaux plus approfondis plutôt que de proposer des recommandations détaillées.

Concernant ce dernier point, un Groupe de travail du Cercle a été mis en place en juin 2010 afin d'organiser une réflexion sur le sujet dans la durée. Ses travaux exploiteront utilement les apports du Livre Bleu 2010, notamment au cours d'une 2nde réunion de travail prévue en novembre 2010. Les membres du Groupe de travail sont des RSSI de tous secteurs d'activité, des représentants des services de l'Etat (ANSSI, OCLCTIC, Gendarmerie Nationale) et des experts reconnus. La conclusion du Livre Bleu reviendra sur ce point.

A la différence des éditions précédentes du Livre Bleu des Assises, nous ne publions pas systématiquement, pour chaque question, une analyse spécifique selon le secteur d'activité ou la taille des entreprises, ni en fonction du champ d'implication géographique des répondants (France, Europe, Monde). Cependant, un document détaillé est disponible en ligne sur le site du Cercle avec des résultats souvent instructifs (www.lecercle.biz). Il permet aux participants de se situer ou de comparer leurs réponses.

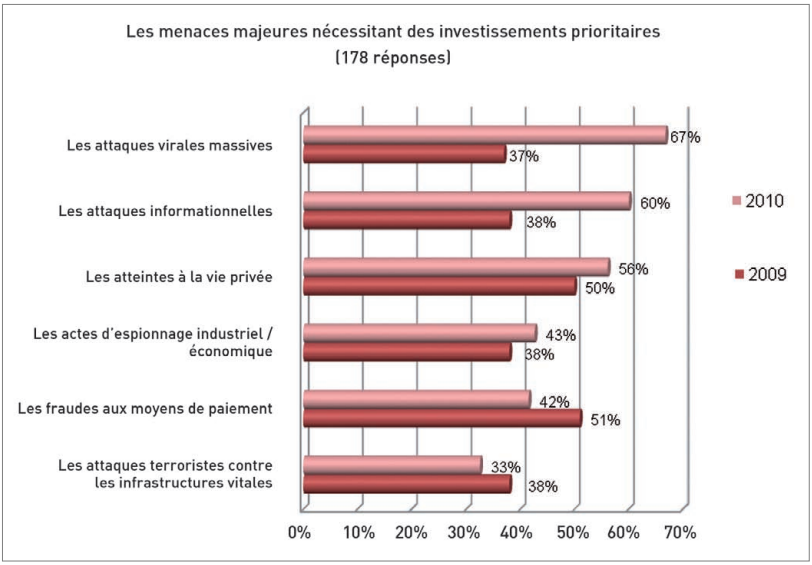
4.2. Impacts économiques des incidents

La question sans doute la plus attractive mais aussi la plus compliquée à aborder concerne les impacts économiques des incidents et attaques touchant les systèmes d'information comme les informations elles-mêmes.

Ne subir aucun incident, aucune attaque peut apparaître anormal ou dangereux, pour deux raisons diamétralement opposées : aveugle ou surprotégé ? Dans les deux cas, les équipes SSI font mal leur travail que ce soit en termes de prévention / protection ou de détection / réaction.

4.2.1. Quelle perception des menaces majeures ?

A la question des menaces majeures les plus « redoutées », le panel 2010 se distingue fortement par rapport à l'an dernier comme l'atteste le schéma ci-dessous.



Un retour très marqué aux attaques virales et informationnelles s'est opéré, suivi de près par les atteintes à la vie privée et l'espionnage économique / industriel. Certainement du fait de la conjonction de plusieurs facteurs :

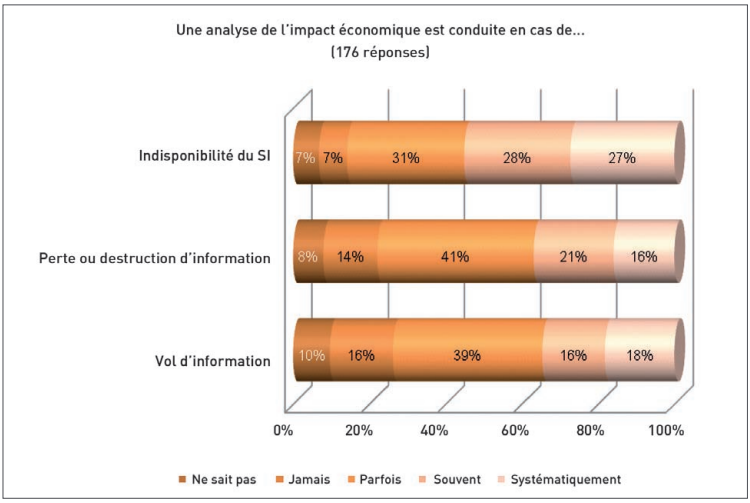
- Une explosion des failles applicatives et du nombre de malwares détectés quotidiennement,
- conjuguée à certaines limites mises en évidence au niveau des logiciels anti-malware,
- en relation avec de nouvelles pratiques désormais répandues (Web 2.0, mobilité, supports amovibles, PDA, etc.).

Le sentiment de vulnérabilité et d'insécurité des professionnels s'est donc accru. Pensent-ils ne pas ou ne plus être en mesure, aujourd'hui ou à terme, de répondre à la menace ?

> ***Au-delà des menaces et vulnérabilités perçues par le panel, et de leur capacité à garantir la protection efficace du SI, la question majeure est : Quels sont les incidents et attaques réellement subis et avec quels impacts économiques ?***
> ***Les mesure-t-on réellement ? A quelles fins ?***

4.2.2. Quelle analyse d'impact économique ?

En fonction de l'incident subi, les répondants n'ont pas la même approche selon que ce sont les infrastructures ou les informations qui sont impactées. Nous avons ici volontairement restreint le champ à des questions simples de Disponibilité et Confidentialité, certainement les plus perceptibles, mettant de côté l'Intégrité (actions de fraude par exemple).



Une majorité de répondants (55%) fait l'effort (systématiquement ou souvent) de l'analyse d'impact économique uniquement lorsque la disponibilité du SI est en cause. A l'opposé, peu de répondants ne savent pas ou ne font jamais cet effort sur ce point. Il va de soi que ce type d'incident est par principe « visible » et impacte immédiatement les utilisateurs. Une perte d'exploitation ou de chiffre d'affaire sera mesurable, ne serait-ce que pour des raisons de déclaration à l'assurance.

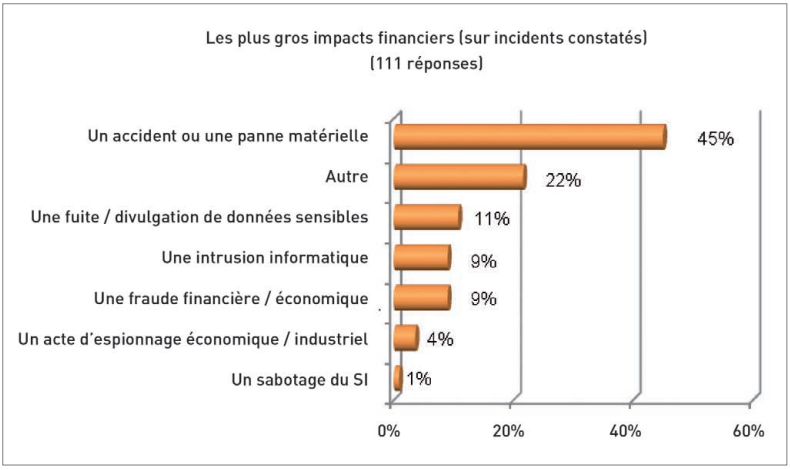
En ce qui concerne les atteintes aux informations, on constate une baisse des pratiques à la fois pour les « pertes / destructions » et les « vols ». Mais celle-ci reste modérée puisque les réponses « parfois » sont assez significatives (41% du panel). Ce résultat est nécessairement lié à la nature de l'information concernée dont la perte ou le vol peut être plus au moins préjudiciable à l'entreprise. Auquel cas, une déclaration à l'assurance sera opportune, voire le cas échéant, un dépôt de plainte en bonne et due forme (généralement dès lors que l'acte est malveillant et qu'aucune négligence n'aura été mise en évidence).

Plus spécifiquement pour le vol d'information, le fait que 73% du panel affirment effectuer une telle analyse (parfois, souvent ou systématiquement), démontre l'importance accordée au contenu par rapport au SI proprement dit (86% du panel). L'écart n'est finalement pas très significatif.

> ***L'analyse des impacts économiques n'est pas encore très répandue mais n'est pas négligée.***
> ***Ceux qui ne mènent jamais ce type de démarche sont soit conscients de son inutilité dans leur contexte ou de la faiblesse de l'impact, soit ne sont pas informés voire impliqués dans le processus.***

4.2.3. Quels impacts économiques des incidents ?

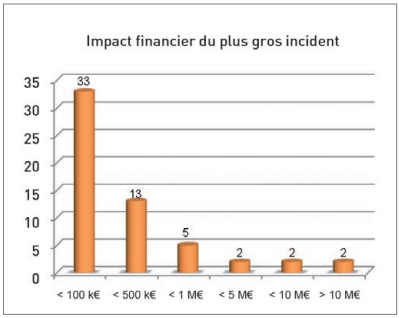
La question portait ici sur l'incident ayant eu le plus gros impact économique au cours des 2 dernières années. Sans surprise les accidents et pannes sont les plus graves d'un point de vue économique dès lors que l'activité est immédiatement impactée (45% des incidents les plus graves constatés par les répondants).



Malgré une typologie assez large d'incidents, une catégorie « autre » apparaît en 2ème position avec 22% des incidents constatés. On peut imaginer y retrouver des atteintes à la propriété intellectuelle, des actes de chantage, il est vrai, non mentionnés explicitement.

Autre enseignement intéressant de ces statistiques, le poids de la malveillance toutes finalités confondues concerne 34% des répondants concernés.

Mais on notera aussi un taux de 19% de répondants qui déclarent ne pas subir d'incident et 17% qui ne le savent pas. Sont-ce les « aveugles » mentionnés plus haut ? Ou tout simplement, ceux qui sont à la fois bien protégés et peu ou pas visés ?



Les impacts économiques supérieurs à 1M€ concernent 6 répondants de tous secteurs d'activité, tandis que les causes des attaques sont plus variées qu'on aurait pu le penser. On recense ainsi 2 accidents, une intrusion informatique, une fraude, une fuite d'information et un « autre » non précisé.

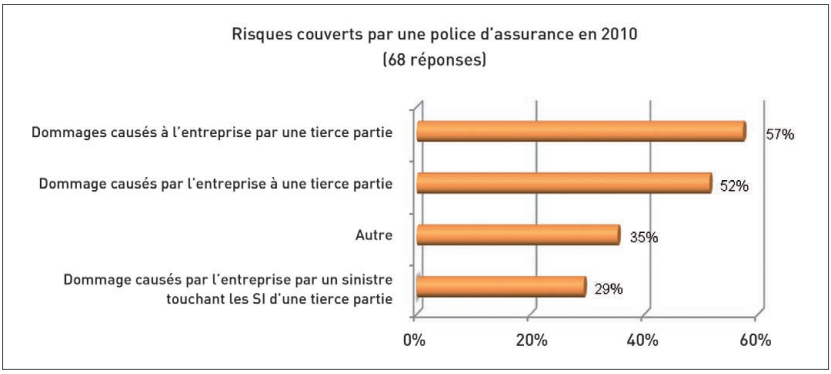
Les attaques et incidents impliquant les Systèmes d'Information sont extrêmement variés et ne sont pas toujours liés au champ d'action de la Sécurité du SI. En effet, le SI est soit la cible soit le moyen de l'attaque (par exemple, une intrusion peut précéder une fraude ou un vol). Dans ces situations, seule une gouvernance efficace impliquant la sécurité des biens et des personnes, la sécurité du SI, la gestion de la fraude, la gestion des risques et l'assurance peut garantir une analyse pertinente des impacts.

4.2.4. Quel rôle de l'assurance ?

Pilier essentiel de la gestion des risques, l'assurance devait être abordée dans l'enquête. Ainsi, nous avons posé une question fermée sur la nature des dommages subis ou causés par l'entreprise en relation avec des incidents liés au SI.

Selon un principe fondamental, l'assurance ne couvre que des risques aléatoires (non sûrs) sous réserve que les mesures de prévention / protection adéquates auront été préalablement prévues et mises en place pour réduire leur potentialité et leurs impacts.

On constate que la démarche reste très partielle, voire encore éloignée des préoccupations des professionnels. Nous prendrons les résultats à cette question avec quelques précautions car 63% du panel ne savent pas quels risques sont couverts par une police d'assurance.



Seulement un tiers du panel s'intéresse à la question de l'Assurance des risques SI. On peut considérer que c'est peu. Mais plus vraisemblablement, en dehors de la couverture des pertes d'exploitation et des frais de retour à la normale en cas de sinistre matériel ou immatériel accidentel, la question de l'Assurance ne s'adresse globalement pas ou peu aux RSSI.

Cependant, regardons le verre à ¾ plein plutôt que vide et apprécions qu'un professionnel sur cinq intègre les dommages causés à l'entreprise par une tierce partie ou à l'inverse par l'entreprise à une tierce partie.

On constate également des différences notables entre secteurs d'activité. La Banque-Assurance se situe dans la moyenne, l'Industrie plutôt plus avancée et l'Administration/Service public – sans surprise – nettement en retrait dans la mesure où ils sont généralement leur propre assureur, couverts par l'État. (cf. analyse détaillée sur le site du Cercle).

> ***La question de l'assurance doit peut-être revenir au premier rang des préoccupations et servir de révélateur, à la fois à ceux qui s'assurent pour se « rassurer » et à ceux qui ne le font pas au regard des mesures de prévention excessives et des polices dissuasives.***

4.3. Dépenses et approches budgétaires

L'axe « dépenses et budgets SSI » n'est pas le plus simple à aborder, mais *in fine*, tout RSSI ne devrait-il pas, *a minima*, savoir quels sont les efforts économiques consentis au titre de la Sécurité du SI ?

La réponse semble évidente mais donner des chiffres (fiables et utiles) se heurte à des écueils majeurs touchant à :

- Ce que l'on entend par budget « SSI »
  - Investissement
  - Fonctionnement
  - Les deux
- Ce que couvrent les dépenses
  - Confidentialité
  - Secours et continuité
  - Gestion des accès
  - Gestion des attaques logiques
  - Gestion des incidents
  - Etc.
- Ce que l'on intègre dans les dépenses
  - Outils (matériel, logiciel)
  - Personnels (interne, externe)
  - Prestations
  - Formation, sensibilisation
  - Services intégrés et externalisés
- Qui engage réellement la dépense
  - DSI (production, études, architecture, etc.)
  - RSSI
  - Métiers
  - Autre

Cet aspect de la question économique de la sécurité du SI est beaucoup moins anodin qu'il n'y paraît car il est en étroite relation avec la structure, la maturité et l'évolution du marché (offre et demande) :

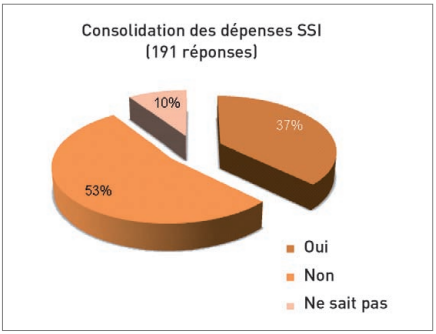
- Pratiques budgétaires des entreprises
  - Réduction des investissements ?
  - Au profit de charges de fonctionnement ?
  - Souplesse et agilité des commandes de services (par trimestre par exemple)
  - Pouvoir des « achats » et distorsion de concurrence (pratique de référencement)
- Modèles économiques de l'offre
  - Progression des services vs outils
  - Gratuité de certaines technologies
  - Développement du SaaS
- Gouvernance des SI et de la SSI
  - Externalisation (cloud computing, off shore)
  - Intégration de la sécurité à des offres globales (avec coût non dissociable)

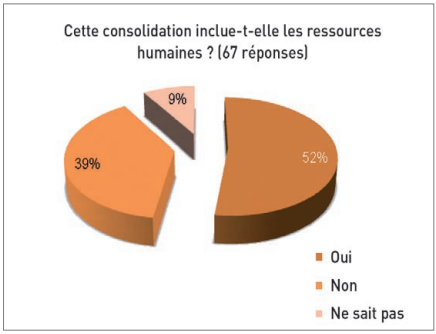
Nous avons posé au panel quelques questions sur ce point dont les résultats sont présentés aux pages suivantes. Ici aussi, une analyse sectorielle ou selon la taille d'entreprise est disponible sur le site du Cercle : www.lecercle.biz.

4.3.1. Consolider les dépenses SSI ?

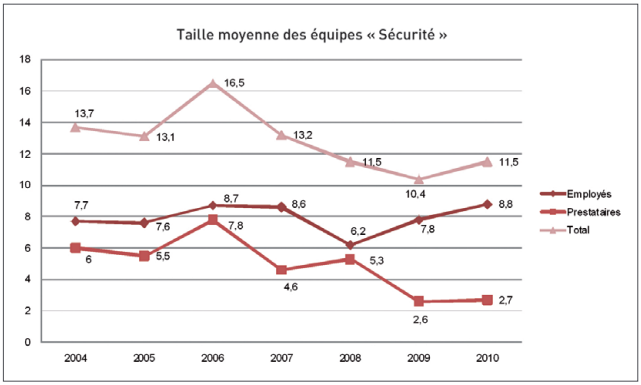
Un budget « SSI » peut être appréhendé au sens de la consolidation des dépenses, pas uniquement en termes de globalisation et de gestion centralisée au niveau d'une DSI ou du RSSI. Ainsi, on constate que seulement 37% des répondants affirment effectuer cette consolidation.

Nous n'avons pas sollicité le panel sur le contenu de cette consolidation car comme nous l'avons indiqué plus haut, elle peut être très variable selon plusieurs hypothèses touchant à la nature (investissement / fonctionnement), la vocation (continuité, confidentialité, etc.) et les types des dépenses (outils, services, personnels, etc.). Sur ce dernier point, on constate que plus de la moitié des professionnels qui disposent d'une consolidation des dépenses SSI y intègrent les ressources humaines.





Depuis 2004, nous avons tenté de définir certains indicateurs quantitatifs sur les ressources humaines, comme la répartition entre les équipes internes et externes. Globalement, on tend à un équilibre moyen de 8 « internes » et 3 « externes » sachant que ne sont pas intégrés les acteurs les plus opérationnels (administrateurs notamment). Au-delà de l'aspect quantitatif (évaluation du secteur à sans doute plus de 10 000 professionnels, fourchettes de salaire présentées en annexe), nous devons sans doute chercher à déterminer des indicateurs qualitatifs, basés sur les formations, l'expérience et les certifications.



Ainsi, l'utilité pratique des consolidations budgétaires mériterait d'être appréciée :

- Pour corréler les dépenses réelles avec les risques évalués et aussi les incidents
- Pour bien cibler les augmentations et réductions annuelles ou semestrielles
- Pour mettre en concurrence des acteurs en cas de surcoût important
- Pour se comparer (au sein d'un secteur d'activité ou d'un Groupe)

Quel est l'impact de la taille de l'entreprise ou de son secteur d'activité ? L'analyse détaillée des réponses apporte un éclairage intéressant.

- La consolidation est plus répandue dans le secteur industriel.
- Une proportion supérieure de « ne sait pas » apparaît dans la banque-assurance (15%).
- La taille de l'entreprise n'impacte pas ces pratiques (statistiques uniformes à l'exception d'une part importante de « non » (63%) pour un nombre de collaborateurs compris entre 50 000 et 100 000).

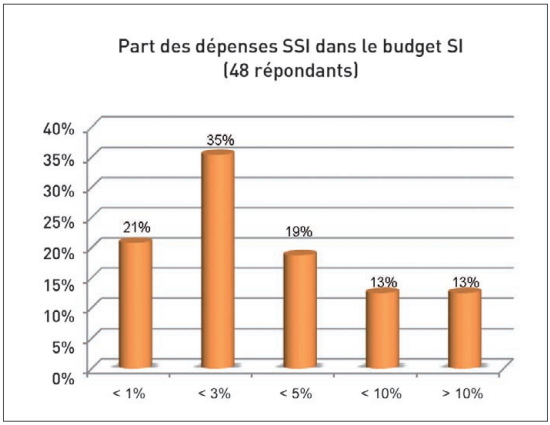
> ***La consolidation des dépenses SSI est un processus encore partiel mais devrait tendre à se développer et nécessitera d'en définir le cadre aussi précisément que possible. Et dans ce cadre, les ressources humaines devront apparaître, autant au plan qualitatif que quantitatif.***

4.3.2. Quelle part du budget SI ?

Cette question, assez classique et régulièrement intégrée à toute enquête auprès des professionnels de la sécurité, a été posée au panel.

Le plus important, en relation avec la question précédente, est que près de la moitié des répondants ne sait pas y répondre. En effet, tant que l'on ne définit pas ce que l'on entend par dépense et qu'on n'effectue aucune consolidation, il est illusoire de rapporter le résultat au budget « SI ». Sachant que ce dernier peut aussi être variable dans le temps (dans l'année même) et qu'il faut s'entendre si on le considère en termes de fonctionnement et/ou d'investissement.

Enfin, on remarquera que parmi ceux qui consolident les dépenses SSI, 28 % ne savent pas dire quelle est la part du budget SSI dans le budget SI.



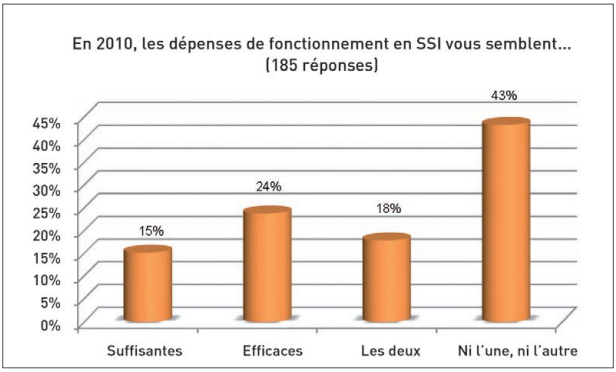
Au final, nous pouvons affirmer que ce type d'indicateur n'a pas beaucoup de sens, pour ne pas dire aucun, et que la question de « ratios » différents mérite d'être posée. Ils devront être plus pertinents et surtout utiles pour :

- Permettre des comparatifs (selon les profils ou la taille d'entreprise)
- Gérer des évolutions (hausse ou baisse),
- Être corrélés avec les incidents réels et les impacts mesurés.

> ***Plus qu'un pourcentage des dépenses SSI rapportées au budget de la DSI, ne devrait-on pas élaborer des indicateurs sous forme de ratios : « par utilisateur » (fixe, nomade) ou rapportés au budget d'un projet (selon des niveaux de criticité).***
> ***Le pré-requis reste ici aussi d'en définir le champ aussi précisément que possible.***

4.3.3. Quelle utilité et pertinence des dépenses de fonctionnement ?

Quelle surprise ! Au-delà des questions quantitatives aperçues ci-dessus et que nous approfondirons ensuite, nous avons posé une question de nature qualitative assez directe et pour tout dire, les réponses apportées sont porteuses d'enseignements intéressants.



On peut sans doute se poser la question du côté « provocateur » de certains répondants visant à se montrer quelque peu insatisfaits de l'ampleur des moyens mis à leur disposition (67% du panel) et de manière corollaire de leur efficacité (58%). Une certaine façon de se dédouaner de tout incident ou risque non ou mal couvert ?

Ainsi, si la question du montant des dépenses reste importante, c'est tout autant leur nature et leur pertinence qui posent problème. La France apparaît généralement quantitativement en retrait en termes de marché SSI par rapport aux pays anglo-saxons notamment. Mais inversement, n'y aurait-il pas une forme de « sagesse française » à ne pas (trop) dépenser sous la pression d'un « marketing de la peur », poussant des technologies américaines avant tout ?

Sur l'efficacité des moyens, nous modulerons la sévérité apparente de ces réponses au regard de la multitude d'outils d'une part (certains ont fait leur preuve) comme de la variété et de l'évolutivité des menaces. Comme l'a démontré le bilan de la décennie, les limites de certaines technologies sont avérées, la difficulté de gérer certaines menaces est grandissante et les efforts à mener au plan de la sensibilisation / formation restent un enjeu majeur. Ainsi, une certaine clairvoyance conduit le panel à considérer l'efficacité des dépenses engagées avec modération.

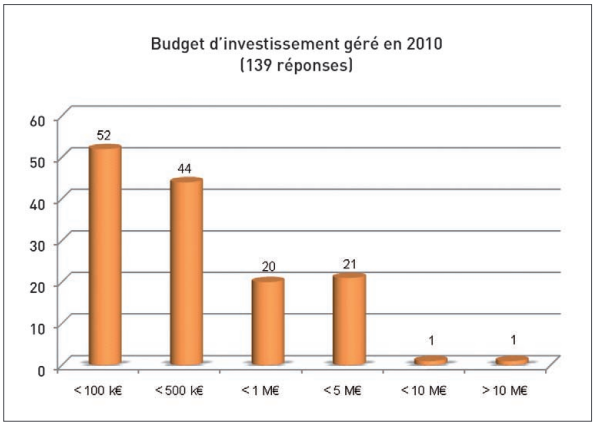
Une analyse des réponses par secteur d'activité apporte un éclairage légèrement différent. En effet :

- La banque-assurance estime les moyens relativement aussi peu suffisants (34%) qu'efficaces (36%).
- L'industrie estime ses moyens relativement plus efficaces (42%) que suffisants (31%).
- L'administration-services publics apparaît la plus satisfaite avec un taux de 28% pour « efficaces et suffisantes » et 32% pour « ni l'une, ni l'autre ».

> ***Les professionnels considèrent globalement que les moyens engagés dans la Sécurité des SI ne sont pas suffisants et, plus important, qu'ils sont généralement aujourd'hui plutôt inefficaces. Ce constat nécessite de mener une réflexion approfondie sur les moyens concernés et les actions correctrices adaptées en relation avec le marché.***

4.3.4. Quels budgets d'investissement en 2010 ?

Revenons aux questions quantitatives en abordant justement l'ampleur des budgets d'investissement gérés par les participants à l'enquête. L'échelle de réponse est évidemment très large au regard de la structure du panel. Ici encore, nous n'apprécierons pas la nature de ces budgets qui sont par principe conjoncturels, et liés à chaque contexte spécifique des répondants.



Globalement, on constate qu'environ la moitié des répondants dispose d'un budget d'investissement inférieur à 500 k€. Et parmi ces répondants, certains appartiennent à des entreprises de taille importante et de secteur d'activité sensible. Le RSSI « sans budget » est une réalité dans tous les secteurs et dans toutes les tailles d'entreprises.

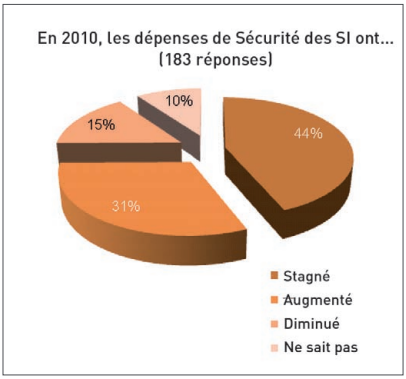
A l'opposé, seulement deux professionnels affirment gérer des budgets très importants, l'un compris entre 5 et 10 M€, le second, supérieur à 10 M€.

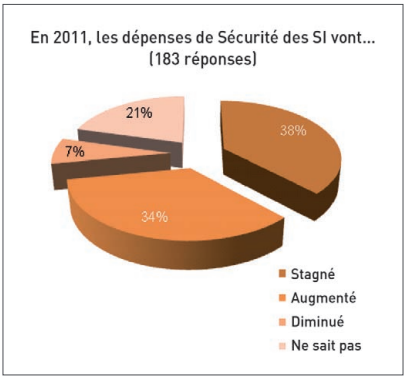
Enfin, dans la tranche médiane, deux groupes équivalents d'une vingtaine de professionnels disposent de budgets d'investissement compris entre 0,5 et 1 M€ ou entre 1 et 5 M€. Les secteurs de l'Industrie et « autres » se situent plus largement dans la fourchette « inférieure à 1M€ ».

> ***En conservant toujours à l'esprit que le champ des dépenses peut être très variable d'une entreprise à l'autre, l'influence du secteur d'activité n'est pas importante tandis que la taille de l'entreprise est plus significative.***
> ***Il ne suffit pas d'être dans une grande structure pour disposer d'un gros budget !***

4.3.5. Quelle progression des dépenses ?

Plaçons-nous dans une vision plus dynamique, sur la période 2010-2011. Sans surprise, la proportion de professionnels sans visibilité sur 2010 s'inscrit à 10% (les plus opérationnels du panel), mais elle progresse à 21% pour 2011 (faute de décision sans doute au moment de l'enquête au printemps 2010).





Sans certitude sur la perspective 2011, la tendance à l'augmentation reste sensiblement la même autour de 34% du panel, ce qui est non négligeable, en période de crise et de tension sur les dépenses informatiques. Il est vrai que les budgets SSI sont généralement épargnés puisque seulement 15% du panel en 2010 et 7% en 2011, ont subi ou entrevoient une baisse.

Nous proposons aussi une analyse corrélée entre les 2 questions afin de déceler des singularités. Elles sont présentées dans le tableau ci-dessous avec un zoom sur quelques secteurs d'activités. Chacun peut ainsi se positionner en fonction de ses propres réponses.

2010	2011			
	Vont diminuer	Vont stagner	Vont augmenter	Ne sait pas
A diminué	7	10	4	7
A stagné	6	42	24	8
A augmenté	0	14	34	9
Ne sait pas	0	3	1	14

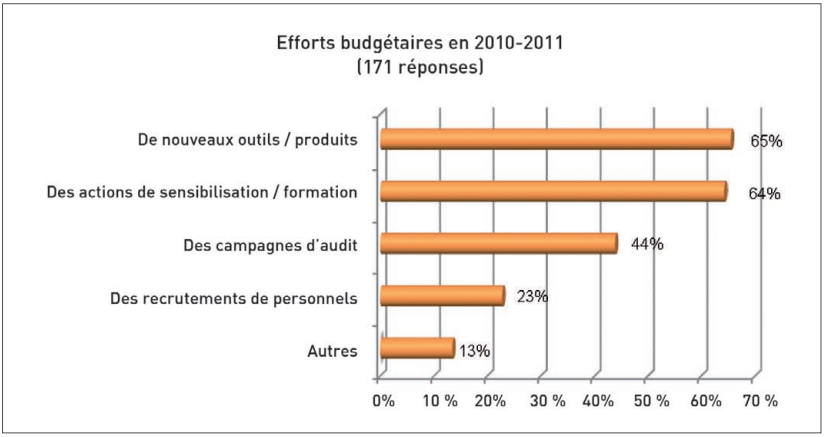
	2010				2011			
	↘	→	↗	?	↘	→	↗	?
Banque/Assurance/ Finance	15 %	48 %	23 %	15 %	10 %	48 %	25 %	17 %
Ministères & Administrations	17 %	42 %	29 %	13 %	8 %	29 %	38 %	25 %
Industrie	24 %	34 %	34 %	7 %	7 %	41 %	24 %	28 %
Services publics (hors santé)	0 %	62 %	33 %	5 %	0 %	52 %	24 %	24 %
Santé	6 %	47 %	41 %	6 %	0 %	24 %	65 %	12 %
Autre	20 %	36 %	34 %	9 %	10 %	27 %	43 %	20 %

> *Même si une certaine incertitude règne au moment où l'enquête a été réalisée, la tendance semble plutôt favorable, notamment dans le secteur de la santé, où il est vrai que les enjeux sont importants et les projets significatifs.*

4.3.6. Quels types de dépenses prioritaires en 2010-2011 ?

Que les dépenses soient en baisse ou en hausse, voire qu'elles n'évoluent pas, il convient encore de les utiliser à bon escient. Nous avons proposé au panel de se positionner sur 4 types d'actions :

- Deux de nature « moyen » : outils et ressources humaines (personnels)
- Deux de nature « processus » : sensibilisation / formation et audit



Pour deux tiers du panel, les produits / outils et la sensibilisation / formation font partie des priorités d'action, confirmant pour la sensibilisation les résultats présentés au chapitre 2.4.3 (55%). Ce résultat est bien sûr satisfaisant et démontre la prise de conscience généralisée de l'insuffisance de la technologie seule, mais aussi de l'importance du facteur humain dans le cadre d'une Politique de Sécurité et d'une Charte qui doivent être connues, comprises et respectées. Et pour 66% du panel, les efforts engagés en termes de sensibilisation / formation en 2010 sont encore jugés insuffisants.

Concernant les campagnes d'audit, on retrouve également un résultat conforme à celui du chapitre 2.4.3 (46%). Cependant, les pratiques évoluent fortement dans le cadre de la mise en œuvre des SMSI ISO27001. Le recours à des professionnels certifiés « Lead Auditor » s'est généralisé, posant la question de la qualité réelle de l'auditeur, dès lors que tous sont certifiés...

D'un autre côté, les tests intrusifs méritent aussi une attention particulière notamment en matière de concurrence forte et de réduction des coûts pouvant impacter la qualité des résultats (voir chapitre 4.3.8).

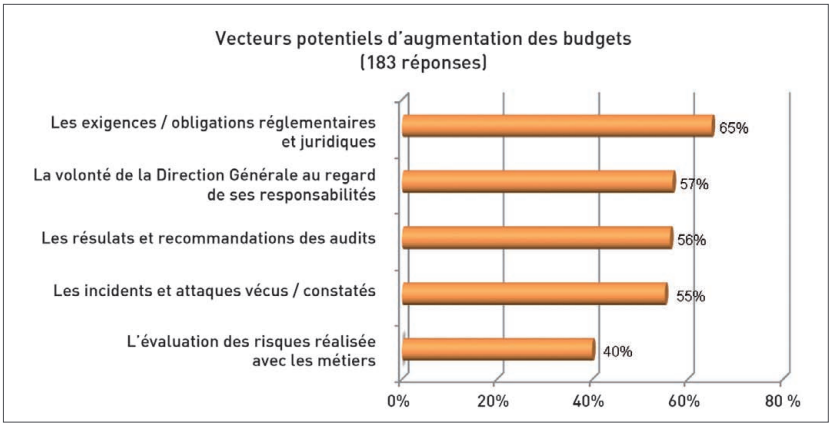
Enfin, le recrutement de personnel bien qu'arrivant en 4ème position avec 23% des répondants, n'est pas négligé. Les secteurs les moins actifs dans ce domaine sont et seront les services publics (hors Santé).

	Outils	Sensibilisation	Audits	Recrutements	Autres
Banque/Assurance/ Finance	46 %	50 %	39 %	22 %	17 %
Ministères & Administrations	67 %	67 %	25 %	25 %	8 %
Industrie	66 %	66 %	45 %	21 %	17 %
Services publics (hors santé)	71 %	67 %	48 %	5 %	19 %
Santé	71 %	65 %	47 %	24 %	6 %
Autre	66 %	61 %	45 %	27 %	7 %

Les efforts engagés en termes de produits resteront soutenus, d'une part, parce que la profusion technologique actuelle n'a pas répondu aux attentes, et, d'autre part, parce que de nouvelles mesures de prévention / protection doivent encore se déployer (IAM, DLP, SIEM).
Concernant la sensibilisation, les approches doivent s'améliorer régulièrement au regard de l'évolution des technologies (web 2.0, mobilité) et des comportements associés qui sont notamment liés à la Net génération.

4.3.7. Quels vecteurs d'augmentation des budgets ?

Qu'ils augmentent aujourd'hui ou demain, qu'ils soient consacrés à du personnel ou à des outils, la question est de savoir quel est le mécanisme qui pousse une entreprise à dépenser plus pour la Sécurité de son SI. Le schéma ci-dessous exprime la position du panel de l'enquête 2010.



Aucune réponse ne ressort véritablement et de manière un peu surprenante, la prise en compte des risques « métiers » reste en retrait avec 40% de réponses.

Michel GERARD
PDG Hapsis

> *« La justification économique des programmes « Sécurité SI » réside dans le lien que l'on peut établir entre les actions menées et les opportunités business qu'elles facilitent.*
>
> *Notre rôle, en tant que professionnel de la Sécurité du SI, est de permettre d'établir ce lien. »*

Alors que nous avons initié ce chapitre en mettant volontairement l'accent sur la réalité des incidents subis pour les mettre ensuite en relation avec la nature et l'ampleur des mesures mises en œuvre, c'est l'approche réglementaire et juridique qui représente le meilleur bras de levier pour les actions et les budgets de sécurité.

Certains RSSI savent que les lois Informatique et Libertés, Sarbanes et Oxley, ou le décret « confidentialité » dans la Santé, ont été les meilleurs alliés de leurs plans d'action ! Aujourd'hui, la preuve, la signature et l'archivage électroniques prennent le relais, notamment via les démarches de dématérialisation des processus « métier » intégrant IAM, gestion d'incidents (SIM / SIEM), traçabilité et conservation de données.

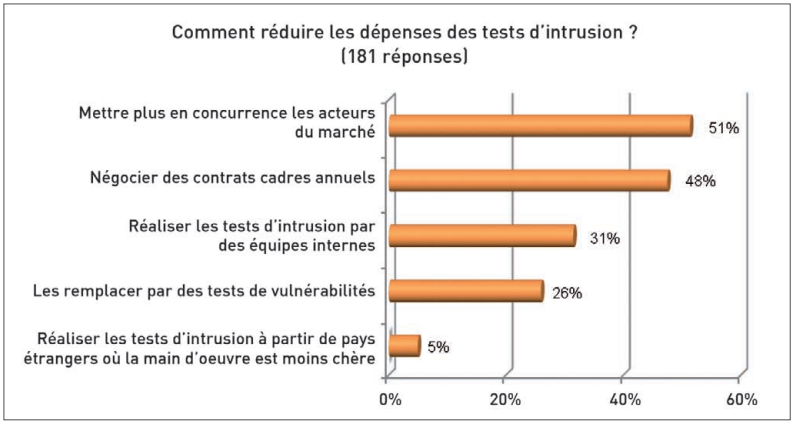
La relation entre la Sécurité SI et les métiers demeure encore distante et ne permet pas de mettre en œuvre des actions / mesures s'appuyant sur une évaluation de risques raisonnée et des arbitrages économiques adaptés.

> ***Les budgets Sécurité SI évoluent plus sous la pression réglementaire que par l'appréhension des risques pour et par les métiers. Ceci démontre une maturité encore insuffisante de la SSI au regard de la « gestion des risques ».***
> ***Le poids du contrôle et de l'audit comme de la réalité des incidents est aussi significatif et ne doit pas être négligé en mettant en place, au préalable, la gouvernance et les processus adéquats.***

4.3.8. Comment réduire les dépenses ? Le cas des tests intrusifs

Dès lors que la question de la réduction des dépenses se pose, le plus simple consiste souvent à supprimer des prestations et de l'assistance technique. Solution rapide et aux effets immédiats !

Cependant, nous avons sollicité le panel sur un type de prestation, ancienne et toujours incontournable aujourd'hui, où la concurrence est forte et les moyens d'actions variés.



Les réponses apportées par le panel ne sont pas vraiment tranchées. C'est au niveau des procédures d'appel d'offre et de négociation de contrats-cadres que se situent apparemment les bras de levier. Des questions clés sont sous-tendues ici :

- Paie-t-on aujourd'hui la meilleure prestation au meilleur prix ?
- Des rentes ne se sont-elles pas mises en place avec quelques acteurs ? Parfois juge et parti ?
- Le critère d'indépendance est-il garanti ?
- La qualité de l'intervenant est-elle dûment contrôlée ?
- Quel est le poids du RSSI devant les Achats lors de la décision ?

Deux alternatives se présentent également en faisant évoluer les processus. Le recours à des équipes internes permettrait pour 31% du panel, de faire des économies alors que se contenter de « tests de vulnérabilités » (qui peuvent être automatisés) suffirait pour 26% des répondants.

Pour une toute petite minorité du panel, faire réaliser ces prestations par des acteurs étrangers à la main d'œuvre moins chère, apparaît comme une solution envisageable, ou déjà mise en œuvre.

> ***Une approche plus qualitative est aussi importante qu'une simple quête de réduction de coût. Au travers de cet exemple, l'adage « faire plus avec autant voire moins » peut être appliqué sans difficulté.***

4.3.9. Vers une sécurité réellement intégrée

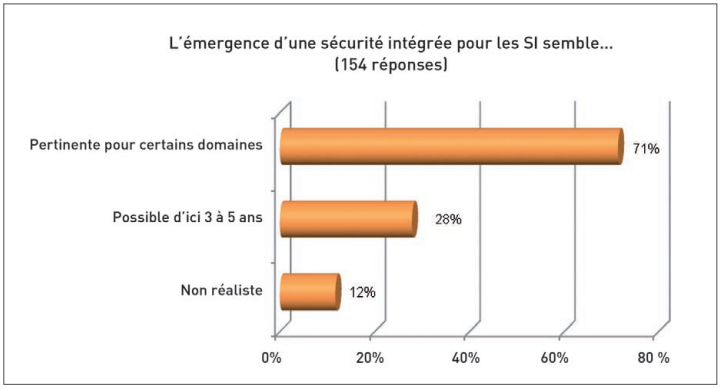
Faisons une analogie avec la sécurité routière. Lors de l'achat d'un véhicule, le propriétaire :

- achète un ensemble de technologies qui participent à sa sécurité (ceinture, ABS, EPS, airbag, ...)
- peut souscrire à un service d'assistance en cas de défaillance, de panne, ...

Lorsque le conducteur emprunte une autoroute, il accepte que des voies d'urgence et d'accès de secours soient prévues pour assister les clients en difficulté.

Lorsque le même conducteur passe au péage, il peut apercevoir les forces de l'ordre (gendarmerie, douane) effectuer des contrôles, fouiller des véhicules, etc.

Analogie simpliste ou tendance de fond ?



Les professionnels du panel expriment sur ce point un avis positif et prometteur mais qui mériterait d'intéressants approfondissements. A l'heure où des acteurs récents de la sphère Internet semblent résister aux attentes et exigences des États et des consommateurs, le rachat de Mac Afee par Intel en août 2010, n'illustre-t-il pas cette tendance de fond ?

> ***Peut-on imaginer, à terme, que l'achat d'un système informatique (personnel comme professionnel), puisse intégrer, en toute connaissance, l'ensemble des mesures de prévention, protection, détection, réaction, protégeant le « pilote » navigant sur les réseaux planétaires ?***

4.4. Approche pénaliste : des sanctions dissuasives ?

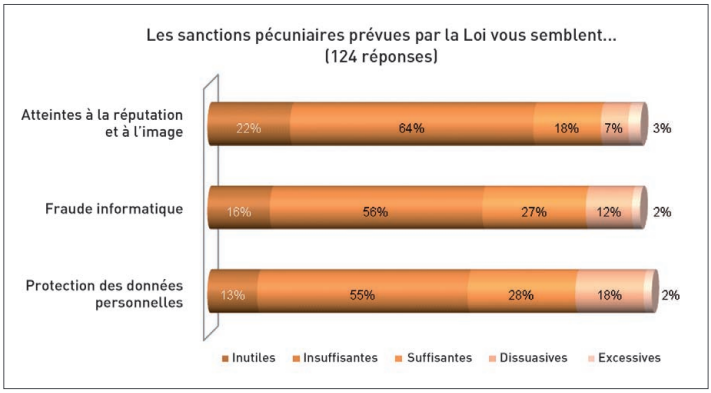
Les textes « sécuritaires » se sont développés depuis plus de 10 ans et touchent également le cadre de la Sécurité du SI au titre de la lutte contre la cybercriminalité. Face au faible nombre de condamnations et aux sanctions peu élevées constatées, il s'avère intéressant de juger du caractère dissuasif des peines encourues au plan économique sur trois paramètres :

- La fraude informatique qui sanctionne globalement les sabotages et les intrusions ainsi que les manipulations frauduleuses de données.
- La protection des données personnelles qui sanctionne en particulier les défauts de sécurité, les divulgations volontaires et involontaires.
- Les atteintes à la réputation et à l'image que l'on peut désormais constater au quotidien sur les réseaux sociaux.

Les résultats présentés sur le schéma ci-dessous (somme supérieure à 100% : plusieurs réponses possibles) démontrent des différences pour les trois sujets. Mais globalement, les sanctions proposées sont insuffisantes pour être réellement dissuasives.

A titre d'exemple, un juge américain a condamné Albert Gonzales à 70 ans de prison pour avoir détourné plusieurs dizaines de milliers de données personnelles de clients d'une banque. A l'opposé, la stagiaire chinoise d'un équipementier automobile a été condamnée au titre de l'intrusion informatique à 2 mois de prison effectués en préventive.

En Angleterre, la compagnie d'assurance Zurich UK a été condamnée à 2,8 M€ pour la perte d'un fichier « clients » lors de son transport vers un site de stockage. En France, les amendes prononcées par la CNIL se montent au maximum à quelques dizaines de milliers d'euros.



> ***Le caractère dissuasif des sanctions pénales ne semble pas établi tandis que les professionnels considèrent que si elles peuvent être excessives voire inutiles, la majorité imagine qu'elles pourraient être supérieures (et être réellement appliquées).***

4.5. La cybercriminalité : entre naïveté et cyber-guerre ?

Afin de lever toute ambiguïté, *« la cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet. Ce terme désigne à la fois :*

- *Les atteintes aux biens : fraude à la carte bleue sur Internet sans le consentement de son titulaire ; vente par petites annonces ou aux enchères d'objets volés ou contrefaits ; encaissement d'un paiement sans livraison de la marchandise ou autres escroqueries en tout genre ; piratage d'ordinateur ; gravure pour soi ou pour autrui de musiques, films ou logiciels.*
- *Les atteintes aux personnes : diffusion d'images pédophiles, de méthodes pour se suicider, de recettes d'explosifs ou d'injures à caractère racial ; diffusion auprès des enfants de photographies à caractère pornographique ou violent ; atteinte à la vie privée.*

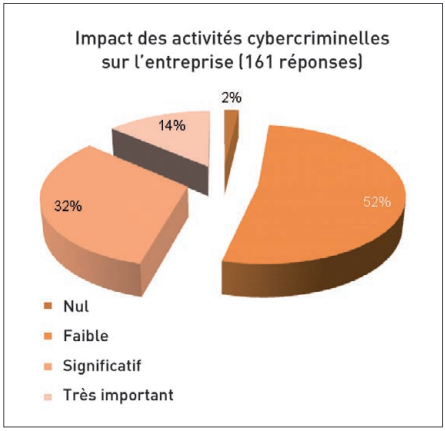
Tous ces faits sont punis d'une peine d'emprisonnement (5 ans maximum) et d'une amende (375 000 euros maximum). »

Source : Ministère de l'Intérieur (www.interieur.gouv.fr)

4.5.1. Perception de la cybercriminalité en entreprise

Terme un peu barbare et pouvant paraître terrifiant pour les profanes, la cybercriminalité n'en demeure pas moins une réalité (cf. bilan de la décennie au chapitre 2). Cependant, qu'en est-il réellement pour l'entreprise ?

Sur la base de 161 réponses, on constate qu'elle est bien une réalité pour un peu moins de la moitié des répondants.



A titre d'exemple, et pour se convaincre de la dimension économique de la cybercriminalité vue sous l'angle de la sécurité du SI :

« Les cas les plus répandus que nous avons observés au cours de ce trimestre étaient des installations de faux produits de sécurité par des chevaux de Troie. Pourquoi de faux anti-virus ? Ils génèrent des profits à la fois pour les développeurs de logiciels malveillants et pour leurs distributeurs. La plupart des chevaux de Troie générant de fausses alertes d'infection fonctionnent à travers un programme affilié, avec un intermédiaire touchant une petite commission pour chacune des nouvelles installations du logiciel. » (Source McAfee, 1er trimestre 2010).

« Le kit Zeus (Zbot) est disponible à partir de seulement 700 dollars et automatise le processus de création de malwares capables de dérober des données personnelles. Les pirates ont ainsi créé des millions de nouvelles variantes de malwares pour éviter d'être détectés par les logiciels de sécurité. Une tendance largement portée par le cheval de Troie Zeus dont 90 000 variantes ont été identifiées. » (Source Symantec, 2010).

« Le prix moyen d'installation d'un programme malveillant est de 3$ pour 1000 ordinateurs en Chine et 150$ pour mille ordinateurs aux USA. » (Source Kaspersky, 2010).

Quelques chiffres encore :

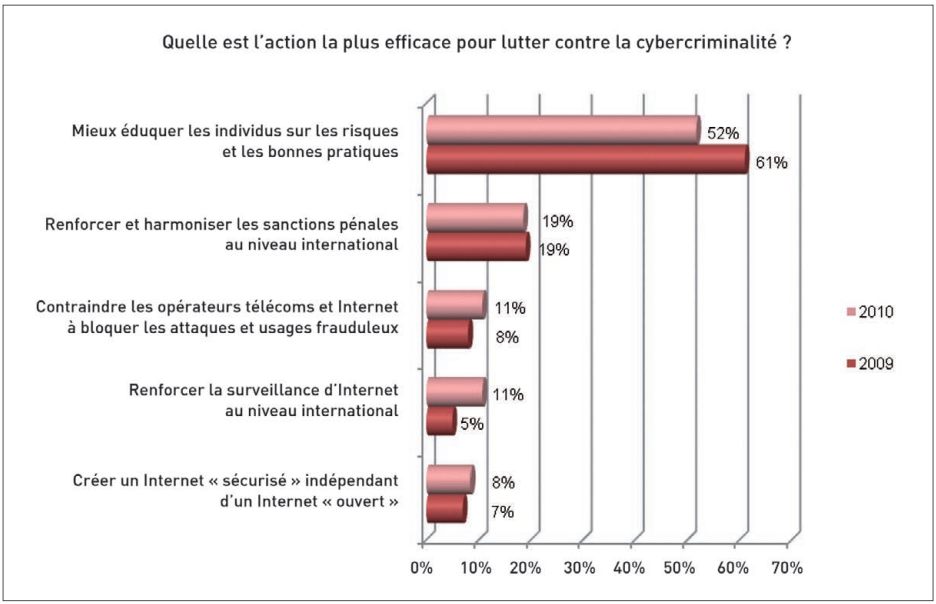
- La location d'un botnet d'une capacité de 1000 messages/minute rapporte en moyenne 2000$ /mois.
- Le coût d'un million d'adresses mails : 20$ à 100$.
- Le coût d'un mailing sur 1 million d'adresses : 150-200$.

Ceci ne doit cependant pas nous faire oublier l'ensemble des autres domaines comme : les trafics de médicaments, de produis de luxe ou encore la pédo-pornographie autrement plus médiatisés et graves.

La cybercriminalité ne s'effectue pas que dans le « virtuel » et ses activités se concrétisent par une véritable économie souterraine, en prise avec le monde réel.

4.5.2. Quels moyens de lutte efficaces ?

L'organisation cybercriminelle est une réalité et son activité économique également. Ne rien faire est de l'inconscience et se reposer uniquement sur les forces de l'ordre de l'illusion. Alors que faire ?



La solution la moins énoncée s'avèrerait pourtant la meilleure d'un point de vue économique dès lors qu'elle consisterait à créer des infrastructures « séparant » par exemple, les relations « État-citoyens » (B2A) et le commerce et les entreprises (B2B, B2C) de la « jungle » ouverte à tous.

Utopie ou sérieux coup d'accélérateur à l'industrie des TIC ?

La raison, à l'heure actuelle, repose sur un accompagnement pragmatique de l'évolution technologique et des risques associés, comme le propose ci-dessous Eugène Kaspersky.

Eugène Kaspersky
CEO Kaspersky Lab

> ***« Pour combattre les cybercriminels, nous devons combiner trois moyens de protection : les suites logicielles de sécurité, la régulation des gouvernements et les forces de cyberpolice. Je soutiens donc les initiatives de filtrage du Web.***
>
> ***Je soutiens les initiatives des gouvernements pour introduire plus de régulation. Pas de contrôle, je pense que « contrôle » n'est pas le bon terme, et de toute façon aucun gouvernement n'a suffisamment de ressources pour tout surveiller, mais de la régulation oui. »***

> ***Cependant, les répondants à notre enquête apportent au triptyque « outil / régulation / répression » indiqué ci-dessus, l'essentielle question de l'éducation, malgré une baisse entre 2009 et 2010 au profit de la régulation vers les opérateurs Internet et le renforcement de la surveillance.***

4.6. Synthèse

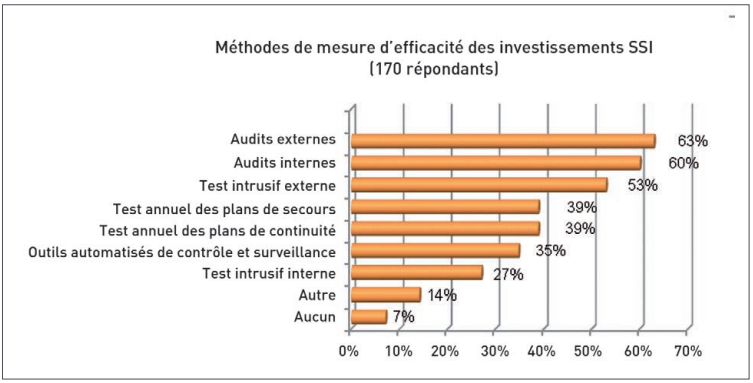
Au final, quelle que soit l'ampleur des moyens mis en œuvre et le niveau de risques à couvrir, la question de la mesure de l'efficacité des dépenses s'avère essentielle. Plus question de risques ou de conformité, c'est de performance qu'il s'agit ici. Et pour cela, il faut aussi de bonnes pratiques et des indicateurs.

Les deux questions suivantes apportent quelques éléments de réponses qui mériteront des approfondissements dans le cadre des travaux du Cercle Européen.

4.6.1. Quelle mesure de l'efficacité ?

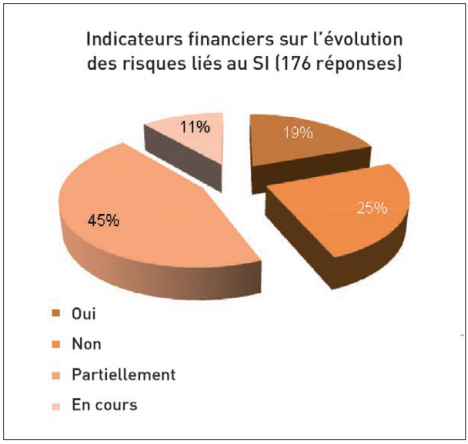
Sur l'ensemble des méthodes de mesure de l'efficacité des investissements, trois ont été citées par une majorité de répondants. Sans grande surprise, les pratiques d'audit et les tests intrusifs sont privilégiés, devançant les tests des plans de secours et de continuité.

Il sera intéressant de mesurer dans la durée les apports des outils automatisés s'inscrivant dans la démarche SIEM présentée lors du bilan du marché.



4.6.2. Quels indicateurs économiques des risques SI et mesures SSI ?

Enfin, alors que la question des tableaux de bord est apparue comme une priorité du panel avec 58% de réponses (cf. bilan de la fonction SSI), il convient encore d'en déterminer les objectifs : maîtrise des risques, niveau de conformité, performance sécuritaire ?



On constate bien que la question est d'actualité même si peu de professionnels ont réellement finalisé leur démarche. Les compétences économiques des professionnels de la sécurité et des synergies avec la Finance et la Gestion de risques seront nécessaires voire indispensables.

5. CONCLUSION

Nous avions terminé le Livre Bleu des Assises 2009 sur le célèbre propos d'Abraham Lincoln, *« Si vous pensez que l'**éducation coûte cher**, essayez l'ignorance ! »*. Il fait le lien entre nos travaux de 2009 et ceux de 2010, entre le social et l'économie. Cette année, c'est l'économie de la sécurité des SI dans son ensemble qui nous a intéressés. Et la citation de Rudyard Kipling (*« Il faut toujours prendre le **maximum de risques** avec le **maximum de précaution** »*) mentionnée en introduction relie à nouveau, l'attitude face au risque et l'ampleur des moyens pour le couvrir.

Ces deux grands hommes n'ont pas connu l'informatique et Internet, mais leurs propos restent certainement valides de nos jours, alors que nous vivons une période troublée de notre histoire. Une période de crise majeure qui nous amène aussi à revenir sur trois questions essentielles :

- **Qu'est-ce qui a de la valeur aujourd'hui ?** Beaucoup diront l'image de marque ou un cours de bourse. Les plus éclairés diront des emplois ou des vies…

- **Quelles sont les véritables menaces désormais ?** Certains diront les concurrents. D'autres des fraudeurs en tous genres. Et le crime organisé ? Et pourquoi pas des États ?

- **Qu'est-on prêt à sacrifier, individuellement ou collectivement, pour se sentir réellement en sécurité ?** Un peu de liberté sûrement. Ou beaucoup d'argent ?

Les enseignements tirés du Livre Bleu des Assises 2010, au regard du nombre de questions posées – et que nous ne reprendrons pas ici – démontrent que l'intégration de la dimension socio-économique doit devenir un enjeu en face d'une réalité technico-juridique qui montre chaque jour ses limites. Et la route est encore longue…

Comme Gérard RIO, fondateur visionnaire des Assises de la Sécurité en 2001, l'a indiqué en introduction, nous initions une réflexion qui devrait accompagner l'ensemble des acteurs pendant les trois prochaines années. Celle-ci a été structurée, lors de la réunion de lancement du Groupe de travail du Cercle Européen de la Sécurité, en 4 grands thèmes :

- Les impacts économiques des attaques, incidents, fraudes, etc.
- Les dépenses des entreprises et administrations
- Les réponses du marché
- L'économie de la cybercriminalité

Les quatre revêtent une certaine importance car elles font écho aux opportunités de développement des entreprises et administrations que procurent les Technologies de l'Information et de la Communication, mais qui sont aussi porteuses de risques, qu'il convient de gérer au bon niveau.

Il sera cependant nécessaire de se focaliser, de définir des priorités et surtout, de ne pas refaire ce qui se fait déjà ailleurs (Études de marché, travaux universitaires, de l'ENISA, études associatives ou d'offreurs, etc.), ni de travailler en vase clos car les liens avec la finance, la gestion des risques, les RH, la gestion de la fraude ou la sécurité des biens et des personnes sont très étroits.

> ***Aussi, et pour répondre aux caractéristiques essentielles du Cercle Européen de la Sécurité qui associe intelligemment, les décideurs de la profession, côté « offre » et côté « demande », c'est au niveau de cette articulation « besoins / solutions » que nous pourrons sans doute avancer en y intégrant la dimension économique et pas uniquement la gestion d'une menace ou d'une vulnérabilité.***

A titre d'exemple, nous pourrons être amenés à déterminer :

- **Un cadre de référence des dépenses** en Sécurité SI permettant :
  - D'établir un (ou plusieurs) indicateur (s) de type « ratio » (en euros / utilisateur et non rapporté au budget de la DSI)
  - De mesurer l'équilibre entre outils / services / ressources humaines

- **L'impact (économique) sur le marché de la sécurité SI**
  - des normes ISO 27001 et 27002
  - d'une règlementation comme le Règlement Général de Sécurité
  - ou demain de la future loi Detraigne-Escoffier

- **Des axes de pilotage budgétaire « à la demande »** liés
  - Au SaaS
  - Au Cloud Computing

La 2ème réunion du Groupe de travail du Cercle, prévue en novembre 2010, permettra de fixer des objectifs précis et de lancer les travaux qui seront relatés lors de nos prochains dîners-débats.

Pour ne pas faillir à la tradition, nous conclurons l'édition 2010 du Livre bleu des Assises, par une citation évocatrice, au cœur de notre sujet !

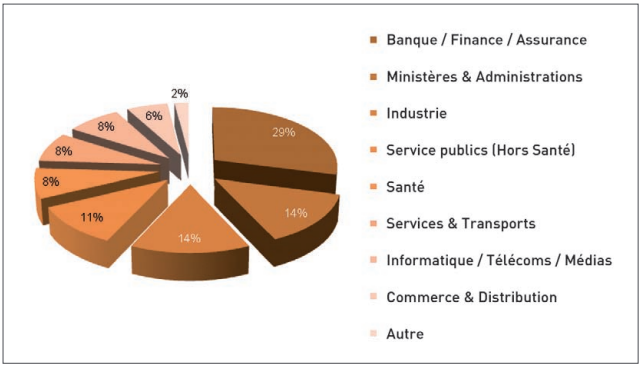
Luc FERRY
Philosophe

> ***« Nous avons l'impression que les forces économiques, les marchés financiers, les nouvelles technologies, transforment notre vie de tous les jours bien davantage que nos ministres ou nos parlementaires. »***
>
> ***(Penser le changement – 2007)***

6. ANNEXE : LE PANEL

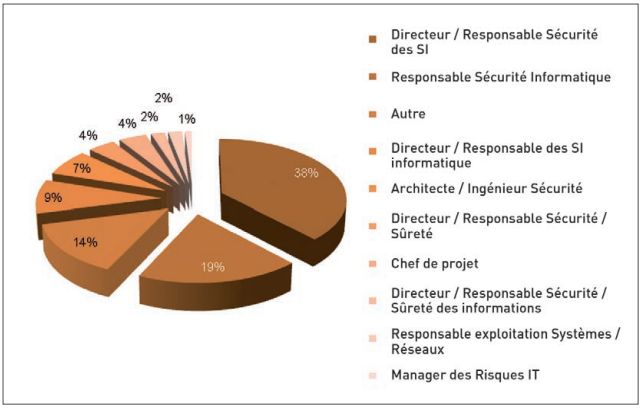
Le panel de l'enquête 2010 est constitué de 236 professionnels. Leurs principales caractéristiques sont présentées ci-dessous.

6.1. Secteurs d'activités



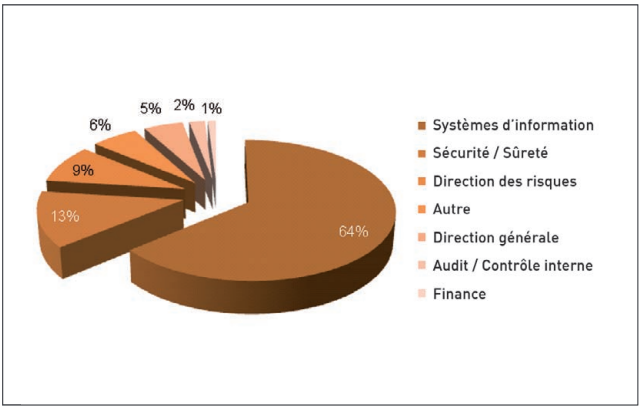
Une représentativité stable d'année en année avec un poids significatif des Banques / Assurances et des Administrations / Services publics.

6.2. Titres et fonctions



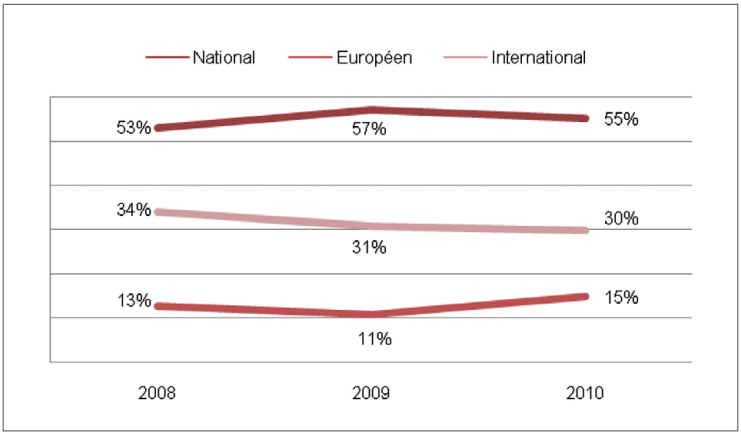
Une répartition qui évolue sensiblement par rapport à 2009, avec notamment une proportion plus importante de Directeurs / Responsables Sécurité des SI.

6.3. Entités d'appartenance



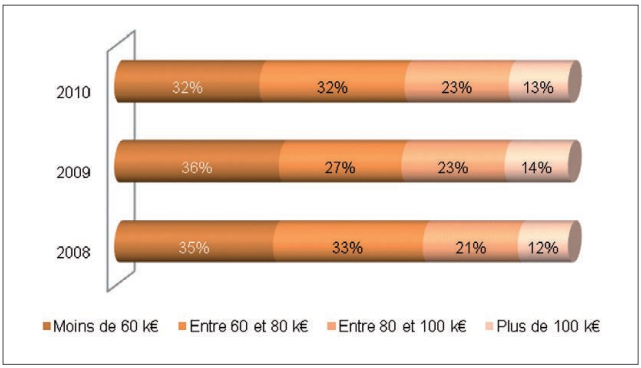
Une proportion plus importante des Directions SI cette année (56% en 2009).

6.4. Couverture géographique



Le champ d'action du panel s'élargit principalement en Europe.

6.5. Rémunération



Une répartition des salaires qui varie peu avec un salaire moyen qui progresse légèrement (74,4 k€ contre 73,8 k€ en 2009 et 73,4 k€ en 2008).

NOTES

NOTES

hapsis
Cabinet de conseil en sécurité
de l'information

La sécurité, une opportunité !

- Dématérialisation & confiance numérique
- Protection des informations & des infrastructures
- Sensibilisation & formation
- Gouvernance SSI & tableaux de bord

45 rue de la Chaussée d'Antin – 75009 Paris
Tél. +33 (0) 153 16 30 60 – Fax. +33 (0) 153 16 30 62
Courriel : contact@hapsis.fr

www.hapsis.fr

VUPEN®

security

Spécialiste des solutions de gestion des vulnérabilités

Vulnerability Notification Service

Service de veille permettant aux professionnels de la sécurité (RSSI, DSI, ingénieurs et consultants) de recevoir, en temps réel, des bulletins d'alertes décrivant les nouvelles failles de sécurité pouvant affecter leurs systèmes et technologies déployés

Web Security Scanner

Solution hébergée (SaaS) permettant d'auditer les sites web et d'identifier, en boite noire et grise, les vulnérabilités pouvant les affecter (SQL injection, cross site scripting, etc)

Bénéficiez d'un essai gratuit en vous inscrivant sur www.vupen.com

Pour plus d'informations : www.vupen.com sales@vupen.com +33 (0)4 67 13 00 94