

*«Comment vendre un projet de sécurité en interne en 2008 ? Est ce que les choses ont changé au cours de ces dernières années»*

*«Une autre approche ?»*

*RSI : La question est probablement de trouver, dans le continuum d'un processus de gestion, la partie traitée par l'informatique pour évaluer l'impact de l'arrêt (ou l'erreur) de l'automatisation.*

## De quoi parlons nous ? RSI ou ROI ?

Le Retour Sur Investissement est une traduction erronée du ROI : Return On Investment, qui est le taux de rendement (ou de rentabilité) de l'investissement. Alors que le RSI correspond à la rentabilité et s'obtient en faisant le rapport du résultat net et le montant des capitaux investis.  
(« *Lexique d'économie* » de A. Silem et al)

La question du RSI vient probablement des freins managériaux. C'est-à-dire de la conviction que le management peut être un moteur ou un frein puissant.

Avec un biais culturel car en France nous privilégions le « *Pourquoi* », alors que les anglo-saxons favorisent le « *Comment* ». Les entreprises françaises vont, ainsi, étudier les besoins puis rechercher un concept, tandis que les anglo-saxons vont rapidement utiliser un outil en cherchant comment en tirer parti. Dès lors, la mise en œuvre de solutions nouvelles se trouve généralement plus lente en France.

Mais pour que le RSI soit audible par le management il semble nécessaire que l'alignement du SI soit en phase avec les trajectoires et manœuvres de l'entreprise. C'est une priorité et une obligation de résultats selon Eric Fimbel (2007).

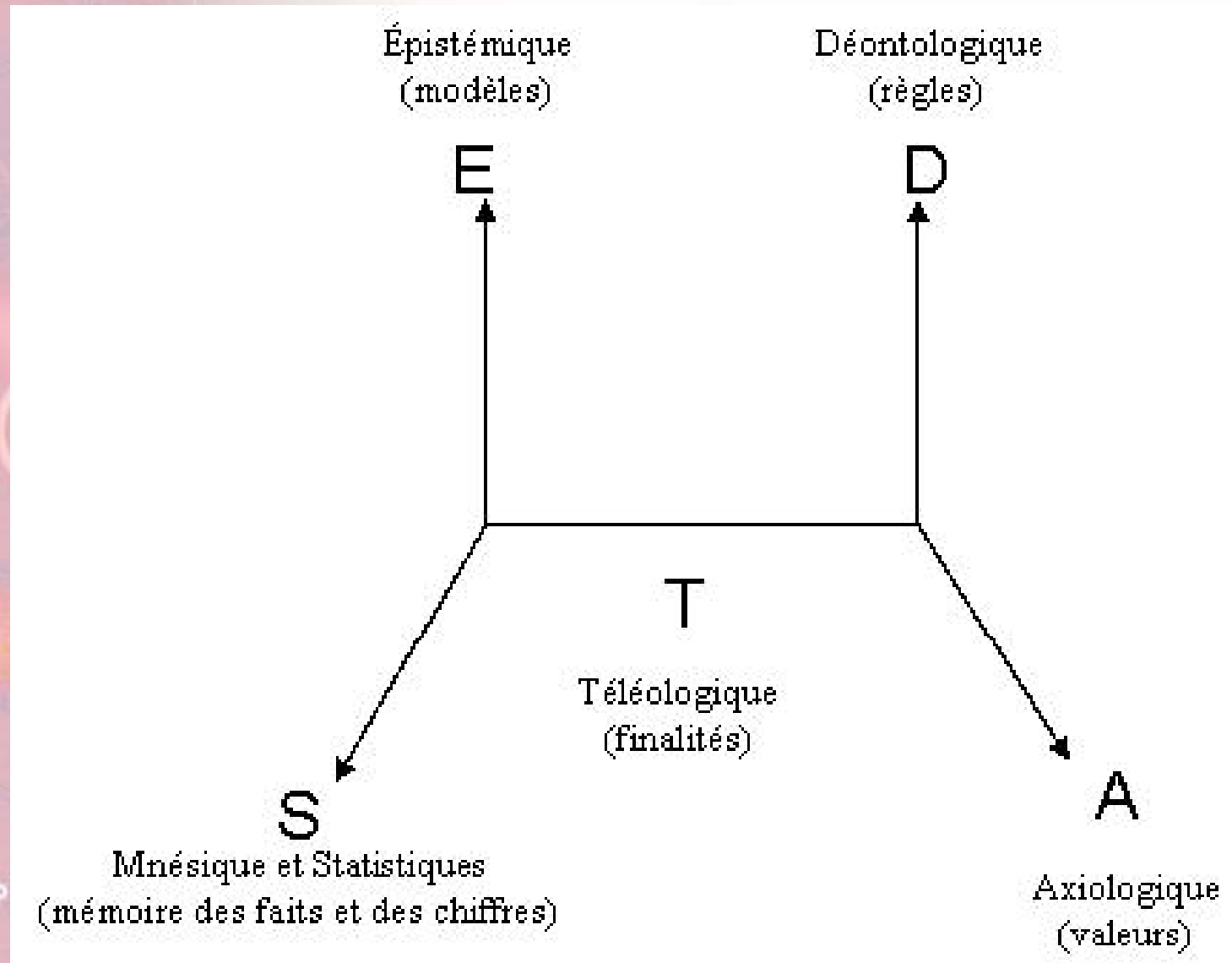
Pour Thiétart et Xuereb (2005) les constituants de la performance d'une entreprise se situent dans trois dimensions : le positionnement stratégique, les compétences et les actifs rares, l'efficacité opérationnelle. C'est dans cette dernière dimension qu'il semble intéressant de nous pencher concernant la sécurité informatique ... *et éventuellement du RSI ...*

Une démarche de protection nécessite l'implication des acteurs, or, on peut voir émerger des blocages dans les organisations avec des problématiques liées au refoulement qui rend inopérant l'analyse du risque. Le refoulement interdit les mesures correctives postule Kerven (1995).

C'est là l'intérêt d'une approche par les sciences des dangers pour diagnostiquer les risques. Les cindyniques conduisent à mieux maîtriser la complexité des vulnérabilités d'un système.

Les sciences des dangers permettent le recueil et l'analyse de données empiriques, ainsi, elles sont génératrices de données et d'informations qui deviennent disponibles. Le RSSI peut alors construire une cartographie des vulnérabilités par une approche scientifique et par l'incorporation de données issues de l'audit du terrain.

Dans cet audit, il semble nécessaire d'emprunter une démarche cybernétique. C'est-à-dire que l'analyse se situe dans des phénomènes d'actions et de rétroactions avec les spécialistes des différents domaines.



« **Retour d'expérience** »

**Les cindyniques étudiées au Clusir RhA, retour de données empiriques.**

Le Clusir RhA a procédé par un examen collectif de données empiriques, fournies par ses membres ainsi qu'une vingtaine d'étudiants de master 2. Ces données sont des exemples pris principalement dans le domaine de la sécurité des systèmes d'information. L'objectif de cette étude était de fournir un exemple de questionnaire utilisant les DSC (Déficits Systémiques Cindynogènes) proposés par Kerven en 1995.

Un hyperespace du danger est pour Kerven le produit de cinq espaces :

L'espace *mnésique*, qui constitue la banque de données, de faits, (S)

L'espace *épistémique* qui est la source des modélisations, (E)

L'espace *téléologique* qui est l'ensemble des finalités, (T)

L'espace *axiologique* qui est le lieu de stockage des systèmes de valeurs, (A)

L'espace *déontologique* qui recueille les « règles du jeu » du réseau (D).

Cet hyperespace prend la forme suivante :



L'hyperespace des dangers

Dans le cadre de l'étude des cindyniques d'un système d'information, l'examen systématique des 27 Déficits Systémiques Cindynogènes semble être un support pour réaliser un questionnaire pour un audit de prévention et de sécurité. Les DSC vont se séparer en quatre groupes d'analyse. Ils se décomposent ainsi :

- 10 D.S.C, vont concerner les lacunes, les absences ou les oublis.

- 8 D.S.C, vont s'intéresser aux disjonctions entre les dimensions de l'hyperespace.
- 5 D.S.C, vont s'attacher aux désorganisations dans les dimensions.
- 4 D.S.C, vont toucher aux blocages de régulation dans l'hyperplan.

Une mise en situation de l'hyperespace et des DSC par les collectifs évoqués en introduction, conduit aux propositions suivantes :

**DSC1 – (Définition) : absence de L'axe Axiologique : pas de système de valeurs**

- Une culture sécurité a-t-elle été développée dans l'entreprise ?
- Les utilisateurs d'ordinateurs portables ont-ils été sensibilisés ?
- L'entreprise a-t-elle conscience de l'espionnage industriel et des techniques d'espionnage ?

**DSC2 – (Définition) : absence de L'axe Déontologique : pas de loi, pas de règles**

- Des consignes en matière de sécurité sont-elles définies pour les utilisateurs ?
- Existe-t-il une charte informatique précisant les droits et obligations des utilisateurs ?
- Existe-t-il une protection anti-virus non désactivable par l'utilisateur ?
- Existe-t-il des mécanismes techniques renforçant la qualité des mots de passe ?

**DSC3 – (Définition) : absence de L'axe Epistémique : pas de modèle**

- L'entreprise s'appuie t'elle sur une méthode pour mettre en œuvre le processus de sécurité ?
- Existe-t-il un modèle pour la gestion des sauvegardes, en particulier pour les ordinateurs portables ?

**DSC4 – (Définition) : absence de L'axe Statistique : pas de données, pas de chiffres**

- Les données sensibles ont-elles été recensées ?
- Existe-t-il un système de retour d'expérience ?

**DSC5 – (Définition) : absence de L'axe Téléologique : pas d'objectifs pas de finalités**

- Les objectifs de la politique de SSI ont-ils été clairement exprimés ?
- Une stratégie de sécurisation a t'elle été définie et formalisée ?
- Une stratégie a-t-elle été menée concernant la disponibilité des environnements ou des applications jugées les plus sensibles par rapport aux risques opérationnels ?

**DSC6 - Manques dans l'axe Axiologique : oubli de certaines valeurs.**

- L'entreprise connaît-t-elle la menace des spywares ?
- Les mises à jour des systèmes sont elles respectées ?

**DSC7 - Manques dans l'axe Déontologique : des règles, des lois font défaut.**

- La charte informatique est-elle conforme aux obligations juridiques ?
- Est-ce que les lois relatives au droit d'auteur sont respectées ?
- L'accès des utilisateurs est-il contrôlé par un login et un mot de passe ?
- Existe t-il des critères pour attribuer les droits d'accès ?

**DSC8 - Manques dans l'axe Epistémique : tout n'est pas modélisé/modélisable.**

- Une cartographie de l'architecture fonctionnelle a-t-elle été réalisée ?
- Les serveurs sont-ils dans leur configuration par défaut ?

**DSC9 - Manques dans l'axe Statistique : manque de données, de chiffres.**

- Ex: Bonnes connaissances des menaces informatiques actuelles mais peu de données sur l'évolution des attaques par moyens non techniques.
- Quelles règles de sécurité sont mises en place pour protéger les documents confidentiels imprimés ?

**DSC10 - Manques dans l'axe Téléologique : tous les objectifs ne sont pas définis ou connus.**

- Ex: Le développement du télétravail, la création de nouvelles succursales et l'augmentation des interconnexions de réseaux entraînent les mêmes risques que les employés internes.
- Des méthodes de déploiement ont-elles été formalisées ?
- Une clause du contrat de travail a-t-elle été ajoutée concernant la confidentialité des activités de l'entreprise ?

**DSC11 - Disjonction/divergence entre objectifs et valeurs.**

- Ex: L'entreprise fait appel à un prestataire externe pour sécuriser son système d'information mais celui-ci travaille également pour certains de ses concurrents
- La pression des dirigeants entraîne-t-elle un manque d'implication de la part des employés dans la politique de SSI.

**DSC12 - Disjonction/divergence entre les règles et les valeurs.**

- Ex: La charte informatique de l'entreprise oblige les employés à choisir des mots de passe difficiles à trouver et à en changer au maximum tous les 30 jours alors que la culture d'entreprise prône l'autonomie et la souplesse dans l'accès au système informatique.
- Ex: l'entreprise mène une politique de SSI appuyée mais certains employés s'adonnent à des pratiques illégales comme le téléchargement d'œuvre musicale.
- Comment l'utilisateur construit-il son mot de passe et comment le retrouve t-il en cas d'oubli ?
- L'entreprise a-t-elle déjà constaté du téléchargement illicite de la part de ses employés ?

**DSC13 - Disjonction/divergence entre les règles et les objectifs.**

- Ex: Les règles de sécurité déployées ne sont pas fondées sur la nature des objectifs métiers de l'entreprise.
- Les accès aux SI sont-ils en conformité avec les objectifs métiers ?
- Les stations hébergeant une application monoposte font-elles l'objet d'une attention particulière ?

**DSC14 - Disjonction/divergence entre les modèles et les données.**

- Ex: L'entreprise a la volonté de sécuriser les données sensibles mais elle n'a pas pris soin de les repérer auparavant et d'identifier les services / personnes qui produisent ces informations.
- Les mécanismes de protection et de contrôle des flux entrants/sortants sont-ils en adéquation avec l'utilisation qui en est faite ?

**DSC15 - Disjonction/divergence entre des objectifs.**

- Ex: Les infrastructures en réseau sont sécurisées mais l'accès aux bâtiments physiques ne l'est pas.

**DSC17 - Disjonction/divergence entre les objectifs et les données.**

- Ex: aucune stratégie de sauvegarde n'a été définie, entraînant ainsi une faille dans la politique de SSI.
- Les objectifs de la politique de sauvegarde ont-ils été déterminés en tenant compte de la réalité dans laquelle évolue l'entreprise ?

**DSC18 - Disjonction/divergence entre les objectifs et les modèles.**

- Ex: On veut avoir des services toujours disponibles, mais on n'installe pas d'infrastructures à haute disponibilité (ex : Cluster).

**DSC19 - Désorganisation des valeurs : pas de classement.**

- Ex: L'entreprise met la priorité sur la sécurisation technique des systèmes d'information plutôt que sur la formation et la sensibilisation des employés.
- Quel est le temps dédié à la sécurisation technique et à la formation du personnel ?

- L'entreprise estime-t-elle qu'il vaille mieux dépenser pour sécuriser son SI ou pour le réparer après un problème ?

**DSC20 - Désorganisation des règles : pas de hiérarchisation.**

- Ex: Une partie des employés n'a pas été sensibilisée à l'importance de sécuriser un SI car l'entreprise n'a pas jugé cela utile.
- L'entreprise a-t-elle établi des priorités dans la mise en place des règles en tenant compte de la réalité et non pas en se fiant à des estimations ?

**DSC21 - Désorganisation des modèles : pas de classification.**

- Ex: Un modèle continue d'être appliqué alors qu'il est obsolète.
- La précision des modèles permet-elle de prendre des décisions pertinentes concernant le SSI ?

**DSC22 - Désorganisation des données : base de données non organisées.**

- Ex: La politique de gestion des données n'est pas appliquée systématiquement par tous les services de l'entreprise.
- L'entreprise possède-t-elle un guide des meilleures pratiques ?
- Les données jugées sensibles sont-elles hiérarchisées selon leur degré de sensibilité ?

**DSC23 - Désorganisation des objectifs : pas de priorité.**

- Ex: L'entreprise n'a pas su estimer la priorité entre les objectifs relevant de la sécurisation des données, des infrastructures, de l'accès aux bâtiments, etc
- En fonction de quoi les objectifs de la politique de SSI ont-ils été définis ?

**DSC24 - Blocage des régulations dans les mesures E et S.**

- Ex: Les modèles élaborés lors de la mise en place de la stratégie SSI n'ont pas évolué alors que les usages ont changé.
- Les modèles se réfèrent-ils à des normes qui ne sont plus en vigueur ?

**DSC25 - Blocage des régulations dans l'éthique D et A.**

- Ex: La volonté de sécuriser au maximum les données entrave la liberté des employés.
- Les contrôles trop fréquents de l'application de la charte ne risquent-ils pas d'entraîner le rejet de son application par les employés ?

**DSC26 - Blocage des régulations dans l'établissement des objectifs : ne pas tenir compte des autres dimensions.**

- Ex: Ne pas prendre en compte la dimension sociale et psychologique de la politique de SSI.
- La dimension humaine fait-elle partie intégrante de la politique de SSI ?

**DSC27 - Blocage des régulations dans les différents stades de validation.**

- Ex: L'entreprise connaît des blocages dans les retours d'expérience.

Cette liste non exhaustive ne veut pas être une vérité, mais un support d'interrogations qu'il convient de critiquer et de compléter.