RECOMMANDATION

RETOUR SUR INVESTISSEMENT EN SECURITE DES SYSTEMES D'INFORMATION : QUELQUES CLES POUR ARGUMENTER

Octobre 2004

Groupe de Travail ROSI (Return On Security Investment)

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, rue Pierre Semard, 75009 PARIS
Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88
e-mail : clusif@clusif.asso.fr - Web : http://www.clusif.asso.fr

TABLE DES MATIERES

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Matthieu Grall	SGDN
Luc Mensah	SIVA
Félix Ndouga	MICROSOFT
Gérald Oualid	ALCATEL
Delphine Pramotton	ERNST & YOUNG
Pierre de Thomasson	LYNX TECHNOLOGIE
Hervé Schauer	HSC
Renaud de la Porte des Vaux	FRANCE TELECOM

Ainsi que les membres ayant participé au comité de relecture.

LISTE DES ACRONYMES, INDEX

1 INTRODUCTION

- **Objet du document**

Ce document est issu des travaux du groupe de travail ROSI (Return On Security Investment[1]) du CLUSIF qui ont eu lieu en 2003 et 2004. Ceux-ci ont porté sur les pistes utilisables afin de démontrer la valeur ajoutée des investissements liés à la sécurité des S.I. La réflexion du groupe de travail a abouti à la formalisation de quelques idées clés dans la justification de la valeur de la sécurité des S.I. et sa contribution à l'activité de l'entreprise ou de l'organisme[2]. Ce document ne prétend pas répondre à toutes les questions relatives au ROSI et ne donne pas de formule pour le calculer, mais il présente quelques arguments clés à utiliser dans la démarche de justification des investissements.

- **Destinataires du document**

Le document s'adresse aux personnes désirant aborder la problématique de la rentabilité des investissements de sécurité, et notamment aux DSI et RSSI, dans le cadre de la construction / justification économique des budgets associés.

- **Objet du débat**

Aujourd'hui encore, le discours sur la gestion des risques et sur la contrainte réglementaire restent les deux facteurs d'influence les plus utilisés par les RSSI[3] pour demander des investissements de sécurité des S.I, le retour sur investissement arrivant loin derrière. Pourtant de nombreuses directions générales demandent cette justification quantitative du retour sur investissement.

Evaluer le retour sur investissement des dépenses consacrées à la sécurité n'est pas chose aisée, tant il est difficile d'apporter la preuve quantifiée des gains réalisés par l'entreprise. D'un côté les décideurs en charge des budgets veulent connaître la rentabilité de leurs investissements, au risque de susciter des divergences autour des différentes techniques de quantification ayant permis le chiffrage, de l'autre de nombreux experts préfèrent adopter une approche d'évaluation des risques moins financière et plus qualitative.

Deux principaux courants de pensée, complémentaires, se positionnent aujourd'hui dans le débat sur la problématique du ROSI :

- la sécurité est une problématique technique, appelant en réponse un produit ou un service, et
- un processus métier transverse, qui doit soutenir les activités stratégiques de l'entreprise.

[1] Retour sur Investissement de Sécurité ; Définition donnée à la fin du paragraphe

[2] Dans tout ce qui suit, le terme « entreprise » sera utilisé au sens large, s'appliquant aussi bien aux entreprises privées qu'aux différents organismes du secteur public.

[3] Source : CIGREF 2002, RSSI Responsable de la Sécurité des Systèmes d'Information

Dans les deux cas, il faudra justifier le retour sur investissement, probablement de façon différente, selon l'intégration de cette problématique dans l'entreprise.

Enfin, le ROSI s'aligne dans le cadre fourni par l' ITIL[4] et l'ITSM[5] (bonnes pratiques pour le management des services informatiques).

- **Définitions ROSI**

Il n'existe pas de définition unique du ROSI tant déjà sur ce point, les opinions divergent.

Le ROSI, est dérivé du ROI (Return On Investment), et peut être compris comme le gain financier net (en monnaie constante) d'un projet de sécurité au regard de son coût total (investissement et fonctionnement) sur une période d'analyse donnée.

Contrairement au TCO (Total Cost of Ownership) qui exprime le coût total du Système associé au cycle achat/déploiement/maintenance sur une période donnée (généralement 3 ans), le ROSI relativise les coûts par rapport aux bénéfices. L'une des formes d'expression la plus courante du ROSI est la suivante : ROSI = (bénéfices – coûts) / coûts.

A cette notion de ROSI, on associe parfois la notion de point de retour « Payback Period » date à partir de laquelle, les gains dépassent les coûts d'investissement d'un projet. On trouve donc également une expression du ROSI en « temps nécessaire pour récupérer la mise de fonds initiale d'un investissement »

Sur le terrain, on observe un « glissement » de cette définition du ROSI vers une définition moins financière, qui tend de plus en plus à inclure la valeur ajoutée d'un investissement en sécurité, qu'elle soit qualifiable et/ou quantifiable.
On retiendra que par le ROSI, on cherche à déterminer à priori la solution de sécurité optimale d'un projet ou d'un système avant sa mise en place.

Remarque :
Les différents scénarios cités dans la suite de ce document doivent être pris à titre d'illustration. Ils ont été sortis de leur contexte et sont basés sur des hypothèses que l'on peut toujours remettre en cause.

[4] Information Technology Infrastructure Library – Approche de gestion des services informatiques, complémentaires à la BS 15000 (British Standards for IT service Management)

[5] Information Technology Service Management

2 ETAT DE L'ART

2.1 Sécurité des S.I. et notion de coût

Avant de traiter de l'analyse de la rentabilité des investissements de sécurité, il paraît nécessaire de rappeler différents concepts en matière d'appréhension des coûts de la sécurité S.I.

2.1.1 Coûts ponctuels et récurrents de la sécurité

Les coûts ponctuels

Les coûts ponctuels correspondent, en général, aux dépenses de mise en place des dispositifs de sécurité (organisationnels, technologiques, humains) et aux effets financiers consécutifs aux incidents. Ce sont :

- le coût des investissements liés aux solutions de sécurité (architecture cluster, disques miroir, redondance réseau, redondance serveurs, …)
- les coûts de déploiement de solutions de sécurité (déploiement d'anti-virus, de clés de chiffrement, …)
- le coût des incidents et accidents : pertes de production, honoraires d'experts, remplacement des matériels, franchises d'assurance, d'investigation, pénalités de retards, pertes de parts de marché, perte d'image de marque, dommages et intérêts, coûts de reconstitution, etc.

Les coûts récurrents

Les coûts récurrents correspondent aux dépenses d'exploitation, d'administration, de maintenance et de contrôle de ces dispositifs. Ils comprennent notamment les coûts de fonctionnement (coût de la structure sécurité en place et des moyens de fonctionnement), qui selon l'étude IDC/Bull 2002 représenteraient 65% du coût global de la sécurité.

2.1.2 Coûts tangibles et intangibles

Sous un angle de vue plus financier, qu'ils soient ponctuels ou récurrents, les coûts peuvent également être analysés selon deux angles :

Les coûts tangibles

- pertes de productivité (équivalent financier de l'effort passé)
- pertes de revenus
- coûts du support informatique nécessaire
- coûts de remplacement, reconstitution
- coûts d'assurances
- …

Les coûts intangibles, plus difficiles à apprécier

- perte de productivité non chiffrable
- perte de réputation
- perte de part de marché, perte de confiance clients
- augmentation du risque de non conformité aux lois
- poursuite juridique (temps passé par les avocats, amendes et autres pénalités, …)
- …

Ce sont principalement ces coûts intangibles qui rendent la quantification financière du ROSI sujette à discussion, sachant que les mesures de protection prises sont parfois sources de bénéfices intangibles (par exemple, l'effet d'une formation des personnels, …).

Quelque soit le terme que l'on utilise, l'idée consiste à distinguer ici les coûts « directement quantifiables » – qui résultent de calculs sur des éléments concrets et « discrets » – des « autres coûts », dont l'évaluation exige, de façon plus ou moins importante, le recours à des approches analogiques ou comparatives.

2.2 Les arguments classiques du ROSI

2.2.1 Les arguments technologiques

Il existe aujourd'hui plusieurs façons d'aborder le retour sur investissement. Historiquement, la sécurité était au départ réduite à sa composante informatique et par là même, la sécurité « informatique » était considérée comme une problématique uniquement technologique, relevant de la direction informatique.

Lorsque la question du retour sur investissement est posée sous l'angle purement technique, la réponse met le plus souvent en exergue l'efficacité opérationnelle, par l'amélioration de la performance. Les arguments utilisés sont alors :

- la réduction des coûts d'infrastructure informatique, grâce aux gains de temps et à l'économie réalisés par la généralisation d'outils ou de procédures de sécurité, ou par le remplacement de technologies devenues obsolètes et coûteuses (par exemple le remplacement de réseaux propriétaires par l'utilisation de l'Internet sécurisé à base de VPN[6]),

- la réduction du nombre ou du coût des incidents de sécurité, c'est le cas par exemple lors du déploiement de logiciels anti-virus (réduction des occurrences de virus et limitation de la propagation),

- l'amélioration du temps de réponse, de la satisfaction des utilisateurs, des clients (par exemple par la mise en place d'un outil de *single sign-on*).

Aujourd'hui, la Direction Informatique tend à devenir la Direction des Systèmes d'Information et la sécurité informatique, la Sécurité des Systèmes d'Information. Même si cette évolution n'est pas encore une réalité dans toutes les entreprises, le degré de maturité des sociétés à l'égard de la sécurité a augmenté. De plus en plus de responsables sont convaincus de la nécessité de protéger le patrimoine informationnel de l'entreprise.

Avec l'augmentation du nombre d'attaques sur Internet, la rapidité et l'étendue croissantes de leur propagation, l'apparition des technologies sans fil et la généralisation de l'informatique nomade, l'argument sécurité au sens de la protection de l'identité s'est imposé de lui-même. Les solutions de chiffrement, de contrôle d'accès et d'authentification peuvent ainsi être justifiées par l'argument de la protection de l'identité et du secret.

[6] *Virtual Private Network* : réseau virtuel privé sur Internet, sécurisé à l'aide d'une version de protocole spécialement conçue à cet effet (IPV6…)

2.2.2 Les arguments « métiers »

Au delà de l'aspect technologique, les responsables ayant une perception accrue de la sécurité des S.I ont compris que l'efficacité de la sécurité ne pouvait être réduite à sa seule valeur technologique, et qu'elle contribuait réellement à la protection du savoir-faire de l'entreprise. De ce fait, la coordination avec les directions métiers est devenue un maillon indispensable pour pouvoir apprécier l'impact de la sécurité et en justifier les investissements : sont donc alors apparus les arguments basés davantage sur les méthodes d'analyse des risques et d'analyse des enjeux métiers.

Par ailleurs, Le Consortium sur la Recherche sur la Politique et Sécurité de l'Information (CRISP[7]) est convaincu que parmi les différents facteurs à prendre en compte dans l'appréciation des risques, trois d'entre eux ont un poids tel qu'ils sont en train de changer le paysage de l'analyse des risques et de le faire évoluer :

- les besoins des assureurs
- les risques juridiques
- la concurrence du marché

Plusieurs sociétés d'assurance étudient des tables tarifaires permettant d'assurer chaque ressource du système d'information. Une des difficultés qui existent encore aujourd'hui quant à la production de ces tables résulte de la réticence des entreprises à partager les informations relatives aux coûts des sinistres qu'elles ont subis.

2.2.3 Les arguments réglementaires et normatifs

L'arsenal juridique français relatif à l'utilisation des nouvelles technologies précise que l'entreprise a obligation de moyens, c'est-à-dire qu'elle est tenue de montrer qu'elle a mis en place ce qu'il était raisonnablement nécessaire pour assurer la protection du système de traitement automatisé. Dans le même ordre d'idées, les Etats-Unis se réfèrent à un jugement émis en 1947 pour définir la notion de négligence : « Est considérée négligente une entreprise qui ne met pas en œuvre des mesures de réduction de risque dont le coût de prévention est inférieur à la probabilité de survenance du sinistre multiplié par la gravité du sinistre. »

On voit donc bien la force de proposition que représentent ces arguments juridiques pour convaincre les décideurs d'investir.

Enfin, ces dernières années ont vu l'émergence de nouvelles réglementations souvent sectorielles (CRBF 97-02, Bâle II, Loi sur la Sécurité Financière, Sarbanes-Oxley, HIPAA, etc…) créant dès lors de nouveaux risques juridiques de non conformité à ces réglementations.

[7] CRISP : organe de recherche issu de l'université de Stanford, de l'institut pour les études internationales et du centre pour la Sécurité et la Coopération Internationale (CISC)

Autre façon de justifier les coûts, le marché fait pression sur les entreprises en les poussant à se conformer aux standards de sécurité (ITSEC, ISO17799, etc…) ou informatiques (BS 15000[8] par exemple) ou bien encore en les encourageant à se comparer les unes par rapport aux autres (publication des enquêtes annuelles de sécurité, etc…).

[8] Meilleures pratiques de gestion d'une DSI, IT Service Management Standard reposant sur le cadre de référence ITIL (IT infrastructure Library)

2.3 Les différents types de ROSI

2.3.1 ROSI orienté amélioration de la performance

Ce type de ROSI est celui qui est le plus communément utilisé parce qu'il n'est pas spécifique à la sécurité. Il se rapproche davantage d'un ROI classique. Ce ROSI consiste à mettre en place une métrique qui permet de quantifier et d'apprécier une amélioration de la performance. Il peut s'agir :

- De la diminution du nombre d'appels à la hot-line
- De la diminution du nombre des incidents
- De l'amélioration du délai de traitement des incidents
- Etc…

Exemple :

Scénario considéré

Soit une entreprise disposant d'une hot line de 5 personnes chargées principalement de rétablir les mots de passe oubliés et d'assister les utilisateurs dans la complexité de leurs différents systèmes d'habilitation.

Solution proposée

L'investissement dans une solution de single sign-on[9] au coût de 250 K€ (TCO) est envisagé.

Retour sur investissement (ROSI)

Une réduction considérable du nombre d'appels est envisagée au point de réaffecter une partie du personnel de la hot-line à d'autres tâches. Diminution de la hot-line de 5 à 2 personnes, faisant passer le coût de fonctionnement de 400 K€ à 160 K€, soit une économie annuelle de 240 K€. Dans ce cas, la société n'aura pas son retour sur investissement la première année, mais sera bénéficiaire l'année suivante.

Avantages

- Largement connu car non spécifique aux projets de sécurité
- S'adresse à un environnement encore peu mature vis à vis de la sécurité des S.I.

[9] Solution logicielle basée sur un annuaire, qui permet aux utilisateurs d'un réseau d'entreprise d'accéder, en toute transparence, à l'ensemble des ressources autorisées, sur la base d'une authentification unique effectuée lors de l'accès initial au réseau.

Limites

- Non spécifique à la sécurité des S.I
- Périmètre Sécurité des S.I., difficile à délimiter, difficulté à isoler la SSI du reste du projet.

2.3.2 ROSI orienté incidents

En 1979, un standard de fait pour la mesure de « Prévision de Pertes Annuelles » de la sécurité (Annual Loss Expectancy ou ALE) a été publié par le FIPS[10] aux Etats-Unis. Cette Prévision de Pertes Annuelles (PPA) de la sécurité exprime les pertes prévisibles annuelles à partir de la fréquence de survenance d'un incident défini et du coût financier de son impact sur l'entreprise s'il survenait :

Prévision de Pertes Annuelles ALE = $\sum$ Coût $_i$ x Fréquence de survenance $_i$

Avec i : incident de sécurité, et $\sum$ la somme annuelle des incidents de sécurité prévisibles ayant un Coût et une Fréquence de survenance définie.

Le ROSI peut être défini comme : ROSI = ALE 1 – ALE2 - CS

ALE1 = ALE avec CD = coût du dommage sans mesure de protection

ALE 2 = ALE avec CDM = coût du dommage avec mesure de protection

CS = coût de la solution mise en place

Exemple :

Scénario considéré

Soit une entreprise dont le sinistre maximum suite à une attaque virale, coûterait 1 million d'euros, la probabilité d'occurrence d'un tel sinistre étant estimée à 70%.

Solution proposée

Pour remédier à ce problème, le RSSI préconise la mise en place d'une infrastructure antivirale. Elle permet une diffusion automatisée et rapide des correctifs et intègre un module d'inventaire de la configuration des machines. La mise en place de cette solution permettrait de diminuer de 20% les occurrences d'attaques virales et coûterait 150 000 euros (TCO).

Retour sur investissement (ROSI)

ALE1 = 0,7 x 1 million = 700 000 euros.
ALE2 = (0,7-0,2) x 1 million = 500 000 euros

ROSI = 700 000 – 500 000 – 150 000 = 50 000 euros

[10] Federal Information Processing Standard (FIPS) du Federal Bureau of Standards

Avantages

Sur le plan théorique, l'approche ROSI « orientée incidents » est séduisante dans la mesure où il s'agit d'une approche mathématique probabiliste de même nature que celles utilisées dans d'autres contextes (assurances en particulier).

Limites

Cette approche :

1. Suppose que l'entreprise dispose de bases de données historiques suffisamment fiables et riches permettant, pour chaque type d'incident, d'évaluer sa probabilité de survenance dans le contexte de l'entreprise et son impact moyen.

2. Exige un effort de modélisation considérable dans la mesure où elle suppose que l'entreprise ait la vision la plus exhaustive possible des incidents susceptibles de survenir et donc dispose d'une cartographie très complète de ses risques, ceci sur un périmètre qui évolue constamment.

3. Ne permet pas de faire la distinction entre les incidents d'occurrence faible à impact potentiel élevé (ex : incendie) et les incidents d'occurrence élevée à impact potentiel faible (ex : virus).

4. Reste discutable dans la mesure où il existe plusieurs théories possibles pour le calcul de l'ALE et où il y aura toujours un débat quant au caractère représentatif et fiable de la base historique « incidents » générée par l'entreprise.

5. Rend le chiffrage ou l'évaluation des dommages parfois difficiles, notamment lors d'impacts sur le business.

2.3.3 ROSI orienté analyse de risques

Au milieu des années 90, l'approche de la sécurité informatique prend une nouvelle tournure. Grâce à l'émergence d'Internet, la sécurité n'est plus uniquement perçue comme un centre de coût mais aussi comme un moyen de générer de nouvelles opportunités d'affaires. Cet essor fait également progresser la sensibilisation aux risques et les vulnérabilités induites par les SI ouverts vers le monde extérieur. De nouvelles approches de gestion des risques font leur apparition, prenant davantage en compte les aspects organisationnels qui faisaient défaut aux méthodes de première génération. La sécurité informatique s'élargit à la sécurité des systèmes d'information

Cette approche calcule le ROSI en comparant le risque potentiel maximal pour l'entreprise par rapport au coût de la solution.

Scénario considéré

Soit un serveur de production hébergé dans une salle non sécurisée ayant des contraintes fortes de disponibilité (24 h sur 24). Le serveur est mis en redondance avec un second serveur situé sur le même site mais à un autre étage. En cas de sinistre majeur sur le bâtiment qui entraînerait la disparition des 2 salles, la société évalue ses pertes à 15 M€.

Solution proposée

La solution d'hébergement sur un site distant sécurisé est envisagée par la société. Le coût de la solution est évalué à 4 M€ (TCO).

Retour sur investissement (ROSI)

L'argument utilisé consiste à comparer le coût de la solution avec le coût maximal du sinistre s'il survenait. La solution coûte 4 M€ par rapport à un sinistre qui potentiellement pourrait en coûter 15.

Avantages

L'analyse de risques est une approche qui a été largement employée et éprouvée dans le cadre de l'utilisation de méthodes, comme par exemple MEHARI, dont le modèle de risques est basé sur ISO 13335. Toute analyse, sans être parfaite, a le mérite d'être un bon outil de sensibilisation interne. Son efficacité est renforcée lorsqu'elle s'appuie sur la méthode de gestion des risques utilisée par le Risk Manager de l'entreprise.

Limites

1. Les techniques de quantification diffèrent d'une méthode à l'autre, voire d'un expert à l'autre, et le chiffrage de la quantification ou de la qualification du risque est souvent sujet à polémique.
2. Les scénarios de risques envisageables ne sauraient être exhaustifs, et les hypothèses des scénarios sont donc susceptibles d'être remises en cause dans le calcul.

2.3.4 ROSI orienté enjeux métiers

L'approche par les enjeux métiers permet de considérer la sécurité comme partie intégrante des processus d'entreprise. Elle cherche à définir les enjeux liés à la sécurité du système d'information,

Soit en terme de valeur ajoutée pour l'entreprise :

- Gain de parts de marché, avantage concurrentiel
- Amélioration de l'image de marque

- Amélioration de la qualité de service, de la productivité

Soit en terme de risque à éviter :

- Perte de parts de marché, retard concurrentiel
- Dégradation de l'image de marque
- Appauvrissement de la qualité de service, perte de productivité
- Risque juridique, risque de procès
- …

Exemple 1 :

Scénario considéré
Soit une société d'assurance possédant un serveur d'assurance IARD[11] contenant des informations privées telles que le détail des biens à assurer, l'adresse du bien et moyens de protection en place ;

Les risques courus par l'assureur en cas d'intrusion sur ce serveur sont : « perte d'image de marque de la société », « risques de poursuite juridique par : « les tiers », « les associations de consommateurs », « la CNIL » ; « demande de dommages et intérêts »….

Solution proposée

Après un audit interne de sécurité, la société d'assurance se voit recommander un renforcement de la sécurité des dossiers par la mise en place d'un contrôle d'accès systématique et d'une authentification forte.

Retour sur investissement (ROSI)

Le ROSI proposé ici pour justifier les coûts de mise en place d'une solution de renforcement des droits d'accès et authentification forte s'appuie sur l'enjeu lié au risque juridique et à la perte d'image.

Le risque de procès est généralement un argument qui permet de sortir de l'argument financier et qui, dans le cas d'une solution n'atteignant pas un coût prohibitif, permet généralement de valider assez rapidement la mise en œuvre des mesures de protection.

[11] Incendie, Accidents et Risques Divers

Exemple 2 :

Scénario considéré

Soit une société offrant un service d'hébergement de site Web pour entreprises. Le scénario considéré est le risque d'accéder aux sites des sociétés concurrentes hébergés sur les mêmes serveurs du prestataire.

Solution proposée

La société d'hébergement a choisi de faire accréditer la sécurité de ses serveurs et obtient une certification de sécurité de type Webtrust ou EAL4. Elle affiche la sécurité de son service comme argument différentiateur. Les coûts de sécurisation des serveurs sont estimés à 200 K€ (TCO).

L'hébergeur « sécurisé » estime gagner des parts de marché, en publiant son accréditation et espère ainsi récupérer une partie des clients ayant été victimes d'intrusion chez des hébergeurs concurrents. Il évalue un gain potentiel de contrats de l'ordre de 1 million d'euros.

Retour sur investissement (ROSI)

Le ROSI proposé ici pour justifier les coûts de sécurisation de son hébergement est basé sur l'avantage concurrentiel et la comparaison du coût de la solution (200 K€) avec le gain potentiel (1 M€).

Avantages

Cette approche utilise le langage « métier » et fédère les différentes directions de l'entreprise. Elle est couramment utilisée et facilement abordable auprès des directeurs fonctionnels. Enfin, elle impacte directement le business, ce qui représente un argument de poids pour une prise de décision.

Limites

- Difficile à mettre en œuvre
- Reste souvent limitée à une approche qualitative, la quantification de l'enjeu étant généralement un exercice particulièrement difficile
- Directeurs fonctionnels pas toujours accessibles car ces solutions sont souvent perçues comme non prioritaires.

2.3.5 ROSI orienté « normes et standards »

Cette approche est fondée sur la conformité avec des standards tels que la BS7799, l'ISO17799, avec la norme ISO 13335 (politique sécurité SI), ou avec des réglementations en vigueur (meilleures pratiques imposées par la Loi sur la Sécurité Financière (LSF), etc..). Son processus de mise en place ne nécessite pas systématiquement d'analyse quantifiée des risques et préconise la mise en place des mesures de protection décrites dans les standards.

Exemple :

Scénario considéré

L'audit de sécurité SAP d'une société soumise à la Loi sur la Sécurité Financière, révèle que cette dernière ne dispose pas d'un système d'attribution et de suivi des habilitations d'accès garantissant une bonne ségrégation des tâches et une protection suffisante vis à vis de la fraude.

Solution proposée

Faire intervenir un expert de sécurité SAP en charge de mettre en place les recommandations et d'élaborer les procédures d'habilitation, dont les honoraires se monteraient à 70 k€.

Retour sur investissement (ROSI)

Le management n'étant pas sensibilisé au risque de fraude et ne se sentant pas concerné par la possibilité d'une fraude interne, c'est l'argument de conformité à la LSF qui finalement décide la société à revoir ses habilitations, afin de se conformer aux nouvelles obligations de contrôle interne informatique.

Avantages

L'approche par les « normes et standards » est complémentaire aux méthodes d'analyse de risques ou d'évaluation des enjeux, plus simple, et plus facile à implémenter. Elle a comme principal avantage de permettre aux sociétés de se prémunir contre le risque de négligence et donc de poursuite par des tiers. C'est une approche viable à court terme qui repose sur l'efficacité des standards utilisés et qui est une très bonne base de départ, pour les entreprises n'ayant pas encore atteint un premier niveau de maturité en sécurité.

Enfin, c'est une approche souvent utilisée pour mener des audits internes ou externes. Les audits internes ou externes permettent de faire un état des lieux et de sensibiliser le Business sur la base d'un référentiel métier : finance avec la LSF, santé avec la FDA, IT avec le référentiel qualité... Etant donné l'importance de ces audits, les projets de mises en conformité sont en haute priorité ce qui amène à renforcer la sécurité efficacement et rapidement. Enfin, avec l'appui de la qualité, un audit permet également d'aligner les processus et systèmes au référentiel qualité de l'entreprise.

Limites

Parce que basée sur des standards, l'approche par les « normes et standards » comporte le risque de s'éloigner des spécificités propres à l'entreprise. Il existe des risques inhérents à l'entreprise qu'il faut savoir prendre en compte. Enfin, elle ne constitue pas, à proprement parler pour les puristes, une variante de « ROSI » puisqu'elle ne prend pas directement en compte les coûts financiers.

2.3.6 ROSI orienté benchmarking

Cette approche s'appuie sur des pratiques observées chez la concurrence et les grands représentants du secteur d'activité.

Exemple :

Scénario considéré

Etude comparative des choix stratégiques de la société avec ceux du marché (par rapport au référentiel de son choix : enquête annuelle de sécurité CLUSIF, enquête annuelle de sécurité CSI/FBI, enquête annuelle de sécurité Ernst & Young, etc…) – Sur la base de ces informations, notre entreprise fait le constat qu'elle se trouve le plus souvent positionnée dans les minorités

Solution proposée

Adopter les choix stratégiques ayant prouvé leur efficacité des autres acteurs du marché

Retour sur investissement (ROSI)

Pression du marché, rejoindre la majorité.

Avantages

Le benchmarking fournit aux sociétés une capacité d'identification, chère à beaucoup de dirigeants.

Limites

Le benchmarking ne prend pas en compte les spécificités individuelles de chaque entreprise et ne constitue pas à proprement parler une variante de « ROSI » puisqu'il ne prend pas forcément en compte la notion d'investissement.

3 COMMENT CHOISIR SON ROSI ?

3.1 Préambule

Nous venons de le voir, il existe plusieurs types de ROSI. L'enjeu principal auquel se heurte le responsable de la sécurité des S.I. est donc de savoir sélectionner, selon des critères définis, le ROSI qui sera le plus efficient dans son contexte.

Le contexte culturel de l'entreprise détermine la façon de justifier l'investissement en sécurité des S.I. tout comme apparaît déterminante la maturité des décisionnaires à l'égard de la sécurité du système d'information.

Au stade actuel de l'état de l'art, il ne semble pas qu'une approche idéale du ROSI puisse être privilégiée *:*

- à un ROSI **purement quantitatif,** basé par exemple sur des **statistiques d'incidents** (type ALE), il y aura toujours possibilité d'opposer la **pertinence du référentiel** utilisé sauf, si celui-ci est défini et alimenté par l'entreprise elle-même. (cf. Bâle II[12])

- à un ROSI **purement qualitatif** basé, par exemple, sur la mise en exergue des risques potentiels, il y aura toujours possibilité d'opposer la **probabilité d'occurrence et la rigueur mathématique.**

Parce que d'une part, le ROSI est parfois difficilement quantifiable sur certains projets de sécurité tel que, par exemple, la mise en œuvre d'une campagne de sensibilisation, et que, d'autre part, le seul argument qualitatif n'est pas recevable par tous les décisionnaires, il est souhaitable d'adopter une démarche qui s'appuie sur l'une et/ou l'autre approche en fonction de facteurs contextuels que nous allons développer par la suite.

3.2 Critères de sélection du ROSI

Si l'on admet que la notion de ROI s'utilise dans le cadre de la justification d'investissements liés à des projets nouveaux, une approche permettant d'organiser la démarche de réflexion prenant le projet comme « point de départ » semble appropriée.

Le propos qui suit présente ainsi quelques pistes exploratoires du ROSI selon le type de projet envisagé, en considérant deux cas de figures :

- le **projet « métier »** : financé par une maîtrise d'ouvrage (opérationnelle ou fonctionnelle), il répond à un besoin métier pour lequel la sécurité ne constitue que rarement la finalité première

- le **projet « sécurité du système d'information »** : financé en général par la maîtrise d'ouvrage SSI (RSSI) ou la DSI, il répond souvent à une problématique sécuritaire transverse (par exemple, dispositif centralisé de gestion/administration de la lutte antivirale, PKI, gestion centralisée des habilitations, WEB SSO, architecture d'accès

[12] Recommandations sur la gestion et la couverture des risques opérationnels associés aux opérations bancaires

distants, monitoring de la sécurité, …). Un tel projet peut également être financé par les centres de coûts (filiales, sites) alors que celui-ci a été décidé en central (par exemple, plan de continuité, programme de sensibilisation, …).

A partir d'un positionnement du projet envisagé (« métier » versus « sécurité SI »), il s'agit d'identifier, au travers de l'élaboration d'une cartographie, les meilleurs moyens d'évaluation du ROSI dans le contexte concerné.
Les résultats de la cartographie contextuelle devraient permettre d'orienter la construction de l'argumentaire ROSI selon **quatre approches complémentaires** :

- une approche par les **risques sécurité S.I.** : la justification est opérée au travers d'une approche classique d'identification du **risque potentiel maximal**[13], en se référant si nécessaire aux bonnes pratiques et à d'éventuels benchmarks ;

- une approche par la **sinistralité S.I.** : la justification est opérée sur la base de **statistiques de sinistralité** (fréquence / impact) que l'entreprise aura choisi a priori comme « référence » en matière d'aide à la prise de décision et sur des **approches de quantification** (telles l'ALE, voir plus haut);

- une approche fondée sur les **enjeux de l'entreprise** : la justification privilégie les **apports complémentaires** (renforcement de l'image de marque, développement de la confiance, etc. …) et la **valeur ajoutée** de la sécurité à l'égard des objectifs métier du projet, tout en s'appuyant, les cas échéant, sur des arguments **qualitatifs** ou quantitatifs (s'ils existent)

- une approche par **l'amélioration de la performance** de certains processus de gestion (dans le domaine de la lutte antivirale par exemple, la mise en place d'un outil d'administration centralisée des versions de moteurs / bases de signatures pourra induire des **gains de productivité** dans la gestion « au quotidien » et également réduire le coût du traitement des infections)

Enfin, trois facteurs (voir description détaillée en section 3.4) vont influencer le choix du type d'approche :

- le **contexte économique :** Secteur d'activité et métier de l'entreprise (banque, assurance, santé, chimie, industrie, organisme public, gouvernemental, etc…)

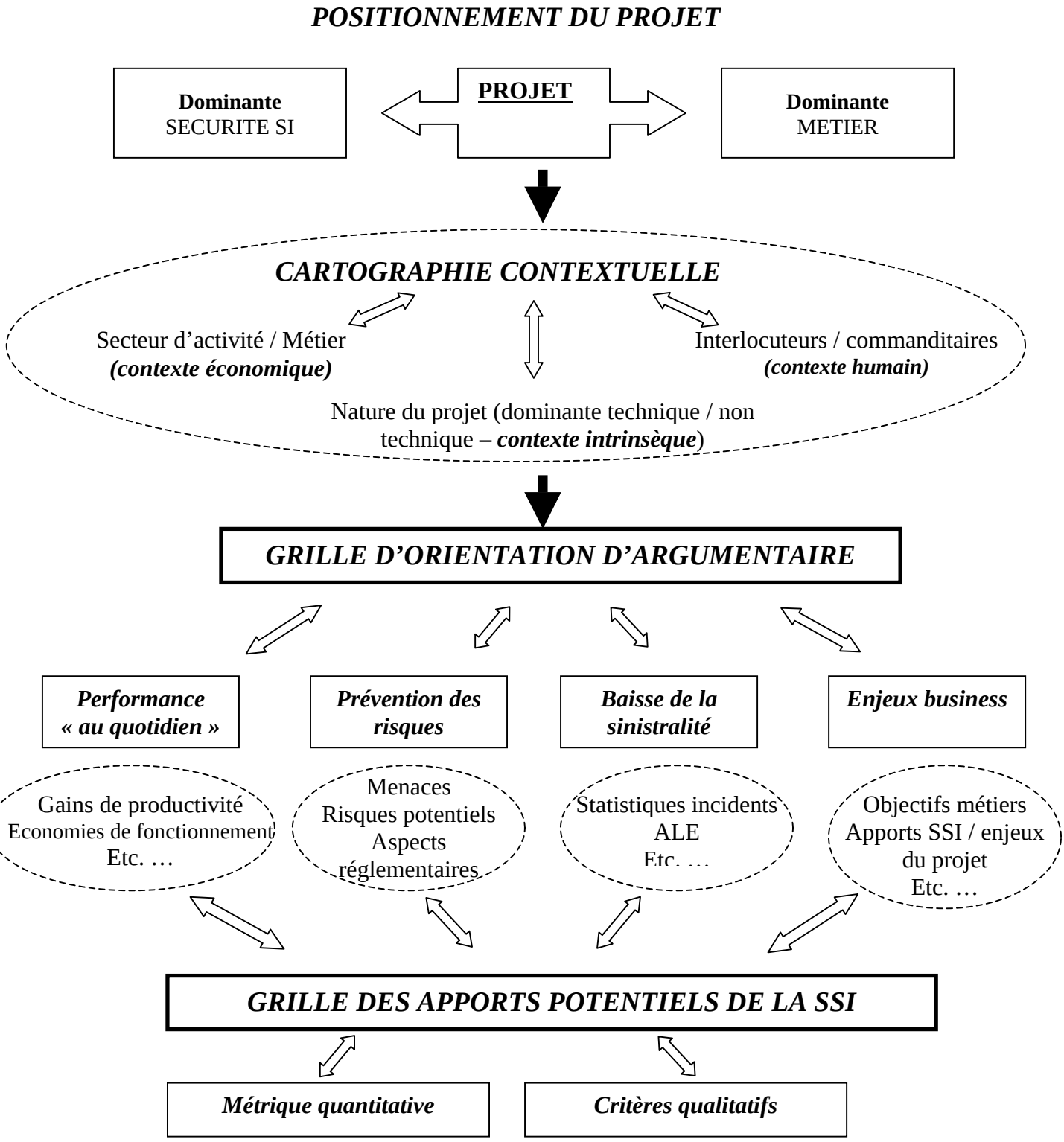
- le **contexte humain :**Profil des interlocuteurs du projet, des décideurs en particulier (formation technique, non-technique, culture sécuritaire, etc…)

- le **contexte intrinsèque** au projet de sécurité lui-même (dominante technologique, organisationnelle, sensibilisation, etc…)

[13] sans considération de probabilité

3.3 Synthèse de la démarche du CLUSIF

3.3.1 Synoptique méthodologique



3.3.2 Contenu méthodologique

3.3.2.1 Etape 1 : Positionnement du projet

La première étape consiste à « positionner » le projet selon deux axes directeurs qui vont influencer le contenu du « discours ROSI », en tenant compte des interlocuteurs qu'il y aura lieu de convaincre :

- **Dominante métier** : importance d'un argumentaire sécurité orienté « Support à l'atteinte des objectifs métier » du projet (exemple : serveur WEB commercial, place de marché, …)

- **Dominante sécurité SI** : importance d'un argumentaire sécurité orienté « Réduction de l'un des risques opérationnels majeurs » de l'entreprise

Cette étape peut également avoir pour objectif d'identifier la Direction qui supportera les coûts du projet.

3.3.2.2 Etape 2 : « cartographie contextuelle » du projet

La deuxième étape consiste à identifier les critères les plus pertinents pour justifier le ROSI dans le contexte du projet envisagé.

- **Contexte économique** :

    - a-t-on affaire à une entreprise ayant une forte culture en matière de gestion du risque (par exemple, la banque ou les organismes financiers) ?

    - a-t-on affaire à une entreprise ayant des contraintes sécuritaires réglementaires fortes (par exemple, le secteur de la défense) ?

    - a-t-on affaire à une entreprise évoluant dans un secteur d'activité où le Savoir-faire industriel représente un avantage concurrentiel « vital » (par exemple, l'aéronautique) ?

    - etc.…

- **Contexte humain** :

    - a-t-on affaire à une entreprise ayant une forte culture de sécurité individuelle ?

    - a-t-on affaire à une entreprise où la gestion de la confidentialité est ancrée dans les comportements ?

    - quels sont les niveaux de sensibilisation du commanditaire et de l'équipe projet à l'égard de la sécurité des S.I. ?

- quels sont les niveaux de culture technique du commanditaire et de l'équipe projet à l'égard de la sécurité des S.I. ?

- etc.…

- **Contexte intrinsèque** :

  - est-ce un projet à dominante technologique vis-à-vis duquel le poids du discours « d'experts » sera essentiel ?

  - est-ce un projet à dominante organisationnelle sensible à tout argumentaire orienté amélioration de processus interne ?

  - est-ce un projet à dominante comportementale, dont l'aboutissement est très tributaire de la culture sécuritaire de l'entreprise ?

  - etc.…

La cartographie contextuelle conduit à l'élaboration d'une **grille d'orientation d'argumentaire** permettant à son utilisateur d'identifier les points d'ancrage clés de son futur discours en matière de ROSI (ventilés au sein des quatre approches). Charge à lui de l'exploiter dans le sens qui conviendra le mieux à l'égard des interlocuteurs à convaincre

Exemple de grille d'orientation d'argumentaire

Le tableau qui suit présente un exemple de grille d'orientation d'argumentaire utilisable dans le cadre de l'étape de « cartographie contextuelle » du projet. Destinée à permettre à son utilisateur d'identifier les **points d'ancrage clés** de son futur argumentaire en matière de ROSI, elle mérite toutefois d'être personnalisée en fonction du contexte de chaque entreprise (*) :

- ajout d'axes d'analyse contextuelle spécifiques, renforcement du questionnement

- choix (et pondération éventuelle) des dominantes contextuelles majeures (axes d'analyse et questionnement) pour chacune des quatre approches

- autres critères contextuels …

La réponse à chaque question permet de privilégier plus ou moins (de « +++ » à « + ») la nature du discours à développer dans le contexte du projet

+	adapté
++	pertinent
+++	très pertinent

Il appartient donc à son utilisateur de faire une lecture de la grille en « cochant », pour chaque question qu'il juge pertinente dans le contexte du projet, les « + » associés. La grille, une fois remplie, lui permettra ainsi d'identifier les dominantes du discours à construire.

(*) : on peut penser en effet que plusieurs grilles d'orientation d'argumentaire puissent être élaborées selon le contexte général au sein duquel le projet est envisagé (métier/activité, secteur géographique, culture (anglo-saxonne / latine), …

Grille d'orientation d'argumentaire – Exemple

Axes d'analyse contextuelle	*Questionnaire*	***Discours à privilégier***			
		Par les risques	*Par la sinistralité*	*Par les enjeux business*	*Par la performance*
Nature du projet	• Le projet est-il à dominante organisationnelle ou humaine ? • Le projet est-il à dominante technique ? • **La sécurité apporte-t-elle une forte valeur ajoutée à l'égard du projet ?** • Le projet présente-t-il une forte criticité à l'égard de la continuité de service ? • **Le projet supporte-t-il un processus critique en terme d'intégrité (confidentialité, disponibilité, fiabilité) ?**	++ + +	++	+++ +++ +++	+++
Contexte du projet	• Le projet concerne-t-il un secteur d'activité à forte culture de gestion de risque (défense, banque, …) ? • **A-t-on une bonne connaissance des enjeux métier du projet ?** • La sécurité peut-elle réduire certains coûts de fonctionnement (amélioration de la productivité) ? • La sécurité peut-elle optimiser l'organisation (éviter des redondances, optimiser l'utilisation de technologies ou de compétences, améliorer la performance de certains processus, …)? • **Un incident de sécurité peut-il remettre en cause les profits escomptés du projet ?**	+++ ++		+ +++ + + +++	+++ +++
Profil des décideurs à l'égard du projet	• Les décideurs ont-ils confiance au « bon sens » en matière de gestion du risque ? • Les décideurs ont-ils une culture technique forte ? • Les décideurs ont-ils une forte « culture financière et/ou comptable » ? • Les décideurs ont-ils un profil commercial ou business ?	++ ++	++	+++	
Environnement légal et réglementaire de l'entreprise	• Le management de l'entreprise est-il fortement sensibilisé aux impératifs légaux et/ou réglementaires imposé à l'activité ? • **Secteur d'activité de l'entreprise est-il très réglementé en matière de sécurité ?** • **Le projet présente-t-il une forte dépendance à l'égard de la réglementation en matière de sécurité ?** • La direction Générale de l'entreprise s'est-elle prononcée sur des impératifs réglementaires exigés	+++ +++ ++ +++		+++	
Culture sécuritaire de l'entreprise	• Le management de l'entreprise est-il sensibilisé à la gestion du risque ? • Le dispositif de contrôle interne de l'entreprise est-il très mature ?	+++ ++			
Caractéristiques du cadre de management des risques au sein de l'entreprise	• Existe-t-il une forte incitation du management (objectifs, évaluation, …) à l'égard de la gestion du risque ? • Existe-t-il une « sensibilité culturelle qualitative » au sein de l'audit et du contrôle interne ? • Existe-t-il une « dominante culturelle financière » au sein de l'audit et du contrôle interne ? • **Y-a-t-il une forte intégration des objectifs des métiers de l'entreprise dans le cadre de référence sécuritaire (politique, règles et principes généraux, …) ?**	+++ ++ +	++	+++	
Gestion des incidents	• Accorde-t-on de la crédibilité aux statistiques et études de marché en matière d'incidents SI ? • Existe-t-il un référent statistique à l'égard des incidents liés au SI (fréquence, coût) ?	++	++ +++		
Benchmark	• Le management est-il sensible aux différentes études comparatives à l'égard de la sécurité SI publiées sur le marché ?	++		++	
Normes et standards	• Le management est-il réceptif à l'application des meilleures pratiques en matière de sécurité SI (ISO 17799, ITSEC, ISO 1508…) ? • Le management s'inscrit-il dans une politique de sécurité de son système d'information (ISO 13335) ?	++ ++	 +	++ ++	 +

3.3.2.3 Etape 3 : synthèse des apports potentiels de la sécurité

Une fois la grille d'orientation d'argumentaire élaborée, il paraît utile de la compléter par une synthèse des **apports** du projet sécurité en tant que tel ou du « volet sécurité » s'il s'agit d'un projet à dominante métier. Celle-ci vient en appui au discours qui sera délivré auprès de chaque interlocuteur. En s'appuyant sur les points d'ancrage clés du discours mis en évidence à l'étape précédente, cette grille résume les enjeux sécuritaires selon des métriques **quantitatives** et/ou **qualitatives**. Un exemple de cette grille est proposé plus loin.

Exemple de grille des apports potentiels de la SSI

Le tableau qui suit propose, selon le **questionnaire clé mis en évidence** lors de l'étape de cartographie contextuelle, des critères potentiels susceptibles d'étayer le « discours ROSI » et le type de métrique « Qualitative » versus « Quantitative » à construire. Il est évident que ce tableau est complètement dépendant du projet considéré.

Axes	Questionnement clé identié	Critères potentiels	Type de métrique
Réduction des risques	Le projet présente une forte dépendance à l'égard de la réglementation en matière de sécurité	Respect de la réglementation	Qualitative
	Le projet présente une forte criticité à l'égard de la continuité de service	Limitation des pertes financières potentielles	Quantitative
		Prévention du risque de dégradation de l'image	Qualitative
Réduction de la sinistralité	Il existe un référent statistique à l'égard des incidents applicable au projet (fréquence, coût)	Réduction nombre / fréquence incidents	Quantitative
		Réduction du montant des pertes	Quantitative
Appui aux enjeux business	Le projet présente une forte criticité à l'égard de la continuité de service	Amélioration confiance	Qualitative
		Création d'avantage concurrentiel	Qualitative
	Le projet présente une forte dépendance à l'égard de la réglementation en matière de sécurité	Respect de la réglementation	Qualitative
		Certification / Accréditation	Qualitative
Amélioration de la performance	La sécurité peut optimiser l'organisation (éviter des redondances, optimiser l'utilisation de technologies ou de compétences, améliorer la performance de certains processus, …)	Réduction des coûts (fonctionnement, administration, support, …)	Quantitative
		Amélioration de la productivité	Quantitative
		Amélioration de la qualité (augmentation d'un niveau de SLA, …)	Quantitative
	…/…	…/…	

Rappel des coûts du projet	Investissements :	Fonctionnement :

3.3.3 Paramètres de déclinaison du discours ROSI

Le tableau qui suit rappelle un certain nombre de paramètres dont il y a lieu d'être conscient, une fois l'orientation du discours ROSI définie (voir § précédent) et qui vont **faciliter** ou, au contraire, **limiter** la portée et l'efficacité du discours optimal à tenir. Sans être évidemment exhaustifs, trois axes caractéristiques ont été identifiés :

- Les **facteurs clés de succès** utiles au support de l'approche choisie
- Les **contraintes** susceptibles de contrecarrer l'approche choisie
- Les **outils d'appui** potentiels

	Approche			
	Par les risques	Par la sinistralité	Par les enjeux business	Par l'amélioration de la performance
Facteurs clés	• Faire référence à un cadre législatif et/ou réglementaire • Cartographier les risques métiers, juridiques et techniques, dans le contexte du projet • Avoir affaire à un décideur sensible aux arguments liés aux principes de base en gestion des risques (RSSI, DSI, …) • Disposer de benchmarks dans des contextes identiques • …/…	• Choisir / imposer une stratégie « en tendance » en matière de statistiques incidents • Définir un « référent incidents » • Définir et mettre en place le processus d'alimentation du référent • Avoir affaire à un décideur sensible aux arguments financiers et mathématiques (ex : DAF) • …/…	• Décliner les objectifs métier liés au projet • Identifier des indicateurs de performance / objectifs • Elaborer une métrique du ROSI dans le contexte du métier impacté par le projet • Renforcer l'argumentaire par des éléments issus d'une approche qualitative • …/…	• Recourir aux outils et critères d'évaluation de la performance habituellement utilisés dans l'entreprise, notamment dans le cadre de projets technologiques SI : • Réduction du taux de pannes, • Réduction des charges d'intervention sur incidents, • Réduction des charges d'administration de certains dispositifs, • Amélioration du service à l'utilisateur final, • …/…
Contraintes	• Niveau de culture SSI « qualitative » des décideurs ? • Manque de rigueur ou de fondement mathématique • …/…	• Nécessité de faire admettre le principe de la stratégie « en tendance »par la DG • Nécessité de faire valider le « référent incidents » par la DG • …/…	• Difficulté de valorisation de certains enjeux « intangibles » ou liés au patrimoine immatériel de l'entreprise (développement de la notoriété de la marque, accroissement de l'image de l'entreprise, augmentation des parts de marché, …)	• Réduction de l'enjeu du projet à sa seule composante « productivité »
Outils / Support	• Elaborer une « métrique d'impact entreprise » • Disposer d'une métrique non financière de quantification des bénéfices d'un projet (définie par la direction financière ?) • Mettre en place un système d'indicateurs spécifiques (évaluation des gains a posteriori) • Certification BS 7799 • …/…	• Disposer d'une base incidents (coûts / fréquence) • Recourir à des statistiques « de référence » (FBI/CSI, éditeurs de solutions/outils de sécurité,…) • …	• Disposer de critères d'analyse de la valeur, en distinguant, par exemple, l'augmentation de valeur ajoutée et le maintien du niveau de valeur actuel	• Disposer de métriques de performance et de productivité reconnues au sein de l'entreprise

3.3.4 Détermination de la métrique

Une fois l'approche ROSI déterminée, il est nécessaire de mettre au point une métrique pour venir étayer les arguments et mesurer les gains potentiels. L'objectif est de définir une matrice d'évaluation des facteurs objectifs qui déterminent ou influencent :

- Le « discours ROSI » (Communication interne, externe vers la hiérarchie,; vers le personnel; commerciale, non commerciale, etc…).
- Le positionnement du projet.
- Le « poids » de chacun des types d'arguments en fonction de la « cartographie contextuelle » du projet.

Elle peut être aussi un moyen de validation a posteriori (à période d'amortissement ou exercice échu) du ROSI.

Suivant l'approche choisie, selon que l'on décide d'aborder les coûts tangibles ou intangibles de la sécurité, on s'orientera vers des paramètres tantôt quantitatifs tantôt qualitatifs, en fonction de la difficulté à mesurer les différents éléments à prendre en compte.

Qualitatifs :

- Observable (tendance : par exemple, croissance ou décroissance)
- Mesurable (approximation : par exemple, forte ou faible croissance)

Quantitatifs :

- Quantifiable (chiffrable : par exemple 10%)
- Financier (chiffrable financièrement parlant : par exemple : +1M€)

Les métriques sont déjà souvent utilisées pour l'élaboration de calculs analytiques (paramètres quantitatifs financiers : diminution d'appels facturés, réduction du coût des connexions nécessaires aux différentes applications métiers) et peuvent aussi l'être pour renforcer un suivi qualitatif dans les cas de solutions relativement sophistiquées (intégration de mesures des incidents, verrouillage de procédures de connexion dans une politique sécurité, contrôle statistiques sur des flux applicatifs…).

Quoiqu'il en soit, chaque projet aura sa propre grille de métrique. Le nombre et les types de métriques utilisés pour faire valoir le ROSI d'un projet ou de l'acquisition d'une solution sécurité sont liés à la nature du projet.

L'avantage de la grille de métrique est de faire connaître le poids objectif des éléments auxquels seront « sensibles » les personnes impliquées de l'entreprise suivant leur culture, leur sensibilisation à la sécurité et autres facteurs définis dans l'approche proposée.

Enfin, elle efface l'alternative « Quantitatif **vs** qualitatif », nécessaire dans la phase de formalisation des différents éléments, pour ne laisser apparaître qu'une méthode dite « mixte », le contexte décidant de la dominante qualitative ou quantitative.

3.3.4.1 Exemple de grille de métrique appliqué à une solution de VPN

L'exemple qui suit illustre un projet d'implantation de VPN site à site (10) et site/clients distants, avec authentification renforcée.

Paramètres	Valeurs
Nombre d'utilisateurs	300
Nombre d'utilisateurs mobiles	30
Nombre de login/utilisateur/mois sans VPN	155
Nombre d'erreurs utilisateur/mois sans VPN	23,25
Tps de recherche du problème par l'utilisateur	~ 2 mn
Gain de performance du fait du VPN	(23,25*2)= 46,5 mn
Delta temps d'un login (Modem – VPN)	0, 20 mn
Temps de login gagné/utilisateur/mois	31mn
Nombre d'erreurs /utilisateur/mois donnant lieu à un appel au support	~ 4,65
Tps moyen d'un appel support	5 mn
Economie réalisée en tps support	23,25 mn
Coût horaire salarial	20 €.
Productivité gagnée/utilisateur/mois :	(20/60)*(46,5+31) = 19,17 €
Economie support réalisée/utilisateur/mois (hors coût télécoms):	[(20/60)*5]*4,65 = 1,67*4,65=7,75 €
Economie Modems- ADSL	(100 € *30 modems.*12)-(144 € *10 sites*12) = 36000-17280= 18620 €
Economie de transfert de cassettes (agrégation de BDD)	30 €*10*12 = 3600 €

Le nombre et les intitulés des colonnes « métriques » du tableau suivant, sont propres à l'exemple considéré, et changeront à chaque fois en fonction du contexte du projet.

Métrique d'évaluation du ROSI – Exemple appliqué à une solution VPN avec authentification forte

Composants Projet	Quantitatif							Qualitatif			
	Financier		Métriques opérationnelles					Conformité Règlement (1 à 5)	Assurance qualité (1 à 5)	Image (1 à 5)	Confort (1 à 5)
	Economie	Gains	Performance	Sinistralité	Appels supports	…	Incidents	*1 : un peu efficace à 5 : très efficace*			
Concentrateur VPN	*1,67*1255,5 *12 = 25 160,22 €*	*(19,17*270)*12= 62110,8 €*	*Connexions supp : 23,25*		*4,65*270 = 1255,5*			*3*	*5*	*5*	*3*
Pare-feux sites distants	*111 600 € (risques couverts)*			*(intrusion, vol d'info, altération…) 0,4/an*			*0,06 (électrique, incendie, pannes..)*	*3*	*4*	*2*	*2*
Lignes télécoms	*18 620 €*		*1 Mb/s*					*na*	*4*	*na*	*4 (débits)*
Clients (Auth. Forte)	*comptabilisé*	*comptabilisé*						*5 (Auth. Forte)*	*5 (tracabilité)*	*5 (Auth bio)*	*4 (Fiabilité)*
Serv. d'authentification								*5 (Auth. Forte)*	*5*	*na*	*4 (Admin.)*
Sites dist.	*Transfert datas 3600 €*		*Applications Intersites*						*3*	*Na*	*5*
Acquisition	*300*165 € = -44550 €*										
Etude	*-1 5000 €*										
Déploiement clients distants	*12j ~ - 4600 €*								*4*	*3 (SLA interne service informatique)*	*5 (tracabilité)*
Gestion incidents clients Administration distante	*- 1,67*120*12 = -2404, 8 €*				*0,4*300 = 120*				*3 (traçabilité)*	*3 (SLA interne service informatique)*	*4 Remote Admin.*
…											
TOTAUX	*-14571,2 €*	*62 110,8 €*						*10% actifs €*	*€*	*€*	

Dans le cas étudié, la disproportion des coûts entre la solution des modems (télécoms+centre d'appel) et celle d'une solution ADSL sécurisée est telle que la solution proposée est amortie la première année.

Par ailleurs, les aspects qualitatifs peuvent être chiffrés selon : les normes réglementaires (couverture financière du risque), l'adoption d'une norme qualité ou en fonction de la valorisation de l'image de la société.

C'est donc en fonction de ces résultats (totaux) et du métier de l'entreprise, que le promoteur du projet orientera son argumentaire.

3.4 Facteurs d'influence du choix du ROSI

3.4.1 Secteur d'activité et métier de l'entreprise

Il est certain que l'on ne justifiera pas les dépenses de sécurité de la même façon selon le secteur d'activité de l'entreprise. Ainsi l'on peut supposer qu'un organisme public en restriction budgétaire aura des moyens différents d'une entreprise du secteur pharmaceutique en pleine croissance. De la même façon, tandis que certains RSSI ont un budget très strictement alloué et surveillé, d'autres n'ont pas à rendre compte du coût des solutions qu'ils choisissent ;

Enfin, selon le type de secteur de l'entreprise, un certain nombre de « standards » ou de contraintes juridiques vont venir appuyer le discours de la gestion des risques.

Ci-après un tableau présentant un panorama non exhaustif des principales réglementations susceptibles d'impacter la stratégie sécurité des S.I. dans différents secteurs.

Secteur	Finance	Santé	Aéronautique
Exemple d'exigences juridiques applicables ayant un impact sur la sécurité des S.I.	- Bâle II - CRBF 97-02	- recommandations CNIL au domaine de la santé suite à la loi du 6 janv 78 sur la protection des données personnelles - loi du 4 mars 2002 pour le libre accès des patients aux données de santé - accréditation ANAES aux USA, standard HIPAA	- Aux Etats Unis, la commission du Président sur les infrastructures critiques a ordonné à la FAA de mettre en place un programme de protection de la sécurité de l'information aérienne - En Europe, l'agence européenne de sûreté aérienne (AESSA) est en charge de veiller à ces aspects.
Tous secteurs	- lois sur les comptabilités informatisées et l'archivage fiscal - lois sur la réglementation des moyens cryptographiques - exigences CNIL - exigences INPI - signature électronique - nouvelle loi sur la sécurité financière (LSF) vis à vis du contrôle interne et notamment du contrôle interne informatique - Sarbanes-Oxley		

3.4.2 Profil des interlocuteurs

Le choix du discours d'argumentation de la sécurité dépend également fortement du profil de l'interlocuteur à convaincre. On ne justifiera pas de la même façon un investissement selon que l'on s'adresse à un dirigeant très orienté « chiffres » , à un directeur financier, à un ingénieur ou à un directeur fonctionnel .

Certains en reviennent toujours aux chiffres et sont donc plus sensibles à l'approche quantitative, tandis que d'autres sont tournés vers des alternatives plus qualitatives, orientées « analyse de la valeur ». Enfin, certains dirigeants sont très réceptifs à la tranquillité d'esprit et estiment que « la sécurité n'a pas de prix », tandis que d'autres attendront d'avoir essuyé un incident avant de commencer à réagir.

Ainsi, pour un interlocuteur technique, la technologie est souvent mise au premier plan au détriment de la rentabilité de l'investissement. Un administrateur système fera par exemple le choix de déployer un pare-feu sur la base de ses fonctionnalités techniques sans mettre en balance le risque qu'il est censé réduire et le coût de l'investissement.

Pour un manager plus fonctionnel (par exemple un Directeur Financier ou certains Directeurs Informatiques), dont le souci principal est la rentabilité des investissements, il sera souvent plus pertinent de mettre en avant une approche financière du ROSI. Ainsi dans l'exemple du pare-feu, on construira plutôt un argumentaire dans lequel on démontrera le retour sur investissement lié à la mise en place du pare-feu.

3.4.3 Nature du projet

Peut-être le critère le plus évident, la nature du projet elle-même va également déterminer quel type d'approche choisir.

Le tableau ci-après présente comment certains types de projet vont avoir tendance à demander un argumentaire plutôt quantitatif que qualitatif, même si les autres facteurs vus précédemment influencent également le choix final du ROSI. A noter toutefois qu'il n'existe pas de façon unique de justifier un même investissement.

Plutôt Quantitatifs, projets « technologiques »	Plutôt Qualitatifs, projets « organisationnels »
- les équipements réseau (VPN, PKI, …) - les moyens de réponse aux incidents - les moyens de sauvegardes de nuit - le chiffrement - les moyens de contrôle d'accès centralisé - les firewalls - le logiciel de verrouillage d'écran - les moyens de management de la sécurité - l'équipement de filtrage sur les routeurs et autocommutateurs - l'anti-virus - les systèmes de détection d'intrusion	- la politique de sécurité - l'organisation - la sensibilisation - l'analyse de risques - l'élaboration de procédures - la continuité d'activité

4 PREPARATION DU DOSSIER D'ARGUMENTATION « ROSI »

Quel que soit le ROSI que le RSSI choisira en fin de compte, la démarche passe par l'identification des risques du projet, l'implication d'acteurs clés et la préparation d'un dossier d'argumentation.

4.1 La sécurité : Un projet de gestion de risques

Pour optimiser le retour sur investissement il faut, soit diminuer l'exposition au risque (avoir moins à perdre), soit diminuer le coût global du projet (TCO).

Que l'on choisisse de justifier le retour sur investissement en sécurité par une approche financière, quantitative ou qualitative, il existe quatre leviers possibles pour optimiser ce retour sur investissement, communs à tous types de projets :

- Diminuer les pertes et risques opérationnels
- Diminuer les investissements
- Etablir le bon compromis entre les dépenses de protection (Sécurité) et l'étendue des risques que l'on choisit de couvrir
- Accélérer le planning d'accès aux résultats

Par ailleurs, dans sa démarche le RSSI devra connaître les éléments suivants pour pouvoir par la suite argumenter son ROSI :

- les objectifs de l'entreprise en matière de sécurité
- les contraintes réglementaires sectorielles ou non qui s'appliquent au contexte particulier de l'entreprise (Bâle II, LSF, HIPAA, signature électronique, CNIL,…)
- les risques sur le système d'information accompagné, autant que possible d'une analyse des risques avec quantification de l'impact, estimation de la probabilité d'occurrence et hiérarchisation des risques et **en particulier d'une comparaison du coût de la solution (achat et maintenance) avec le coût du sinistre s'il survenait**
- les ressources nécessaires à la réussite du projet : quelles ressources seront dédiées au projet ? Ces ressources seront-elles partagées avec d'autres métiers / directions ? quelles sont les contraintes budgétaires ? la date butoir ? le TCO (Total Cost of Ownerhsip – coût du projet)
- L'identification de la métrique nécessaire au calcul du ROSI

4.2 Les acteurs clés

Pour monter son dossier de justification de l'investissement sécurité, le RSSI peut :

- Solliciter la Direction du Contrôle Interne / le Risk Manager
    - Obtenir un correspondant du Contrôle Interne ou du Risk Management sur le projet et valider le plan de gestion des risques avec eux
    - Présenter les résultats de l'analyse de risque au management afin d'obtenir une première validation des risques acceptables / non acceptables par le contrôle interne
- Collaborer avec la Direction Financière
    - Comprendre les enjeux financiers sur les projets similaires et les attentes du comité exécutif dans ce type de cas
    - Définir avec la Direction Financière les critères économiques, comparer les risques potentiels avec le coût du projet (TCO)
    - Etudier les diminutions de coût possibles au niveau des ressources
    - Mettre au point une métrique qui permettra de refléter les progrès du projet : réponse sur incident, détection d'intrusion, coût évité
    - Capitaliser, fédérer ce qui est possible sur d'autres projets
    - Choisir le mode de calcul du ROSI et faire valider le calcul du ROSI par la direction financière avant toute présentation aux autres directions

De plus, le RSSI doit :

- Sensibiliser le Management et obtenir son sponsoring
    - Identifier le plus haut niveau de direction impacté par le projet
    - Formaliser les attentes des sponsors
    - Identifier les tâches leur incombant (financement, mise en place de l'organisation, gestion des ressources, etc…)
    - Leur présenter comment le plan de gestion des risques répond à leurs attentes sous
        - 1) l'angle stratégique/tactique des actions à mener
        - 2) l'angle financier
        - 3) l'angle du contrôle interne et de la gestion des risques d'entreprise

- Obtenir leur acceptation du plan de gestion des risques
- Leur fournir un reporting basé sur les indicateurs clés sécurité du projet

4.3 Contenu du dossier d'argumentation

En complément de la grille d'orientation de l'argumentaire et du tableau de synthèse des apports potentiels de la sécurité, le « dossier ROSI », partie intégrante du projet, doit également exposer :

1. Les contraintes réglementaires auxquelles répond le projet et comment cette conformité aux exigences réglementaires est contrôlée ou mesurée au travers d'indicateurs ;

2. les objectifs stratégiques du projet : le plan doit décrire comment le projet s'articule éventuellement dans un projet plus transversal de l'entreprise (sécurité des établissements, plans de continuité, etc…) et comment il s'inscrit dans la politique globale de sécurité ;

3. Les économies d'échelles (mutualisation notamment) escomptées : toute partie de coût mutualisée en interne ou en externe doit être mentionnée afin de faire réaliser l'économie ;

4. l'alignement avec les méthodes de contrôle interne : utiliser les outils du contrôle interne pour la métrique de gestion des risques ;

5. le plan de financement/ retour sur investissement du projet : montrer l'alignement avec les objectifs de l'entreprise.

5 L'OUTILLAGE DU ROSI

5.1 Les bases de connaissances

Nous l'avons vu plus haut, tout calcul de ROSI qui se voudrait être basé sur une approche quantitative dépend de la fiabilité des tables de coûts qui sont utilisées. Or comme aucune base commune de calcul de ces coûts et de définition de la terminologie n'est fournie par les organismes lors des enquêtes annuelles de sécurité, les chiffres publiés dans les magazines de sécurité doivent être pris avec précaution.

Pour étayer le point de vue, on pourra utiliser les tableaux publiés par le CSI/FBI[14], par Information Week et par Information Security Magazine. On devra cependant tenir compte, pour leur interprétation, du fait que ces organismes annoncent clairement que les enquêtes, dont ils sont le résultat, n'ont pas été menées scientifiquement, sont purement illustratives et ne doivent pas être interprétées autrement.

2003 CSI/FBI Computer Crime and Security Survey

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 48-month period

In 2003, 75% of our survey respondents acknowledged financial losses, but only 47% could quantify the losses.

How Money Was Lost

	Lowest Reported				Highest Reported				Average Losses				Total Annual Losses			
	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03
Theft of proprietary info.	$1K	$100	$1K	$2K	$25M	$50M	$50M	$35M	$3,032,818	$4,447,900	$6,571,000	$2,699,842	$66,708,000	$151,230,100	$170,827,000	70,195,900
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	199,350	541,000	214,521	27,148,000	5,183,100	15,134,000	5,148,500
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,000	346,0000	76,000
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,104,000	19,066,600	13,055,000	2,754,400
Insider abuse of Net access	240	100	1K	100	15M	10M	10M	6M	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200
Financial fraud	500	500	1K	1K	21M	40M	50M	4M	1,646,941	4,420,738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,370,500	65,643,300
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,000	27,382,340
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,124,725	275,636	300,00	31,254	22,554,500	6,064,000	4,503,000	406,300
Telecom fraud	1K	500	1K	100	3M	8M	100K	250K	212,000	502,278	22,000	50,107	4,028,000	9,041,000	6,015,00	701,500
Active wiretapping	5M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,000	0	0	705,000
Laptop theft	500	1K	1K	2400	1.2M	2M	5M	2M	58,794	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500
												Total Annual Losses	265,337,990	377,828,700	455,848,000	201,797,340

CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

[14] Computer Security Institute / Federal Bureau of Investigation

Table 4. Safeguard Reductions in Bad Event Frequencies						
	Info Theft	Info Mod.	Info Destr.	System Outage	Employee Theft	System Degrad.
Security Awareness	0.35	0.3	0.3	0.05	0.6	0.5
HW/SW Network Upgrade	0.45	0.45	0.45	0.45	0	0.45
Response Team	0.4	0.4	0.4	0.4	0	0.2
Nightly Back-ups	0	0	0	0	0	0
Encryption	0	0	0	0	0	0
Central Access Control	0.3	0.15	0.15	0	0.5	0
Firewalls	0.75	0.75	0.75	0.75	0.2	0.1
Screen Locking Software	0.15	0.2	0.2	0	0.4	0
Security Management Team	0.5	0.5	0.5	0.5	0.5	0.5
Comm Content Screening	0.75	0	0	0	0.3	0
Anti-Virus Software	0	0.35	0.4	0	0	0.4
Intrusion Detection System	0.51	0.51	0.51	0.51	0.25	0.51

Table 5. Safeguard Reductions in Bad Event Consequences						
	Info Theft	Info Mod.	Info Destr.	System Outage	Employee Theft	System Degrad.
Security Awareness	0	0	0	0	0	0
HW/SW Network Upgrade	0	0	0	0	0	0
Response Team	0	0.2	0.2	0.7	0	0.65
Nightly Back-ups	0	0.6	0.95	0	0	0
Encryption	0.95	0.95	0	0	0	0
Central Access Control	0	0	0	0	0	0
Firewalls	0	0	0	0	0	0
Screen Locking Software	0	0	0	0	0	0
Security Management Team	0	0	0	0	0	0
Comm Content Screening	0	0	0	0	0	0
Anti-Virus Software	0	0	0	0	0	0
Intrusion Detection System	0	0	0	0	0	0

Côté français, le CLUSIF publie tous les ans les chiffres de la sinistralité informatique mais nous ne disposons pas de chiffre de fréquence d'occurrence des sinistres.

5.2 Retour sur expérience

Un certain nombre d'éditeurs de solutions de sécurité ont publié des outils dits de « ROSI » pour permettre à leurs clients de calculer le retour sur investissement de leurs solutions de sécurité.

Ces outils évaluent le ROSI du point de vue strictement financier / comptable, pour ne considérer que les économies potentielles sur des bases de coûts estimés (incidents, remises en service), dans un souci d'optimisation des coûts [(Prix d'acquisition+coûts d'exploitation)- économie réalisée].

Cette vision, présente l'inconvénient d'exclure les bénéfices obtenus par les gains de performance observables en fonctionnement normal hors incidents (SSO, VPN, biométrie) et les aspects qualitatifs relevés dans notre étude (confort, amélioration d'image, amélioration de la qualité, traçabilité).

Si ces outils ont le mérite d'exister, ils contribuent néanmoins à donner une perception de la sécurité réduite à un centre de coût.

5.2.1 Illustration d'un ROSI dans une entreprise du secteur public

L'outil ci-après, est utilisé par un utilisateur final (administration) dans le cadre de la communication interne sur sa politique de sécurité du S.I. Son intérêt principal réside dans le tableau de valorisation des risques.

Il est structuré en deux grandes phases :

- phase intermédiaire : elle définit la métrique indispensable au calcul final du ROSI. Elle pose les échelles de probabilités, d'impacts et en déduit une grille de coût des incidents en fonction de la probabilité de survenance de l'incident et de son niveau impact.

  - Le tableau 1 propose une **échelle de probabilités d'occurrence** d'incidents en fonction de la fréquence estimée des incidents.

  - Le tableau 2 propose une **échelle d'impact** d'incidents sur le système d'information.

  - Le tableau 3 propose une qualification du **niveau de risque** selon le niveau de probabilité d'occurrence et le niveau d'impact.

  - Le tableau 4 permet d'estimer les **pertes potentielles** en introduisant le « poids » de chacun des paramètres pour calculer le coût annuel des incidents.

Tableau 1 - Echelle de probabilité des occurrences d'incident		Max fréq./an
Négligeable	Très peu probable	0,05
Très basse	Probabilité d'occurrence de deux à trois fois tous les cinq ans	0,6
Basse	Probabilité d'occurrence d'une fois par an au moins	1,0
Moyenne	Probabilité d'occurrence d'une fois tous les six mois au moins	2,0
Haute	Probabilité d'occurrence d'une fois tous les mois au moins	12,0
Très haute	Probabilité d'occurrence plusieurs fois par mois au moins	36,0
Extrême	Probabilité d'occurrence une fois par jour	365,0

Tableau 2 - Hiérarchisation des impacts		Coût
Insignifiant	Pratiquement aucun impact	€ -
Mineur	Coût de reconfiguration/réparation/ remise en route négligeable.	€ 1 000
Significatif	Effets de bord tangibles, ressentis par quelques entités ou personnes. Coût de remise en service à prendre en compte (Plus « effets politique interne »).	€ 10 000
Dommageable	Entache la crédibilité de la DSI et/ou la confiance dans les services impliqués. Coût de remise en services significatifs.	€ 100 000
Sérieux	Engendre des interruptions de services, déconnecte les utilisateurs et perte d'image de marque..	€ 1 000 000
Grave	Arrêt total du système, Compromission de plusieurs entités de l'entreprise, arrêt d'activité possible.	€ 10 000 000

Tableau 3 - Calculs des niveaux de risques

		Niveau d'impact					
		Insignifiant	**Mineur**	**Significatif**	**Dommageable**	**Sérieux**	**Grave**
Probabilité	**Négligeable**	Négligeable	Négligeable	Négligeable	Négligeable	Négligeable	Négligeable
	Très basse	Négligeable	Basse	Basse	Basse	Moyenne	Moyenne
	Basse	Négligeable	Basse	Moyenne	Moyenne	Haute	Haute
	Moyenne	Négligeable	Basse	Moyenne	Haute	Haute	Critique
	Haute	Négligeable	Moyenne	Haute	Haute	Extrême	Extrême
	Très Haute	Négligeable	Moyenne	Haute	Critique	Extrême	Extrême
	Extrême	Négligeable	Moyenne	Haute	Critique	Extrême	Extrême

Tableau 4 - Coûts annuels d'incidents selon le niveau de risque							
		Niveau d'impact et coût par Incident					
		Insignifiant	Mineur	Significatif	Dommageable	Sérieux	Grave
Probabilité	**Annuelle**	**€ -**	**€ 1 000**	**€ 10 000**	**€ 100 000**	**€ 1 000 000**	**€ 10 000 000**
Négligeable	0,05	€ -	€ 50	€ 500	€ 5 000	€ 50 000	€ 500 000
Très Basse	0,60	€ -	€ 600	€ 6 000	€ 60 000	€ 600 000	€ 6 000 000
Basse	1,00	€ -	€ 1 000	€ 10 000	€ 100 000	€ 1 000 000	€ 10 000 000
Moyenne	2,00	€ -	€ 2 000	€ 20 000	€ 200 000	€ 2 000 000	€ 10 000 000
Haute	12,00	€ -	€ 12 000	€ 120 000	€ 1 200 000	€10 000 000	€ 10 000 000
Très Haute	36,00	€ -	€ 36 000	€ 360 000	€ 3 600 000	€10 000 000	€ 10 000 000
Extrême	365,00	€ -	€365 000	€3 650 000	€10 000 000	€10 000 000	€ 10 000 000

- la seconde phase permet de dresser le bilan financier des incidents annuels. Elle consiste à identifier et chiffrer les risques en fonction de leurs qualifications (probabilité, impact) et les solutions de sécurité mises en place (coûts d'acquisition, d'administration, amortissement).

    - Dans un premier temps, un inventaire des incidents susceptibles de survenir est mené et une estimation du coût du risque non couvert estimé (tableau 5)

    - Puis, les mesures de sécurité à mettre en place sont recensées et une estimation du risque résiduel est calculée (tableau 6)

Tableau 5 - Exemple d'évaluation des risques et analyse de leur impact financier									
No.	**Equipement**	**Incident potentiel (Menaces encourues)**	**Probabilité**	**Conséquences**	**Risque estimé**	**Incident/an**	**Coût direct du risque**	**Coût indirect du risque**	**Coût total an/risque non couvert**
A8	Infrastructure de la connexion Internet	Destruction d'un élément de l'infrastructure. (routeurs, Pare-feu, commutateurs)	Négligeable	Sérieuses	Négligeable	0,05	€ 1 000 000		€ 50 000
A9		Défaillance de la clim.	Moyen	Significatives	Moyen	2	€ 10 000		€ 20 000
A10		Mauvaise configuration de l'infrastructure (routeurs, Pare-feu, commutateurs)	Basse	Sérieuses	Haut	1	€ 1 000		€ 1 000
A11		Panne matérielle (routeurs, Pare-feu, commutateurs)	Très basse	Dommageables	Bas	0,6	€ 100 000		€ 60 000
A12		Problème de sécurité bâtiment	Basse	Significatives	Moyen	1	€ 10 000		€ 10 000
A13		Attaque Déni de service sur le réseau Télécom ou FAI	Très basse	Significatives	Bas	0,6	€ 10 000		€ 6 000
A14		Problème mat. Serveurs DNS	Négligeable	Dommageables	Négligeable	0,05	€ 100 000		€ 5 000
A15	Infrastructure Messagerie Internet	Attaque déni de service sur le système de messagerie	Haute	Dommageables	Haut	12	€ 100 000		€ 1 200 000
A16		Problème de configuration des serveurs messagerie	Basse	Dommageables	Moyen	1	€ 100 000		€ 100 000
TOTAUX ANNUELS									**€ 2 451 000**

Tableau 6 - Exemple d'évaluation du coût des mesures de sécurité et analyse de leur impact financier

TABLEAU 6							
Mesures de sécurité	**Coût de mise en oeuvre**	**Coût d'administration**	**Probabilité résiduelle**	**Impact résiduel**	**Coût/an du risque résiduel**	**Economie réalisée**	**Notes**
Plan de continuité (BCP) (1)	€ 50 000	€ 20 000					
Stock de pièces standard (4)	€ 50 000	€ 10 000					
Niv. de service garanti (SLA) (5)	€ -	€ -					
Sécurité physique (procédures de contrôle d'accès et salles blanches) (6)	€ 10 000	€ 10 000	Négligeable	Mineur	€ 50	€ 49 950	
Contrôles Environnemental salles blanches (2)	€ 30 000	€ 5 000					Impact réduit à mineur par le BCP; probabilité à très basse par le contrôle d'envt
Plan de continuité (BCP) (1)	Comptabilisé	Comptabilisé					
Niv. de service garanti (SLA) (5)	Comptabilisé	Comptabilisé	Très basse	Mineur	€ 600	€ 19 400	
Système de gestion de Config (8)	€ 70 000	€ 10 000					Probabilité de mauvaise config réduite : gestion de Config
Procédures de contrôle Changt (15)	€ 30 000	€ 5 000	Négligeable	Sérieux	€ 50 000	€ 950 000	
Business Continuity Plan (1)	Comptabilisé	Comptabilisé					Probabilité de panne non réduite, impact réduit par le plan de reprise
Spare parts (4)	Comptabilisé	Comptabilisé					
Service level agreements (5)	Comptabilisé	Comptabilisé	Très basse	Mineur	€ 600	€ 59 400	
Standardisation du câblage (9)	€ 10 000	€ -					
Sécurité physique (6)	Comptabilisé	Comptabilisé	Très basse	Significatif	€ 6 000	€ 4 000	
Connectivité Internet haut débit (10)	€ 10 000	€ 10 000					Impact réduit à mineur du fait de la redondance
Redondance des connexions (7)	€ 10 000	€ 10 000	Très basse	Mineur	€ 600	€ 5 400	
Réplication des serveurs DNS (11)	€ 10 000	€ -	Négligeable	Mineur	€ 50	€ 4 950	

Implantation de sondes de Détection d'intrusion (NIDS) (12)	€	70 000	€	20 000							
Utilisation de produits qualifiés (13)	€	20 000	€	5 000							
Appliquer la politique "tout ce qui n'est pas autorisé est interdit sur les Pare-feu (14)	€	-	€	-	Basse	Significatif	€	10 000	€	1 190 000	Aucune baisse du niveau d'impact
Procédures de contrôle Changt (15)		Comptabilisé		Comptabilisé	Très basse	Dommageable	€	60 000	€	40 000	
TOTAUX ANNUELS	**€**	**370 000**	**€**	**105 000**			**€**	**127 900**	**€**	**2 323 100**	

Enfin, un bilan peut être dressé à partir des informations financières calculées précédemment.

BILAN	
Coût annuel du risque non couverts	€ 2 451 000
Coûts des risques Résiduels	€ 127 900
Economies annuelles	**€ 2 323 100**
Coût des contre-mesures	€ 370 000
Période d'amortissement (années)	3
Coût des amortissements	€ 123 333
Coût d'administration de la sécurité	€ 105 000
Coût annuel de la sécurité	**€ 228 333**
Total économies réalisées	**€ 2 094 767**

Le résultat final présente le calcul du ROSI de façon « classique » en minorant les économies estimées par les coûts de la sécurité (acquisition, fonctionnement).

5.2.2 Illustration de ROSI chez un éditeur de solution SSO

L'outil présenté ci-après est tiré du modèle utilisé par un éditeur afin de soutenir la vente d'une solution de SSO. Comme le premier outil présenté, il se cantonne à une approche comptable du ROSI.

Exemple de calcul ROSI pour un projet d'implantation de Solution SSO	
Nombre d'utilisateurs :	3000
Nombre de login par utilisateur/mois sans SSO (**b**)	155
Proportion d'erreur (**e**)	15%
Proportion d'erreurs corrigées après recherche (**f**)	80%
Temps passé en recherche par utilisateur (en mn) (**g**)	2
Productivité perdue en appel au support (en mn) (**j**)	10
Coût horaire du salaire (**a**)	€ 20,00
Login par utilisateur/mois avec SSO (**l**)	35
tps de logins sans erreur par utilisateur/appli (en mn) (**o**)	0,25
Nbre de login erroné par utilisateur/mois (**d = b*e**)	23,25
Productivité perdue du fait d'erreur par utilisateur/mois (en mn) (**h = d*g**)	**46,5**
Nbre d'erreurs de login donnant lieu à un appel au support par utilisateur/mois (**i = d * (100%-f)**)	4,65
Temps total perdu passé au tél (en mn) (**k**)	46,5
Coût total des erreurs, procédures de correction par utilisateur/mois (**perte de prod = a * (k/60 + h/60)**)	€ 31,00
Economie potentielle avec SSO par utilisateur/mois (**p = a * [(b *o/60)-(l * o/60)]**)	€ 10,00
Economie potentielle de support par utilisateur/mois avec SSO (**s = a* (k/60 + h/60) - a * [(k/60 + h/60) * l/b]**)	€ 24,00
Economie totale pour toute l'entreprise par an avec SSO (*Economie réalisée* = 3000 * (s * 12 + p * 12))	**€ 1 224 000,00**

Les outils que nous avons pu trouver se cantonnent à cette vision financière et réduite de la sécurité. Ils n'incluent ni les gains corollaires d'augmentation de performance des processus, ni les répercussions de la sécurité sur la qualité du suivi de ces processus.

6 CONCLUSION

Nous l'avons vu, il n'existe pas d'approche unique du ROSI, mais des arguments clés en fonction du contexte, de la nature du projet et des interlocuteurs.

Il est important de retenir que même si les arguments technologiques sont faciles à utiliser, ils restent insuffisants car cette approche n'intègre pas l'analyse de la valeur du patrimoine informationnel de l'entreprise qui va bien au-delà des seules ressources informatiques.

Sous un autre angle, les arguments financiers ne doivent pas faire oublier que tout n'est pas quantifiable et mesurable en Euros. Les S.I intègrent des éléments qu'il est nécessaire d'apprécier autrement qu'avec des chiffres, tels que certains phénomènes (impact de la médiatisation d'un incident grave sur le métier de l'entreprise par exemple) qui ne sont pas directement mesurables, mais demeurent prépondérants.

Par ailleurs, argumenter en mettant trop en avant les effets destructeurs potentiels sur le SI risque d'aller à l'encontre de la recherche d'objectivité alors que c'est précisément ce que l'on recherche pour prendre une décision d'investissement.
Une fois les risques constatés, l'optimisation du niveau de protection obtenu en fonction du coût de l'investissement se situe entre la négligence coupable consistant à ne pas se protéger et à ne rien dépenser, et le perfectionnisme sécuritaire cherchant à se protéger toujours plus pour des coûts croissant exponentiellement. La recherche du bon compromis entre le niveau de protection et le coût de la protection passe par une combinaison d'évaluations quantitatives et qualitatives. Du fait de l'évolution très rapide des technologies et des risques, la recherche d'une récupération rapide (< à 18 mois) de l'investissement consacré à la protection du SI sera pratiquement toujours privilégiée.

En synthèse, on retiendra que la façon dont on justifiera un retour sur investissement en sécurité dépendra avant tout du niveau d'éveil et de maturité de l'entreprise concernée dans ce domaine et des principaux acteurs concernés.

C'est ainsi qu'en pratique, cette étude montre que le ROSI peut, dans un premier temps être abordé de façon relativement simple, suivant l'angle d'attaque et les objectifs recherchés, en s'appuyant sur des arguments classiques. Il peut être envisagé à l'aide d'une approche beaucoup plus globale (comme celle qui est proposée par le CLUSIF), s'appuyant sur différents facteurs clés, pour les entreprises qui ont atteint un niveau de maturité dans la sécurisation de leur S.I et qui entrent dans une phase d'optimisation des investissements.

7 ANNEXES

7.1 Exemples de calcul de ROSI

7.1.1 Exemple de ROSI sur une solution d'accès distant – comparatif modems / VPN

Scénario considéré

Prenons pour hypothèse une entreprise de 5000 utilisateurs, dont le coût mensuel des communications est de 100 € à ajouter au coût de la solution actuelle d'accès distant de 200000 € incluant modems, serveurs d'accès distant et autres matériels. Le coût annuel de cette solution est de 5000 * 100 € * 12 + 200000 € = 6.2 millions €. Ce qui revient à dépenser 1240 € /an/utilisateur.

Le coût des appels longue distance et les coûts de maintenance des batteries de modems poussent la plupart des entreprises à déployer des solutions d'accès distant basées sur le VPN (Virtual Private Network) plus sécurisé.

Solution proposée

Concernant la solution VPN, nous prenons comme hypothèse, les coûts suivants pour la même entreprise de 5000 utilisateurs : un abonnement Internet de 30 €/mois/utilisateur, 100 €/mois/utilisateur pour l'utilisation des services PKI et 100 €/utilisateur/an pour les composants VPN (serveur et client). Le coût annuel de cette solution est de
5000 * 30 € *12 + 5000 * 100€ * 12 + 5000 * 100 = 8300 M€. Ce qui revient à 30€ * 12 + 100€ * 12 + 100 = 1660€/utilisateur/an.

Retour sur investissement (ROSI)

Dans cet exemple, le retour sur investissement utilisé est quantitatif et bien axé sur l'économie de coût que va générer la nouvelle solution. Dans un autre contexte auprès d'un dirigeant beaucoup plus inquiet de la sécurité de ses accès distants et de la confidentialité de ses données, le seul argument qualitatif prouvant que la sécurité d'un VPN est bien supérieure à celle fournit par les modems sur un réseau RTC classique aurait pu suffire.

7.1.2 Exemple de ROSI sur la mise en place d'un mécanisme d'authentification forte

Scénario considéré

Un laboratoire pharmaceutique souhaite équiper tout son personnel mobile (267 visiteurs médicaux) d'un système par authentification forte afin de protéger l'accès à la base clients contenant les prix et notes de frais du laboratoire, jugées très confidentielles vis à vis de la concurrence.

Solution proposée

Le coût de la configuration par poste est estimé à 165 €. La configuration des 267 visiteurs correspondrait donc à un total de 33375 €. A cela doit être ajouté le test de la solution : 20 jours hommes, soit environ 4000 €. Nous parvenons donc à un total de 37375 € à répartir de la façon suivante :

Investissement : 40000€

Fonctionnement 1ere année : 13335 €, fonctionnement 2nde année : 10000 €.

Ce coût de 53335 € sera considéré par le laboratoire très largement inférieur à ce que lui coûterait la divulgation de sa base de données à la concurrence.

Retour sur investissement (ROSI)

Dans cet exemple, le retour sur investissement est basé sur un argument quantitatif (coût de la solution) et sur un enjeu métier : risque de perte de business liée à la divulgation de la base de données.

7.1.3 Exemple de ROSI sur la mise en place d'une solution de SSO

Scénario considéré

Un laboratoire pharmaceutique utilise aujourd'hui plusieurs systèmes d'habilitations d'accès. Seul l'administrateur sait gérer ce système d'habilitation jugé complexe et les audits ont montré que, dans bien des cas, les comptes étaient partagés et pas toujours mis à jour.

La multiplicité des mots de passe a conduit les utilisateurs à inscrire leurs différents mots de passe sur des Post-it collés sur leur écran, augmentant ainsi considérablement les risques d'accès frauduleux aux applications métiers. Par ailleurs, la non centralisation des différents systèmes empêche la bonne détection des anomalies.

Solution proposée

L'audit interne propose de renforcer la sensibilisation autour de la politique de gestion du mot de passe pour en imposer un seul. Le management approuve la mise en place d'une solution de Single Sign On (SSO).

La mise en place de la solution de SSO réduit le risque d'accès frauduleux mais augmente potentiellement l'impact de compromission d'un mot de passe (accès à toutes les applications auxquelles l'utilisateur est habilité). – Le risque introduit par la solution de SSO peut être atténué en demandant aux utilisateurs de verrouiller l'ordinateur en cas d'absence, en mettant en oeuvre une solution d'authentification forte.

Retour sur investissement (ROSI)

Le retour sur investissement quantitatif doit être calculé en estimant les coûts potentiels des sinistres dans le contexte où aucune mesure de protection n'est mise en place – les coûts de la mise en place de la solution de SSO + les coûts de la mise en place d'une solution d'authentification forte.

7.1.4 Exemple de ROSI pour une politique de sécurité

Scénario considéré

La mise en œuvre de la politique de sécurité se traduit par la mise en œuvre de moyens de prévention qui vont permettre, dès la première année de mise en application, de réduire la fréquence d'occurrence d'un certain nombre d'incidents.

On pourrait ainsi considérer qu'une entreprise qui n'a pas ou qui a peu d'incidents de sécurité n'a pas besoin de mettre en place de politique de sécurité car il n'y a pas de retour sur investissement. Encore faut-il être certain que les moyens de détection des incidents de sécurité ont été mis en place, ce qui est peu souvent le cas.

Solution proposée

La mise en place d'une politique de sécurité peut s'inscrire dans un programme plus large de sensibilisation des utilisateurs à la sécurité. Les études du CSI/FBI estiment que la mise en place d'un tel programme conduit notamment à une réduction de 0.3 la probabilité de voir une information détruite. (Voir chapitre 4)

Au niveau de la démarche, il est préférable, face à une direction peu réceptive au besoin de disposer d'une politique claire et formalisée en sécurité des S.I., de procéder à un audit sécurité de l'existant et à une estimation de l'effort / coût des mesures à mettre en place en distinguant les coûts récurrents, des investissements initiaux. Enfin, on s'attachera à montrer comment la mise en place d'une politique de sécurité permet de diminuer les coûts récurrents des incidents (ou l'effort de réparer les dommages)

Retour sur investissement (ROSI)

Soit une société ayant annuellement en moyenne :

30 jours x hommes d'effort supplémentaire dus à la récupération d'indisponibilités de systèmes

15 jours x hommes d'effort nécessaires à la reconstruction d'informations ayant été malencontreusement détruites ou perdues

50 jours x hommes d'effort nécessaires à la lutte contre les virus avérés sur les postes utilisateurs

Soit un total non exhaustif des incidents se montant déjà à 95 jours x hommes de surcroît de travail.

Soit un projet de mise en place d'un référentiel complet de sécurité avec politique de sécurité estimé à 20 jours x homme.

D'après les études du CSI/FBI, la mise en place d'un programme de sensibilisation dont ferait partie la politique de sécurité et le référentiel, en baissant la probabilité d'occurrence, ramènerait le coût des incidents à :

(1-0,05) 30 = 28,5 jours d'effort dus à la récupération d'indisponibilités de systèmes

(1-0,3) 15 = 10,5 jours d'efforts dus à la reconstruction d'informations ayant été malencontreusement détruites ou perdues

(1-0,3)50 = 35 jours d'effort nécessaires à la lutte contre les virus

Soit un total de 74 jours x hommes d'effort.

On voit que l'on parvient dans ce cas à l'équilibre dès la première année et à un retour sur investissement certain dès la seconde année.

7.1.5 Exemple de ROSI en rapport avec la notion de négligence

Scénario considéré
Soit une société offrant à ses clients la possibilité d'acheter ses produits via Internet. Son site Web héberge une base de données contenant les numéros de cartes bancaires de ses clients.
Le vol de fichiers contenant les numéros des cartes bancaires causerait un préjudice dont le coût est évalué à 800 K€. La probabilité d'une telle intrusion est estimée à 0,2.

Solution proposée

Suite à une revue de sécurité, une solution de sécurisation de l'infrastructure de son site (durcissement des systèmes, mise en place de SSL et outils de détection d'intrusion) d'un coût global de 100 K€ est proposée à la société.

Notion de non-respect des réglementations du métier et Retour sur Investissement (ROSI)

L'hébergeur est considéré non-respectueux des réglementations du métier s'il ne met pas en place la mesure de protection dans la mesure ou la solution raisonnable (ici 100 K€) coûte moins cher que le coût du sinistre modéré par sa fréquence d'occurrence (ici 160 K€). La limite de ce raisonnement tient cependant à la fiabilité de la valeur attribuée à la fréquence d'occurrence.

Dans cet exemple, le ROSI peut être calculé par la différence : (800 x 0,2) – 100 = 60 K€ .

7.2 Bibliographie

« The Economic Consequences of Sharing Security Information » – Esther Gal-Or, Anindya Ghose, University of Pittsburgh and Carnegie Mellon University

« Sécurité : l'évaluation des risques à la rescousse du ROI » – article JDNet du 5 mai 2003 – Fabrice Deblock

« Handbook for Computer Security Incident Response Teams » (CSIRTs) – 1998 – Moira J.West-Brown, Don Stikvoort, Klaus-Peter Kossakowski

« I-Camp II – Incident Cost Analysis and Modeling Project » – A report to the USENIX association

« Etude des coûts de sécurité informatique et de leurs méthodes d'évaluation » – mémoire de Valérie Barlet 1993 – Université Libre de Bruxelles

« Une approche opérationnelle de la sécurité – Quels enjeux liés à la sécurisation des processus métiers pour les entreprises européennes ? » livre blanc préparé par IDC/BULL France 2002

« Les facteurs humains et budgétaires pas encore au cœur de la sécurité » - article JDNet du 9 décembre 2002

« E-security et Confiance : les chiffres clés 2003-2004 » : extrait de l'enquête annuelle de NetCost & Security

« Organisez votre gestion des risques – gestion des risques et maîtrise des coûts » - MISCmag mai-juin 2003

« Getting the security budget you need and spending it wisely » Information Security Magazine – march 2003

« Solutions for IT Security » David Pike, Ernst & Young, Mai 2002

« How much is enough ? A risk management approach to computer security » Kevin J.Soo-hoo, june 2002, Consortium for Research on Information Security and Policy

« A model for evaluating IT security investments », University of Dallas, Texas, septembre 2002, Huseyin Cavusuglo, Birendra Mishra, Srinivasan Raghunathan

« Return On Security Investment », Ian McKenzie, VISTORM,

« The Return of Investment for Information Security », Raghy Raman, business briefing global infosecurity 2002,

« The reality about investing in Information Security », Eva Kuiper, HP

« Calculated Risk : guide to determining security ROI », Scott Berinato, CSO on line, decembre 2002

« Finally, a real return on security spending », Scott Berinato, , CIO Magazine, Fevrier 2002

« Insight on Return on Security Investment », Eric Karofsky, Secure Business quaterly, dernier trimester 2001.

« VPN Security and Return on Investment » white paper, RSA Security 2001

« The Return on Investment for Network Security », white paper, decembre 2002, CISCO

« Is Return on Security Investment Impossible », SYGATE, Octobre 2002

« Justify the Return on Security Investment », Crafting a quantifiable business case, August 2003