



LE MANAGEMENT INTELLIGENT, UNE FORME DE PENSEE ET D'ACTION

La finalité d'une entreprise est de pérenniser son développement. L'entreprise possède des richesses, des savoirs faire, des connaissances, qu'il faut protéger et faire fructifier.

Avec la mondialisation galopante, la pérennité des entreprises est de plus en plus fragilisée. Le management intelligent s'appuie sur l'intelligence économique et permet de valoriser l'ensemble des richesses de l'entreprise indispensable à sa pérennité, ainsi que de détecter opportunités et menaces.

Les PME-PMI sont les entreprises les plus fragiles. Mais l'intelligence économique y est plus facile à mettre en œuvre que dans une grande entreprise car le champ de l'intelligence économique y est beaucoup plus restreint, voire souvent limité à une ou deux activités, et la sensibilisation du ou des responsables est immédiate. D'autre part, il n'y a pas de conflit de pouvoir entre les différentes activités car une PME ne recherche pas sans cesse l'activité à renforcer de façon prioritaire, au détriment d'autres activités. Comme il n'y a pas de conflit d'intérêt au sommet de l'entreprise, il est plus facile de trouver une personne pour développer les activités transverses. Dans une très petite entreprise, cette personne est le chef d'entreprise. Dans une entreprise de 100 à 500 salariés, cette personne va remplir les fonctions de secrétaire général, quelque soit son titre. Si l'entreprise est un peu plus technique, ce sera le spécialiste qualité, sécurité, sûreté, environnement ou intelligence économique. Dans les entreprises de plus de 1000 salariés, il y a plus de choix, mais les conflits apparaissent entre des systèmes complémentaires qui deviennent concurrents (audit et sûreté, sécurité santé du travail et environnement, études de marchés, etc.).

Le management intelligent s'appuie sur l'intelligence des risques. Le principe qui guide l'entreprise vers le management intelligent part de l'existant : le contrôle de la situation financière et la capacité à identifier les risques qu'elle peut subir, risques classiques et risques émergents liés à la sûreté de l'information, aux questions de communication et de gestion de crise. Le directeur de PME doit décider au risque maîtrisé, c'est-à-dire en recherchant des opportunités et en minorant les risques.

La taille réduite d'une PME facilite l'intégration du management intelligent dans le projet d'entreprise, et donc permet de mettre en valeur le rôle social de l'intelligence économique.

Les PME PMI sont l'espace privilégié pour le management intelligent car d'une part, il n'y a pas de conflit de pouvoir entre les activités, et d'autre part, le champ d'action y est plus restreint. En outre, par nécessité, elles ont à leur disposition des personnes qui occupent des fonctions polyvalentes.

1.- Le management offensif

Le management offensif, c'est d'abord le réseau

L'intelligence économique est une valorisation de l'ensemble des disciplines qui fait travailler autrement l'ensemble du personnel. C'est la mise en réseau de ces compétences qui peut améliorer le fonctionnement de l'entreprise. Le réseau doit être aussi bien interne qu'externe à l'entreprise.

En interne, il faut faire remonter les dysfonctionnements que tout le monde voit mais que personne ne signale (utilisation des rapports d'étonnement)

En externe, la constitution d'un réseau multidisciplinaire performant est difficile. Il y a de nombreux sujets qu'une PME ne peut pas connaître par elle-même. Le réseau se limitera à quelques personnes nécessaires comme relais, par exemple un expert au sein d'une Chambre de commerce et d'industrie, un senior spécialiste des risques, etc.

Une PME doit soigner son réseau externe et son lien avec les acteurs de la recherche.



Le management offensif, c'est aussi la gestion de l'intégralité des risques

Les risques doivent être maîtrisés. Un risque ne peut être assuré que lorsqu'il y a une méthode de réduction du risque et que s'il existe des statistiques sur ce risque. Il faut avoir la connaissance critique et être capable de mesurer le risque en termes de fréquence et de gravité. Le croisement de la fréquence et de la gravité donne la notion de criticité du risque. L'analyse n'a pas besoin d'être très fine, l'identification est suffisante.

Il ne faut pas croire que l'entreprise est protégée parce qu'elle a respecté les lois et règlements de l'espace économique dans lequel elle vit (par exemple, obligations liées au code du travail, obligations financières). Une entreprise est à l'abri quand elle est capable d'identifier les risques possibles, d'en mesurer les conséquences, et qu'elle a mis en place des mesures de réduction de ces risques.

Le management offensif, c'est la recherche des opportunités

Pour se développer, une PME ne cherchera pas une nouvelle activité mais une activité complémentaire, ou une nouvelle façon d'appréhender son activité. Contrairement à un grand groupe, une PME restera dans la filiation. La recherche des opportunités c'est la recherche d'un partenaire ou d'une acquisition (il faut, par exemple, s'intéresser aux difficultés de trésorerie des concurrents).

Le management offensif, c'est encore la détection des menaces : fragilisation du capital, apparition de nouveaux produits concurrents, etc.

Si la veille stratégique est nécessaire, ses objectifs doivent être ciblés et en permanence réorientés, car une veille tous azimuts est lourde et permet difficilement de faire émerger l'information utile.

L'analyse stratégique est par définition l'étude de marché, c'est-à-dire l'étude des attentes du marché (attentes clients), les perspectives techniques du marché, et les comportements techniques commerciaux et financiers des concurrents (les structures de coût et de marges opérationnelles). Le benchmarking - qui est la comparaison de ces comportements avec ceux de l'entreprise - doit être une attitude naturelle. Il faut être aussi attentif à la contre-intelligence possible à travers des leurres.

Le management offensif, c'est enfin le lobbying

Le lobbying est une méthode offensive qui n'est pas dans les habitudes françaises. Or la meilleure manière de rester compétitif et de progresser sur un marché, c'est de faire en sorte que ce marché soit organisé à la fois pour le bien public et pour les intérêts propres de l'entreprise.

Le lobbying permet souvent d'arriver à un consensus dans l'intérêt général et d'éviter des situations conflictuelles.

A titre d'exemple, pour éviter qu'un concurrent puisse afficher des prix cassés en détournant les règlements de la profession, la meilleure démarche est d'organiser soi-même la profession de manière la plus transparente possible pour que la libre concurrence soit la même pour tous. Cette démarche profite au marché ; elle profite au consommateur, à l'espace sociétal qu'est aujourd'hui l'Europe, et à l'industriel qui est en avance sur le marché. Cette démarche n'est jamais entreprise en France parce qu'elle nécessite un investissement humain pour faire du lobbying auprès des instances professionnelles et des instances publiques. A défaut d'investissement humain, il faut prendre le pouvoir à la chambre syndicale, à la chambre de commerce ou à la fédération professionnelle, pour qu'un organisme fasse la démarche à la place de l'entreprise, à la fois pour le bien du syndicat, de la fédération ou de la CCI auquel appartient l'entreprise, pour le bien de l'espace économique dans lequel vit l'entreprise, et pour l'image personnelle de l'entreprise.



L'entente avec l'organisme professionnel repose sur l'intérêt public au sens large. Celui-ci recouvre l'intérêt de la profession, l'intérêt du consommateur, et l'intérêt de l'entreprise. Il faut éviter les actions isolées qui sont plus néfastes qu'utiles.

Un expert du lobbying accompagnera la démarche en s'appuyant sur les experts de l'entreprise, voire des entreprises concurrentes du secteur, pour démontrer au fonctionnaire de l'Etat qui établit les lois et règlements que l'intérêt public est supérieur à l'intérêt privé, y compris sur le plan économique. Le message a plus de poids vis-à-vis du pouvoir public lorsqu'on passe par un organisme professionnel.

L'action de lobbying consiste à agir sous couvert de l'intérêt général pour influencer les organismes concernés dans un sens favorable à un intérêt privé ou professionnel.

2.- Le management des connaissances

La validation de l'information

Toute information récoltée doit faire l'objet d'un processus de validation collégial, par moyens humains et/ou techniques, pour s'assurer de son origine, de sa vraisemblance et en l'occurrence, de sa pertinence. Il faut aussi identifier les écueils à éviter de contaminations possibles. En la matière, le réseau externe peut apporter une aide efficace.

Naturellement, il faut maintenir l'indépendance des sources, et veiller aux tentatives de désinformation, voire de modulation de l'information (contre-intelligence).

La circulation de l'information passe par l'intranet et doit être au cœur du système d'information de l'entreprise, ne serait-ce que pour mieux protéger l'information. Ce réseau ne doit servir qu'à des opérations de fonctionnement interne. Il doit être confiné dans l'entreprise, et physiquement séparé de l'extranet et de l'internet.

Le système d'information est élaboré dans le souci de faciliter l'enregistrement pertinent des informations utiles et de permettre leur exploitation par tous, de manière différenciée en fonction de leur classement et des autorisations d'accès. Les entreprises d'une certaine taille, ou particulièrement sensibles, doivent envisager des moteurs de recherche propres.

Par ailleurs, il y a des recherches d'information, notamment en matière de développement, qu'il vaut mieux faire sous couvert d'anonymat, c'est-à-dire dans un lieu anodin (cabinet d'intelligence économique) plutôt qu'à partir de l'entreprise, pour que cette recherche soit noyée dans un flux de recherches.

La gestion des compétences

L'entreprise doit naturellement veiller à une gestion rationnelle des compétences au sein de son personnel. Une attention particulière doit être apportée à la conservation des savoirs et des savoirs faire des personnels en fin de carrière.

La gestion des hommes clés doit être suivie de manière à ce que le départ ou la disparition de l'un d'entre eux ne perturbe que faiblement l'entreprise.

Une bonne gestion des compétences des personnels dans les PME-PMI est indispensable à la pérennité de celles-ci, malgré de réelles difficultés liées à leurs tailles.

Le retour d'expérience

Après chaque échec, ou chaque crise, un retour d'expérience précis est nécessaire



3.- Le management défensif

La meilleure défense c'est l'attaque, et d'ailleurs, les entreprises qui se protègent le mieux sont celles qui cherchent le mieux.

La maîtrise préalable des risques aléatoires traditionnels :

Il est vain pour une entreprise d'envisager de maîtriser les nouvelles vulnérabilités sans avoir expérimenté avec succès la méthode de maîtrise des risques sur les risques aléatoires traditionnels liés à l'exercice de son activité. Cette méthode se caractérise par les actions suivantes :

- Identifier les risques liés aux hommes, matières, procédés, énergies, organisation, produits, environnement, systèmes et services commercialisés ;
- Rechercher toutes leurs combinaisons possibles comme sources ou cibles de réalisation de risques ayant des conséquences financières directes et indirectes sur la pérennité et/ou la rentabilité de l'entreprise ;
- Mesurer la fréquence et la gravité financière en cas de survenance de ces scénarii de risques avec des outils d'analyse éprouvés ;
- Mettre en place des programmes de réduction de ces risques intégrant les lois et règlements, mais ne se limitant pas à leur seul respect, car tournés vers la recherche de la fiabilité de l'organisation considérée comme un système cohérent et homogène ;
- Procéder à la préparation du financement de ces risques en prévoyant un Plan de Continuité de l'Activité intégrant la gestion des crises dans tous leurs aspects notamment en matière de communication médiatique.

Le point clé de la méthode de maîtrise des risques aléatoires est la mesure de leur fréquence et de leur gravité financière

La mise en protection de l'entreprise

Toutes les entreprises vivent dans le même monde. Elles ont toutes le même objectif : ne pas rester figées sur des positions acquises mais grandir pour ne pas régresser, voire disparaître. Elles vivent toutes avec les mêmes règles, mais toutes ne les appliquent pas. La protection doit être prise en fonction des méthodes des concurrents, et non pas en fonction de ses propres méthodes, car les armes utilisées par les concurrents ne sont pas nécessairement les mêmes que les siennes. Elles peuvent être moins propres. L'éthique des concurrents pouvant être différente, il convient de se protéger vis-à-vis des méthodes illégales, visibles ou invisibles, par exemple l'espionnage.

De concurrent, on peut devenir partenaire, et vice versa. Dans le partenariat il faut mettre en synergie des savoirs et des savoirs faire respectifs strictement limités à l'objet du partenariat, et renforcer la protection autour des informations partagées. Externalisation et sous-traitance nécessitent les mêmes protections qu'un partenariat.

En situation de concurrence, il peut être bon d'accélérer la mise en œuvre de capacités jusqu'alors tenues secrètes.

Tout secret n'a qu'un temps, et l'innovation est la meilleure protection de l'entreprise.

Les menaces sont plus diverses qu'on ne pense. Elles proviennent non seulement des concurrents, mais aussi de groupes de pression divers, voire de l'Etat, directement ou indirectement. Les entreprises qui se protègent le mieux sont celles qui recherchent le mieux, car elles ont mis en place un système de protection adapté aux menaces qu'elles ont bien identifiées. Pour analyser les risques il faut savoir ce qui est arrivé aux autres. Les CCI - qui sont en mesure de mettre en relation avec les services spécialisés de l'Etat - les ambassades et divers organismes publics et privés d'intelligence



économique peuvent apporter des éléments de réponse. Des sociétés de presse spécialisées font tous les jours des synthèses remarquables, accessibles à peu de frais.

Les risques externes

Ici, c'est le facteur humain qui joue, notamment à travers des initiatives hostiles ou malveillantes, ou tout simplement l'habile stratégie de personnes, d'organismes ou de structures étrangères à l'entreprise. Il faut identifier les points vulnérables de l'entreprise, renforcer et protéger physiquement les points faibles, avec beaucoup d'énergie plutôt que de chercher à les camoufler.

S'imaginer qu'un secret est parfaitement tenu sur tel ou tel point de vulnérabilité relève d'une attitude irresponsable. Il faut exiger la confiance, mais prévoir son non respect, et en tirer les conséquences.

Les risques internes

Les risques provoqués dans les murs de l'entreprise par l'imprudence, la négligence et surtout la malveillance ne doivent pas être sous-estimés. Toutes sortes de mesures de précaution sont recommandées et certaines d'entre elles s'inscrivent tout naturellement dans le management défensif. La vigilance qui s'impose entre dans le cadre de l'intelligence économique.

La lutte contre les risques internes est multiforme et complexe. Elle est toutefois théoriquement plus simple et plus facile à mettre en place dans une PME-PMI que dans une grande entreprise où les conflits d'attribution peuvent surgir fréquemment et s'exacerber. En revanche, dans une petite structure, il est plus difficile d'admettre que le risque d'erreur humaine est toujours sous-évalué, et que personne n'est à l'abri d'une manipulation, d'un chantage ou d'une trahison. La culture de l'intelligence économique qui doit y être développée est d'abord une prise de conscience du devoir de sauvegarder prioritairement deux grands domaines du savoir-faire de l'entreprise :

- le premier concerne l'art du choix des secteurs de marchés visés par la production ainsi que les grandes orientations stratégiques, la prise de conscience de ses motifs profonds, par nature confidentiels. Et on oublie trop souvent que le service juridique détient beaucoup d'éléments pertinents à cet égard.

- le second concerne la technique de production, la culture et la mémoire d'entreprise qui tiennent dans les mains et les esprits des gens de l'atelier et du bureau d'études. Heureusement, même si sur ce point le secret n'est pas toujours convenablement sauvegardé, il y a des impondérables issus du cercle de qualité qui ne s'exportent pas facilement.

La propriété intellectuelle et industrielle (cf. code de la propriété intellectuelle et industrielle)

La propriété intellectuelle est l'ensemble des droits dont peuvent bénéficier des personnes physiques ou morales sur l'œuvre de leur esprit. On distingue la propriété intellectuelle littéraire ou artistique de la propriété intellectuelle et industrielle. C'est cette dernière qui nous intéresse. Le processus à mettre en place pour faire vivre cette propriété doit être défini au sein de l'entreprise.

En premier lieu, il est nécessaire d'identifier les domaines d'informations, les sites d'activités et le mode de conception et de détention des informations qui correspondent à cette définition. En second lieu, il convient de procéder à une analyse des vulnérabilités avec la même méthode que pour les risques aléatoires traditionnels. Enfin, un plan de gestion doit être mis en place comportant une politique internationale de dépôt de demandes de brevets.

Rappelons à ce sujet, que les entreprises françaises, en particulier les PME et les individuels, déposaient jusqu'à présent beaucoup moins de demandes de brevets à l'étranger que leurs principaux concurrents, en raison notamment du coût des traductions obligatoires des brevets accordés. La récente ratification du "protocole de Londres", qui permet d'enregistrer les brevets dans une seule langue, est de nature à améliorer cette situation et donc à diminuer la vulnérabilité de "l'entreprise France". (Une adresse pratique : www.inpi.org)



Les risques informatiques

Aujourd'hui, toutes les entreprises archivent leurs données sur support informatique. Ces données doivent faire l'objet de sauvegardes systématiques et récurrentes, car leur perte peut avoir de graves conséquences pour la pérennité de l'entreprise. L'emploi d'ordinateurs ou de serveurs à technologie RAID (c'est-à-dire disposant d'un enregistrement double) est un avantage indéniable. Il faut protéger ses ordinateurs à l'aide :

- d'un antivirus à jour (Norton, Avast antivirus, Orange Securitoo,...)
- complété d'un Firewall logiciel et physique (modem routeur) (ZoneAlarm, Tiny,...)

Le système d'exploitation (O.S.) le plus répandu – Windows – est le plus attaqué par virus, chevaux de Troie, logiciels espions,... C'est donc le plus vulnérable. Il est judicieux de lui préférer les O.S. libres comme Linux. De même, le disque dur doit être partitionné c'est-à-dire scindé en créant deux disques virtuels (ou plus). Ainsi en cas de crash du système d'exploitation nécessitant un reformatage, les données ne seront pas perdues.

Les machines contenant des données sensibles ne doivent jamais être connectées à Internet

Toute mise en relation par Internet peut être interceptée par un tiers. Le contenu de l'ordinateur peut donc être lu, téléchargé et ré-exploité, voire détruit.

De même, les transferts d'informations sensibles ne doivent pas transiter par Internet à moins d'être cryptées. Ce n'est pas suffisant : les données stratégiques de l'entreprise seront découpées et expédiées en plusieurs envois, si possible sous des adresses IP (*Internet Protocol*) différentes.

Dans l'attente de l'identification biométrique, les ordinateurs sont protégés par mots de passe qui doivent être difficiles à reconstituer et changés régulièrement. Il est recommandé d'utiliser les caractères spéciaux, symboles et chiffres.

En voyage, dans le train ou en avion, beaucoup de regards lisent ce qui est écrit sur les ordinateurs portables. En mission à l'étranger, il ne faut pas laisser ses données sensibles dans la chambre d'hôtel.

Quelques adresses pratiques :

- faire le ménage sur ses disques : www.cleanup.com
- inspecter son système : logiciel Ad-Aware de Lavasoft : www.lavasoft.de/ ou www.safer-networking.org/fr/index.html
- organiser et protéger ses mots de passe : <http://keepass.info/>
- surfer anonymement : <http://torproject.org>
- crypter ses données (algorithme 128 bits) : www.axantum.com/AxCrypt/default.html
- effacer vraiment ses données : www.heidi.ie/eraser/

En conclusion,

L'intelligence économique est à la portée de tous. Elle concerne l'ensemble de l'entreprise, personnel et activités. Le dirigeant doit être visiblement impliqué, et chacun, à son niveau, doit pouvoir faire valoir sa perception.

Le management intelligent - et en particulier le mode de fonctionnement en réseau - exige une rigueur de tous les instants et donc des efforts permanents.

La prise de décision suit les mêmes règles que celles du management intelligent et ne doit pas être dictée par l'émotionnel.

Enfin, l'évaluation permanente des résultats dans tous les domaines est une démarche naturelle et indispensable au progrès de l'entreprise.

Annexe : références bibliographiques

Management de l'intelligence économique

- 1- "Intelligence économique et stratégie des entreprises"; Travaux du groupe de travail présidé par Henri Martre, Commissariat Général du Plan, La documentation Française, janvier 1994
« Ouvrage fondateur »
- 2- "Du Renseignement à l'Intelligence Economique", de Bernard Besson et Jean-Claude Possin, Dunod, novembre 2006
« Ouvrage d'initiation particulièrement accessible »
- 3- "L'intelligence économique", de Bruno Martinet et Y.M. Marti, 2^{ème} édition, Les éditions d'organisation, 2001
« Ouvrage pédagogique »
- 4- "Intelligence économique et gouvernance compétitive"; sous la direction de Serge Perrine; INHES, La documentation française, juin 2006
« Ouvrage d'évaluation au très large spectre, 10 ans après le rapport Martre »
- 5- "L'Intelligence des risques" de Bernard Besson et Jean-Claude Possin; Institut Français de l'Intelligence Economique, IFIE, 2006
« Ouvrage de référence pour initiés et spécialistes »
- 6- "Le droit de l'intelligence économique", de Thibault du Manoir de Juaye; LexisNexis Litec, avril 2007
« Ouvrage juridique (unique) de référence »

Rapports officiels et autres publications

- 7- Travaux de Bernard Carayon :
 - "Intelligence économique, compétitivité et cohésion sociale"; rapport au Premier Ministre, juin 2003
 - Rapport 1664 sur la stratégie de sécurité économique nationale, 9 juin 2004
- 8- "L'intelligence économique pratique", de François Jakobiak; Les éditions d'organisation, 1998
« ouvrage concret mais nécessitant une initiation »
- 9- "Système de management de la sûreté", Référentiel CNPP n°1302, CNPP Entreprise, 2005
- 10- "L'intelligence économique, guide pratique pour les PME", rapport 2006 du Cercle d'intelligence économique de MEDEF Paris

Référentiels du CNISF

- 11- "Fiches Vulnérabilité et Sûreté des PMI"; CNISF, IHESI, AGREPI, 1996 (édition 1999)
- 12- "Guide pour l'innovateur" (pratique de l'exploitation des brevets, recherche, management, export), CNISF, 2001
- 13- "Guide Ingénieurs, entreprise et internet", CNISF, 2004
- 14- "Guide de la sécurité industrielle", CNISF, 2007

Filmographie

- 15- "Trace, l'intelligence économique au service du développement d'une PME", HRIE et association Ecole de guerre économique, avril 2008
«film pédagogique, dédié à la sensibilisation à l'IE au sein de l'entreprise»