WHITE PAPER DES ASSISES 2011

Le Cercle Européen propose les premiers indicateurs « ratios » sur les dépenses en Sécurité des SI

Paris / Monaco, le 5 octobre 2011

1. Combler le manque d'indicateurs économiques de la Sécurité des SI

Depuis plus de 10 ans, les données économiques du domaine de la Sécurité des SI concernent, d'une part les impacts économiques des attaques / incidents (virus, dénis de services, vols d'information et fraudes en ligne) et d'autre part, l'évaluation du marché en termes d'offre (produits et services). Pourtant, la fiabilité des données produites prête à discussion dans la mesure où elles sont souvent issues de fournisseurs et de prestataires dont l'indépendance n'est pas garantie.

Par exemple, en mai 2000, les impacts économiques du virus I Love You étaient déjà évalués à 7 milliards de dollars en basant le calcul sur la perte de productivité ramenée au PIB des Etats Unis. Dix ans plus tard, le coût de la cybercriminalité est évalué en centaines de milliards de dollars. Et l'analyse porte désormais sur les pertes / vols d'information et les fraudes en ligne. A titre d'exemple, la seule amende de la FSA[1] (UK) auprès de Zurich Insurance, suite à la perte de données clients, s'est élevée à près de 2,3 M£.

Par ailleurs, les dépenses des entreprises dans le domaine de la Sécurité SI sont exclusivement exprimées en pourcentage du budget de la DSI. Or, de l'avis même de nombreux professionnels, ce ratio n'a pas de sens tant les définitions et les contours des budgets de la DSI comme en termes de Sécurité SI sont variables d'une entreprise à l'autre. Certains les expriment d'ailleurs en TTC, d'autres en HT.

Cependant, les dépenses de sécurité sont une dépense comme les autres et elles servent parfois de variable d'ajustement. Elles sont donc mesurées, ici ou là, quelques soient leur champ et leur ampleur. Par exemple, selon les résultats de la dernière enquête menée par PWC[2], 56% des répondants européens affirment avoir réduit leurs dépenses SSI (investissement comme fonctionnement) et autant les avoir reportées.

Enfin, des différences plus ou moins marquées doivent nécessairement exister entre secteurs d'activité (certains très réglementés, d'autres moins), et selon les tailles et les cultures des entreprises / organismes (Groupes internationaux vs grosse PME vs service public). Une vision trop globale masquera des écarts qui peuvent aussi être significatifs.

Ainsi, pour des raisons de crédibilité voire de professionnalisation des acteurs, le marché de la SSI ne peut plus se satisfaire de :
« Les dépenses SSI des entreprises sont comprises entre 1 et 15% du budget de la DSI ».

[1] Financial Services Authority
[2] Eye of the storm – Key findings from the 2012 Global State of Information Security Survey (PWC 2012)

2. Accompagner le renforcement et l'importance de la fonction Sécurité SI

Tandis que la fonction SSI prend plus d'importance et tend à se renforcer[3], ne faut-il pas mieux intégrer la dimension économique aux compétences des professionnels ? Une telle évolution leur permettrait :

- De compléter leur démarche avant tout technique et réglementaire par un volet économique (notamment pour les projets « cloud computing » ou DLP[4])
- De communiquer intelligemment avec un DAF et des acheteurs
- De proposer de « dépenser mieux » plutôt que de se voir imposer de « dépenser moins »
- De rapprocher les dépenses des évaluations de risques et des impacts d'incidents vécus

La réflexion et les travaux menés au sein du Cercle Européen de la Sécurité sont ceux de DSI / RSSI à l'attention des DSI / RSSI.

3. L'approche proposée par le Cercle Européen de la Sécurité

En 2010, l'enquête annuelle du Cercle Européen de la Sécurité (cf. Livre Bleu des Assises 2010) menée auprès d'un échantillon de 220 DSI/RSSI, a sondé leurs visions et leurs pratiques sur les questions économiques. On a pu remarquer que :

- La consolidation des dépenses « SSI » n'est effectuée que par 37% de l'échantillon.
- La moitié de ceux qui consolident n'intègre pas les ressources humaines.
- De manière très surprenante, 43% des répondants jugeaient leurs dépenses à la fois insuffisantes et inefficaces …

De toute évidence, ces premiers travaux se devaient d'être approfondis et un Groupe de travail *ad 'hoc* a été mis en place. La réflexion porte prioritairement sur les « dépenses SSI » (voir la méthodologie en annexe). L'objectif fixé consiste à produire de premiers indicateurs « ratios » pour des dépenses mesurables *a priori*. Cinq types de dépenses ont été retenus :

- Equipes de pilotage de la Sécurité SI
- Actions de communication / sensibilisation / formation en SSI
- Actions de contrôle et audit en SSI
- Outils de protection des postes de travail
- Gestion des accès logiques au SI

Ce white paper[5] présente les résultats des travaux menés et quelques éléments d'analyse discutés lors d'un atelier des Assises de la Sécurité le 5 octobre 2011.

Le Cercle Européen propose aux participants des Assises de la Sécurité 2011 les premiers indicateurs « ratios » sur les dépenses SSI des entreprises / administrations.

[3] Voir le « white paper » du Cercle Européen sur l'étude qualitative de la fonction SSI, produit pour les Assises 2011
[4] Data Loss Prevention
[5] White paper rédigé par Pierre-Luc REFALO (Associé HAPSIS) et validé par le Groupe de travail.

4. Les apports et les enseignements majeurs

a. *Une première étape au bilan satisfaisant*

Environ 140 DSI / RSSI ont répondu à une enquête (voir la méthodologie et les questions posées en annexe). C'est un échantillon représentatif qui a cependant nécessité des ajustements. On notera que :

- Les répondants n'apportent pas de réponse à toutes les questions.
- Entre 50 et 100 réponses sont exploitables pour chaque question.
- Le calcul des ratios masque des écarts parfois importants.

Le Groupe de travail a fixé des axes et des objectifs qui se sont concrétisés par :

- Un choix volontaire de dépenses maitrisées *a priori* plutôt que LE budget sécurité.
- Un benchmark possible avec des entreprises comparables.
- Un outil complémentaire aux évaluations de risques et d'incidents, à l'attention des DSI / RSSI.
- Des indicateurs produits à partir de données issues du terrain, par les professionnels SSI eux-mêmes.

Deux grands enseignements peuvent être dégagés et mériteront discussion.

b. *De grandes inégalités face à l'achat*

Il ressort des indicateurs produits de grandes différences selon les secteurs d'activités et la taille des entreprises / organismes. Si ce n'est pas une grande surprise, elles démontrent que les pratiques d'achats de produits et de services SSI font considérablement varier, *in fine*, le montant des dépenses. Ainsi, il est sans doute possible d'acheter mieux, voire de dépenser plus, d'autant plus que les données extrêmes ont été éliminées.

A titre d'exemple, les dépenses relatives à la protection des postes de travail (outils uniquement) ont été évaluées ainsi.

Protection du poste de travail	**< 5 000 p**	**5 000 – 20 000 p**	**> 20 000 p**
	23 répondants	*21 répondants*	*12 répondants*
Dépense moyenne (€ / poste)	27,9 €	15,9 €	4,9 €

Protection du poste de travail	**Banques Assurances**	**Services publics Administrations**	**Industries Services**
	14 répondants	*19 répondants*	*16 répondants*
Dépense moyenne (€ / poste)	23,1 €	28,3 €	16,6 €

Certains (en fonction du secteur mais surtout de la taille) se trouvent dans des situations d'acheteur « privilégié ». Ils disposent de structures dédiées en la matière, peuvent « délocaliser » l'achat des produits / services pour bénéficier des effets de change, voire bénéficient d'un « guichet privilégié » auprès des vendeurs.

Dans une situation intermédiaire, d'autres bénéficient d'un marché de volume et de réductions quantitatives dont ne bénéficient pas les plus petites structures. Ces dernières souffrent d'une chaîne de valeur des fournisseurs de produits / services plus longue, d'un fort éclatement des circuits de distribution et d'un besoin de conseil plus grand, impactant significativement les prix.

c. *Un marché à trois vitesses*

Un autre enseignement significatif concerne les écarts pour les trois secteurs d'activité. En cumulant les ratios calculés par poste de travail ou par collaborateur, on obtient les montants indiqués dans le tableau ci-dessous.

- Les Banques / Assurances dépensent le plus car plus réglementées, mais sans réellement dominer.
- Les Industries / Services, souvent de tailles plus réduite, apparaissent moins dépensiers voire plus « agiles ».
- Les Administrations / Services publics privilégient les mesures techniques et de contrôle dans une logique de « ligne Maginot » (moyens humains et protection du poste). Elles peuvent aussi bénéficier de services « gratuits » proposés par exemple via l'ANSSI[6] et la DCRI[7].

	ETP « Pilotage SSI »	Sensibilisation / Formation + Gestion d'accès logique	Protection du poste de travail + Contrôle / Audit
Banques / Assurances	1,7 ETP / 1000 p	67,2 € / personne	43 € / poste
Administrations Services publics	2,2 ETP / 1000 p	49,8 € / personne	44,6 € / poste
Industries / Services	1,6 ETP / 1000 p	43,1 € / personne	26,2 € / poste

d. *Une place de marché traditionnelle avec des marges de progression*

En définitive, au regard des ratios calculés (voir pages suivantes), nous pouvons considérer que le marché de la Sécurité SI est un marché somme toute classique où plus on est gros, mieux on achète. Les effets de volumes et de tailles sont considérables. On remarquera aussi des variations importantes dans la chaine de valeur, où le poids des grossistes, des revendeurs, distributeurs et intégrateurs est d'autant plus important que les entreprises sont petites.

La dimension « humaine » propose également des marges de progression significatives. Le réflexe d'achat de produits pour couvrir les risques n'atteint-il pas ici des limites ? Les équipes de pilotage restent globalement très limitées. Deux ETP de « pilotage SSI » au delà de 1000 personnes semblent une cible réaliste et minimale. En termes de sensibilisation / formation, une dépense moyenne de 20 € / personne / an est-elle superflue au regard de l'importance du facteur humain dans la gestion des risques numériques ?

Enfin, le poids de la réglementation (et des dépenses contraintes associées) apparaît au regard des dépenses supérieure des Banques / Assurances.

[6] Agence Nationale de la Sécurité des Systèmes d'Information
[7] Direction Centrale du Renseignement Intérieur

5. Résultats détaillés

a. *Une influence majeure de la taille des organisations*

Les ratios calculés selon la taille des organisations ont mis en évidence des données cohérentes pour 3 segments. Des ruptures nettes sont en effet apparues autour de 5000 collaborateurs et de 20 000 collaborateurs.

Les tableaux ci-dessous présentent les résultats obtenus pour les 3 segments retenus.

Equipe de pilotage SSI	**< 5000 p** *44 répondants*	**5000 – 20 000 p** *33 répondants*	**> 20 000 p** *24 répondants*
ETP pour 1000 personnes	2,9 ETP	1,1 ETP	0,2 ETP

Sensibilisation / Formation SSI	**< 5 000 p** *31 répondants*	**5 000 – 20 000 p** *21 répondants*	**> 20 000 p** *15 répondants*
Dépense moyenne (€ / personne)	24,7 €	4,8 €	2,9 €

Contrôle et Audit SSI	**< 5 000 p** *39 répondants*	**5 000 – 20 000 p** *30 répondants*	**> 20 000 p** *17 répondants*
Dépense moyenne (€ / poste)	23,4 €	11,1 €	2,3 €

Gestion des accès logiques	**< 5 000 p** *23 répondants*	**5 000 – 20 000 p** *22 répondants*	**> 20 000 p** *8 répondants*
Dépense moyenne (€ / personne)	43,7 €	33,6 €	9,1 €

Précision pour les plus petites structures : < 2 000 personnes / 45,8 € - 2000 – 5000 personnes / 36 €

Protection du poste de travail	**< 5 000 p** *23 répondants*	**5 000 – 20 000 p** *21 répondants*	**> 20 000 p** *10 répondants*
Dépense moyenne (€ / poste)	27,9 €	15,9 €	4,9 €

Précision pour les plus petites structures : < 2 000 postes / 35,7 € - de 2 000 à 5 000 postes / 19,1 €

b. *Des différences remarquables par secteur d'activité*

Les ratios sont calculés pour trois secteurs d'activité disposant d'échantillons suffisants :

- Banques / Assurances
- Administrations / Services publics (incluant la Santé)
- Industries / Services (incluant Transports, Médias, Télécoms / IT, etc.)

Un « Zoom santé » est proposé si une différence est perceptible par rapport à l'ensemble du secteur « Administrations / Services publics ».

Les tableaux ci-dessous présentent les résultats obtenus pour les 3 secteurs retenus.

Equipe de pilotage SSI	**Banques Assurances**	**Services publics Administrations**	**Industries Services**
	28 répondants	*34 répondants*	*35 répondants*
ETP pour 1000 personnes	1,7 ETP	2,2 ETP	1,6 ETP

Sensibilisation / Formation SSI	**Banques Assurances**	**Services publics Administrations**	**Industries Services**
	25 répondants	*17 répondants*	*23 répondants*
Dépense moyenne (€ / personne)	15,3 €	11,9 €	14,2 €

Contrôle et Audit SSI	**Banques Assurances**	**Services publics Administrations**	**Industries Services**
	24 répondants	*24 répondants*	*19 répondants*
Dépense moyenne (€ / poste)	19,9 €	16,3 €	9,6 €

Gestion des accès logiques	**Banques Assurances**	**Services publics Administrations**	**Industries Services**
	15 répondants	*18 répondants*	*17 répondants*
Dépense moyenne (€ / personne)	51,9 €	37,9 €	28,9 €

Zoom Santé *(9 répondants) :* 31,9 € / collaborateur

Protection du poste de travail	**Banques Assurances**	**Services publics Administrations**	**Industries Services**
	14 répondants	*19 répondants*	*16 répondants*
Dépense moyenne (€ / poste)	23,1 €	28,3 €	16,6 €

Zoom Santé *(11 répondants)* : 23 € / poste

6. Méthodologie

Groupe de travail : Le Groupe de travail du Cercle Européen est constitué de 6 RSSI et un DSI :

- Pascal BASSET (Responsable Sécurité et Conformité – PMU)
- Eric DOYEN (Responsable Sécurité des SI / CISO – GENERALI)
- Didier GRAS (Responsable Sécurité des SI / CISO – Groupe BNP Paribas)
- Dominique GUIFFARD (Directeur des SI / CIO – CELINE – Groupe LVMH)
- Stéphane JOGUET (RSSI / CISO – Groupe DAHER)
- Jean-François LOUÂPRE (Responsable Sécurité / CSO – AG2R La Mondiale)
- Sylvain THIRY (Responsable Sécurité des SI / CISO – SNCF)

Des acteurs des secteurs publics et privés ont été sollicités lors des réunions de réflexion initiale :

- Michel BENEDITTINI (ANSSI)
- Capitaine Régis CHAPELLIERE (Gendarmerie Nationale)
- Patrick LANGRAND (Groupe La Poste)
- Hervé SCHAUER (HSC)

Le Groupe de travail est piloté par : Pierre-Luc REFALO (Associé – HAPSIS)

Une expertise méthodologique sur la préparation et la synthèse de l'enquête a été apportée par Eric DOMAGE (IDC).

Huit réunions du Groupe de travail et plusieurs conférences téléphoniques ont permis de préparer l'étude et d'en effectuer l'analyse et la synthèse. Il a fixé comme objectif de produire des indicateurs sur les dépenses des entreprises / administrations de type « ratio » (en euros / collaborateur ou euros / poste de travail), en essayant de distinguer les secteurs d'activité (si l'échantillon est suffisamment large).

Il a produit ce document et le support de présentation de l'Atelier des Assises de la Sécurité.

Enquête en ligne : Le Groupe de travail a construit une enquête en ligne demandant (voir page suivante).

- Le secteur d'activité de l'entreprise / organisme
- Le nombre de collaborateurs
- Le nombre de postes de travail
- Le nombre de personnels (ETP) chargés du pilotage de la SSI en 2011
- Les dépenses des actions de communication / sensibilisation / formation en 2011
- Les dépenses des actions de contrôle et audit en SSI en 2011
- Les dépenses des dispositifs de protection des postes de travail en 2011
- Les dépenses des processus de gestion d'accès logiques en 2011

L'enquête a été mise en ligne du 23 juin au 31 août 2011. Un workshop s'est déroulé le 14 juin 2011 afin de présenter aux membres du Cercle Européen l'organisation de l'enquête et de finaliser les questions posées.

Analyse des données : L'analyse des données recueillies a nécessité des ajustements et une sélection.

- Les réponses des très petites structures et des doublons ont été supprimés.
- Les réponses aberrantes ou surprenantes (11111, 12345, etc.) ou incohérentes (1000 collaborateurs pour 10000 postes de travail) ont été supprimées.
- Les réponses dont les ratios proposaient un écart trop important par rapport aux moyennes calculées ont été éliminées.
- Les réponses données en euros et non en k euros ont été corrigées.
- Les réponses des structures de 5000 personnes et 20 000 personnes ont été pris en compte 2 fois (dans deux des trois segments).

L'analyse des données et le calcul des ratios a été menée par Eléonore GRANDEMANGE et Pierre-Luc REFALO (HAPSIS) avec l'assistance méthodologique d'Eric DOMAGE (IDC).

Les questions et les réponses récoltées / exploitées

Question 1 : **Combien de collaborateurs (ETP et vous compris)** composent les équipes en charge des activités de **pilotage de la SSI** au sein de votre entreprise / organisme ? Pour les DSI / RSSI de Groupes ou Ministères, consolider l'ensemble de la Filière SSI (en rattachement fonctionnel).

- *Prendre en compte les internes et les prestataires, répondant compris en évaluant les ETP sur l'ensemble de l'année 2011 : acteurs en charge des activités liées à la Politique et à la Gouvernance SSI, à la coordination des plans d'action SSI, à l'assistance / expertise projets, aux analyses de risque, à la communication / sensibilisation, au contrôle des risques et audits Sécurité, à la gestion des incidents, aux tableaux de bord.*
- *Ne pas prendre en compte les activités PCA et de mise en œuvre / exploitation des outils et procédures SSI.*

Réponses collectées : 138	Réponses exploitées : 96

Question 2 : Quel est le **montant des dépenses globales (en k€) pour des actions de communication / sensibilisation / formation** en Sécurité des SI menées en 2011 ?

- *Consolider à votre propre budget, les dépenses engagées par la DSI, la Communication interne, la DRH / Formation*
- *Prendre en compte les actions relatives à : Ingénierie pédagogique / Etudes, guides, supports et animation de sessions, outils et modules en ligne, vidéos, goodies, etc.*

Réponses collectées : 90	Réponses exploitées : 66

Question 3 : Quel est le montant des **dépenses globales (en k€) pour des actions de contrôle et d'audit** menées en 2011 en termes de SSI ?

- *Consolider à votre propre budget, les dépenses engagées par la DSI, l'audit interne.*
- *Prendre en compte les actions relatives à : audits généraux SSI, Audit ISO 27001 / 27002, tests d'intrusion, audits techniques, de systèmes, de codes, etc.*
- *Ne pas prendre en compte les activités liées à la conformité à des référentiels sectoriels (SoX, PCI-DSS, ARJEL, etc.)*

Réponses collectées : 103	Réponses exploitées : 80

Question 4 : Quel est le montant des **dépenses globales (en k€) des mesures de protection des postes de travail** engagées en 2011 ?

- *Pour l'ensemble du parc entrant dans votre champ d'action : tout poste connecté au réseau (fixe, portable, PDA, smartphone, tablettes)*
- *Avec des outils et des procédures déployés au moment de l'enquête (Juin 2011)*
- *Prendre en compte les dépenses d'outils et de maintenance relatives à la protection :*
  - *du poste (anti virus / malware, firewall personnel, correctifs, etc.)*
  - *des données (sauvegardes, DLP, authentification forte, chiffrement)*
- *Ne pas prendre en compte les mesures de protection d'infrastructure / serveurs / réseaux (anti virus / malware, filtrage URL, anti spam, IDS, IPS, patch management)*

Réponses collectées : 88	Réponses exploitées : 49

Question 5 : Quel est le montant des **dépenses globales (en k€) relatives à la gestion des accès logiques** engagées en 2011 ?

- *Pour l'ensemble des collaborateurs entrant dans le champ d'action du répondant*
- *Avec des outils et des procédures déployés au moment de l'enquête (Juin 2011)*
- *Prendre en compte les dépenses d'outils, de maintenance et de support :*
  - *provisionning (arrivée / création d'un compte)*
  - *gestion des identités*
  - *gestion de l'annuaire*
  - *gestion des accès et des profils*
  - *gestion des mots de passe*
  - *gestion des supports d'authentification forte*
- *Ne pas prendre en compte les projets en cours : IAM par exemple*

Réponses collectées : 91	Réponses exploitées : 52