L'équation de la sécurité, une analyse systémique des vulnérabilités de l'entreprise : vers un outil de gestion globale des risques

Franck Bulinge
Enseignant-chercheur en sciences de l'information et de la communication

Responsable du projet EPICES (*Etudes prospectives en intelligence compétitive, économique et stratégique*)

Laboratoire LePont ; Université de Toulon – Var
BP 132 – 83 957 La Garde Cedex
bulinge@univ-tln.fr

Tel : 04.94.14.25.75 / 06.62.24.81.34

Résumé : La sécurité en entreprise est généralement abordée selon des approches spécialisées, où la sécurité des systèmes d'information apparaît comme une composante majeure dédiée aux informaticiens. Toutefois, la problématique de sécurité est complexe et mérite selon nous d'être envisagée de manière systémique et globale, approche que nous qualifions d'holistique. Il s'agit en effet de traiter un ensemble de problèmes plus ou moins interactifs dont la résolution passe par une mise en synergie des compétences. L'enjeu est avant tout culturel, il procède d'un changement de paradigme : la sécurité n'est plus un objet finalisé réservé au spécialiste de l'entreprise, elle doit être envisagée dans une optique globale, permanente et universelle par l'ensemble du personnel. De ce point de vue, l'intelligence économique, par son approche transversale et collective, se présente comme une opportunité pour la mise en œuvre d'un concept de sécurité globale au sein de l'entreprise.

Abstract : The security of the firm is generally considered as a job for specialists, so that SIS appears as a major element dedicated to computer engineers. Nevertheless, we expect that security is complex and it must be considered as a holistic problem, as far as it is a systemic and global concept. The issue should be a cultural change of paradigm: security is no longer a final object for specialists but a global, permanent and universal philosophy for everybody inside the firm. From this point of view, competitive intelligence, as a transversal and collective approach, appears to be one of the best way to integrate a global security concept into the firm.

Introduction

L'analyse du risque en entreprise est une pratique déjà ancienne chez les professionnels de l'assurance (Charbonnier, 1990), de l'informatique et chez les responsables de la sécurité prise au sens le plus général. L'ouverture d'un champ de recherche dans ce domaine intervient a posteriori et ne saurait se développer sans tenir compte de l'existant construit de manière empirique au fil du temps et des expériences souvent douloureuses : une approche scientifique ne pourrait substituer la théorie à la pratique sans risque de rejet de la part de la communauté professionnelle.

Le terme même de sécurité est polysémique : il représente à la fois un concept, une fonction, un cadre d'action. Son champ couvre de multiples domaines qui vont de l'information à la protection des personnes et des biens.

La sécurité comme champ de recherche peut être considérée selon deux approches.

La première consiste à étudier la sécurité en tant qu'objet final, dans la perspective d'une spécialité à part entière. Une telle approche distingue des sous-ensembles relativement indépendants (sécurité des systèmes d'information, sécurité incendie etc) qui font d'ores et déjà l'objet de formations spécifiques. Nous citerons à cet égard le Centre national de prévention et de protection comme organisme de référence en matière de formation dans ce domaine.

L'approche spécialiste répond assez bien à la structure classique des grandes organisations par la création de services spécifiques et/ou par la sous-traitance à des sociétés spécialisées.

Pour notre part, et dans le cadre de nos recherches sur les petites et moyennes organisations, nous abordons la problématique de sécurité sous un angle plus global à travers une double approche que nous qualifierons d'holistique:

- approche systémique de la sécurité tenant compte des interrelations entre différents éléments constitutifs (le personnel, les structures, l'organisation, l'environnement) d'un ensemble homogène et vivant (l'entreprise).

- approche synergique considérant la sécurité comme élément dimensionnel constitutif de l'intelligence économique et stratégique.

Dans cet article, nous présenterons la sécurité dans le contexte de l'intelligence économique et stratégique, puis nous mettrons en évidence son caractère systémique avant de proposer une équation de la sécurité comme base d'une analyse globale de la sécurité au sein de l'entreprise. Nous poserons enfin les bases d'un outil simple de gestion du risque destiné aux petites et moyennes organisation auxquelles nous nous référons.

Compte tenu de la nouveauté de ce champ de recherche, il est difficile de se référer à une bibliographie scientifique. A l'instar de l'intelligence économique à laquelle nous nous référons, nombre d'ouvrages sont d'abord l'œuvre de consultants, de professionnels ou de journalistes (Melot, 1999) avant d'être celle de scientifiques reconnus. Nous nous appuierons par ailleurs sur l'expérience acquise durant vingt ans au ministère de la défense, en particulier sur les bâtiments de la Marine nationale et dans le contrôle aérien.

L'approche synergique à laquelle nous nous référons ne saurait en aucun cas exclure les approches spécialistes. En effet, notre volonté n'est pas de nous approprier ce champ de recherche mais de l'enrichir à travers le partage et le croisement de regards différents.

Nous tenons enfin à préciser que notre recherche dans le domaine de la sécurité ne fait que débuter, aussi nous serions gré au lecteur de bien vouloir considérer avec indulgence cette contribution encore très imparfaite, en particulier pour ce qui concerne la classification des risques qui mérite d'être corrigée et enrichie.

1- Pour une approche croisée de la sécurité et de l'intelligence économique

1.1 La sécurité comme dimension de l'intelligence économique

L'intelligence économique peut se définir comme « *l'ensemble des actions coordonnées de recherche, de traitement et de diffusion de l'information utile aux acteurs économiques, en vue de son exploitation à des fins stratégiques et opérationnelles. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de qualité, de délais et de coût.* » (Martre, 1994)

Le rapport Martre précise que l'intelligence économique permet aux différents acteurs d'anticiper sur la situation des marchés et l'évolution de la concurrence, de détecter et d'évaluer les menaces et les opportunités dans leur environnement pour définir les actions offensives et défensives les mieux adaptées à leur stratégie de développement. Larivet (2000) évoque une dimension défensive de l'intelligence économique, recouvrant la contre-intelligence et la protection du patrimoine de l'organisation (Levet et Paturel, 1996). Baron (1996) précise que la protection du patrimoine concurrentiel, entendu au sens global,

est partie intégrante du concept d'intelligence économique.

Cette approche, inspirée des services de renseignement, marque volontairement la dimension sécuritaire de l'intelligence économique dans le domaine de l'information et du patrimoine de l'entreprise. Bournois et Romani (2000) analysent les liens entre l'intelligence économique et la sécurité des systèmes d'information. Trois types de rapports apparaissent : les SSI englobent l'IES ; l'un et l'autre sont en coordination étroite ; enfin les deux aspects sont traités séparément. Nous retenons comme hypothèse de travail la seconde solution en ce qu'elle fait apparaître une continuité synergique entre les acteurs de l'organisation.

L'intelligence économique, par ses dimensions multiples, apparaît comme un champ structurant à la fois transdisciplinaire et protéiforme. Elle marque par ailleurs le transfert des pouvoirs régaliens de l'Etat vers une prise en charge par les entreprises à travers l'émergence d'une sensibilité collective aux enjeux de sécurité économique (Warusfel, 1996).

La démarche de sécurité entreprise dans le cadre ou associée à une démarche plus globale d'intelligence économique présente à notre avis l'avantage de la cohérence et de la mutualisation des processus de mise en œuvre, notamment sur le plan culturel (Bulinge, 2001)

1.2 Une approche systémique de la sécurité

La notion de menace ne saurait être isolée de celle de vulnérabilité. En ce sens, l'intelligence économique, dans sa dimension téléologique (Bournois et Romani, 2000), procède à une analyse stratégique de la sécurité en termes de vulnérabilités, de menaces et de risques, voire de danger dans une approche cindynique (Kervern, 1995), dont découlera notre proposition d'équation.

Faut-il pour autant élargir le concept de sécurité informationnelle, de patrimoine immatériel, vers un concept global de sécurité intégrant les dimensions matérielles de l'entreprise?

L'approche holistique met en avant la dimension universelle de la sécurité puisqu'elle intéresse aussi bien les logiques publiques de défense des intérêts des personnes que les logiques privées des entreprises dans des perspectives aussi bien micro économiques que macro économiques.

Une approche holistique de la sécurité présente l'avantage de ne pas séparer les éléments de ce que l'on considérera comme une chaîne de sécurité, laquelle dépend essentiellement de son maillon le plus faible.

Prenons l'exemple de la sécurité de l'information : elle prend en compte trois objectifs qui sont l'intégrité, la confidentialité et la disponibilité de l'information. Pour atteindre ces objectifs, les spécialistes dégagent une typologie de la sécurité qui se réfère simultanément aux dimensions physique, organisationnelle et logique de la sécurité. On pressent ici les liens indissociables entre une sécurité physique d'un bien immatériel et la sécurité du patrimoine matériel ou individuel de l'entreprise. Le rapport entre un incendie et la perte de données informatiques, c'est à dire des connaissances formalisées et mémorisées de l'entreprise, et leur impact sur l'économie de l'organisation, ne peut être ignoré au point de traiter séparément les trois problématiques. La sécurité ne peut, par conséquent, être envisagée hors du cadre d'une analyse systémique.

1.3 L'entreprise et l'intelligence du risque

L'entreprise, et les organisations en général, sont confrontées à une difficulté majeure dès lors qu'elles tentent de mettre en place une politique de sécurité : l'analyse du risque, dans la logique de renforcement homogène de la chaîne sécuritaire, doit être exhaustive et globale. Cela implique de bien vouloir prendre en compte la totalité des risques potentiels existants ; cela suppose également une vision d'ensemble des interactions possibles entre les vulnérabilités, les risques, les menaces et les dangers.

Nous nous trouvons face à une problématique culturelle au terme de laquelle interfèrent des systèmes de valeurs plus ou moins partagés par les acteurs d'une organisation. La culture « sécuritaire » de l'entreprise est une donnée variable qui s'appuie à la fois sur des niveaux de conscience, de sensibilisation, de formation voire d'entraînement à la gestion des risques. La question de la légitimité, qui fait référence à la compatibilité entre les buts personnels et les valeurs du milieu dans lequel on opère (Marchesnay et Fourcade, 1997), est essentielle dans la perspective d'une adhésion de l'ensemble des acteurs.

Le retour d'expérience et la mise en évidence des déficits systémiques cindynogènes (Kervern, 1995), qui semblent ouvrir une voie intéressante dans le domaine de la sensibilisation, démontrent clairement la nécessité d'adopter une attitude à la fois proactive et participative en matière de sécurité. On pourrait à cet égard opposer la dynamique apprenante développée dans le concept d'intelligence économique (Achard et Bernat, 1998) au phénomène de refoulement cindynique qui consiste à nier ou à sous-estimer le danger,

fréquemment observé dans les collectivités humaines. Barlette (2002), dans ses travaux sur la sinistralité, émet l'hypothèse selon laquelle les entreprises perçoivent mal leurs vulnérabilités et les risques auxquelles elles sont confrontées.

De fait, nous postulons que l'analyse du risque, dans une perspective d'adhésion collective au concept de sécurité, doit être effectuée par les acteurs mêmes de l'entreprise, préalablement sensibilisés, formés et soutenus dans leur démarche par un ensemble simple d'outils et de supports pédagogiques .

2- Un modèle rationnel d'approche de la sécurité

L'expérience empirique de la sécurité, vécue notamment à bord des sous-marins nucléaires ou du porte-avions Foch, ou encore dans l'environnement opérationnel complexe du contrôle aérien, nous a permis de dégager un certains nombre d'éléments constitutifs d'une équation de la sécurité que nous proposons dans cette étude. Parmi ces éléments nous distinguons :

a) Les facteurs intrinsèques ou extrinsèques :

- Les vulnérabilités : facteurs intrinsèques, faiblesse du système qui le rend sensible à une menace[1]

- Les menaces: facteurs extrinsèques : dangers potentiels, latents

- Les risques : ils résultent de l'interaction entre les facteurs intrinsèques et extrinsèques

- Les attaques : correspondent aux dangers réalisés

- Les sinistres : ils sont le résultat d'attaques ayant atteint leur but, Guinier (1992), cité par Barlette (2002), décrit le sinistre comme la réalisation d'un risque

b) Les comportements, mesures ou modes opératoires :

- L'analyse : elle marque la prise de conscience et la volonté de mettre en œuvre une politique de sécurité

- La prévention : elle découle de l'analyse des vulnérabilités et des risques et relève d'une stratégie d'évitement (sensibilisation, mesures préventives)

- La protection : elle tient compte de la réalisation possible du danger et tend à circonscrire ou à limiter le sinistre. Elle procède d'une stratégie d'affrontement.

- La réaction : elle repose sur la capacité des acteurs à réagir en situation dégradée, que ce soit vis à vis de circonstances prévisibles ou face à des situations aléatoires (contingences).

2.1 Typologie des vulnérabilités

Si l'on reprend la définition usuelle de la vulnérabilité (« *Vulnérable : qui peut être atteint, blessé, qui offre peu de résistance. Perméabilité aux menaces et aux dangers. Défaut dans la cuirasse* ». *Petit Robert*), on perçoit la part intrinsèque de l'individu ou de l'organisation dans son rapport avec l'environnement. Les vulnérabilités peuvent être regroupées en fonction de leur origine. On distingue ainsi les vulnérabilités:

- des personnes que l'on retrouve en terme de sécurité sous l'appellation de facteur humain

- des organisations, au niveau de la hiérarchie, des relations internes/externes, de la culture

- des structures, dans la conception des locaux, des matériels, des installations

- stratégiques ou opérationnelles, à travers les facteurs environnementaux caractérisés par leur complexité et leur niveau de turbulence

L'analyse des vulnérabilités est un acte responsable concomitant à l'analyse des menaces. Le premier des déficits systémiques cindynogènes (Kervern, 1995) est le culte de l'infaillibilité (DSC1 ou syndrome du Titanique). Il représente une barrière immédiate à toute tentative de réflexion en matière de sécurité.

[1] Nous reprenons les définitions de la vulnérabilité, de la menace et du risque selon Archimbaud et Longeon (1999), cités par Barlette (2002), qui correspondent à notre approche sémantique de la sécurité

Origine	Niveau
Personnes	Psychotechnique (motivation, compétence, intégrité morale, esprit d'équipe)
	Physique (état de santé, intégrité physique)
	Social (situation familiale, contexte)
Organisations	Equipe (cohésion, discipline, dynamisme)
	Management
Stratégies	Choix et options
	Patrimoine (savoirs faire, projet, innovation, brevets)
	Environnement concurrentiel (clients, fournisseurs, conccurrents)
Structures	Installations (immeubles, locaux)
	Matériels (machine, informatique)

Tableau 1: Typologie des vulnérabilités

2.2 L'équation de la sécurité

Une approche rationnelle de la sécurité nous permet d'envisager une modélisation à connotation mathématique dont l'intérêt est d'accrocher l'attention dans une démarche de sensibilisation. Contrairement à l'intelligence économique, la sécurité interpelle plus aisément la raison en ce qu'elle se réfère au danger, à la peur voire à notre instinct de conservation. La mise en équation est ici toute relative et ne saura servir de base à un système expert. Pour autant, à travers le retour d'expérience relevé dans le cadre de nos formations, cette équation est appréciée dans la mesure où elle pose les principes globaux d'une culture de la sécurité.

La sécurité est présentée comme une somme de probabilités plus ou moins complexes d'occurrences dangereuses. A chacune de ces occurrences correspondent des mesures ou des attitudes en fonction desquelles un équilibre minimum doit être maintenu. La notion d'équilibre est purement économique dans la mesure où la situation idéale serait de maintenir le niveau le plus élevé de sécurité, mais à quel prix ? Le chef d'entreprise, qui répond à des contraintes budgétaires, préfèrera maintenir l'équilibre et calculer un coefficient de rentabilité au-dessous duquel la sécurité serait compromise. L'équation que nous présentons met en évidence un constat mathématique : il n'existe pas de sécurité absolue pour la seule raison qu'il n'y pas de risque égal à zéro.

Enoncé de l'équation : sachant que le risque est le produit des vulnérabilités par les menaces, nous présentons le niveau de sécurité comme la somme des rapports suivants :

Si Risque = Vulnérabilités x Menaces et P(attaque) = probabilité d'occurrence d'une attaque

$$\textit{Niveau de sécurité} = \frac{\textit{Analyse x Prévention}}{\textit{Risque}} + \frac{\textit{Protection}}{\textit{P(Attaque)}} + \frac{\textit{Réaction}}{\textit{Aléas}}$$

Le niveau de sécurité est relatif, a priori non nul, dans la mesure où, en l'absence de mesures de prévention ou de protection, il reste une probabilité de réaction (facteur humain, chance) non appréciable . A contrario, le niveau de sécurité n'est jamais absolu ; il peut être tout au plus optimum en fonction de critères d'ordre téléologique. Ainsi Le problème peut-il se traduire mathématiquement par l'optimisation de la fonction sécurité sous contrainte de coût.

3- Vers un outil d'analyse des risques en entreprise

Une approche holistique de la sécurité prendra en compte l'ensemble des facteurs de risque intrinsèques et extrinsèques de l'entreprise. Cela suppose une analyse exhaustive au terme de laquelle un oubli pourrait s'avérer fatal. L'intérêt d'une grille d évaluation est évident. Nous proposons dans cet article une première approche qui mérite à coup sûr d'être modifiée et enrichie.

Une grille d'analyse simple doit reposer sur l'identification d'une liste de menaces auxquelles peut être confrontée une organisation. Nous définissons pour ces menaces, ou risques bruts, une potentialité d'occurrence d'un événement P(*Risque i*) propre à la situation de cette organisation (zone sismique, contexte géopolitique, etc).

Nous définissons ensuite un coefficient d'impact CI*mpact* des risques sur l'entreprise. L'impact d'un sinistre peut affecter l'entreprise à plusieurs niveaux : personnel, organisation, patrimoine matériel et immatériel, stratégie. L'entreprise étant considérée comme un système, chacun de ces niveaux est en interaction de sorte que l'impact d'un sinistre n'est jamais isolé. ***Notons à quel point les notions de vulnérabilité, de menace et de risque sont étroitement liées !***

Chaque menace, ou risque brut, est alors mesurée en terme de potentialité et d'impact sur l'organisation comme une **zone de vulnérabilité**.

Les zones de vulnérabilité de l'entreprise peuvent alors évaluées de la façon suivante :

$$Vul_i = P\left(Risque_i\right) \times \sum C\,\mathrm{Im}\,pact$$

L'objectivité de l'évaluation de l'impact est par essence relative dans la mesure où elle reste le fait des dirigeants de l'entreprise qui, même conseillés, restent seuls juges de la valeur de leurs intérêts. Si l'analyse des vulnérabilités peut encore être envisagée de manière rationnelle dans une perspective stratégique, elle trouve cependant sa limite dans une approche économique plus pragmatique à laquelle se réfère généralement le dirigeant pour exercer ses compétences personnelles en matière de leadership.

L'optimisation de la fonction sécurité sous contrainte de coût apparaît en effet clairement comme une prérogative du chef d'entreprise. L'évaluation économique de la fonction sécurité fait apparaître des **zones de contrainte**. Elle peut être envisagée à partir du modèle mathématique suivant :

$$Vul_i = P(Risque_i) \times \mathrm{Im}\,pact(Risque_i)$$

Où :

- *P(Risque i) désigne la potentialité d'un événement i*

- Impact désigne le coût associé à la réalisation du risque i

Deux approches sont donc possibles :

- une approche stratégique qui permet d'identifier des zones de vulnérabilité. Elle peut être considéré comme la solution idéale pour un modèle de décision rationnelle (Aubert et al, 1999).

- une approche économique qui permet d'identifier des zones de contrainte. Le dirigeant définit alors le seuil à partir duquel une vulnérabilité doit être considérée comme critique au regard du rapport Investissement/Pertes qu'elle engendre.

A court terme, nous pouvons envisager une représentation cartographique des zones de vulnérabilités de l'entreprise. Ce type de représentation, très utilisée en analyse d'information, pourra être la base d'indicateurs utiles au management de la sécurité globale au sein de l'entreprise. Nos recherches se poursuivent actuellement dans cette direction.

Conclusion

Notre démarche s'inscrit dans le cadre d'une recherche sur le développement de la culture informationnelle, expérimentée à travers le programme Epices (Etudes prospectives en intelligence compétitive, économique et stratégique), développé sous la direction du Professeur Philippe Dumas, directeur du laboratoire LePont à l'université de Toulon et du Var.

Cette contribution montre que l'approche croisée de la sécurité par l'intelligence économique et l'expérience empirique permet d'envisager le concept de sécurité sous un angle global et tendant vers l'exhaustivité.

Il n'existe pas, en dehors de l'idéal théorique, de solution parfaite en matière de sécurité. Nous aurions à cet égard pu développer la notion de contrainte d'usage vécu par les utilisateurs d'information sensible au sein des services de renseignement (Dewerpe, 1994) pour démontrer que « trop de sécurité tue la sécurité ». De même certaines mesures de sécurité ne sont pas économiquement viables.

La notion même de sécurité nous appelle cependant à beaucoup d'humilité, c'est la raison pour laquelle nos propositions ne sauraient être envisagées en tant que démarche axiomatique. Par ailleurs, les enjeux d'une réflexion scientifique collective sur la sécurité, tels qu'ils émergent dans l'esprit du Centre de recherche en information et communication (CRIC) nous encouragent à partager cette étude et à soumettre son contenu à la critique des experts.

Bibliographie

Achard P., Bernat J.P. 1998, L'intelligence économique : mode d'emploi, ADBS Editions

Archimbaud J.L., Longeon R., (1999) Guide de la sécurité des systèmes d'information à l'usage des directeurs, CNRS, Paris

Aubert N., J.P.Gruère, J.Jabes, H.Laroche, S.Michel, 1999, Management aspects humains et organisationnels, PUF

Barlette Y., (2002), La sécurité des informations, quels risques pour quelles entreprises ?, Actes préliminaires du colloque de recherche du CRIC, Paris, 27 mai 2002

Baron G, (1996), Intelligence économique, objectifs et politique d'information, Institut des hautes études de la sécurité intérieure, Etudes et recherches

Bournois, F., P.J. Romani, L'intelligence économique et stratégique dans les entreprises françaises, Economica

Bulinge F. (2001), Pme-Pmi et intelligence compétitive : les difficultés d'un mariage de raison, *Actes du colloque Vsst'2001*, Barcelone, Octobre 2001

Charbonnier, J. (1990), Risques et assurances des PME-PMI, Dunod

Dewerpe A., 1994, Espion, une anthropologie du secret d'Etat contemporain, Grasset

Guinier D., (1992), Sécurité et qualité des systèmes d'information, Paris, Masson

Kervern, G.Y., P. Rubise, 1991; L'archipel du danger, Economica

Kervern, G.Y., 1995 ; Eléments fondamentaux des cindyniques, Economica

Kervern, G.Y., 1998 ; Une perspective historique et conceptuelle sur les sciences du danger : les cindyniques, Introduction aux cindyniques, sous la direction de Jean-Luc Wybot, Eska 1998

Larivet, S. (2000) Proposition d'une définition opérationnelle de l'intelligence économique, CERAG n°04-00

Levet, J.L., Paturel R. (1996), L'intégration de la démarche d'intelligence économique dans le management stratégique, *Actes de la Vème Conférence Internationale de Management Stratégique*, Lille, 1996

Marchesnay M., Fourcade C. 1997, Gestion des PME-PMI, Nathan

Martre, H. (1994), Intelligence économique et stratégie des entreprises, La documentation française

Melot F. 1999, Sécurité, le premier guide pour l'entreprise, Editions Carnot

Warusfel, Bertrand, Intelligence économique et sécurité de l'entreprise*, in Entreprise et sécurité*, Les cahiers de la sécurité intérieure n°24, 1996