



VERS LA NORMALISATION DE L'AUDIT DE RISQUES INFORMATIONNELS

(Article paru en novembre 2001
dans le magazine *Veille*)

*Par Didier Lucas
Directeur adjoint de l'école de guerre économique*

*et Alain Tiffreau
Consultant associé chez C4ifr*

MOTS CLES :

Intelligence économique, sécurité des entreprises, sécurité de l'information

En 1994, le rapport Martre donna naissance au concept d'intelligence économique en France. De nombreuses entreprises perçurent alors les enjeux et la nécessité de développer en interne des structures de veille stratégique. L'apport de cette étude dans l'appréhension des facteurs de développement économique fut essentiel car il permit réellement de décomplexer les organisations vis-à-vis de cette doctrine. Si aujourd'hui les principaux acteurs économiques reconnaissent volontiers pratiquer l'intelligence économique, en revanche il apparaît clairement qu'il convient de réaliser de nouveaux progrès dans la gestion offensive des sources ouvertes. L'acceptation de pratiques offensives demeure encore marginale. Pourtant les cas de déstabilisation stratégique par l'information abondent et ils révèlent les lacunes organisationnelles des entreprises confrontées quotidiennement aux agissements agressifs de la concurrence. L'ouvrage publié récemment par l'Institut des Hautes Etudes de la Défense Nationale constitue une avancée décisive dans la connaissance des pratiques en vigueur. Les recherches du Professeur Bournois et de Pierre-Jacquelin Romani menées auprès de 1200 entreprises françaises dressent aujourd'hui une cartographie exhaustive des pratiques en vigueur. Parions que ce benchmarking original figurera très bientôt parmi les ouvrages de références auprès des spécialistes du sujet.

Guerre économique et sécurité des entreprises

Cette étude révèle quelques paradoxes dans le discours des cadres dirigeants et des responsables de l'intelligence économique et stratégique qui ont accepté de livrer leur perception de l'environnement. Une immense majorité d'entre eux (95%) déclarent ainsi évoluer dans un climat de guerre économique. S'il ne nous appartient pas de juger de l'effectivité de ce contexte, en revanche il semble surprenant d'observer qu'il existe à cet égard peu de structures dévolues à l'évaluation, la prévention et la gestion des menaces qui découlent de cette compétition exacerbée. Autrement dit, pourquoi les entreprises ne sont-elles généralement pas dotées de *war room* destinées à la conduite d'opérations en situation de crise ? Le durcissement du jeu concurrentiel ne tolère désormais plus de minimiser les risques nouveaux issus de la globalisation des échanges. Il importe donc de prendre conscience des pratiques offensives existantes, pratiques dont la finalité consiste en la déstabilisation stratégique de l'adversaire. Qu'il s'agisse de désinformation, de rumeurs savamment orchestrées ou de stratégies d'influences, ces manœuvres subversives visent toutes au discrédit et à l'affaiblissement financier de l'entreprise qui en est la cible. Dès lors, il apparaît urgent et fondamental que chaque entreprise s'organise afin d'assurer la protection de son patrimoine immatériel et notamment informationnel. Les *war room* idéalement constituées devraient réunir les structures dédiées à l'intelligence économique, la prospective et la stratégie, la communication de crise et le lobbying. A cet égard, il convient de saluer l'initiative du groupe Danone qui vient récemment de communiquer sur la fusion de ces cellules au sein d'une seule et même entité afin d'optimiser la prévention et le suivi des actions de contre-communication en cas de crise ou d'agression extérieure,

Les enjeux de l'audit de risques informationnels

La démarche d'audit de risques informationnels se présente donc comme une solution simple et relativement aisée dans sa mise en œuvre. Elle devient fondamentale pour prévenir et détecter toute crise susceptible de déboucher sur la perte de parts de marchés. Si le pilotage d'actions classiques de communication, à l'occasion de catastrophes naturelles ou de défaillance, conduit généralement à la résolution de la crise, en revanche ces procédés ont démontré leurs limites opérationnelles lorsqu'une entreprise est confrontée à des crises liées à des opérations de guerre par l'information. Il ne s'agit donc plus de penser ces scénarii en terme de gestion des risques accidentels, mais au contraire de les anticiper. Une telle démarche nécessite donc

l'élaboration de mesures destinées à l'évaluation des vulnérabilités informationnelles auxquelles sont soumises les entreprises. Bien qu'encore hétérodoxe, elle devrait constituer un point de réflexion élémentaire des dirigeants en charge de la sûreté économique. Est-il nécessaire de rappeler les coûts financiers engendrés par une attaque majeure, au regard de l'investissement qu'il convient de réaliser afin de s'assurer la réduction de ces risques ?

De l'évaluation à la procédure d'audit

L'évaluation des vulnérabilités préalables à l'audit repose sur une exigence naturelle d'objectivité et de systématisation. Elle consiste, en ce qui nous concerne, à analyser l'environnement de l'entreprise afin de détecter les failles potentielles exploitables par la concurrence ou un tiers. Sa nature intuitive se caractérise donc par une construction aussi logique que formelle. Toute la difficulté de cette démarche réside dans l'éventail très large de pratiques cognitives auxquelles est confrontée l'évaluateur. On se trouve donc face à un continuum de pratiques impliquant la collecte et le traitement d'informations, de préoccupations normatives et/ou instrumentales. Mais on pourrait aussi bien, dans beaucoup de cas, parler de contrôle ou d'analyse de gestion, de contrôle de conformité, de conseil, d'expertise ou de recherche appliquée. La définition du rapport Viveret (1989) met l'accent sur la dimension normative de l'évaluation: «évaluer, c'est former un jugement sur sa valeur ». Le terme d'évaluation contient le mot « valeur », et il est aisé de constater que des valeurs de référence sont à l'arrière plan de la plupart des évaluations. La décision d'évaluer est toujours liée à la volonté d'argumenter sur la réussite finale ou le bien fondé d'une action. Evaluer sa vulnérabilité informationnelle consiste donc à déterminer la valeur des mesures de sécurité et de protection de son image corporate.

Cela renvoie à l'unique question: quels sont les dysfonctionnements de mon organisation qui pourraient être utilisés à mon encontre par un acteur soucieux de me déstabiliser? La démarche évaluative de type objectif se définit comme une procédure formalisée, productrice de connaissances inédites au regard de la propre vision et de la réalité du commanditaire de l'évaluation, ainsi que des autres destinataires. Les jugements de valeur portés par l'évaluation doivent être perçus par eux comme fondés sur des arguments légitimes. Cette exigence de légitimité de l'argumentation n'impose pas à l'évaluateur de ne formuler que des conclusions qu'il estime acceptable pour le commanditaire. Compte tenu de ce qui vient d'être dit, cette démarche fera appel à deux registres d'élaboration méthodologique: le référentiel, et au débat quantitatif/qualitatif. Qu'elles soient de nature qualitatives ou quantitatives, les données s'intègrent dans des assertions qui visent à qualifier la réalité et à former le jugement des lecteurs du rapport. On peut distinguer trois registres principaux d'argumentation, qui contribuent de manière complémentaire à assurer la crédibilité des conclusions de l'évaluation:

- le registre du constat : ces constats semblent induits par l'observation directe de la réalité, même si tout constat comprend nécessairement un mixte d'inductions et de déductions (les constats quantitatifs peuvent s'apparenter à un comptage physique ou financier et les constats qualitatifs sont orientés vers la description de processus socio-organisationnel) :
- le registre démonstratif et interprétatif.
- le registre de l'opinion: le point de vue de groupes d'intérêts concernés par une mesure constitue parfois la principale information disponible pour évaluer sa réussite.

Les critères de qualités de l'évaluation, parfois appelés « standards » ou « valeurs » de l'évaluation, sont des caractéristiques typiques d'une « bonne évaluation », susceptibles de fournir des références pour juger la méthode, le déroulement ou le résultat d'une évaluation. Ces critères concernent à la fois la qualité scientifique des connaissances produites, le respect des règles déontologiques dans les rapports entre les différents protagonistes de l'évaluation, et enfin les éléments qui conditionnent l'utilisation pratique des résultats de l'évaluation. L'une des possibilités de juger de la qualité consiste à réaliser des méta-évaluations, revues comparatives

portant sur un ensemble d'évaluations. Les méta-évaluations sont une pratique courante aux Pays-Bas et aux Etats-Unis.

A l'issue de l'évaluation, la démarche d'audit opérationnelle prend forme, déclinée en trois parties distinctes :

- environnement économique de l'entreprise (positionnement de l'entreprise, environnement concurrentiel, perception de l'entreprise par ses clients, relation avec ses partenaires, analyse de l'environnement juridique)
- image de l'entreprise sur Internet (gestion de l'image sur Internet, analyse du site et comparaison avec la concurrence, détection de la rumeur et des sources contestataires, analyse des signaux faibles)
- mise en place d'une cartographie des acteurs susceptibles d'engager des attaques informationnelles intégrant les risques potentiels (Comment ces informations peuvent-elles être exploitées contre l'entreprise ? Quelles en sont les conséquences pour l'entreprise ? Quelle est l'importance du risque ? Est-il d'une intensité faible, moyenne ou importante?)

L'information dans son acceptation offensive perturbe fortement l'activité des entreprises. Chaque stratégie d'attaque par l'information se décline autour des grands principes que sont le mensonge, la dénonciation ou la protestation. Dans chacun des cas, le but est de créer le doute dans l'esprit des clients et des consommateurs, afin d'altérer l'image de l'entreprise et de l'enfermer dans un discours de justification. Quand la justification est assimilée à la reconnaissance effective d'un problème, une image dégradée se traduit au final par des pertes de parts de marchés.

La finalité de l'audit des risques informationnels vise donc à analyser les failles potentielles des sociétés qui pourraient être utilisées par la concurrence voire par certaines organisations de consommateurs. Cet audit doit conduire à l'anticipation de ce type d'agression et préparer plus efficacement à la gestion des risques dans le cadre d'une déstabilisation par l'information.

La normalisation de l'audit de risques informationnels

L'identification par l'entreprise d'une pratique offensive à son égard au cours des trois dernières années révèle des disparités suivant la typologie dans laquelle elle se classe. Ainsi les « Internationales » ont identifié plusieurs attaques majeures à concurrence de 21.1% d'entre elles. Quant aux « Nationales », 12.6 % attestent de l'effectivité de telles agressions. L'observation de ces statistiques confortent donc l'obligation nouvelle qui est faite aux entreprises de se prémunir contre ces agissements. L'audit comptable et financier relève de l'obligation légale pour les sociétés anonymes qui sont tenues de faire certifier la conformité de leurs comptes. Cela semble aujourd'hui naturel car cela concourt au respect du droit d'information élémentaire des actionnaires. Au même titre, il est devenu courant, pour un dirigeant de grand groupe de faire authentifier sa politique générale par un prestataire de conseil renommé tel Mc Kinsey ou le Boston Consulting Group, car elle consiste à légitimer les plans d'actions stratégiques auprès du conseil d'administration. Pareillement, l'audit des risques informationnels tend à s'imposer comme un standard, au même titre que les normes sur la qualité, afin de satisfaire aux doléances des actionnaires, avant tout soucieux de la compétitivité de leur entreprise.

Les demandes croissantes des acteurs économiques envers cette démarche d'audit des risques informationnels, attestent de la nécessité de poursuivre l'élaboration d'outils de diagnostic plus performants, afin de réduire les risques nouveaux auxquels les entreprises sont aujourd'hui confrontées. A cet égard, il importe de persévérer dans la recherche et le développement, et d'inciter les entreprises à une pratique systématique de cet audit.