tome VI

Octobre 2009

Le Livre Bleu

Développer la culture des risques informatiques et informationnels

réalisé par

hapsis

pour

les assises de la sécurité et des systèmes d'information

le cercle
européen de la sécurité et des systèmes d'information

Face à la menace,
vous n'êtes pas seul...

Sécurité des systèmes d'information : enjeux, perspectives, retours d'expérience.

Face à la complexité croissante des « cyber-menaces », il est devenu essentiel de mettre en commun expériences, réflexions, compétences pour relever les défis stratégiques de demain en matière de sécurité des systèmes d'information.

Le Cercle, communauté d'utilisateurs et de décideurs du secteur, fédère des professionnels et compte plus de 600 membres actifs : responsables, directeurs de la Sécurité des Systèmes d'Information, experts en sécurité, présents chaque année aux Assises.
Il vise l'élargissement des compétences et permet les échanges sur tous les enjeux liés aux risques, solutions et moyens de protection des patrimoines numériques des entreprises et institutions. Sa mission consiste également à détecter des solutions innovantes et à en favoriser le développement.
Dès le mois de février 2009, prenez part aux rendez-vous du Cercle : un levier pour renforcer votre réseau, approfondir votre réflexion sur la stratégie des Systèmes d'Information et faire les bons choix.

Pour plus d'informations : 01 41 93 07 07 - www.lecercle.biz

comexposium

un événement

les assises
de la sécurité et des systèmes d'information

SOMMAIRE

1- Introduction **2**
2- Notions de « culture » et de « culture du risque » **4**
2.1. Le constat 4
2.2. Qu'est-ce que la culture ? 5
2.3. Les risques informatiques et informationnels 6
2.4. Culture du risque informatique et informationnel 7
2.5. Quelques apports philosophiques, scientifiques et humanistes 8
2.6. Exploitation des résultats de l'enquête 2009 9
3 - Bilan de la culture des risques **10**
3.1. Préambule 10
3.2. Enjeux majeurs et risques visés 10
3.3. La culture par le management 12
3.3.1. Les actions de pilotage prioritaires 12
3.3.2. Les actions opérationnelles prioritaires 15
3.4. Renforcement de la veille et du contrôle 17
3.5. Avis d'expert : l'impact des Directives Nationales de Sécurité (Diane BAUDRY – Hapsis) 17
3.6. La culture par les ressources humaines 19
3.6.1. Rôle des professionnels 19
3.6.2. Taille des équipes 20
3.6.3. Coopération avec les métiers et autres activités 21
3.6.4. Avis d'expert : casting des membres d'une cellule de gestion de crises (Isabelle TISSERAND – Coordinatrice du Cercle) 23
3.7. Quelle maturité globale ? 24
3.8. En synthèse 27
4 - Développement de la culture des risques **28**
4.1. Risques majeurs et implication des décideurs 28
4.1.1. Quels risques majeurs à intégrer ? 28
4.1.2. Quelle influence et quelle implication des décideurs ? 29
4.2. Quelles actions les plus efficaces ? 29
4.2.1. Pour lutter contre la cybercriminalité 30
4.2.2. En termes de communication 30
4.2.3. En termes de sensibilisation 31
4.2.4. Avis d'expert : les apports de la communication engageante (Michel GERARD – PDG Conscio Technologies) 33
4.3. Quelle implication des acteurs publics et privés ? 35
4.3.1. Les pouvoirs publics 35
4.3.2. Les acteurs privés 35
4.3.3. Avis d'expert : « L'impact des médias sur la culture des risques. » (Nicolas ARPAGIAN) 37
4.4. En synthèse 39
5 - Conclusion **40**
6 - Annexe 1 : Rubriques d'information / sensibilisation **41**
7 - Annexe 2 : le panel **42**
7.1. Secteurs d'activités 42
7.2. Titres et fonctions 42
7.3. Entités d'appartenance 43
7.4. Couverture géographique 43
7.5. Rémunération 43

1- INTRODUCTION

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

L'année dernière, nous avons traité le thème de la Sécurité globale qui, au-delà des questions de gouvernance, pose clairement la question de la globalisation des risques et de leur appréhension par l'ensemble des populations, en tout lieu, à tout instant.

La 1ère décennie du XXIème siècle aura été celle de tous les dangers. Les attaques terroristes du 11 septembre 2001, les pandémies, la crise, les fraudes financières, le réchauffement climatique, les prises d'otages et la piraterie, les atteintes à l'enfance, les vols de données, la cybercriminalité, etc. montrent un univers rongé par la peur. Tel Pythagore qui affirmait il y a 2500 ans que « Tout est nombre ! », devons nous aujourd'hui admettre l'idée que « Tout est risque ! » ?

A contrario, et en réponse à cette situation, l'exigence de sécurité est telle, qu'elle conduit parfois à des excès : le rejet du risque, voire la quête du « risque zéro ». Le principe de précaution est institutionnalisé et le marketing de la sécurité bat alors son plein. La fonction Sécurité gagne, mécaniquement, en notoriété. Les lois et règlements deviennent pléthoriques et de plus en plus liberticides.

Par ailleurs, l'arsenal technologique n'est pas toujours efficace et reste assez aisément contourné. Certains secteurs d'activité, les PME restent en retard en termes de gouvernance des risques. Mais à quoi tout cela rime-t-il au fond ?

La dépendance de la Société à l'informatique et à Internet ne doit-elle pas aussi s'accompagner d'une véritable « culture des risques informatiques et informationnels » ?

La sécurité réelle, ou du moins le sentiment de sécurité, ne repose-t-elle pas, comme toujours, sur l'individu, quel qu'il soit (de l'adolescent au dirigeant) ? Cependant :

- A-t-il seulement conscience des menaces et des impacts ?
- Quels sacrifices est-il prêt à consentir pour être, ou se sentir, en sécurité ?
- Connaît-il les champs de responsabilité dans le domaine ?
- Peut-il faire confiance aux informaticiens et opérateurs, comme aux outils de protection, garants de la sécurité opérationnelle ?
- Comment lui faire accepter les règles et contraintes de prévention et protection ?
- Que doit-il faire face à une situation anormale ou dangereuse ?
- Une sécurité transparente, intégrée et gratuite est-elle la solution ? A quelles conditions ?
- Comment peut se développer une « culture des risques » liés aux technologies de l'information ?

Le thème de l'année « Bilan et développement de la culture des risques informatiques et informationnels » est encore une fois ambitieux. Nous l'aborderons, comme toujours, avec humilité, en nous appuyant sur les résultats d'une enquête menée en juin et juillet 2009 auprès d'un panel de 240 professionnels.

Indiquons d'entrée que nous n'avons pas retenu une approche segmentée par typologies[1] d'acteurs comme les grandes entreprises, les administrations, les PME, les individus qu'ils soient parents ou enfants, citoyens, consommateurs, salariés, etc.

L'approche retenue nous conduit à rester extrêmement factuels, proches de la réalité du terrain. Les chiffres présentés traduisent les pratiques et la vision des acteurs du secteur.Ils n'ont de valeur que par la qualité d'un panel qui s'est progressivement élargi passant de 40 personnes en 2004 à 237 en 2009 contre 174 en 2008 et 107 en 2007. Le succès des enquêtes du Cercle est ainsi confirmé par une participation en forte progression.

L'analyse du panel et des statistiques (voir annexe 2) :
- Apparait cohérente depuis 3 ans
- Montre une grande stabilité des chiffres (fiabilité à +/- 2 %) en fonction de filtres sur la fonction ou l'entité organisationnelle du répondant
- Permet d'effectuer des « zooms », toujours instructifs, pour 3 secteurs d'activité : Banque/Assurance, Administration/Services publics, Industrie

Nous avons aussi sollicité 4 experts qui apporteront leur éclairage sur des sujets majeurs de la dialectique :
- La dimension stratégique : « *Impacts des Directives Nationales de Sécurité sur la culture des risques* » par Diane Baudry (Hapsis)
- La dimension organisationnelle : « *Casting des membres d'une cellule de gestion de crises* » par Isabelle Tisserand (Coordinatrice du Cercle)
- La dimension psychologique : « *Apports de la communication engageante sur le développement de la culture des risques* » par Michel Gérard (Conscio Technologies)
- La dimension médiatique : « *Rôle des médias dans le développement de la culture des risques.* » par Nicolas Arpagian, Rédacteur en chef de « *Prospective Stratégique* »

Enfin, nous remercions chaleureusement tous ceux qui œuvrent à cette démarche, chez DG Consultants, au Cercle Européen de la Sécurité et des Systèmes d'Information mais aussi et surtout, tous les participants anciens et nouveaux à cette enquête annuelle.

Nous espérons vivement que ce 6ème volet des Livres Bleus des Assises vous éclairera dans vos activités quotidiennes, présentes et futures.

Pierre-Luc REFALO
Hapsis

[1] L'ENISA (European Network and Information Security Agency) a produit, à ce titre, en 2006, un document de référence, de type politique et méthodologique, toujours utile. www.enisa.europa.eu

2- NOTIONS DE « CULTURE » ET DE « CULTURE DU RISQUE »

2.1. Le constat

Le domaine de la Sécurité du SI semble atteindre une certaine forme de maturité. En effet, les innovations technologiques et méthodologiques sont désormais rares pour ne pas dire inexistantes. Cause ou conséquence de la crise actuelle ?

A en croire le rapport du Conseil d'Analyse de la Société, « Face à la crise », (Odile Jacob - Mai 2009), rédigé par l'ancien Ministre Luc Ferry, les maux qui dévorent aujourd'hui la société occidentale trouvent leur source dans cette quête sans fin d'innovation et de consommation. En sécurité des systèmes d'information aussi, les outils se sont multipliés. Et ils ont quasi totalement déchargé l'utilisateur d'une quelconque responsabilité face à une multiplication de menaces toujours, très innovantes, simples et de plus en plus répandues.

Et pourtant, on continue de penser et de dire que c'est par l'éducation et la sensibilisation que l'on parviendra à mieux protéger notre patrimoine informatique et informationnel.

« L'attaque informatique est aujourd'hui un sport international. C'est tellement facile que tout le monde est ciblé. Les particuliers mais surtout les entreprises. Il s'agit surtout de vol d'informations pour soustraire les secrets dans ces entreprises et dans ces Etats. C'est pourquoi le travail de sensibilisation est un élément essentiel de notre stratégie. »

Patrick Pailloux
Directeur de l'Agence Nationale à la Sécurité des Systèmes d'Information
La Tribune, le 10 juillet 2009

Mais souvenons-nous.

- Fin 1999 : L'affaire « Humpich » crée la psychose en France. L'Est Républicain titre en Une, « Le secret percé des cartes à puce. » Et VSD de titrer « Ce pirate qui fait trembler les banques. » L'individu sera condamné au titre de l'intrusion dans un système de traitement de données.

- Février 2000 : L'affaire « Mafiaboy » défraie la chronique. Un adolescent canadien de 15 ans crée un bombardement électronique sur les sites d'Amazon, e-Bay et Yahoo (et d'autres) en pleine bulle Internet. Arrêté par le FBI, il sera condamné à des travaux d'intérêt général et interdit d'utilisation d'un ordinateur pendant 2 ans.

- Mai 2000 : La lettre de l'Amour (virus I Love You) se répand comme une trainée de poudre d'Asie, en Europe puis aux Etats Unis, impactant le fonctionnement de milliers d'entreprises. Des étudiants philippins seront arrêtés par le FBI.

A-t-on tiré les leçons de ces faits déjà anciens, à la fois en termes de prévention, de protection et de comportement ? Il semble malheureusement que non ; ces derniers mois encore :

- Des trafics de numéros et de fausses cartes bancaires sont démantelés chaque jour et le 18 août 2009, un américain est arrêté pour un trafic de 150 millions de numéros de cartes valides. Il risque 70 ans de prison.

- Des sites gouvernementaux et bancaires (réputés les plus sûrs) sont victimes d'attaques, comme ceux d'Estonie ou de Géorgie (vraisemblablement par des sites russes) ou de l'ambassade de France en Chine.

• Le ver Conficker s'est introduit sur les sites de la Marine Nationale et de nombreuses grandes entreprises françaises créant des indisponibilités du système d'information et des accès Internet de plusieurs jours.

• Le phishing et le skimming, sous la houlette de groupuscules mafieux, génèrent chaque année plusieurs milliards de dollars de préjudice pour les uns, de revenus pour les autres.

Et pourtant, la volonté politique a toujours été très forte, au moins par le verbe :

Juste après le passage à l'an 2000, le 11 janvier 2000, Bill Clinton débloque 2 milliards de dollars pour lutter contre la cybercriminalité, *« faire face au terrorisme informatique »* et faire du gouvernement américain *« un modèle en matière de sécurité informatique, en développant un partenariat public – privé. »*

A l'occasion du G8 « cybercriminalité » de Paris en mai 2000, le Président de la République, Jacques Chirac, insistait sur deux points fondamentaux :

- *« Hommes et femmes d'entreprises, élus, responsables d'associations, magistrats, policiers, diplomates et administrateurs, vous poursuivez les mêmes objectifs : étendre au cyberespace le droit fondamental à la sécurité, assurer la confiance indispensable à son développement. »*
- *« Est-ce que les concepts qui ont fondé nos ordres juridiques – l'identité, la preuve, l'authenticité – sont-ils encore valides, alors qu'ils sont confrontés à des technologies numériques qui permettent la reproduction et presque gratuite, la transmission instantanée, la manipulation des signes et la falsification ? »*

De son côté, lors de l'enquête sur Mafiaboy, Janet Reno (Department of Justice) avouait toute la difficulté de la bataille engagée : *« Even if criminals do not hide identities online, we still might be unable to find them. »*

Doit-on alors baisser les bras ? Se dire que la lutte est perdue ? Et se contenter de faire, malgré tout, confiance aux forces de l'ordre pour surveiller, retrouver et sanctionner les cybercriminels ?

Le propos n'est pas de dire ici que les mesures de protection et les techniques d'investigation ont des limites ou sont inefficaces. C'est faux ! Et si elles n'existaient pas, la situation serait bien pire. Il est temps de (re) dire haut et fort, plus fort que jamais, qu'il manque toujours un maillon à la chaîne de la sécurité, ou du moins, que le facteur humain, demeure le parent pauvre de la Sécurité des SI.

Mais indiquons aussi immédiatement que la question n'est pas aisée ! Existe-il une seule approche possible ? Alors que les risques sont si variés et évolutifs. Une (ou des) culture (s) des risques informatiques et informationnels devra-t-elle émerger ? Quand ? Comment ?

C'est une partie du débat que nous engageons par ce travail. Nous apporterons sans doute plus de questions que de réponses, mais l'exercice est utile.

2.2. Qu'est-ce que la culture ?

La notion de « culture » étant extrêmement vaste, il convient d'en dresser les contours pour ensuite se focaliser sur les questions de « risques » et de « sécurité ».

La culture se caractérise généralement par des aspects anthropologiques, historiques et éducatifs : elle intègre donc de l'inné et de l'acquis.

Elle possède des aspects collectifs mais aussi très personnels : elle s'adresse à une société dans son ensemble mais aussi au monde de l'entreprise, en relation avec l'Etat et les individus (salariés, citoyens, consommateurs, parents). Elle possède des dimensions politique, économique et psychologique.

Il faut surtout distinguer et ne pas confondre la culture au sens « classique » du terme (La culture), « sociétal » et bien souvent traduit sous un angle « artistique », et la culture en tant qu'apprentissage, construction, ou création spécifique (une culture de quelque chose). En allemand on distingue d'ailleurs la première (Kultur) de la seconde (Bildung) qui correspond plus à un savoir.

La culture spécifique à une entreprise (banque, industrie, médias, transports, etc.) ou une activité donnée (alimentation, loisirs, télévision, voiture, santé, etc.), dépend fortement de décisions politiques (collectives) et personnelles (individuelles). Il faut donc comprendre cette culture comme une construction progressive partant d'un ensemencement initial, d'un accompagnement permanent, de bilans et de corrections. Cette culture particulière peut aussi fortement être influencée par la Culture !

Les questions de risques (ou de dangers) ont toujours fait partie de la Culture (guerres et pandémies par exemple). Et ceux d'hier ne sont pas ceux d'aujourd'hui ! Notre propos est d'adresser ici les risques relatifs aux systèmes d'information et informations.

2.3. Les risques informatiques et informationnels

Dresser une typologie de ces risques est un exercice délicat. En les abordant sous l'angle de la menace, les Livres Bleus des Assises ont exploité le modèle proposé dans l'ouvrage « Sécuriser l'entreprise connectée » (Editions d'Organisation – 2002).

En termes de malveillance, on peut distinguer les risques qui portent atteinte au système d'information et ceux qui utilisent, ou exploitent, un système d'information pour commettre un délit, un crime « classique » ou créer toutes sortes de préjudices. L'ensemble s'inscrit clairement dans le cadre global de la cybercriminalité.

Une typologie des risques informatiques et informationnels est proposée dans le tableau ci-dessous. Mais n'oublions pas aussi qu'erreurs, inconsciences, négligences, voire parfois stress ou excès de confiance facilitent souvent l'acte malveillant.

Type	**Exemple**
Sabotage	Destruction physique, déni de service, bombe logique
Intrusion	Spoofing, Scanning, usurpation d'identité
Vol	Vol de support, CD, USB, documents, de portable, PDA, Vol d'identité Interception de communications, copie illicite de données
Atteinte à la vie privée	Logiciel espion, cookies Exploitation frauduleuse de données personnelles Divulgation intentionnelle ou non Interception de communication
Fraude	Spamming / Phishing Détournement de fond, escroquerie
Piratage	Contrefaçon de contenu numérique Contrefaçon de logiciel Contrefaçon de carte bancaire, carte à puce
Contenus illégaux	Pédo-pornographie Délit de presse, diffamation, injures, menaces, etc.

Ces données confirment que la culture des risques informatiques et informationnels doit intégrer une dimension historique. Le 1er ordinateur personnel et Internet ont moins de 30 ans ! Pourtant l'espionnage ou la fraude ne datent pas d'hier !

Cette typologie, incomplète et perfectible, montre surtout l'ampleur de la problématique et du champ d'investigation. Cet aspect n'est pas sans conséquence sur la dialectique de ce Livre Bleu. Une culture ou des cultures ?

2.4. Culture du risque informatique et informationnel

A ce titre, il est fondamental de rappeler que nos « anciens », n'ont eu du risque, qu'une appréhension extrêmement simpliste : Les 4 cavaliers de l'Apocalypse étaient représentés par les prédateurs, les maladies, la famine et les catastrophes climatiques. Peu nombreux, certains et aux impacts catastrophiques.

Pour les plus jeunes générations, la situation a totalement changé. Les risques sont omniprésents, très nombreux, hyper médiatisés, mais sans aucune certitude quand à leur véritable réalité ou survenance. En clair, les périls sont multiples, mais pris isolément, ils sont statistiquement peu probables (accidents de voiture ou d'avion, infection virale, sida, maladie grave, chômage, etc.). C'est une mutation anthropologique majeure.

La perception des risques est fondamentalement liée à la dimension culturelle (historique et politique) du domaine ou du contexte. C'est vrai en termes de :
- compréhension des concepts : menaces, dangers, vulnérabilités, actifs critiques, etc.
- processus de gestion : prévention/réaction, technique/juridique/humain, financement et assurance, gestion de la crise, etc.
- comportements : degré de vigilance, respect des bonnes pratiques, détection de la menace, reporting, etc.

Dans la revue Alliage (N°48-49 - 2002), un article intitulé « Pour une nouvelle culture du risque », insistait sur une double exigence : développer une *« intelligence du risque faible »* et une *« maîtrise collective de la notion de probabilité »*. Les questions clés étaient posées :
- *Comment des cultures différentes, dans le temps et/ou l'espace, désignent-elles les risques qu'elles assument, ceux qu'elles redoutent, ceux qu'elles ignorent ?*
- *Quelle est la symbolique du risque et que révèle sa formulation langagière ? Le risque serait-il aujourd'hui le nouveau mal absolu ?*
- *Comment affiner ou déplacer la distinction entre risque choisi et risque subi, ainsi qu'entre risque individuellement assumé et risque socialement imposé ?*
- *Quel rapport (ou absence de...) entre les évaluations mathématiques du risque (probabilités) et leurs évaluations informelles ?*
- *Comment les représentations culturelles dominantes (télévision, cinéma, littérature, etc.) contribuent-elles à construire la notion collective de risque ?*
- *Comment imaginer les formes d'un débat démocratique permettant d'assumer collectivement les risques ?*
- *Comment intégrer cette thématique dans l'éducation ?*

Par delà cette vision et ces questionnements globaux, une approche plus individuelle de la culture du risque s'impose. Douglas et Wildavsky (« Risk and Culture. An essay on the selection of technological and environmental dangers » – 1983), mettent en évidence des points essentiels sur la perception psychologique des individus et le rôle de médiation des experts entre le politique et le grand public.
- *La division erronée entre la réalité du monde extérieur et les tâtonnements du psychisme humain ont attribué la vraie connaissance aux sciences physiques et laissé les illusions et les erreurs au champ de la psychologie.*

- *Une approche subjective sous-entend que les individus ont une façon de se comporter face au risque en général plutôt que face à certaines formes de risque.*
- *Entre la perception personnelle subjective et la perception collective, la science physique se mêle à la culture, délimite une zone moyenne de croyance et de valeurs partagées. Cette division du sujet qui ignore la culture est arbitraire et induit à l'erreur.*
- *Si nous ne pouvons connaître le risque encouru, comment pouvons-nous échapper aux dangers inconnus ?*

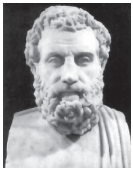
Afin de dresser un bilan et de proposer des perspectives de développement de la culture des risques informatiques et informationnels, nous nous appuierons sur ces questionnements et orienterons l'analyse autour de deux aspects clés :

1- Comment peut-on caractériser et évaluer cette culture en fonction des actions engagées et des mesures mises en œuvre ?
2- Comment peut-on agir pour la renforcer dans la durée, le cas échéant, en fonction de typologies d'individus ?

L'enquête 2009 apporte des éléments de réponses dans les 2 acceptions du terme « culture », en intégrant le champ d'action géographique du panel (national, européen, international) et les secteurs d'activité (Banque/Finance, Administration/Services publics, Industrie).

2.5. Quelques apports philosophiques, scientifiques et humanistes

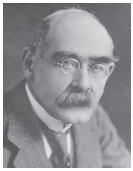
Culture et risques sont au cœur du développement de toutes les sociétés. Bref aperçu des pensées de quelques personnalités.



« Plus faibles sont les risques, meilleure est l'entreprise. » **Sophocle**

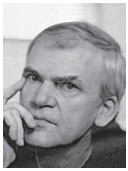
« Tu me dis, j'oublie. Tu m'enseignes, je me souviens. Tu m'impliques, j'apprends. » **Benjamin Franklin**

« Rien n'est plus dangereux que d'être trop moderne ; on risque de devenir soudain ultra démodé. » **Oscar Wilde**



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

« La culture ne s'hérite pas, elle se conquiert. »
André Malraux



« La culture, c'est la mémoire du peuple, la conscience collective de la continuité historique, le mode de penser et de vivre. »
Milan Kundera

« Il n'y a pas de liberté sans risque, sans ignorance, sans aventure. » **Jacques Attali**

« On ne peut vivre qu'en dominant ses peurs, pas en refusant le risque d'avoir peur. » **Nicolas Hulot**

2.6. Exploitation des résultats de l'enquête 2009

Le Livre Bleu des Assises 2009 présente l'analyse de l'enquête du Cercle Européen de la Sécurité et des Systèmes d'Information, orientée selon la thématique de la « Culture ». Il est structuré en 2 volets :

1- Les caractéristiques de la culture des risques dans le management et les activités « SSI » des professionnels
2- Les actions adaptées au développement de cette culture des risques au sein des entreprises et administrations

Des analyses particulières seront réalisées pour tenir compte de deux paramètres caractéristiques d'une culture (ou d'approches) spécifique dépendant du secteur d'activité de l'interviewer ou de son champ d'action.

Les 3 secteurs d'activité analysés		
Banque/Assurance	Administration/Services publics	Industrie
Les 3 zones géographiques analysées		
France	Europe	Monde

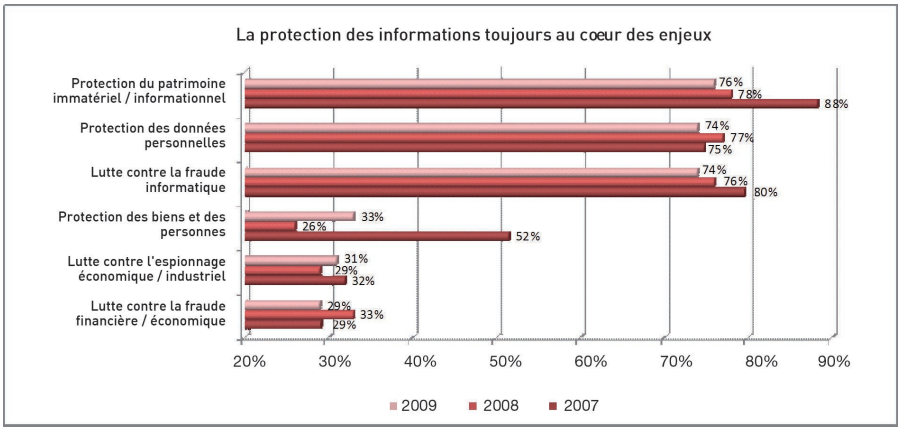
3- BILAN DE LA CULTURE DES RISQUES

3.1. Préambule

Le bilan de la culture des risques est présenté dans ce chapitre sous plusieurs angles :
- Les enjeux sécuritaires couverts par les entreprises et administrations
- Les risques majeurs perçus et à intégrer dans une démarche d'éducation
- Les actions prioritaires en 2009, en termes de pilotage et de processus
- La veille et le contrôle
- Les rôles des professionnels
- La taille des équipes et le recours à la sous-traitance
- La coopération avec les métiers et autres activités

3.2. Enjeux majeurs et risques visés

Les domaines d'action caractérisés sous l'angle des enjeux sécuritaires ont été analysés depuis l'origine des enquêtes du Cercle. Depuis deux ans, la forte évolution du panel tend à proposer une structuration type dans un schéma « ¾ - ¼ » (voir schéma ci-dessous).



En effet, environ 75% du panel concentrent leur activité autour de 3 enjeux, l'un historique (la fraude informatique), les deux autres, plus récemment intégrés, relatifs à la protection de l'information.

La prise en compte des risques visant le patrimoine (SI et informations) est donc privilégiée. La distinction entre « contenant » et « contenu » n'a plus lieu d'être et c'est le cas pour certains, depuis longtemps. Les autres aspects, connexes à la sécurité du SI, comme la protection des biens, personnes, des marchés, clients et revenus, sans être marginaux, ne concernent qu'environ 30% du panel. Son élargissement vers les fonctions « Sécurité / Sûreté » explique cette évolution.

L'influence du secteur d'activité est très significative comme l'attestent les chiffres présentés dans le tableau ci-dessous. La culture propre au secteur d'activité impacte considérablement certains chiffres. La Banque/Assurance conserve une approche classique plus « informatique », tandis que l'Administration/ Services publics et l'Industrie sont clairement plus centrés sur la protection de l'information.

Enjeux majeurs			
Fraude informatique	**89 %**	57 %	**81 %**
Données personnelles	74 %	71 %	71 %
Patrimoine informationnel	67 %	**75 %**	77 %
Fraude financière	38 %	19 %	35 %
Biens et personnes	32 %	41 %	23 %
Espionnage économique	17 %	28 %	58 %

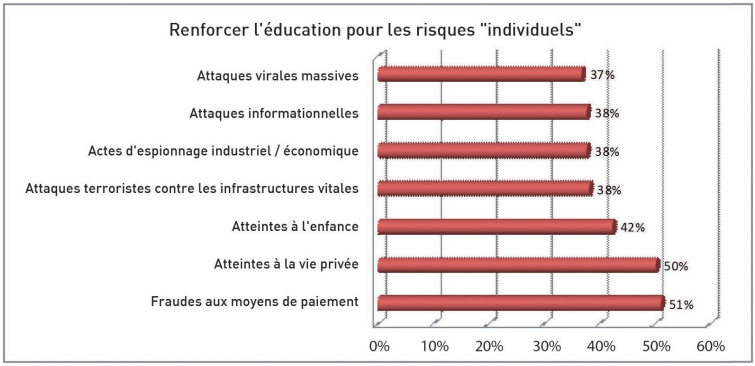
Zoom par secteur d'activité

L'influence du champ d'activité géographique des répondants est aussi significative sans être uniforme. Pour les trois enjeux majeurs, seuls les participants œuvrant dans un contexte européen se préoccupent beaucoup moins des questions de protection du patrimoine informationnel que des questions de fraude financière. Les professionnels dont l'activité se situe au niveau international mettent davantage en exergue les menaces stratégiques liées à la guerre économique.

Enjeux majeurs			
Lutte contre la fraude informatique	**74 %**	**78 %**	73 %
Protection des données personnelles	**75 %**	**78 %**	71 %
Protection du patrimoine informationnel	**75 %**	59 %	**83 %**
Lutte contre la fraude financière	24 %	48 %	29 %
Protection des biens et personnes	32 %	26 %	40 %
Lutte contre l'espionnage économique	23 %	22 %	48 %

Zoom par zone géographique d'activité

Au-delà de cette appréciation de la culture sécuritaire sous l'angle des « enjeux » couverts au sein des entreprises et administrations, nous avons sollicité le panel afin d'indiquer les trois risques pour lesquels des actions de communication / sensibilisation devaient se renforcer auprès des individus (schéma ci-dessous).



La priorité, sans que les écarts ne soient très importants, porte sur des risques touchant directement les individus par des attaques ciblées : données sociales, bancaires, santé. Ce constat n'est pas sans rappeler l'évolution de la perception des risques qui deviennent plus « personnels » et moins « collectifs ». Le salarié-citoyen s'efface-t-il devant le parent-consommateur ?

Cette analyse est ici aussi renforcée par une influence significative du secteur d'activité pour plusieurs types de risques. La culture d'entreprise impacte significativement celle sur les risques.

Là où les banques insistent sur la fraude aux moyens de paiement, loin devant les autres aspects, l'industrie place les attaques liées à la guerre économique tandis que l'administration et les services publics privilégient des atteintes aux infrastructures. Toutes ces préoccupations tendent à montrer une attention centrée sur les clients et marchés pour les uns, citoyens et usagers pour les autres.

Enjeux majeurs			
Attaques terroristes	26 %	42 %	48 %
Fraudes aux moyens de paiement	**66 %**	43 %	23 %
Attaques virales massives	34 %	**45 %**	39%
Actes d'espionnage économique / industriel	32 %	22 %	**55 %**
Attaques informationnelles	35 %	34 %	52%

Zoom par secteur d'activité

Sans surprise, le secteur d'activité détermine fortement l'orientation de la culture sous l'angle des enjeux et des risques considérés. Chaque secteur inscrit visiblement sa démarche dans une approche « client » en termes de développement de la culture des risques. Mais aucun risque n'émerge réellement, ne facilitant pas l'orientation d'actions d'éducation.

3.3. La culture par le management

3.3.1. Les actions de pilotage prioritaires

La culture sur les risques informatiques / informationnels s'exprime aussi dans l'art de les gérer notamment en termes de pilotage. Et en particulier dans l'importance accordée à la sensibilisation.

Nous avons demandé au panel quelles étaient les 3 actions prioritaires engagées en 2009 dans ce domaine. Aucun des choix proposés ne remporte une forte adhésion (voir schéma page suivante). Les stratégies en la matière sont donc intimement liées à la maturité « du moment » voire à la conjoncture interne ou externe des organisations. Mais il est remarquable que les priorités s'adressent directement aux entités métiers et aux utilisateurs, confirmant le constat du point précédent.

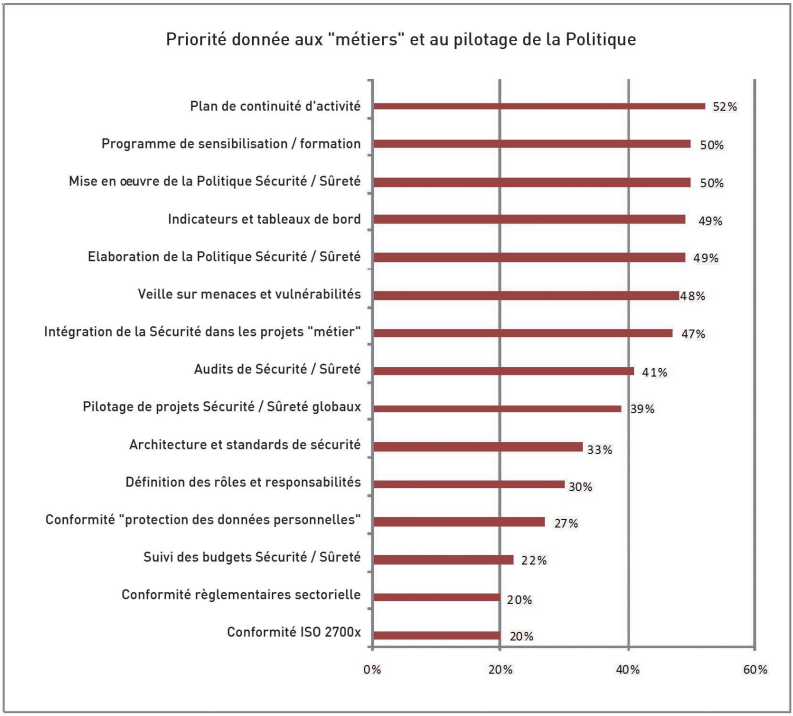
L'apparition des plans de continuité d'activité en tête des réponses s'explique certainement par la préparation de la possible pandémie grippale annoncée à l'automne 2009. Un constat sans doute conjoncturel.

Il est par contre notable de constater que c'est la mise en œuvre effective de la Politique Sécurité et son suivi par des tableaux de bord qui préoccupent principalement le panel. Pour beaucoup, il est temps de démontrer les apports de cette politique et de ses actions.

Les programmes de sensibilisation / formation se maintiennent à un niveau élevé (cf Livres Bleus des années précédentes), démontrant que des efforts doivent toujours être consentis dans ce domaine majeur. Nouveaux risques, nouvelles technologies, crise économique et sociale nécessitent d'intégrer le facteur humain à toute démarche de gestion de risque. La moitié du panel maintient l'effort !

Comme cela a été mis en évidence dans de nombreuses études et signalé aussi par des conférenciers, l'importance de la conformité s'amenuise fortement. Ce constat s'explique par plusieurs considérations :

- Les entreprises ont déjà bien avancé dans ce domaine, depuis près de 10 ans pour certaines.
- Les décideurs ont demandé des comptes aux acteurs de la SSI et doutent parfois des apports réels des efforts consentis en termes de conformité (SoX notamment).
- La conjoncture de crise oblige à revoir les priorités et la conformité n'en est clairement pas une.
- Des actions de pilotage plus significatives sont utiles aux métiers et aux professionnels.



L'impact du secteur et de la zone géographique d'activité a été analysé sur les actions les plus importantes, avec les résultats ci-dessous.

Actions de pilotage prioritaires en 2009			
Mise en œuvre de la Politique	47 %	**60 %**	**52 %**
Programmes de sensibilisation / formation	44 %	49 %	**55 %**
Veille sur les menaces et vulnérabilités	47 %	47 %	45 %
Intégration de la sécurité dans les projets	**53 %**	47 %	39 %
Plans de continuité d'activité	43 %	**56 %**	**52 %**
Audits de sécurité	43 %	29 %	42 %
Indicateurs et tableaux de bord	**60 %**	44 %	45 %

Zoom par secteur d'activité

L'influence du secteur d'activité est ici encore parfois significative et démontre des différences de maturité ou plus simplement d'approche des questions de sécurité du SI.

Alors que l'Industrie et l'Administration/Services publics placent en priorité des fondamentaux, qui peuvent être liés à la conjoncture (continuité d'activité), les banques apparaissent plus mûres en mettant en avant la culture « projet » en soutien des métiers et une exigence de « résultats » (via les tableaux de bord). L'Industrie privilégie aussi la sensibilisation / formation par rapport aux autres secteurs.

Actions de pilotage prioritaires en 2009			
Elaboration / Révision de la Politique	**57 %**	33 %	41 %
Mise en œuvre de la Politique	49 %	**52 %**	**52 %**
Programmes de sensibilisation / formation	49 %	**48 %**	**53 %**
Veille sur les menaces et vulnérabilités	**52 %**	19 %	**51 %**
Pilotage de projets sécurité globaux	33 %	26 %	**55 %**
Intégration de la sécurité dans les projets	49 %	19 %	**53 %**
Plans de continuité d'activité	**55 %**	41 %	**52 %**
Audits de sécurité	39 %	**48 %**	40 %
Suivi des budgets sécurité	39 %	**48 %**	32 %
Indicateurs et tableaux de bord	48 %	41 %	**53 %**

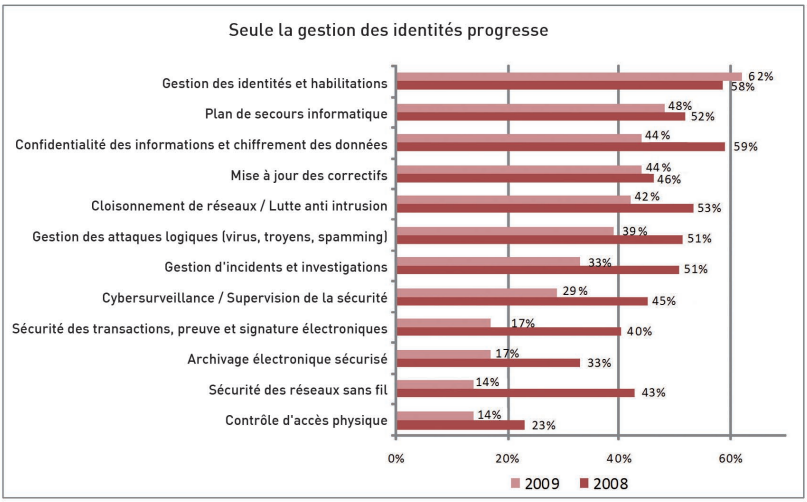
Zoom par zone géographique d'activité

L'influence de la zone géographique d'activité du panel est ici encore assez significative. Elle indique une grande répartition des actions de pilotage. Aucune ne ressort véritablement pour les professionnels œuvrant au plan international. Les acteurs européens se situent visiblement plus dans un rôle de « contrôle » que dans le pilotage de projets.

Les actions de pilotage ne permettent pas de caractériser une culture des risques. Les priorités sont très variées en 2009 et aucune règle générale ne se dégage. Les banques / assurances apparaissent cependant les plus mûres et portent plus attention aux activités « métiers » alors que l'Industrie privilégie légèrement le facteur humain.

3.3.2. Les actions opérationnelles prioritaires

Au-delà des actions de pilotage, la culture des risques peut aussi s'exprimer par la nature des actions réellement mises en œuvre pour les gérer. Depuis 2004, nous demandons parmi une liste de 12 actions, celles dans lesquelles sont impliqués les répondants. Cette année, nous avons demandé les 3 actions prioritaires menées en 2009. Le schéma ci-dessous présente les résultats globaux et l'évolution par rapport à 2008.



L'évolution à la baisse des statistiques s'explique par le changement de question (priorités en 2009 vs implication en 2008). Cette modification de la question apporte un recentrage des actions et une unique progression : la gestion des identités. Qui est qui ? Qui fait quoi ? Voilà deux questions essentielles auxquelles une majorité du panel cherche à répondre encore et toujours.

Si la multiplication des usages et des modes d'accès oblige à simplifier cette gestion pour l'utilisateur lui-même (ergonomie, productivité), l'actualité des vols et usurpations d'identités conduit aussi à se poser la question des menaces et des mesures de sécurité associées. C'est un projet « gagnant-gagnant » entre les métiers, l'informatique et la sécurité. S'il peut être long et fastidieux, des expériences réussies démontrent que le jeu en vaut sans doute la chandelle !

Avec moins de 50% mais des taux de réponses significatifs (entre 40 et 50%), les projets classiques de la Sécurité SI font bonne figure, alors qu'on retrouve juste après avec près d'un tiers des répondants, les questions de gestion d'incident / investigation et de cybersurveillance / supervision. Est-ce le signe notable de la réalité de la menace interne ?

L'impact du secteur et de la zone géographique d'activité a été analysé sur les actions qui présentent des écarts significatifs (voir tableaux ci-dessous).

Actions opérationnelles prioritaires en 2009			
Gestion des identités	**76 %**	**53 %**	**58 %**
Confidentialité et chiffrement des données	38 %	46 %	48 %
Cloisonnement de réseaux	31 %	44 %	48 %
Cybersurveillance et Supervision sécurité	13 %	32 %	42 %
Plan de secours informatique	18 %	**49 %**	**52 %**
Gestion d'incidents et Investigations	**42 %**	37 %	19 %

Zoom par secteur d'activité

L'influence du secteur d'activité est ici encore notable mais plus uniforme que précédemment. Elle démontre sans doute des différences de maturité ou plus simplement d'approche des questions de sécurité du SI. Les profils de l'Administration / Services publics et de l'Industrie apparaissent assez similaires et différents de la Banque / Assurance. Ainsi :

- Les banques / assurances privilégient très fortement la gestion des identités *a contrario* des autres secteurs qui répartissent plus leurs actions.
- Le plan de secours informatique apparaît maîtrisé dans les banques / assurances alors que les autres secteurs le placent en 2ème position de leurs priorités.

Actions opérationnelles prioritaires en 2009			
Gestion des identités	**61 %**	**63 %**	**67 %**
Confidentialité et chiffrement des données	39 %	33 %	**59 %**
Mise à jour des correctifs	**53 %**	26 %	35 %
Cybersurveillance et Supervision sécurité	27 %	19 %	36 %
Plan de secours informatique	**53 %**	33 %	43 %
Gestion d'incidents et Investigations	36 %	19 %	32 %

Zoom par zone géographique d'activité

S'il y a consensus sur la gestion des identités, l'influence du champ d'activité géographique des répondants est très significative à la fois en termes de priorités et de répartition des réponses. Ainsi :

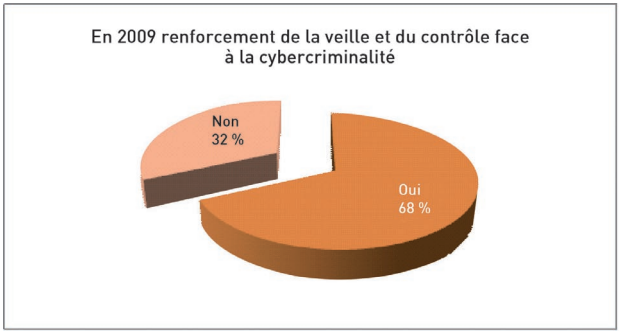
- Les acteurs « européens » se focalisent plus (2 priorités en moyenne)
- Les acteurs français privilégient en second lieu la continuité de service et les questions d'infrastructures
- Les acteurs « internationaux » mettent l'accent sur la confidentialité et les menaces externes.

Les actions opérationnelles mettent l'accent sur une préoccupation majeure concernant la gestion des identités, notamment dans la banque / assurance. Au-delà, des divergences notables apparaissent entre les secteurs d'activité.

3.4. Renforcement de la veille et du contrôle

Les questions de veille, de contrôle, voire de cybersurveillance peuvent aussi traduire une évolution certaine de la culture « sécurité » d'une organisation. Le constat ici est sans équivoque. La menace est bien perçue et oblige les professionnels soit à anticiper sur des incidents, attaques ou fraudes, soit à se mettre en capacité de réagir rapidement.

Ainsi, au-delà des questions classiques de « prévention » et « protection », les professionnels de la sécurité et leurs responsables, ont bien conscience que cela ne suffit pas. L'enjeu ici, sera alors de bien expliciter les domaines de responsabilités, généralement, dans le cadre d'une gouvernance formelle et de chartes concernant les collaborateurs, les informaticiens, les managers et les professionnels de la sécurité eux-mêmes.



Il n'y a pas d'écart significatif entre les différents secteurs d'activité. On notera simplement que la Banque / Assurance apparaît en retrait (mais dans la moyenne) avec 69% alors que l'Administration / Services publics affichent un résultat de 80%, démontrant une importance accrue de l'anticipation et une prise de conscience renforcée de la menace, peut-être sous l'influence des Directives Nationales de Sécurité ou suite à de récents incidents.

3.5. Avis d'expert : l'impact des Directives Nationales de Sécurité (Diane BAUDRY – Hapsis)

La menace terroriste, jusqu'ici prioritairement appréhendée sous l'angle de la défense du territoire, fait aujourd'hui partie intégrante de la politique de sécurité française. La globalisation de nos sociétés et de notre économie amène à prendre en compte des scénarios de risques visant des infrastructures stratégiques, et dont les conséquences pourraient être catastrophiques, a minima à l'échelle européenne. C'est dans ce contexte que l'État français, en adéquation avec la démarche engagée par l'Union européenne, a mis en place les Directives Nationales de Sécurité (DNS) : instigatrices d'une politique de « défense en profondeur » dans l'entreprise, elles visent à intégrer les acteurs du secteur privé concernés dans une dynamique collective, participant ainsi à la construction d'une « sécurité globale » avec et au sein même de l'entreprise.

Définition et objectifs des DNS

La démarche des DNS s'inscrit dans le cadre du décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale. Elles relèvent du Code de la Défense, et leur mise en œuvre est présentée dans l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale n°6600/SGDN/PSE/PPS du 26 septembre 2008. Le Premier ministre, par l'intermédiaire du SGDN, est l'autorité compétente en la matière, en étroite collaboration avec le Ministre de la Défense.

Une DNS s'applique à une partie ou à l'ensemble d'un Secteur d'Activités d'Importance Vitale (SAIV). Elle décrit le périmètre du secteur concerné et elle identifie les personnes clés responsables. La DNS met en exergue les enjeux propres à chaque secteur et définit le besoin de sécurité à assurer.

Elle peut ainsi définir la nature des opérateurs et des infrastructures qui pourront être désignés comme d'importance vitale, et préciser les critères de désignation.
Après réalisation d'une analyse de risques par l'opérateur du secteur, dans laquelle sont précisés et hiérarchisés des scénarios de menaces, la DNS précise les objectifs de sécurité à atteindre et les politiques correspondantes à mettre en place. Elle présente ainsi des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, dont celle d'origine terroriste, en rappelant les mesures du plan VIGIPIRATE applicables aux opérateurs du secteur en question.

Typologie des SAIV et attribution des rôles
Un secteur d'importance vitale est composé d'activités qui ont trait à la production et à la distribution de biens ou de services indispensables, ou qui présentent potentiellement un danger grave pour la population. (Art. R.1332-2 et suivants du Code de la Défense). Les 12 domaines d'activités concernés et les ministres coordonateurs associés sont identifiés dans l'arrêté du 2 juin 2006 : (1) activités civiles de l'État, (2) activités judiciaires, (3) activités militaires de l'État, (4) alimentation, (5) communications électroniques, audiovisuel et information, (6) énergie, (7) espace et recherche, (8) finances, (9) gestion de l'eau, (10) industrie, (11) santé, (12) transports.

Conjointement à cet arrêté, Michèle Alliot-Marie, ancien Ministre de l'Intérieur, a évoqué la possibilité d'intégrer Internet comme 13ème SAIV lors du Forum International sur la Cybercriminalité du 24 mars 2009. Cette proposition n'a pour l'instant pas fait l'objet d'une étude plus approfondie, et nécessite préalablement de s'interroger sur la façon dont un domaine aussi vaste et illimité qu'Internet pourrait fait l'objet d'une directive.
A chaque SAIV correspond un opérateur d'importance vitale (OIV) qui peut être une entreprise, une association ou encore une fondation. C'est lui qui nomme un Délégué pour la Défense et la Sécurité qui devra être habilité Confidentiel Défense. Le Délégué devient ainsi l'interlocuteur principal du ministre coordonnateur.

Processus de mise en œuvre d'une DNS
Après habilitation Confidentiel Défense du Délégué pour la Défense et la Sécurité, l'opérateur d'importance vitale reçoit la DNS par son ministre coordonnateur. L'opérateur peut alors élaborer son plan de sécurité, un plan particulier de protection par point d'importance vitale, et éventuellement un plan particulier de protection de zone d'importance vitale. Après approbation et validation des plans, c'est à lui qu'il revient de les mettre en œuvre à travers des mesures concrètes physiques (vigiles, clôtures, serrures, caméras de surveillance, détecteur de produits toxiques, alarmes, moyens de secours) et d'organisation (vérifications plus approfondies à l'embauche, gestion des visiteurs, contrôles des livraisons, flux de circulation, ressources de substitution, etc.).
Le **plan de sécurité d'opérateur (PSO)** a pour but de décrire l'organisation et la politique de sûreté et de sécurité de l'opérateur, en s'appropriant le contenu de la directive à travers l'analyse de risques propre au secteur d'activités. La première version du plan de sécurité d'opérateur doit être présentée au ministre coordonnateur compétent dans un délai de 6 mois à compter de la date de notification de la DNS.
Le **plan particulier de protection (PPP) du point d'importance vitale** s'appuie sur la directive et sur le PSO. Il comporte une analyse de risques et présente les mesures de protection conformes aux objectifs de sécurité fixés par la DNS. Celles-ci peuvent être consignées sous forme de fiches réflexes.
Enfin, selon les secteurs d'activités, le Délégué réalise un **plan particulier de protection (PPP) de la zone d'importance vitale**. Ce document présente des mesures communes de protection, en cohérence avec les mesures décrites dans le plan particulier de protection des points d'importance vitale. Il dispose d'un délai de 2 ans maximum pour présenter son plan au préfet de département ou au préfet coordonnateur, à compter de la date de notification de la DNS.

Conclusion : DNS et culture sécurité : dilemme ou opportunité ?
Il semble évident que le déploiement des DNS au sein des entreprises des Secteurs d'Activités d'Importance Vitale oblige, du moins nécessite, d'intégrer une culture de défense, gouvernementale, et surtout

transversale qui ne correspond pas, a priori, à la culture de l'entreprise. En attribuant aux acteurs du secteur privé un rôle essentiel dans la protection de l'intégrité du pays et des citoyens, les DNS ne participent-elles pas à la construction d'une culture de « sécurité globale » au sein même des entreprises ? Car si elles peuvent effectivement s'immiscer dans les affaires du secteur privé (rappelons que leur application est obligatoire), elles constituent davantage une opportunité de développer une culture des risques « démocratique », autrement dit accessible à tous, et où chaque collaborateur participe à un effort de sécurité collectif. Car l'impact des DNS en termes de culture des risques se situe bien là : participer à l'émergence d'une culture de sécurité globale, intégrant nécessairement une bonne connaissance des risques et des comportements adaptés de veille et d'intelligence, au sein des entreprises ; et surtout leur donner l'opportunité de faire évoluer elles-mêmes, en fonction de leur contexte, de leurs objectifs et de leurs ressources techniques et humaines, leur propre culture sécurité.

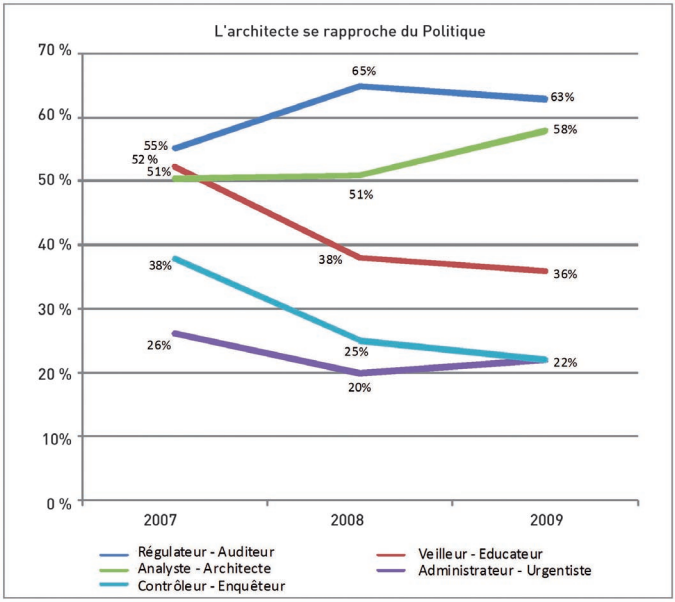
3.6. La culture par les ressources humaines

3.6.1. Rôle des professionnels

Nous abordons ici une des caractéristiques plus « personnelle » de l'enquête. Les acteurs qui incarnent la fonction Sécurité au quotidien, jouent un rôle, qui traduit aussi une forme de culture : Politique ou Gendarme ? Technicien ou Educateur ? Manager ou Expert ? Ou l'ensemble ?

Le schéma ci-dessous présente la cartographie des « 2 fonctions clés » assumées par le panel. Il confirme les tendances des années précédentes et apporte une confirmation importante.

- C'est désormais 80% du panel qui est impliqué au plan du pilotage beaucoup plus que sur des questions opérationnelles.
- La fonction clé de « veilleur – éducateur » assumée par les RSSI pendant longtemps, et notamment au début de leur mission, est désormais largement sous-traitée à des spécialistes.
- La fonction clé d'« analyste – architecte » devient plus que jamais politique pour ne pas dire stratégique : proche des métiers, des choix de technologies, de fournisseurs, etc.



La culture des risques informatiques / informationnels prend sa véritable valeur par une attribution très régalienne et stratégique de la fonction, proches des pouvoirs de décision. Ce n'est pas tant une question de rattachement hiérarchique, que d'attribution de missions avec les moyens associés !

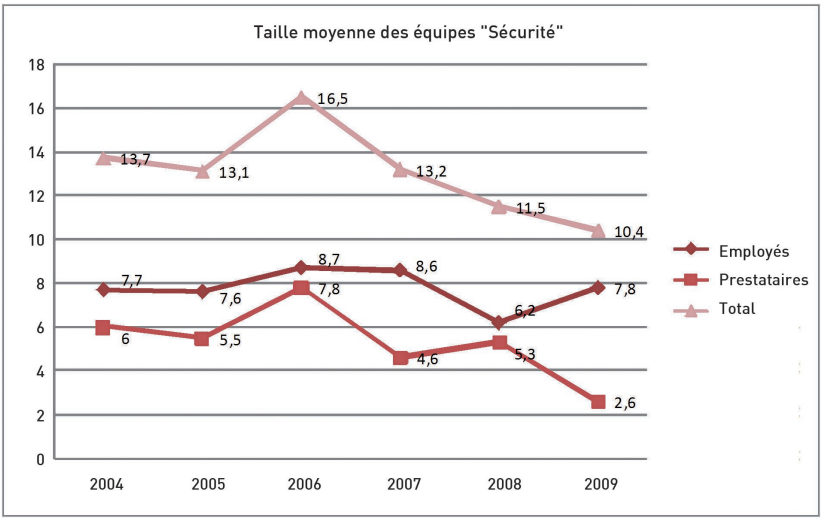
En cohérence avec les actions de pilotage, les professionnels se doivent de donner des résultats et de répondre aux besoins « métiers ». L'analyste / architecte devient plus stratégique.

3.6.2. Taille des équipes

Autre chiffre « phare » des enquêtes du Cercle, l'évolution de la population de professionnels en entreprise traduit les efforts consentis au plan humain et l'équilibre à trouver entre collaborateurs internes et prestataires. C'est aussi une question de culture !

Depuis 6 ans maintenant, nous avons pu déterminer une valeur moyenne des équipes « Sécurité », qui tend à diminuer régulièrement du fait de l'élargissement du panel à de plus petites structures. Cette tendance se confirme encore cette année malgré l'anomalie de 2006 où le poids des prestataires avait été très important.

Par rapport à 2008, le nombre de professionnels « solitaires » a considérablement baissé passant de 26% à 4% alors que les « binômes » stagnent autour de 20%.



Les fluctuations entre collaborateurs et prestataires sont importantes. Si l'influence du panel est l'hypothèse la plus probable en 2008, la conjoncture et la crise économique ont peut être justifié un renforcement des ressources internes et la baisse (très significative) des prestataires.

Cependant, ces chiffres globaux ne doivent pas masquer des différences très importantes entre secteurs d'activité et aussi en fonction des champs d'action géographiques (voir tableaux ci-dessous).

Collaborateurs internes	7,5	7,8	6,4
Prestataires	8,2	2,3	1,5
Total	15,7	10,1	7,9

Zoom par secteur d'activité

L'évolution quantitative des professionnels en entreprise trouve son explication dans la croissance des efforts du secteur « banques / assurances » (effets de l'affaire Kerviel ?), tandis que l'Industrie et l'Administration / Services publics semblent avoir considérablement réduit le nombre de leurs prestataires. Mais tout ceci reste des moyennes à prendre avec précaution. Encore une fois, l'élargissement du panel explique sans doute plus certainement ces évolutions.

Collaborateurs internes	7,1	5	10
Prestataires	2,8	2,1	2,3
Total	9,9	7,1	12,3

Zoom par zone géographique d'activité

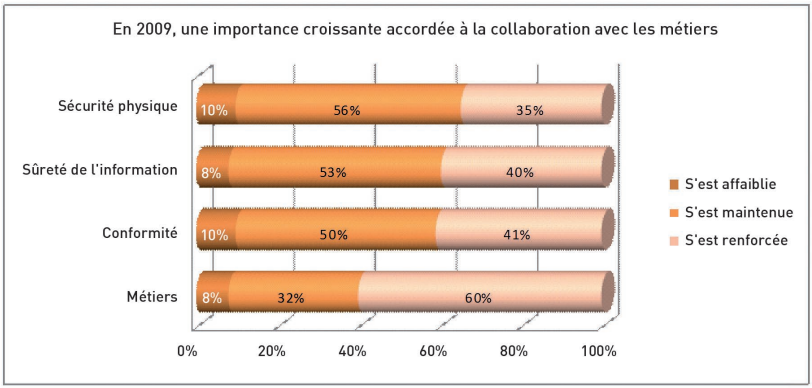
L'impact de la couverture géographique de l'activité du panel est aussi intéressant car on constate :
- Qu'œuvrer à l'international procure une taille significative de collaborateurs internes (bonne connaissance des métiers et des cultures).
- Que les équipes « européennes » sont les moins importantes.
- Que les professionnels travaillant uniquement au plan national font le plus appel à des prestataires.

Le secteur Banque / Assurance a renforcé ses équipes en 2009 alors que l'Industrie apparaît en retrait. Le poids des prestataires (à temps plein) s'est considérablement réduit.

3.6.3. Coopération avec les métiers et autres activités

Pour traduire la culture des risques informatiques et informationnels, nous avons questionné le panel sur l'évolution de leur collaboration avec les autres entités / activités internes concernées et notamment avec les métiers.

Le bilan est très contrasté comme l'atteste le schéma ci-dessous. Si 10% du panel environ notent une détérioration de la situation, la moitié du panel maintient une relation que l'on supposera acceptable. Il faut néanmoins positiver ce constat et noter qu'environ 40% des professionnels améliorent leur relation avec la conformité, la sécurité physique et la sûreté de l'information et qu'avec 60% des réponses, ce sont les métiers qui devraient le plus profiter de cette amélioration.



Une analyse par secteur d'activité, apporte un éclairage plus précis sur ce constat comme le démontrent les chiffres ci-dessous.

Métiers	72 %	55 %	39 %
Conformité	59 %	33 %	23 %
Sûreté de l'information	41 %	44 %	29 %
Sécurité physique	34 %	38 %	35 %

Zoom par secteur d'activité

Le secteur de la Banque / Assurance est celui pour lequel la coopération continue de se renforcer avec les métiers et la conformité, et globalement de manière supérieure à l'ensemble du panel. Etait-elle moindre ? Pour les autres secteurs d'activité, il est notable que l'Industrie apparaît très en retrait par rapport aux autres secteurs pour 3 des 4 aspects de cette coopération. Signe d'une maturité organisationnelle plus forte ? Avec 16% de réponses, la coopération s'est le plus détérioré avec les métiers dans l'Administration / Services publics et avec la sécurité physique dans l'Industrie.

L'analyse selon la couverture géographique de l'activité des professionnels ne présente pas d'écarts significatifs par rapport à l'ensemble du panel.

La fonction sécurité renforce globalement ses positions au sein des organisations avec de fortes disparités. C'est avec les métiers que les synergies se développement le plus.

3.6.4. Avis d'expert : casting des membres d'une cellule de gestion de crises (Isabelle TISSERAND – Coordinatrice du Cercle Européen de la Sécurité et des Systèmes d'Information)

Comment sélectionner, recruter, former et entraîner les membres de nos cellules de gestion de crises : telles sont les questions qui se posent à tous les responsables de la sécurité des systèmes d'information à l'heure des mises en oeuvre de directives nationales de sécurité[1].

La structuration **d'une cellule de gestion de crises S.I.**, quelle que soit sa configuration car toutes sont uniques et faites sur mesure, détermine une grande partie des critères de sélection, de recrutement et d'entraînement. Les représentants des Direction Sécurité de l'Information, Sécurité des Systèmes d'Information, télécommunications et communication de crise forment -dans le modèle étudié ici-, le noyau dur de la cellule. Ces piliers doivent, en phase d'action, pouvoir compter sur un collège d'experts capables de les assister : analyse, conseil, support technique et comportemental en matière de droit des nouvelles technologies de l'information et de la communication, veille informationnelle et renseignement, direction des ressources humaines, logistique, services de santé au travail. Le collège peut être étendu selon la nature et les activités de l'environnement (direction financière, déontologie, etc.) Tous les membres doivent avoir un binôme pour la relève en cas d'indisponibilité des uns ou des autres. Tous doivent disposer d'installations et d'instruments de gestion de crises efficaces.

La **sélection des membres** de la cellule ne s'appuie pas uniquement sur les compétences professionnelles avérées (« savoir être stratégique » et « savoir être opérationnel ») En effet, un certain nombre de qualités physiques, psychologiques et sociales garantissent les succès de fonctionnement de cette dream team qui doit être hyper performante et créative en cas de chaos, situation de laquelle elle doit faire un émerger un nouvel ordre modifié pour le plan de continuité des activités après sinistre.

Les **qualités physiques** sont essentielles dans des situations de travail de longues durées, ceci dans des conditions parfois tendues qui appellent de forts niveaux de résistances et d'adaptation (manques de confort sanitaire, de sommeil et alimentaire notamment).

Les **qualités psychologiques** sont éminemment importantes. La structuration, l'équilibre, la stabilité, l'empathie, la résistance aux stress mental et occupationnel, les capacités à garder un regard critique sur soi et sur la situation (distanciation), à coopérer à un projet commun, à construire l'espace de confiance sont indispensables. On peut aller jusqu'à évaluer -voire exiger- des qualités neuropsychologiques spécifiques chez les candidats (niveaux de résilience après chocs, réhabilitation après sinistres, etc.) selon la nature des missions de la cellule de gestion de crises.

Les **qualités sociales** requises pourraient se résumer à la capacité de composer avec les autres au cours de deux séquences spatio-temporelles très particulières : celles de la gestion de crise et du retour à la norme ; autrement dit de participer à la volonté d'émergence du « cerveau collectif », à la praticité de l'intelligence mutualisée. Le professionnalisme, l'humilité, la solidarité, la capacité d'écoute et de partage des connaissances, l'empathie, le sens de la négociation, le sens de la confidentialité -voire du secret- sont des garanties recherchées.

Le **moment de sélection** est crucial. Il consiste à qualifier et à quantifier les compétences professionnelles, les pouvoirs de décisions, la motivation, les expériences passées, l'épaisseur du sentiment d'appartenance à l'entreprise, le sens de l'intérêt général, etc. Autant de traits que l'on ne trouve pas forcément au complet au moment du repérage mais que l'instructeur peut juger potentiels, c'est-à-dire développables avec un entraînement.

---

[1] Les mises en oeuvre des Directives Nationales de Sécurité ont pour objectif de garantir de bons niveaux de continuité en cas de sinistre majeur. La structuration de cellules de gestion de crises fait partie du processus organisationnel des mises en oeuvre.

Dans le modèle étudié, le **recrutement** a lieu une fois que le responsable de la cellule de gestion de crises a approuvé la sélection et que les membres élus aient accepté les engagements proposés (disponibilité, déontologie, etc.)

Les phases de **solidification et de lancement de la cellule de gestion de crises** incluent un **entraînement** préalable complet. Celui-ci est **comportemental, technique, transversal** (intermétiers).
Dans nos domaines d'exercice, il n'est pas commun de commencer par un entraînement humain des professionnels de la SSI (mises en situations extrêmes associant des exercices physiques, pschiques et sociaux) C'est donc de l'intérêt de repenser les modalités de préparation des cellules de gestion de crises S.I. dont nous débattrons en exclusivité lors de l'atelier ***« Directives Nationales : faut-il être habilités ? »*** pour vous, à Monaco. Les intervenants, tous issus du monde de la Défense (Commandos de Marine, Forces Spéciales) vous présenteront leurs approches, utiles et possibles à mettre en oeuvre pour l'efficacité des cellules de gestion de crises S.I. dans le cadre des mises en oeuvre des 3 directives nationales de sécurité parce que celles-ci induisent de forts niveaux de stress et génèrent de nombreuses crises qu'il convient d'apprendre à gérer.

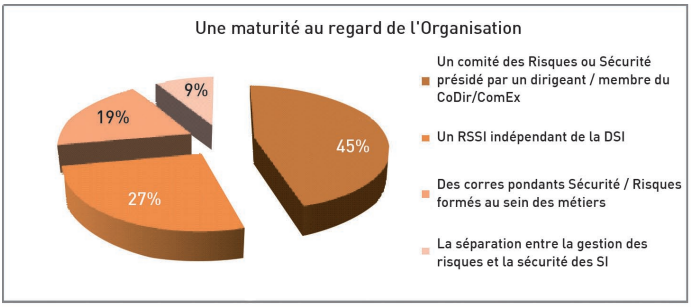
3.7. Quelle maturité globale ?

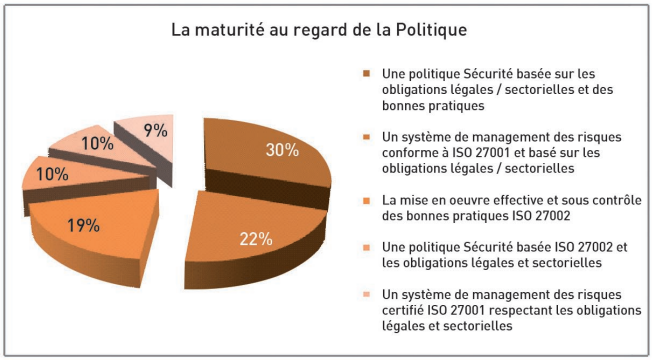
Pour tenter de qualifier au mieux la culture des entreprises et administration, nous avons posé des questions visant à déterminer leur maturité en gestion des risques informatiques / informationnels selon 5 critères.

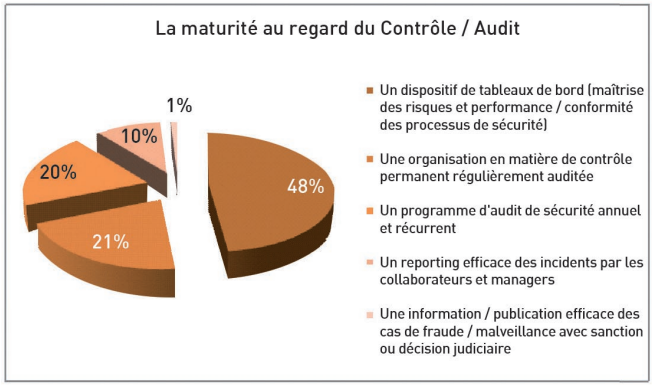
- L'organisation
- La politique et la réglementation
- Le contrôle et l'audit
- La démarche « projet »
- Les bonnes pratiques au quotidien

Autrement dit, pour chaque axe d'analyse, qu'est-ce qui peut déterminer objectivement, de manière visible, la culture d'une entreprise sur les risques informatiques / informationnels, au-delà de ce qui a été analysé aux chapitres précédents ?

Les 5 graphiques des pages suivantes présentent les statistiques obtenues pour l'ensemble du panel. Un tableau indique ensuite les divergences significatives selon les 3 secteurs d'activité analysés.







Sur ces trois paramètres, le panel considère qu'une culture des risques passe par cinq points de « maturité » ou de « maîtrise » :

- L'implication d'un dirigeant au sein d'un Comité des risques ou de la Sécurité
- Une fonction « SSI », régalienne et indépendante de la DSI
- La prise en compte des obligations réglementaires comme levier de la démarche
- La mise en œuvre et le respect des normes ISO 2700x
- Un dispositif de tableaux de bord en termes de maîtrise des risques et de performance / conformité des processus de sécurité

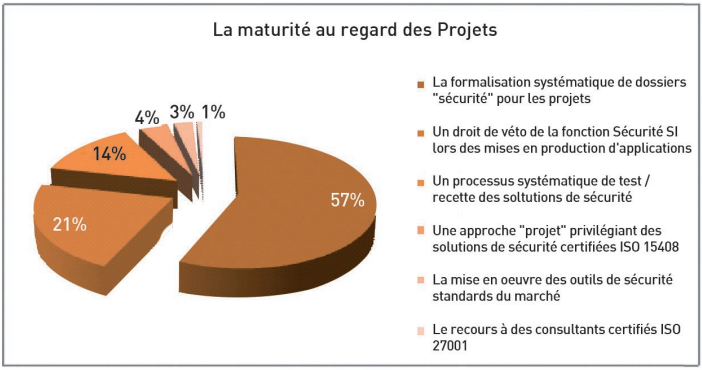
Mais des divergences significatives apparaissent lors d'une analyse par secteur d'activités.

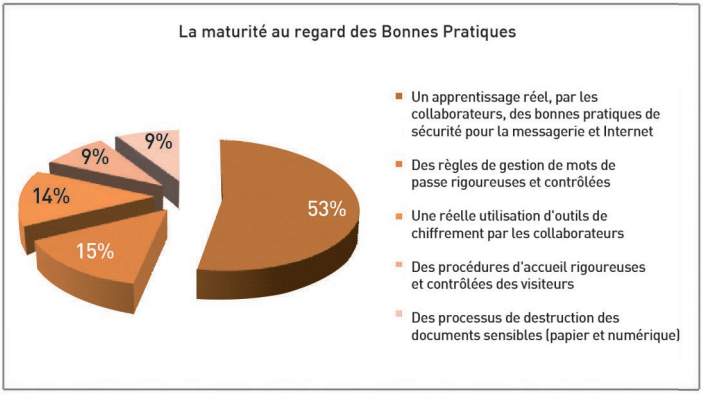
Comité des Risques ou Sécurité	41 %	43 %	30 %
Fonction « SSI indépendante de la DSI	21 %	21 %	33 %
Démarche basée sur obligations réglementaires	29 %	29 %	40 %
Système de management conforme ISO27001	19 %	26%	13 %
Dispositif de tableaux de bord	35 %	49 %	60 %

Zoom par secteur d'activité

Deux autres aspects, plus opérationnels et quotidiens ont été soumis à l'appréciation du panel (voir schémas ci-dessous). Ainsi, la maturité d'une entreprise, et de manière sous jacente, sa culture, sera appréciée concrètement par :

- La formalisation systématique de dossiers « sécurité » pour les projets
- Un apprentissage réel par les collaborateurs des bonnes pratiques de sécurité pour Internet et la messagerie





Mais des divergences significatives apparaissent lors d'une analyse par secteur d'activités.

Formalisation des dossiers sécurité des projets	49 %	62 %	50 %
Apprentissage réel des bonnes pratiques	43 %	56 %	63 %
Gestion rigoureuse de mots de passe	14 %	21 %	7 %

Zoom par secteur d'activité

Le lien entre la maturité observée et culture des risques informatiques / informationnels n'est pas très complexe. Indépendamment des risques encourus ou de contextes spécifiques, les 7 paramètres mis en évidence par le panel décrivent l'art de gérer les risques aux plans stratégique et opérationnel, malgré une importance variable, néanmoins, selon les secteurs d'activité.

3.8. En synthèse

Le bilan de la culture des risques proposée dans ce premier chapitre apporte des confirmations et des éléments instructifs.

Côté confirmations, il est difficile de parler de la culture des risques, mais plus aisément des cultures des risques et ce pour deux raisons :

1. Dans notre domaine, les risques sont extrêmement nombreux et variés. Leur traitement nécessite des approches ciblées. Et l'humain n'en a pas toujours la même perception et n'aura pas non plus la même implication selon les efforts requis et les contraintes.
2. Si les statistiques globales apportent un éclairage cohérent, des divergences notables existent entre les secteurs d'activité et comme on l'a vu aussi, en fonction d'une implication plus ou moins internationale des acteurs.

Enfin, trois points méritent d'être mis en évidence :

- Les risques « redoutés » s'adressent prioritairement aux individus (clients, usagers) montrant un souci moindre du collectif et de l'entreprise.
- Néanmoins, la tendance est de renforcer la prise en compte des préoccupations des métiers, et ne plus traiter des risques informatiques éloignés des aspects « business ».
- Au plan du management, la culture des risques peut être aisément caractérisée par 7 facteurs clairement mis en évidence par les participants, malgré quelques divergences notables, pour l'Industrie en particulier.

4- DEVELOPPEMENT DE LA CULTURE DES RISQUES

La 2ème partie du Livre Bleu des Assises 2009 va chercher à répondre à une question clé : « comment développer la culture des risques informatiques / informationnels ? » sachant que :

- Comme nous venons de le voir, elle est variable dans le temps et l'espace. Elle est souvent liée à une situation particulière des organisations.
- Comme cela a été indiqué l'année dernière dans le Livre Bleu consacré à la Sécurité globale, à l'heure des pandémies, du terrorisme et de la cybercriminalité, les frontières tendent à ne plus exister. L'influence géographique ne sera pas analysée ici.
- L'existence de secteurs stratégiques (Infrastructures vitales) et les différences de moyens attribués entre les secteurs d'activité, entre grandes entreprises, administrations, PME, tissu associatif, etc. ne devrait pas conduire à une approche unique et uniforme pour la mise en œuvre des actions adaptées.

Nous allons analyser les perspectives de développement de la culture selon trois paramètres :

- La dimension managériale
- Les actions possibles en termes de communication / sensibilisation
- Le rôle des acteurs publics et privés

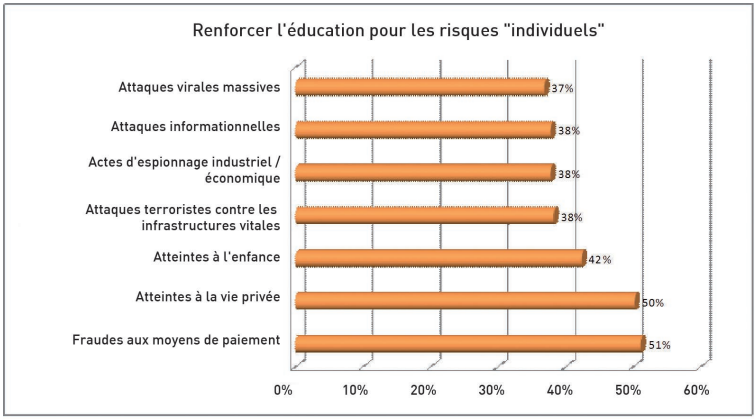
4.1. Risques majeurs et implication des décideurs

Nous avons sollicité le panel pour connaître leur appréhension des risques majeurs pour lesquels le développement de la culture était un enjeu important, et en quoi, les décideurs avaient un rôle, même limité, à jouer.

4.1.1. Quels risques majeurs à intégrer ?

Les répondants ont indiqué ici les 3 risques majeurs pour lesquels il fallait développer et renforcer la culture des individus. Si aucun des choix proposés ne ressort fortement, deux sont cités par la moitié du panel : moyens de paiement et données personnelles / vie privée. Voilà les enjeux prioritaires en termes d'éducation !

Il est remarquable de noter que ce sont des préoccupations très « personnelles » (comme celle arrivée en 3ème position sur la protection de l'enfance) qui dépassent celles, plus collectives, touchant plus globalement des organisations entières (38% des réponses).



Une analyse par secteur d'activité apporte un éclairage intéressant et montre des différences importantes.

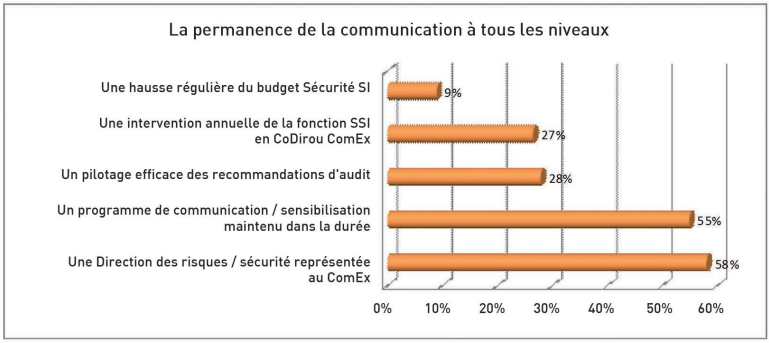
- Le poids de la Banque / Assurance dans le panel, qui place la fraude aux moyens de paiement en tête (avec 66%), se fait ici particulièrement sentir.
- L'Administration / Services publics répartit très uniformément ses réponses et place en tête les attaques virales et les atteintes à la vie privée (45%).
- L'Industrie redoute plus fortement les attaques informationnelles (52%) et l'espionnage (55%).

4.1.2. Quelle influence et quelle implication des décideurs ?

Une fois que la conscience des risques à aborder est intégrée, en se focalisant sur ce que l'on redoute le plus, quel peut-être le rôle des décideurs, pour veiller à ce que la culture de ces risques se maintienne et se développe ?

Ici aussi, nous avons demandé à quel niveau pouvait se situer l'action. C'est au plan de la gouvernance et de la communication / sensibilisation que la priorité doit se situer. S'améliorer par des pratiques d'audit, par le soutien annuel d'un Comité de Direction ou par des budgets croissants ne recueille pas une très forte adhésion.

En revanche, un dirigeant incarnant la fonction « risque / sécurité » associé à des actions planifiées et régulières de communication / sensibilisation semblent représenter le meilleur cocktail pour notre panel, afin de garantir le développement de la culture des risques. Un lien avec les dirigeants et une diffusion auprès des collaborateurs apparaît en effet comme une approche idéale.



Il n'y a pas de différence notable entre secteurs d'activité. Mais on notera néanmoins, une petite singularité pour la banque / assurance qui positionne la hausse des budgets Sécurité à 13%.

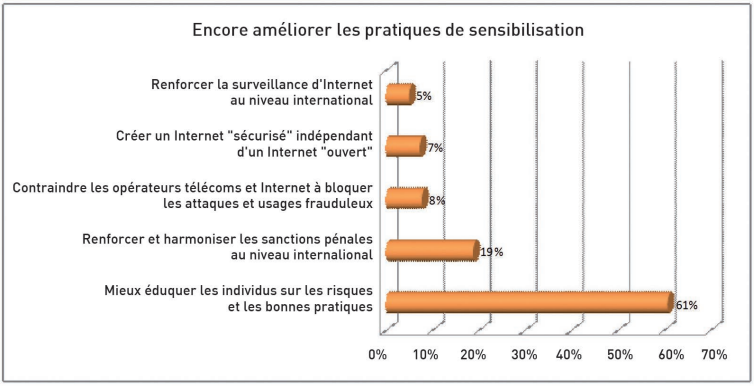
4.2. Quelles actions les plus efficaces ?

Au-delà des actions de communication / sensibilisation, que nous aborderons spécifiquement, nous avons sollicité le panel pour identifier d'autres actions, plus structurelles, qui auraient un impact global sur le développement d'une culture des risques.

4.2.1. Pour lutter contre la cybercriminalité

Le panel positionne l'éducation comme le meilleur rempart face à la cybercriminalité. Conscience de l'insuffisance des mesures technico-juridiques, qui atteignent leurs limites ? Mais ce sont les autres choix proposés que nous analysons ici. Entre le renforcement de pratiques existantes ou en cours (surveillance d'Internet, harmonisations pénales) et d'autres plus « avant-gardistes » (Internet « sûr » distinct d'un « ouvert » ou « nettoyage » industriel mené par les opérateurs), c'est l'approche « juridique » qui semble la plus judicieuse pour le panel. Dans la plus pure tradition française voire européenne.

Mais le choix privilégié, « mieux éduquer », indique surtout qu'il faut améliorer les pratiques en la matière. Ce n'est pas qu'une question de volume ou de puissance. Le panel indique sans doute, la recherche d'une plus grande efficacité !

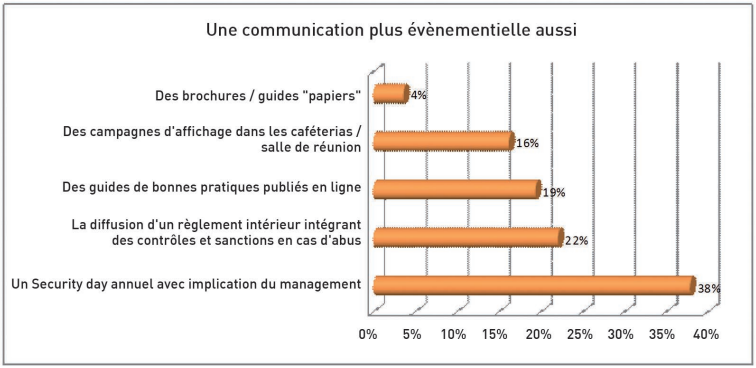


L'approche éducative doit encore s'améliorer, autant sur la forme que sur le fond.
La question n'est pas d'éduquer, mais de bien éduquer.
Sans oublier que c'est une solution particulièrement économique !

4.2.2. En termes de communication

Nous avons proposé au panel une liste de 5 actions possibles orientées « communication » (transmission d'un « savoir » auprès du plus grand nombre). Les résultats obtenus sont sans équivoque. Une solution « évènementielle » (la journée « Sécurité ») se détache assez nettement, alors qu'elle n'est pas extrêmement développée.

Elle est suivie par 3 actions aux vocations très différentes. La diffusion de la charte (idéalement par courrier) aura une portée juridique forte alors que des affiches, bien visibles, peuvent s'apparenter à de la « pub » pour la SSI. Enfin les guides publiés en ligne n'offrent aucune garantie quand à leur lecture, voire leur application.



Une analyse par secteur d'activité apporte ici un éclairage intéressant avec des différences notables pour 3 types d'action.

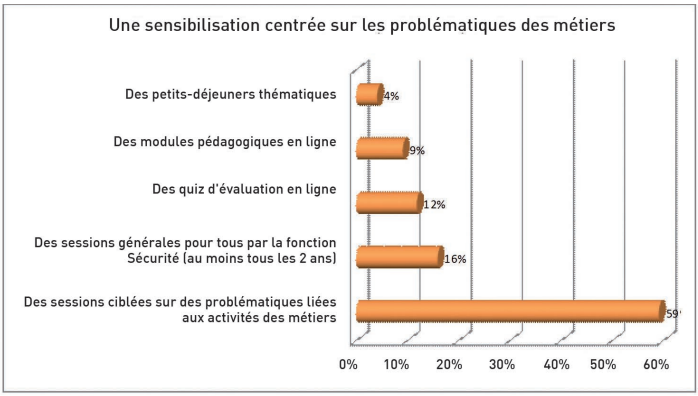
Security day annuel	26 %	48 %	48 %
Guides de bonnes pratiques en ligne	19 %	23 %	10 %
Campagne d'affichage	21 %	10 %	13 %

Zoom par secteur d'activité

La Banque / Assurance répartit assez uniformément les actions proposées autour de 20 %, tandis que l'Administration / Services publics et l'Industrie mettent bien l'accent sur l'évènement annuel.

4.2.3. En termes de sensibilisation

Nous avons proposé au panel une liste de 5 actions possibles orientées « sensibilisation » (amélioration du « savoir être »). Ici aussi, les résultats obtenus sont sans équivoque. L'enjeu est désormais de s'adresser aux métiers, sur leurs problématiques spécifiques, sans discours généraux et théoriques. Les autres solutions proposées apparaissent alors comme complémentaires et variables d'ajustement ou de renouvellement.



Cependant, une analyse par secteur d'activité apporte, ici aussi, un éclairage intéressant et montre des différences importantes.

Sessions ciblées	49 %	65 %	74 %
Modules pédagogiques en ligne	13 %	3 %	6 %
Quiz d'évaluation en ligne	16 %	10 %	6 %

Zoom par secteur d'activité

L'Industrie, et l'Administration / Services publics dans une moindre mesure, maintiennent une approche classique, en sessions, tandis que la Banque / Assurance a franchi le pas des solutions « en ligne » (près de 30% des réponses).

Ici aussi, il faut considérer les actions les moins citées, comme des outils complémentaires à la solution idéale, qui n'est pas toujours simple à mettre en œuvre (coût, disponibilité du personnel, planification).

La clé du développement de la culture des risques repose sur une approche plus évènementielle et engageante, proche des préoccupations des métiers (clients, usagers).

4.2.4. Avis d'expert : les apports de la communication engageante (Michel GERARD – PDG Conscio Technologies)

Une campagne de sensibilisation nécessite avant tout de faire preuve de pédagogie, d'informer et d'expliquer les enjeux, les risques et les règles à suivre. L'objectif ultime d'une telle campagne, cependant, est bien d'agir sur les comportements et de faire en sorte que ceux-ci soient bien conformes aux règles de sécurité et aux bonnes pratiques. **Alors comment agir efficacement sur les comportements ?**

Depuis cinquante ans les chercheurs en Sciences Humaines et Sociales (en particulier en psychologie sociale) s'intéressent à cette question. En 2005, lors de premiers travaux sur cette problématique dans le contexte de la Sécurité SI, nous avions pris contact avec Robert-Vincent Joule, directeur du laboratoire de psychosociologie de l'Université de Provence et auteur de nombreuses publications et ouvrages sur le thème : « Comment obtenir d'une population donnée les comportements que l'on attend d'eux ? ».

Plusieurs séances de travail ont permis d'adapter les principes développés par Robert-Vincent Joule aux questions de sensibilisation à la sécurité SI. Qu'en retenir ?

Les recherches montrent d'abord les limites de **l'autorité**.

L'ombre du bâton disparue, chacun retrouve peu ou prou ses mauvaises habitudes. Cela peut facilement se comprendre. Si dans une organisation donnée un collaborateur se comporte dans telle ou telle situation comme un agent de pouvoir l'exige, il peut éviter d'en appeler à ses valeurs ou à ses propres motivations pour expliquer ce qu'il fait, car il dispose d'une raison « externe » toute prête : éviter une punition. Les changements obtenus autoritairement ne sont pas durables. Si, en matière de sécurité, l'autorité est évidemment, nécessaire, elle n'est en aucun cas suffisante.

Les recherches montrent ensuite les limites de l'**information et de la persuasion.**

Pourtant, l'information et la persuasion, peuvent s'avérer très efficaces pour modifier les idées que quelqu'un peut avoir sur telle ou telle question. Malheureusement, il ne suffit pas d'avoir les « bonnes idées » pour avoir les « bons comportements ». Il ressort d'une très sérieuse étude longitudinale réalisée il y a quelques années aux Etats-Unis que la probabilité d'être fumeur à 17 ans n'est pas plus faible chez des élèves ayant pourtant suivi pas moins de 65 séances de « sensibilisation » entre 8 ans et 17 ans (condition expérimentale) - et donc parfaitement informés des méfaits du tabac – que chez des élèves n'ayant pas suivi ces séances (condition contrôle). Et cette étude n'est qu'une des très nombreuses recherches qui illustrent le décalage qu'il peut y avoir entre nos idées – en l'occurrence nos « bonnes idées » - et nos actes. Evidemment, cela ne signifie pas qu'informer ne sert à rien ou qu'argumenter ne sert à rien. L'information et l'argumentation servent incontestablement au fil du temps à modifier les savoirs, les idées, les attitudes et même, certainement, à provoquer de réelles prises de conscience. Il reste que, pas plus que l'autorité, elles ne sont suffisantes.

Heureusement les recherches montrent aussi qu'il suffit parfois de peu de chose pour passer des idées aux actes. Et les chercheurs n'ont pas manqué de faire de ce peu de chose un objet d'étude privilégié, si bien qu'on dispose aujourd'hui de tout un savoir scientifique sur lequel on peut s'appuyer pour gagner en efficacité. Robert-Vincent Joule et Jean-Léon Beauvois, deux chercheurs français réputés et auteurs de nombreux ouvrages, ont contribué à faire avancer les connaissances sur cette question. Dans leur ouvrage de référence, ils font état d'une bonne dizaine de techniques qui permettent d'aider autrui à modifier librement ses comportements (cf. Joule et Beauvois, 2002).

Ces techniques passent pour la plupart par l'obtention d'un petit comportement, très facile à obtenir tant il est peu coûteux, mais qui va prédisposer celles et ceux qui l'ont réalisé à en réaliser d'autres, par la suite, bien plus coûteux. La dynamique de changement est ainsi enclenchée. C'est la raison pour laquelle ces petits comportements, qui sont à la base même du processus de changement

sont appelés : « comportements préparatoires ». L'intérêt de ces techniques, est de conduire à la responsabilisation des acteurs qui en arrivent à prendre librement les engagements que l'on attend d'eux, à les assumer, et à intérioriser les traits ou les valeurs qui vont assurer la pérennité de leurs nouvelles conduites. C'est dire l'intérêt de ces techniques dont l'efficacité est démontrée dans de nombreux domaines de la vie sociale (cf. notamment, Joule et Beauvois, 1998).

La notion d'engagement est ici centrale comme le résume l'extrait d'un texte de Robert-Vincent Joule sur : **LA PSYCHOLOGIE DE L'ENGAGEMENT**.

C'est dans la psychologie de l'engagement qu'il convient de rechercher l'assise théorique sur laquelle reposent les principales techniques permettant d'**obtenir sans imposer**. Gardons en mémoire que c'est la situation qui, en fonction de ses caractéristiques objectives, engage ou n'engage pas l'individu dans ses actes.

Définitions de l'engagement
« L'engagement correspond, dans une situation donnée, aux conditions dans lesquelles la réalisation d'un acte ne peut être imputable qu'à celui qui l'a réalisé. » (Joule et Beauvois, 1998, p. 60).

Les effets de l'engagement
- *Sur le plan cognitif*, l'engagement débouche sur une consolidation des attitudes, et sur une plus grande résistance au changement (effet de gel), il peut même déboucher sur un meilleur ajustement de l'attitude à l'acte réalisé (effet de rationalisation).
- *Sur le plan comportemental*, l'engagement débouche sur une stabilisation du comportement et sur la réalisation de nouveaux comportements allant dans le même sens.
- Aussi, la psychologie de l'engagement propose-t-elle un éclairage théorique différent de certains processus psychologiques (appropriation, rationalisation, ou au contraire rejet, extrêmisation, etc.) en jeu dans les organisations, processus susceptibles de favoriser le changement ou, au contraire de le freiner.

Comment obtenir un fort engagement ?
On peut obtenir un fort engagement en jouant sur plusieurs facteurs :
- *Le contexte de liberté dans lequel l'acte est réalisé* : un acte réalisé dans un contexte de liberté est plus engageant qu'un acte réalisé dans un contexte de contrainte.
- *Le caractère public de l'acte* : un acte réalisé publiquement est plus engageant qu'un acte dont l'anonymat est garanti.
- *Le caractère explicite de l'acte :* un acte explicite est plus engageant qu'un acte ambigu.
- *L'irrévocabilité de l'acte* : un acte irrévocable est plus engageant qu'un acte qui ne l'est pas.
- *La répétition de l'acte* : un acte que l'on répète est plus engageant qu'un acte qu'on ne réalise qu'une fois.
- *Les conséquences de l'acte* : un acte est d'autant plus engageant qu'il est lourd de conséquences.
- *Le coût de l'acte :* un acte est d'autant plus engageant qu'il est coûteux (en argent, en temps, en énergie, etc.).
- *Les raisons de l'acte* : un acte est d'autant plus engageant qu'il ne peut être imputé à des raisons externes (par exemple : promesses de récompenses, menaces de punition) et qu'il peut être imputé à des raisons internes (par exemple : valeurs personnelles, traits de personnalité).

En conclusion, l'enjeu de toute démarche de sensibilisation dans le domaine du risque ou de la sécurité, où le facteur humain est clé, réside dans cette prise en compte des actes engageants, et des comportements préparatoires : se protéger soi même, c'est protéger les autres. Le comportement des autres me protège comme moi-même je participe à la sécurité d'autrui.

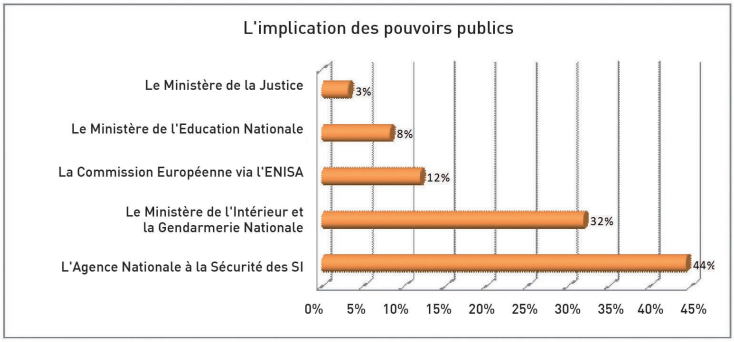
[1] Joule, R.V. & Beauvois, J.L. (2002). *Petit traité de manipulation à l'usage des honnêtes gens.* Grenoble : Presses Universitaires de Grenoble.
[2] Joule, R.V. & Beauvois J.L. (1998). La soumission librement consentie. Paris : Presses Universitaires de France.

4.3. Quelle implication des acteurs publics et privés ?

Dépassant la problématique spécifique aux entreprises et administrations, nous avons sollicité le panel afin de déterminer, qui étaient, selon eux, les acteurs les mieux placés pour améliorer et renforcer, de manière globale, la culture des risques informatiques / informationnels.

4.3.1. Les pouvoirs publics

La grande majorité du panel est d'origine française, et deux structures nationales se placent en tête avec une préférence pour la nouvelle Agence Nationale créée en juillet 2009. La question qui s'impose est : « Comment une structure transverse et une autre opérationnelle pourront-elles se répartir l'action dans le domaine ? »



Une analyse par secteurs d'activité ne montre qu'une seule singularité mais importante car elle concerne l'agence européenne (ENISA).

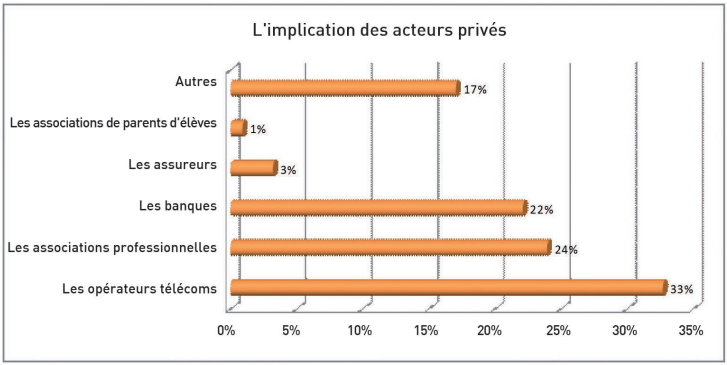
ENISA	17 %	5 %	10 %

Zoom par secteur d'activité

L'Administration / Service Public s'appuie naturellement plus sur les ressources nationales tandis que les Banques / Assurances considèrent une approche européenne assez intéressante, voire utile.

4.3.2. Les acteurs privés

L'étendue des choix proposés était importante et un seul était possible. Ainsi, les professionnels du panel ont eu une approche « opérationnelle » que l'on peut qualifier de bon sens. En effet, qui mieux que les opérateurs ou les banques sont les plus au contact des individus, voire des PME, là où se situe sans doute l'enjeu majeur ?



Néanmoins, des associations professionnelles, qui n'étaient pas spécifiées dans la question, apparaissent en 2nde position (24%) et une catégorie « autres » recueille 17%. Cet aspect de la problématique mériterait une analyse complémentaire, impossible ici. Quid de l'implication des médias ?

Pour les trois acteurs placés en tête, on constate des différences significatives en fonction des secteurs d'activité.

Opérateurs télécoms	31 %	42 %	26 %
Banques	25 %	19 %	32 %
Associations professionnelles	30 %	16 %	23 %

Zoom par secteur d'activité

On consultera en annexe, le bilan des rubriques d'information et sensibilisation en ligne proposées par l'Etat, les banques, les opérateurs et quelques associations. Instructif !

Deux acteurs nationaux (ANSSI et Ministère de l'intérieur) ont un rôle majeur à jouer et devront définir leur champ d'action respectif.
Côté privé, banques et opérateurs doivent agir fortement auprès de leurs clients alors que l'implication des associations professionnelles doit être précisée.

4.3.3. Avis d'expert : « L'impact des médias sur la culture des risques. » Nicolas ARPAGIAN

Parce que les journalistes ne doivent pas être les « idiots utiles » de la sécurité.

Entre 100 et 1 000 milliards de dollars par an. C'est selon les estimations publiées par l'OTAN au printemps 2009 le coût annuel de la cybercriminalité dans le monde. On ne peut pas dire que la photographie du phénomène se distingue par sa netteté ! Au contraire, même. Il semble difficile de trouver un autre domaine d'activité concernant d'aussi près à la fois le grand public, le secteur public et les entreprises de tous les secteurs, dont les contours soient aussi mal connus. Et pourtant... Si elle occupe régulièrement la une de l'actualité, la cybersécurité n'est généralement abordée que sous son aspect le plus spectaculaire. A l'instar, du jeune Albert Gonzalez arrêté aux Etats-Unis à la mi-août 2009 au motif qu'il est soupçonné d'avoir piraté les bases de données d'entreprises afin de récupérer quelque 130 millions de coordonnées bancaires destinées à la revente à des escrocs du Net. Un record qui n'a pas manqué d'occuper le terrain médiatique... quelques heures. Selon une gradation des sentiments déjà largement éprouvée : on commence par s'extasier sur les talents de l' « artiste », on s'inquiète ensuite d'un possible équivalent en France, on se rassure enfin en indiquant qu'il est désormais entre les mains de la justice... Et on passe à autre chose. Pas de quoi installer durablement dans les esprits une culture de la sécurité digne de ce nom. On est dans le registre de l'exceptionnel : sorte d'aléa imparable qui rendrait vain toute protection digne de ce nom. Un fatalisme technologique, en quelque sorte.

Nourrir l'hydre médiatique

Ce mode de traitement journalistique peut s'expliquer –sans pour autant se justifier- si on prend la peine de s'intéresser au mécanisme qui l'anime. Les technologies de l'information portent en elles un paradoxe majeur. Elles sont omniprésentes dans nos vies quotidiennes et professionnelles, sans que la plupart de ses utilisateurs en connaissent réellement le mode de fonctionnement. Avec en outre un fort sentiment d'impunité : comment un simple « clic » de souris pourrait –il s'avérer dommageable ? La peur de la contamination informatique s'éteignant généralement au moment où l'internaute ferme son ordinateur. Un peu comme le conducteur ayant bu un verre de trop qui est arrivé sans encombre chez lui, sans avoir causé d'accident ni subi de contrôle policier. Pour faire œuvre utile de pédagogie en matière de risque technologique, et cela vaut donc également en ce qui concerne l'informatique, deux qualités principales doivent être réunies par le journaliste chargé de lui faire écho.

Cela exige, d'une part, une certaine maîtrise des enjeux technologiques. Afin de comprendre les modalités d'organisation de l'univers dans lequel vont émerger les risques et menaces en question. Par exemple, il devra comprendre qu'il est vain de miser sur une recension des adresses IP des ordinateurs pour fonder l'application d'une loi, dès lors que des procédés multiples permettent aisément de masquer ou modifier cette plaque d'immatriculation attachée à chaque ordinateur. Sans être nécessairement docteur en informatique ou ingénieur, il est nécessaire de saisir les règles majeures de fonctionnement de la Toile. Et d'être en mesure de faire le tri parmi les propos tenus par ses interlocuteurs. Chacun ayant souvent tendance à lui suggérer un discours en phase avec ses intérêts. L'éditeur de solutions de sécurité, le fournisseur d'accès, l'assureur... les uns et les autres ont tous une bonne raison de livrer au journaliste un avis « intéressé ». Il lui revient en principe de faire le tri entre ces positions, pas toujours dénuées d'arrières pensées.

L'autre composante indispensable est assurément la mémoire. C'est-à-dire cette capacité à ne pas accepter systématiquement toute information du jour comme une nouveauté inédite. Avoir conscience de l'historique qui conduit tel acteur du marché à prendre telle ou telle décision, à faire telle ou telle annonce, apporte un précieux éclairage à l'actualité quotidienne. Et permet de prendre en conscience une plus juste mesure des risques volontiers présentés sous leur jour le plus dramatique. Par des professionnels de la communication ou des équipes commerciales en quête - largement compréhensible-

de performance. A chacun son rôle. Alors que les cybercommerçants ou les banquiers communiquent sur la sécurité des échanges sur le Net, les fournisseurs de solutions de sécurité, les auditeurs ès-sécurité et autres sociétés de service pourraient avoir tendance à noircir le tableau de la fiabilité de la circulation sur la Toile. Leur prospérité se nourrissant notamment de l'inquiétude collective.

Information & influence

Alors que ces thématiques des risques et de la cybersécurité se complexifient chaque jour davantage, la crise économique structurelle qui frappe les médias tous supports confondus conduit à une rétractation des effectifs permanents des rédactions. C'est-à-dire justement ces profils de professionnels de la presse dotés d'une mémoire du secteur et d'une expertise technique. Les médias choisissant alors de plus en plus de tendre le micro à un « expert » qui aura avant tout les talents d'un pédagogue, un discours synthétique comme exigé par les formats audiovisuels, et une grande disponibilité pour répondre au pieds levé. En ne s'interrogeant que rarement sur ce qui pourrait orienter le discours tenu par ledit « expert ». En clair, sans se poser systématiquement la question basique qui a fait les beaux jours des amphithéâtres de la Sorbonne au mois de mai 1968 : « d'où parles-tu, camarade ? ».

L'identification au plus juste des risques bénéficiera à tous les utilisateurs des technologies. Qu'il s'agisse du particulier ou des membres des états-majors des entreprises ou des administrations. Afin que ceux-ci prennent aussi en compte le volet sécurité, et autrement que comme une dépense dont on pourrait aisément se priver en période de ralentissement économique. Cette pédagogie du risque leur est donc également destinée. Mais les entreprises de presse, qui sont actuellement au cœur de profondes restructurations qui les voient délaisser les profils les plus expérimentés, ne pourront pas assumer seuls à l'avenir ce rôle de médiateur de l'information technique. L'avenir étant plutôt pour ces sujets techniques à des médias de niche, à la ligne de flottaison économique plus basse, qui seront vraisemblablement réservés à une minorité de lecteurs/auditeurs/internautes. Une perspective qui ne doit pas laisser indifférents les professionnels du secteur de la sécurité et de la gestion des risques.

[1] Nicolas ARPAGIAN est Rédacteur en chef de la revue Prospective Stratégique et Coordonnateur des enseignements *« Stratégies d'influence & Lobbying »* à l'IERSE. Chargé de cours à l'Institut des Relations Internationales et Stratégiques (IRIS) et à HEC, il est l'auteur de plusieurs ouvrages. Parmi lesquels : *Liberté, Egalité... Sécurité* (Dalloz, 2007), *Pour une stratégie globale de sécurité nationale* (Dalloz, 2008) et *La Cyberguerre – La guerre numérique a commencé* (Vuibert, 2009). www.cyberguerre.eu

[2] Rapport *L'Otan et la Cyberdéfense de Sverre Myrli* (Norvège) – réf. 027 DSCFC 09F. Assemblée parlementaire de l'OTAN, session de printemps 2009.

[3] Voir à ce propos: *Sur le Net, la cyberguerre est déjà déclarée.* Interview de Nicolas Arpagian par Bernard Poulet, L'EXPANSION, n°744, septembre 2009.

4.4. En synthèse

Le développement de la culture des risques sera garanti par un savant cocktail qui associera une bonne gouvernance (légitimité des messages) et une révision des pratiques anciennes (amélioration de la forme et des médias). L'usage de la radio et de la télévision restent quasi-inexistant à l'heure actuelle.

Le pré-requis consistera à prioriser les menaces et les dangers pour lesquels des actions de communication / sensibilisation doivent être menées. Face à la multitude et la variété des risques, il est vital de cibler ceux pour lesquels les individus ont ou auront un rôle majeur et pratique à jouer.

Quant à l'implication des acteurs, répétons ici que le rôle de l'Etat demeure essentiel mais que l'ANSSI et les forces de l'ordre devront bien répartir leurs efforts, et ne pas démultiplier les initiatives. Alors que côté privé, les banques et les opérateurs doivent encore mieux agir auprès de leurs clients.

Enfin, de son côté, la Commission Européenne a déjà lancé des actions au sein de l'ENISA. L'initiative communautaire « Safer Internet » prépare un plan à 4 ans (2009-2013) qui fait l'objet d'un appel à projets jusqu'en novembre 2009. Une des actions concerne la sensibilisation du grand public. Ses impacts devront être appréciés dans la durée.

5- CONCLUSION

En cette année 2009, de crise économique et sociale, de menace grippale planétaire et de réel lancement des Directives Nationales de Sécurité en France, la question de la gestion des risques majeurs est plus que jamais d'actualité.

Chacun a son avis sur la pertinence d'un danger (psychose ou réalité ? suis-je concerné ?). Chacun a son avis sur l'opportunité ou l'adaptation d'une mesure de prévention (à quoi ça sert ? Est-ce que ce sera efficace ?). La gestion de la grippe A en est le meilleur exemple récent. La pandémie sera-t-elle d'ailleurs déclenchée au moment des Assises ?

En final, en multipliant les mesures de sécurité, on réduit considérablement la potentialité d'occurrence réelle du risque. Et on entend alors, après : « A quoi ça servait tout ça ? ». « Et si on n'avait rien fait, que se serait-il passé ? » On ne le saura évidemment jamais !

Du « Tout est risque ! » exprimé en introduction, ne tend on pas, de manière assez impressionnante désormais, à « La fin du risque » ?

Non pas en tant que phénomène omniprésent et incontournable de nos sociétés, mais en tant que réalité concrète : Des guerres sans morts, des vieux toujours jeunes et en bonne santé, des enfants plus libres mais sous surveillance en ligne, des villes surpeuplées et attirantes mais sous vidéo-surveillance, des salariés sans emploi mais aux revenus maintenus, des traders sous contrôle avec bonus et malus, etc.

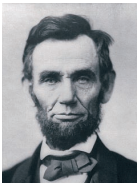
Les mesures de prévention et de protection ont un coût de plus en plus important. La culture des risques doit systématiquement intégrer une dimension économique que nous aborderons prochainement sans doute. A ce titre, méditons l'exemple suivant :

La **protection des droits numériques** anime avec passion le secteur de la culture depuis 10 ans. Que se passe-t-il en fait ? Une mutation de la distribution des biens culturels qui consiste désormais à concevoir les albums comme des outils de promotion des futurs spectacles des artistes (où ils gagneront sans doute beaucoup plus d'argent qu'avec des CDs !). Steve Jobs lui-même, affirme que les DRM (Digital Right Management) ne sont pas la solution. Au plan juridique, l'équilibre visé par la Loi HADOPI se concrétisera-t-il ? Influencera-t-elle les comportements excessifs ? En termes d'éducation, le message « Pirater c'est du vol ! » est-il vraiment porteur ?

Les professionnels de la sécurité doivent rester en alerte devant cette exigence économique, en maintenant l'exercice de style consistant à ne pas confondre risque, menace et vulnérabilité, et à systématiquement identifier puis quantifier, pour les décideurs, les risques réels et résiduels. Ces derniers existeront toujours et la crise, quelle qu'elle soit, surviendra. On ne sait simplement pas quand, ni où, ni comment !

Le développement d'une culture du risque ne doit pas conduire à l'annulation du risque ! Elle doit donc surtout s'accompagner d'une culture de crise ...

« Si vous pensez que l'éducation coûte cher, essayez l'ignorance ! »



6- ANNEXE 1 : Rubriques d'information / sensibilisation

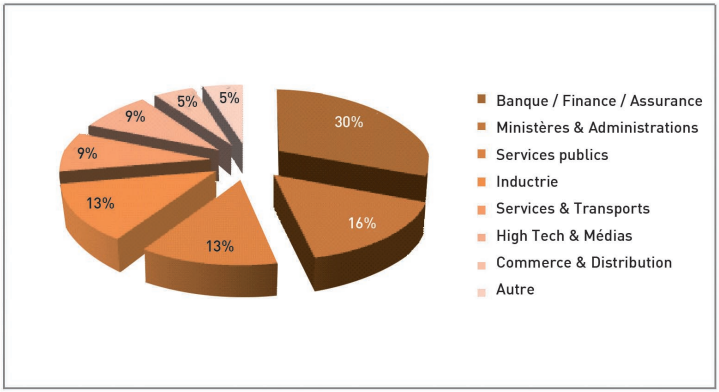
Nous signalons ici quelques caractéristiques des sites d'information / sensibilisation. A consulter !

Site	URL	Rubrique accessibles en page d'accueil
Gouvernement		
1er Ministre / SGDN	www.securite.informatique.gouv.fr	Conseils pratiques entreprises et particuliers
1er Ministre / SGDN	www.ssi.gouv.fr	Technique, actualités, formation
1er Ministre / PDEN	www.surfez-intelligent.gouv.fr	Sécurité Internet, actualités
Délégation Internet	www.protegetonordi.com	Sécurité Internet au domicile
Banques		
BNP Paribas	www.bnpparibas.net	Espace sécurité (complet)
Crédit Agricole	www.credit-agricole.fr	Rubrique sécurité (banque et mobile)
Crédit Lyonnais	https://informations.lcl.fr/securite	Rubrique sécurité (banque et mobile)
Crédit Mutuel	www.créditmutuel.fr	Paiements en ligne
Société Générale	https://particuliers.societegenerale.fr	Configuration et sécurité
Opérateurs		
Bouygues Télécom	www.ideo.bouyguestelecom.fr	Cnil et spam
Darty	www.darty.com	Protection de l'enfance - Signaler contenu illicite - Contrôle parental - Espace sécurité
Free	www.portail.free.fr	Protection de l'enfance Signaler contenu illicite
Neuf Box	http://offres.neuf.fr	Protection de l'enfance - Signaler contenu illicite - Contrôle parental
Numéricâble	http://client.numericable.fr	Portail Sécurité (pack sécurité et contrôle parental)
Orange	www.orange.fr	Prévention et protection (protection de l'enfance, signaler contenu illicite spam et virus)
Orange	Blog.orange-business.com/securite	Focus Entreprise / Technique
SFR	www.sfr.fr	Lutte contre le spam - Signaler contenu illicite - Contrôle parental
Associations professionnelles		
Clusif	www.clusif.asso.org	Actualité / groupes de travail / publications
OSSIR	www.ossir.org	Groupes de travail
FNTC	www.fntc.org	Actualité, groupes de travail, publications
FEDISA	www.fedisa.org	Actualité, formations, publications, conférences
Associations Protection de l'enfance		
Action Innocence	www.actioninnocence.org	Bonnes pratiques, points de contact, conférences et formations
Criminonet	www.criminonet.com	
e-enfance	www.e-enfance.com	
Internet sans crainte	www.internetsanscrainte.fr	

7- ANNEXE 2 : le panel

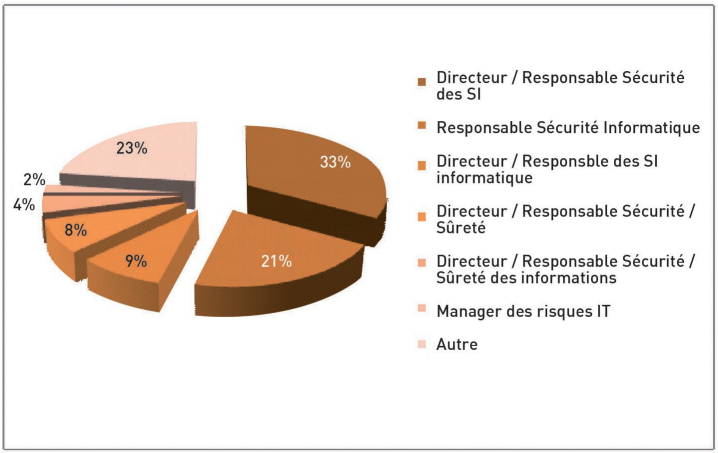
Le panel de l'enquête 2009 est constitué de 237 professionnels (contre 174 en 2008) soit une progression de 36%. Leurs principales caractéristiques sont présentées ci-dessous.

7.1. Secteurs d'activités



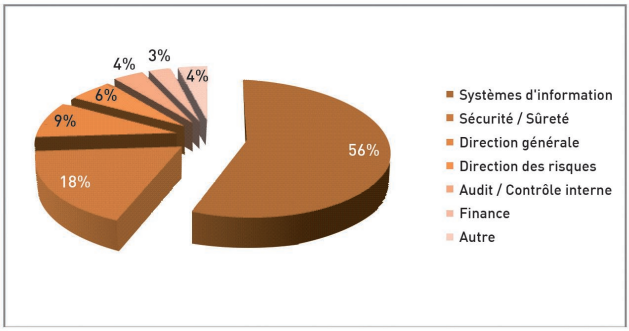
Une représentativité qui reste stable d'année en année avec un poids significatif des banques / assurances et des Administrations / Services publics.

7.2. Titres et fonctions



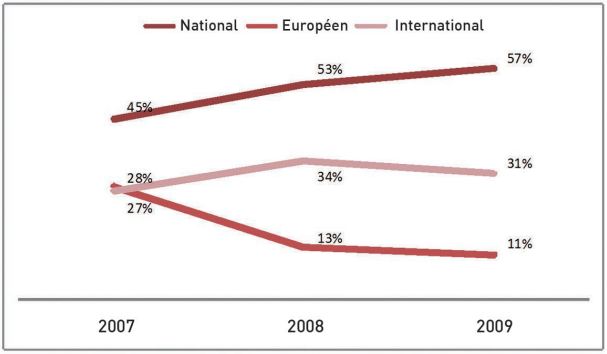
Une répartition qui évolue peu par rapport à 2008 et notamment une proportion d'acteurs opérationnels identique. Une baisse notable des managers des risques IT et des acteurs « sécurité / sûreté de l'information ».

7.3. Entités d'appartenance



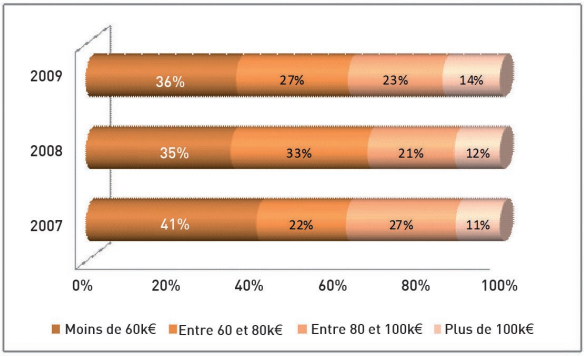
Une représentativité quasi identique d'année en année avec néanmoins une proportion croissante des Directions Sécurité / Sûreté (10% en 2008).

7.4. Couverture géographique



Le panel s'élargit principalement en France mais la part des acteurs « internationaux » reste significative.

7.5. Rémunération



Une répartition des salaires qui varie peu avec un salaire moyen quasi stable à 73,8 k€ contre 73,4 k€ en 2008.

9e édition

Rencontrez les acteurs majeurs de la sécurité et des systèmes d'information à Monaco du 7 au 10 octobre 2009.

Aujourd'hui plus que jamais, dans un contexte économique critique, vous devez faire face aux normes réglementaires, contraintes budgétaires et projets complexes inhérents à votre activité.
Que vous soyez RSSI, DSSI, RSI ou DSI, les Assises sont pour vous l'occasion de faire le plein d'expériences et de networking.

Rendez-vous annuel de la communauté sécurité, les Assises sont depuis neuf ans le lieu de tous les échanges : conférences et tables-rondes explorent les tendances de l'année à venir, tout en dispensant une veille technologique et juridique.

Venez enrichir votre réseau, anticipez les grands mouvements de la SSI et découvrez des réponses pragmatiques et stratégiques à toutes vos problématiques.

Pour plus d'informations : 01 41 93 07 07
www.lesassisesdelasecurite.com

www.infoflash.fr

Avec la participation de :

01 Informatique · cnis mag · Global Security Mag · Hôpitaux Magazine Santé & Société · Hospitalia · Mag Securs · Regards IE · Santé & technologies · Security Vibes

comexposium · un événement · lesassises de la sécurité et des systèmes d'information · prix de l'innovation · le cercle

Pour un éclairage
pertinent et novateur
sur vos problématiques.

8i Network · Actividentity · Alcatel-Lucent · ArcSight · Arismore · Arkon Networks · Aruba Networks · Avocent · LANDesk · Axis Communications

BeeWare · BlackBerry · BlueCoat · BT · ca · Check Point · Cisco · commonIT · Crossbeam

denyall · Dictao · enterasys · eset · Evidian · F5 · Fortify · Fortinet · gemalto · Global Knowledge

Google Enterprise · Guardium · hapsis · HSC · IBM · ilex · INL · Integralis · Juniper

kalistick · Kaspersky · Keynectis · Linagora · logica · loglogic · McAfee · Microsoft

mobilegov · Netasq · netfo · nexthink · Novell · Ofeo · OpenTrust · Oracle

orange Business Services · paloalto · PGP · Polycom · Prim'X · 1Labs · Qualys · Ricoh

Rittal · RSA · SafeNet · ScanSafe · SkyRecon · solucom · SonicWall · Sophos

SourceFire · SPIE · Stonesoft · Sun · symantec · telindus · Thales · TippingPoint

Trend Micro · verizon business · vmware · Vupen · Wallix · webroot · websense · Zscaler

www.infoflash.fr

2001-2010

10e édition

10 ans de réflexion stratégique,
10 ans à l'écoute des tendances et innovations,
10 ans de rencontres, d'échange et de partage autour de la SSI.

En 2010, les Assises seront plus que jamais l'occasion de trouver
des réponses à vos problématiques et d'enrichir votre réseau.

Rendez-vous à Monaco du 6 au 8 octobre 2010,
pour cette 10e édition anniversaire
des Assises de la Sécurité et des Systèmes d'Information.

Pour plus d'informations : +33 (0)1 41 93 07 07 - www.lesassisesdelasecurite.com

comexposium

un événement

lesassises
de la sécurité et des systèmes d'information

prix de l'innovation

lecercle