



Sensibilisation aux enjeux
de l'Intelligence Économique

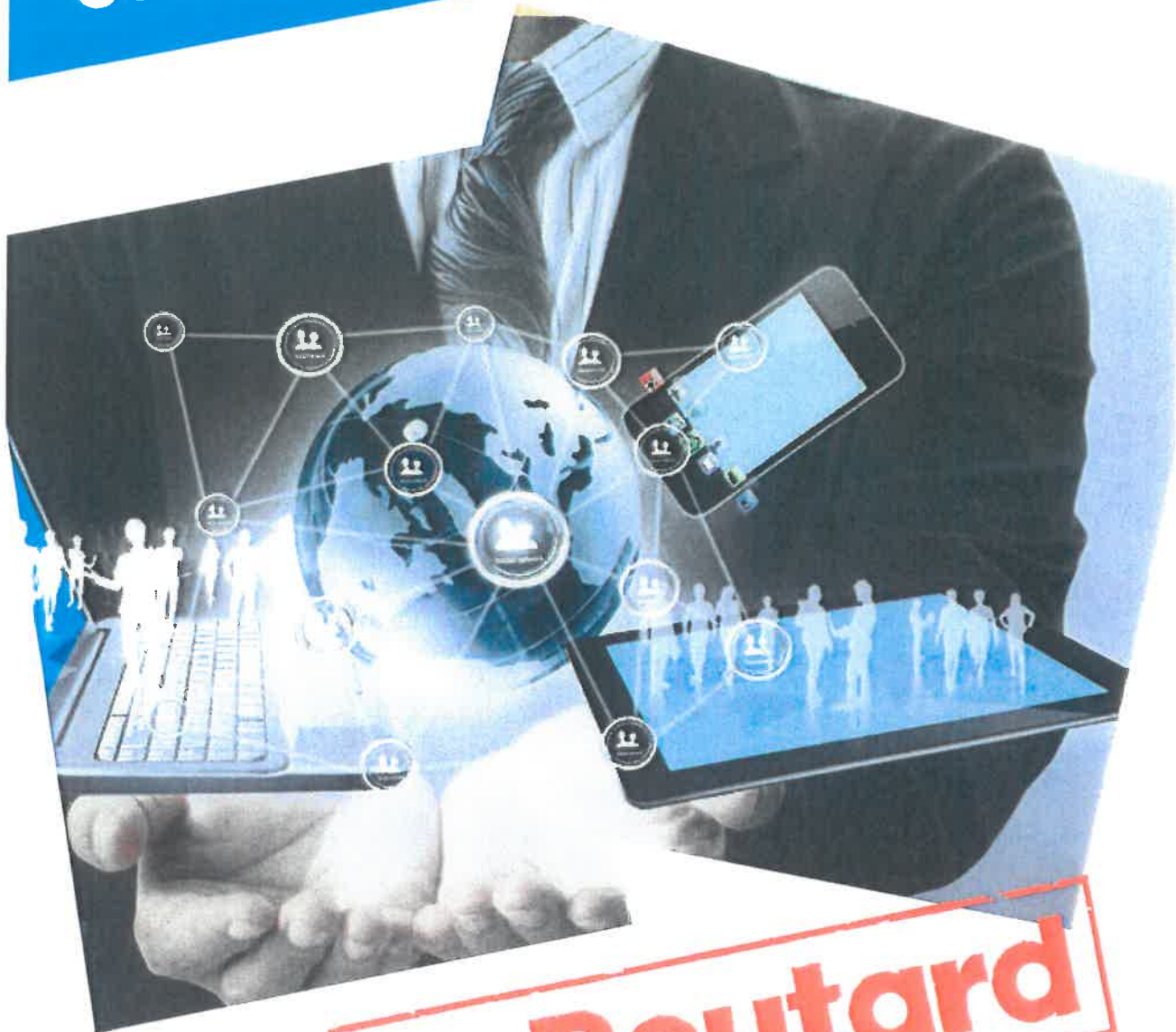
Mercredi 12 Octobre 2016

Intervention de Mme Agnès BRICARD

Coordinatrice du Guide du Routard de l'intelligence économique

Présidente d'honneur du Conseil Supérieur de l'Ordre de Experts-Comptables

Le guide de l'intelligence économique



Le Routard



Conseil
National
des Barreaux



Thomas Legrain
Conseil
Stratégie • Lobbying • Communication d'influence

routard.com

hachette

2014

Intelligence Économique

Trois Volets

Extraits du Guide du Routard de l'Intelligence Économique

- | | |
|------------------------------------|---------------|
| 1. <u>La Veille</u> | Pages 20 à 31 |
| 2. <u>L'Influence</u> | Pages 32 à 38 |
| 3. <u>La Sécurité Économique</u> | Pages 39 à 48 |
| 4. <u>Questionnaires par volet</u> | A, B et C |

Guide du Routard de l'Intelligence Économique à télécharger sur
le Blog d'Agnès BRICARD : <http://www.agnes-bricard.com/>

Et à rechercher dans la barre de recherche.

LA VEILLE

RÉPONDRE AUX BESOINS EN INFORMATIONS DES ENTREPRISES

La veille: une étape incontournable de l'IE

Selon l'Afnor, « la veille est une activité continue, en grande partie itérative, visant à une surveillance active de l'environnement technologique, commercial... pour en anticiper les évolutions ». (Prestations de veille et prestations de mise en place d'un système de veille, Afnor, 1998).

RÉPONDRE AUX BESOINS EN INFORMATIONS DES ENTREPRISES

Il existe deux types de besoins en informations nécessaires au chef d'entreprise dans ses décisions stratégiques :

- **les besoins permanents:** il s'agit de la surveillance du marché pour répondre aux objectifs de l'entreprise sur le long terme. Ils nécessitent la mise en place d'une activité de veille permanente ;
- **les besoins ponctuels:** ce sont les besoins d'informations qui répondront à une question ponctuelle visant la prise d'une décision stratégique spécifique. La démarche de recherche d'informations sera limitée dans le temps, son objectif étant juste d'apporter une réponse adaptée à la question posée.

S'il existe différentes veilles, toutes sont constituées d'une base commune, à savoir le recueil, la sélection, le traitement et la diffusion des informations. Selon la demande du dirigeant, la veille est plus axée sur l'entreprise elle-même avec ses produits, sa politique de recherche et de développement, ou alors sur les concurrents et les fournisseurs qui composent son environnement. La veille marketing et la veille concurrentielle sont assez proches en termes de bénéfices attendus et d'informations recherchées, mais leur objectif est distinct : se connaître et connaître l'autre.

Si le bien-fondé de la démarche n'est plus à démontrer, penser et structurer un dispositif de veille n'est pas un exercice simple pour une TPE-PME. Avant même le développement de l'intelligence économique en tant que fonction à part entière, les TPE-PME ont progressivement commencé à intégrer les démarches de collecte, de traitement et d'analyse de l'information ouverte afin de mieux comprendre et de mieux connaître leur environnement, qu'il soit concurrentiel, scientifique, technologique, financier, ou encore stratégique.

Une collecte d'informations externes décisive

Même si elle ne se nomme pas intelligence économique, la collecte d'informations stratégiques est assez répandue dans les TPE-PME. Pour autant, on s'aperçoit que les informations ne sont pas recueillies de manière structurée : la diffusion, le partage et le mode de présentation de l'information ne sont pas le point fort des TPE-PME. Très souvent, l'information n'est pas organisée et hiérarchisée de manière à pouvoir être distribuée facilement à l'intérieur de l'entreprise. Si le dirigeant est globalement bien informé, il existe une réelle difficulté à voir l'information redescendre vers l'ensemble des collaborateurs. Cependant, l'intérêt des entreprises évolue favorablement et elles souhaitent en savoir plus sur la gestion de l'information externe. En général, le dirigeant

d'entreprise est conscient que le fait de posséder des informations sur ses marchés, ses clients ou ses fournisseurs est d'une importance capitale pour définir la stratégie de son entreprise. Afin de renforcer la politique de son entreprise à l'égard de l'information externe, il y consacre désormais un budget spécifique et cherche à y motiver et à y former ses collaborateurs.

Les sources d'information les plus utilisées par les dirigeants des TPE-PME sont, par ordre d'importance, les publications, Internet, les réseaux sociaux, les contacts personnels et les événements publics. **Bien que 82 % des entreprises utilisent régulièrement Internet, elles ne vont pas jusqu'à utiliser ses possibilités avancées, comme les systèmes d'alerte.**

LES 5 ÉTAPES DU PROCESSUS DE VEILLE

1. L'expression des besoins ou l'élaboration du plan de veille

Il s'agit de l'opération qui vise à délimiter la partie de l'environnement et les problématiques que le chef d'entreprise veut mettre sous surveillance en fonction des enjeux qui sont les siens. Il va traduire ces problématiques en axes de veille. Cette étape a pour objectif de rendre la veille la plus efficace possible, en sélectionnant au mieux les capteurs de l'information. Elle relève généralement de la responsabilité du chef d'entreprise lui-même.

2. La recherche des sources ou *sourcing*

Elle vise à définir le périmètre des sources (Internet, réseaux sociaux, bases de données payantes...). Elle permet d'identifier, de hiérarchiser et de qualifier les sources d'informations disponibles afin de les exploiter en les traduisant sous forme d'objectifs ou de recherche. L'aspect récurrent de cette étape est indispensable dans la mesure où c'est du *sourcing* que vont largement dépendre les résultats obtenus par la veille. Aussi la personne en charge de la veille devra-t-elle impérativement surveiller les sources d'informations, les coter et les hiérarchiser en fonction de la légitimité de l'émetteur et de la valeur de leur contenu. En parallèle, elle devra organiser le plan de classement des documents.

3. La collecte ou la surveillance

Il s'agit de l'opération par laquelle la personne en charge de la veille recueille à proprement parler l'information. La base documentaire pourra être enrichie avec des documents externes, venant d'autres sources que celles retenues au départ. Cette étape peut être faite manuellement ou peut être automatisée, en fonction du degré de sophistication des outils de veille dont dispose l'entreprise. Il faut savoir que bon nombre d'outils gratuits existent, qui peuvent parfaitement répondre aux besoins des TPE-PME (voir page 112).

4. Le traitement, l'analyse et l'exploitation de l'information

Ces opérations permettent, parmi la masse d'informations recueillies, de ne retenir que celles qui sont susceptibles d'intéresser l'entreprise, d'esti-

mer/évaluer/quantifier (des notions) et de faire une cartographie des acteurs en fonction de leur influence. Le produit de l'analyse constitue l'information stratégique. Là encore, le travail de traitement peut être facilité par le recours à des outils plus ou moins automatisés.

5. La diffusion de l'information stratégique

L'information valorisée et mise en forme est adressée à son destinataire et utilisateur. Ce dernier pourra alors s'appuyer sur cette information pour apprécier une situation donnée et décider des actions éventuelles à entreprendre.

LES DIFFÉRENTS TYPES DE VEILLE

LES DIFFÉRENTS TYPES DE VEILLE

• La veille de l'environnement stratégique

Elle consiste à identifier les évolutions qui s'opèrent dans la société et qui risquent d'impacter l'activité économique des entreprises.

• La veille juridique

Elle consiste à surveiller de manière permanente la législation et ses évolutions, sur un domaine ou une activité donnée. Elle s'intéresse autant à la mise en place de nouveaux textes nationaux ou européens (lois, décrets, directives...) qui impactent directement la vie de l'entreprise qu'aux nouvelles normes. La rapidité d'évolution du droit et des normes, tant en France et en Europe que dans le monde rend cette veille incontournable. Les TPE-PME doivent en confier la responsabilité à leurs conseils extérieurs. La jurisprudence peut également faire l'objet d'une veille.

• La veille marché

Elle consiste à surveiller et à analyser un marché (offre, demande, concurrence, distribution...). Elle est souvent liée au lancement de nouveaux produits et à la détection de nouveaux marchés. Une attention particulière est consacrée aux études de marché qualitatives et quantitatives, ainsi qu'à l'observation des clients, des fournisseurs, des sous-traitants, ou encore des distributeurs. Enfin, elle inclut la surveillance des concurrents actuels ou potentiels de l'entreprise, l'analyse de leurs méthodes de production, de vente ou encore de recherche et développement. Une meilleure vision de son marché permet à l'entreprise d'ajuster sa politique de développement à travers des actions d'ordre tactique ou stratégique.

• La veille technologique

Elle consiste à surveiller les nouveaux produits à travers leurs techniques de fabrication et de production, ainsi que leurs moyens de distribution. Elle peut aborder les transferts de technologies, les dépôts de brevets et les travaux de recherche, mais aussi la protection des marques (recherche d'antériorité...). Elle s'appuie sur l'observation et l'analyse d'informations scientifiques, technologiques et techniques.

• La veille d'image

Elle permet de mesurer l'impact d'une campagne de communication, la satisfaction des clients et la notoriété d'une marque, d'un produit, d'un service ou encore d'une personnalité. Elle vise également, pour une entreprise, à surveiller son « e-réputation » en étant à l'écoute des actualités et des *buzz* qui peuvent affecter sa réputation à la fois *online* et *offline*.

• La veille comptable et financière

Elle permet à l'entreprise d'identifier, à l'occasion de l'établissement de ses business plans et de ses comptes annuels, à la fois ses faiblesses et ses opportunités de développement. Cela lui permet ensuite de couvrir ses risques à travers des actions de sécurisation et de se développer dans son secteur.

Vers qui se tourner, en fonction du type de veille ?

Si les recours à la presse, à Internet, aux réseaux sociaux, à des logiciels de veille ou encore à des cabinets d'intelligence économique sont autant de moyens adaptés, il est important de ne pas oublier les réseaux humains qui comptent de nombreux experts capables, en fonction de leurs compétences métier, de mettre en place et de gérer des dispositifs de veille. Les dirigeants de TPE-PME doivent avoir le réflexe de travailler en réseau avec eux.

Type de veille	Exemples d'experts
Environnement stratégique	Pouvoirs publics, ONG, conseils en stratégie...
Réglementaire	Pouvoirs publics, organismes de normalisation, avocats, experts-comptables, organismes de gestion agréés, notaires...
Marché	Chambres de commerce et d'industrie, Chambres de métiers et de l'artisanat, organisations professionnelles, UbiFrance...
Technologique	INPI, ARIST, réseau des conseillers et attachés scientifiques et techniques des ambassades de France, pôles de compétitivité, AFNOR...
Image	Experts en communication et en « e-réputation »... Conseils en propriété intellectuelle (dessins, modèles...)
Comptable et financière	Experts-comptables, commissaires aux comptes, organismes de gestion agréés, Autorité des marchés financiers (AMF)...

Note : ces experts sont cités à titre d'exemple, le tableau n'ayant en aucun cas la prétention de recenser de manière exhaustive tous les acteurs impliqués dans la veille.

LES PIÈGES À ÉVITER

LES PIÈGES À ÉVITER

1. Ne pas maîtriser l'ensemble des sources et des flux d'informations auxquels votre entreprise a accès

Vous devez avant tout être capable d'identifier et de hiérarchiser vos sources.

2. Penser que, parce vous maîtrisez Google, vous savez faire de la veille

Chercher sur Google, c'est trouver ce que tout le monde trouve, voir ce que tout le monde voit... mais aussi informer Google et vos concurrents sur ce qui vous intéresse !

3. Croire qu'une information gratuite ne coûte rien

Collecter, traiter, analyser, diffuser une information, même gratuite, mobilise du temps, de l'argent et des ressources... et pendant ce temps, vous ne faites pas autre chose !

4. Penser qu'un outil très performant permet de ne pas mobiliser ses collaborateurs

Le meilleur et le plus cher des outils de veille sera toujours moins performant que la personne qui sait qui appeler pour valider une information cruciale. Seul, un outil est sans valeur. Il est uniquement ce que les praticiens de l'IE et de l'entreprise en font.

5. Croire que sur Internet, l'unanimité, c'est la vérité

Internet n'est pas une source d'informations, mais une caisse de résonance pour ceux qui veulent faire du bruit. Face à la surabondance d'informations, aux copier/coller et aux consensus faciles, prenez du recul, mobilisez vos réseaux humains, croisez les informations, capitalisez sur vos relations.

6. Agir au coup par coup

Vous devez nécessairement inscrire votre démarche dans le temps si vous voulez qu'elle soit utile à votre entreprise.

7. Ne pas organiser le stockage des informations

Il est stratégique que vous ayez des bases de données structurées sur les serveurs de l'entreprise.

8. Vouloir tout savoir sur tout

Évitez de définir un spectre de veille trop large ; établissez des priorités et fixez-vous vous des objectifs précis. La veille pour la veille, c'est une perte de temps et d'argent.

9. Limiter l'intelligence économique à la veille

La veille n'est pas une fin, ce n'est qu'une étape. L'IE couvre aussi l'utilisation de ces informations dans une logique d'influence, et elle concerne également la protection d'informations sensibles (le patrimoine informationnel interne de l'entreprise).

10. Espionner son concurrent

L'IE n'est pas une arme contre votre concurrent, mais vous permet de penser comme lui : c'est plus efficace, moins risqué, moins coûteux... et vous évitera de passer par la case prison !

11. Ne pas partager avec les collaborateurs les informations collectées à l'extérieur

Travaillez en réseau et impliquez le plus grand nombre possible de collaborateurs dans cette démarche.

12. Ne pas allouer assez de moyens à la veille

Vous devez allouer des moyens suffisants pour structurer au quotidien le processus de collecte de l'information, classer les sources et valoriser les connaissances.

L'INFLUENCE

DÉFENDRE SES INTÉRÊTS PARTICULIERS, DANS LE RESPECT DE L'INTÉRÊT GÉNÉRAL

DÉFENDRE SES INTÉRÊTS PARTICULIERS, DANS LE RESPECT DE L'INTÉRÊT GÉNÉRAL

Le terme « influence » est souvent galvaudé. Il faut donc revenir aux fondamentaux et rappeler que la notion de légitimité est à la base de toute stratégie d'influence. Avoir de l'influence consiste à amener une personne ou un groupe à changer son point de vue par la persuasion, sans contrainte ni manipulation. L'influence induit un changement des perceptions, puis du comportement.

Très souvent, on associe le terme « influence » à celui de « lobby », qui désigne étymologiquement le lieu où s'expriment les groupes d'intérêts. En Grande-Bretagne, le terme « lobby » désignait, en 1830, les couloirs de la Chambre des communes britannique, où les membres de groupes de pression pouvaient venir discuter avec les membres du Parlement. Aujourd'hui, le terme « lobby » désigne ces groupes eux-mêmes.

L'influence consiste avant tout à utiliser l'information comme un levier d'action, permettant de promouvoir les intérêts de votre entreprise dans un cadre légal, à travers la mise en place d'actions de lobbying et de communication d'influence.

L'influence peut être envisagée comme la modification d'un rapport de force, obtenu par l'emploi délibéré d'informations visant à transformer l'évaluation d'un individu ou d'un groupe d'individus.

- Elle s'appuie directement sur le premier volet de l'intelligence économique : la veille est, en effet, absolument indispensable pour une entreprise qui veut avoir une quelconque influence sur son environnement.
- Elle emploie des techniques qui consistent toutes à **apporter de l'information** à l'individu ou au groupe d'individus qu'elle désire influencer, dans le sens de la **défense des intérêts de l'entreprise**. Les actions d'influence ou de lobbying consistent à injecter de l'information dans le processus de décision d'un individu ou d'un groupe d'individus qui appartiennent à l'environnement de l'entreprise.
- Elle doit être appréhendée à travers une **composante symbolique** (puisqu'elle mobilise les ressorts du faire-croire), une **composante technique** (puisqu'elle passe par des médias et médiations) et, enfin, une **composante stratégique** (puisqu'elle doit servir à la mise en place d'un projet ou à la défense d'intérêts).
- Elle s'appuie largement sur la **notion de réseau** dans la mesure où elle doit s'exercer dans un environnement décroisé pour être efficace.

Qu'il s'agisse d'éviter une décision publique contraignante, d'orienter la rédaction d'une norme, ou de bénéficier de dispositions financières avantageuses, l'intérêt pour une entreprise de mener des actions d'influence paraît évident. Elle dispose pour cela de multiples leviers, qui vont du simple contact avec un élu local, en passant par les associations professionnelles et la presse spécialisée, jusqu'aux actions de lobbying à Bruxelles. Le travail d'influence développe et met en œuvre des argumentaires adaptés pour convaincre, séduire ou dissuader des interlocuteurs ciblés.

Les éléments clés de l'influence sont:

- la **confiance** sans laquelle l'interlocuteur n'est pas réceptif ;
- la **crédibilité** du message ;
- la **puissance de sa diffusion**.

METTRE EN PLACE DES ACTIONS D'INFLUENCE**Repérez les décisions publiques susceptibles d'impacter votre entreprise**

Vous devez avant tout surveiller votre environnement et identifier à l'avance les décisions publiques. Il est essentiel de les repérer le plus tôt possible : plus vous agirez en amont, plus grandes seront vos chances de succès. Connaître les circuits de la décision publique facilitera cette tâche de surveillance. N'hésitez pas à vous faire accompagner par un cabinet spécialisé. Les avocats, de par leur statut, peuvent conduire des actions de lobbying. Ils sont particulièrement familiarisés avec les actions d'influence dont ils savent garantir la légalité.

Une fois repérés les projets publics susceptibles d'impacter votre entreprise, il convient de décider ce que vous souhaitez obtenir par rapport à ces projets et la position que vous allez défendre. L'objectif de vos actions d'influence ne pourra pas systématiquement consister à empêcher la concrétisation des projets : il pourra s'agir de les différer, le temps de vous y préparer, ou d'obtenir des modalités d'application qui en limitent l'impact.

Ciblez vos interlocuteurs

Vos interlocuteurs principaux seront souvent l' élu ou la commission d'élus qui donnera ou non le feu vert au projet. Mais vous pouvez aussi faire valoir vos arguments auprès des autres personnes en charge du dossier : le conseil qui mène l'étude préalable, l'expert ou le consultant dont les avis vont compter... Pour vous aider à repérer les décisionnaires et les services concernés, le recours à certains répertoires d'administrations peut s'avérer très utile :

- *le bottin administratif* : bottin-administratif.fr
 - *le bottin des communes et de l'intercommunalité* : lexisnexis.fr/solutions/inforecherche/Bottin_Communes/index.html
 - *l'annuaire de l'administration* : annuaire.service-public.fr
- Afin d'adapter votre discours à l'interlocuteur que vous aurez repéré, il est nécessaire de le connaître. Pensez à vous procurer sa biographie sur des annuaires ou des guides, comme l'annuaire européen Whoiswho (europa.eu/whoiswho/public) et autres sources en ligne :
- *Societe.com* : societe.com
 - *Wikipedia* : fr.wikipedia.org
 - *123people* : 123people.com
 - *Le Guide du pouvoir* : le.guidedupouvoir.fr

Utilisez différents moyens

- **Les réseaux** : ils favorisent les contacts, disposent de moyens de communication souvent plus variés qu'une seule entreprise et apportent leur légitimité. Le choix du réseau dépend, bien sûr, du pro-

jet sur lequel on cherche à influencer. On peut citer les syndicats professionnels ou fédérations, les clubs, les Chambres de commerce ou de métiers, les pôles de compétitivité, les associations d'anciens élèves... On peut d'ailleurs recourir à plusieurs réseaux, pourvu qu'on ne se disperse pas et que leurs actions se complètent. Bien évidemment, les bénéfices que vous tirerez d'un réseau dépendront de votre implication dans ce réseau. Il ne suffit pas d'arriver en demandeur : il faut aussi se comporter comme une ressource pour les autres membres du réseau.

- **Les manifestations professionnelles** (séminaires, congrès, foires, salons) : elles vous fournissent des occasions pour faire passer vos messages – des contacts avec de nombreux professionnels, des interventions ou des questions lors de conférences, des ateliers thématiques...
- **La presse** : elle vous permet de communiquer vos points de vue (interviews, tribunes, rédaction d'articles), soit auprès du grand public (presse locale ou nationale), soit auprès d'une profession (presse technique et sectorielle).
- **Internet** : le Web offre de nombreux canaux d'expression avec l'avantage d'un coût très faible, d'une large diffusion et d'une grande réactivité : blogs d'entreprises, forums, lettres d'informations électroniques...
- **Les réseaux sociaux** : tels que Twitter, Viadeo, LinkedIn, Facebook, ou encore Google+, facilitent également la construction de communautés d'intérêt autour d'un même thème, sans que leurs membres aient à se rencontrer physiquement.

Faites des alliances

En général, vous n'aurez que peu d'influence si vous restez seul pour faire valoir vos intérêts. Se trouver des alliés qui partagent (au moins en partie) vos intérêts vous rendra plus efficace et vous permettra d'avancer de façon plus discrète. En effet, ce ne sont plus vos seuls intérêts que vous défendrez, et vous pourrez plus aisément convaincre le décideur que les solutions que vous mettez en avant coïncident avec l'intérêt général. Les premiers alliés auxquels vous pouvez penser sont vos partenaires naturels : vos clients, vos fournisseurs, vos partenaires commerciaux. Selon le cas de figure, vous pourrez également vous appuyer sur les entreprises de votre secteur, des *think tanks* ou des associations de consommateurs. Enfin, pensez à recourir à un cabinet conseil en lobbying et affaires publiques, comme à un cabinet d'avocats – dont c'est le métier et qui est en mesure d'approcher les décideurs politiques, y compris au niveau national ou européen.

Adaptez votre comportement à vos interlocuteurs

Pour faire aboutir votre stratégie d'influence, il vous faudra faire preuve de professionnalisme et de persévérance. Le professionnalisme passe par une bonne connaissance de votre dossier, tant sur le plan technique que juridique. Vous devez également connaître les positions des différents acteurs concernés, avoir préparé vos rendez-vous et être très clair et très précis dans vos messages. Avant d'aller défendre votre point de vue auprès d'un élu ou de la personne en charge du dossier, prenez le temps de tester vos arguments en interne avec vos collaborateurs ou auprès des gens qui vous sont proches. Assurez-vous également que les chiffres et les données que vous citerez en appui de votre démonstration sont à jour et incontestables.

L'approche diffère selon que l'on traite avec un élu ou un représentant de l'administration. Dans le premier cas, il faut tenir compte du fait que le temps de l'homme politique est compté et lui fournir un argumentaire prêt à l'emploi, qu'il pourra réutiliser tel quel. Ne vous offusquez pas s'il s'attribue ensuite vos idées et laissez-lui le bénéfice du succès. Avec un fonctionnaire, faites-lui plutôt comprendre que vous connaissez ses contraintes et que vous allez apporter votre contribution à son dossier. Dans tous les cas, soyez clair et transparent dans votre démarche, ne cherchez pas à abuser votre interlocuteur ou à faire pression sur lui, sachez le valoriser.

Inscrivez vos actions d'influence dans la durée

Après un rendez-vous ou une réunion avec un élu ou un représentant de l'administration, un certain suivi s'impose. Si vous lui avez promis de lui fournir un complément d'information ou de mener une démarche supplémentaire, vous devez vous y tenir. Votre comportement professionnel et le respect de vos engagements militeront en votre faveur. Une approche complémentaire, passant par des canaux différents, augmentera vos chances de réussite – même s'il ne faut pas en abuser. Enfin, si la décision qui est prise vous est favorable, n'oubliez pas de remercier et d'exprimer votre reconnaissance aux élus et aux représentants de l'administration qui sont intervenus dans votre dossier.

Soyez prudent lors d'opérations de communication et de négociations

Gardez à l'esprit que tous les efforts que vous avez déployés pour parvenir à influencer sur une décision peuvent être mis à mal par une erreur de communication. Soignez votre communication (site internet, communiqués de presse, supports de communication) et contrôlez bien l'ensemble des informations qui sortent de votre entreprise.

– **La communication interne :** vous devez vous montrer convaincant et transparent dans l'information divulguée en interne, afin de motiver vos collaborateurs et focaliser les énergies vers une stratégie commune, tout en restant prudent sur le contenu : tout ne doit pas être dévoilé car, par imprudence ou par volonté de nuire en interne, des informations confidentielles pourraient être transmises vers l'extérieur.

– **La communication externe :** art sensible et délicat à maîtriser, la communication à destination du public (conférences, interviews, documents écrits ou multimédias, contenu internet) doit être soigneusement préparée, en particulier en identifiant ce qui ne doit pas être divulgué. Une attitude prudente est de mise pour éviter de divulguer une information confidentielle auprès d'experts, de journalistes, ou de personnes malveillantes qui se présentent sous des identités anodines.

Il faut savoir éveiller la curiosité des auditeurs ou des journalistes tout en faisant très attention de ne pas se faire piéger. Pour anticiper les questions délicates, prenez le temps de préparer votre communication en élaborant des éléments de langage adaptés et en essayant d'identifier au préalable les questions pièges afin de proposer des réponses adaptées.

Si c'est un collaborateur qui intervient, le dirigeant de la TPE-PME doit prendre le temps de relire sa présentation.

– **Les négociations :** la protection du contenu des négociations est souvent essentielle pour ne pas divulguer des informations stratégiques.

- Avant le début des négociations – et de tout échange de données confidentielles –, protégez juridiquement, par un accord de confidentialité, le contenu et les modalités des échanges jusqu'à la fin des discussions. La protection ainsi offerte peut paraître simple ; mais il ne faut pas négliger l'effet psychologique associé à une demande qui engage au plus haut niveau la société « adverse » devant une juridiction pénale en cas de manquement caractérisé aux obligations de cet accord.
- Prévoyez les mesures à prendre en cas de rupture de négociations.
- Choisissez avec soin le personnel qui sera impliqué, sensibilisez-le aux risques d'indiscrétions.
- Optez pour des lieux de rencontre neutres et discrets.
- Définissez des règles strictes de télécommunications ou d'échanges de données d'une part, de protection des documents d'autre part.

Surveillez votre e-réputation

Vous devez à tout prix éviter le mauvais buzz, faire face aux critiques et défendre votre image sur Internet et les réseaux sociaux. À la suite du développement de l'Internet participatif, il faut bien avoir en tête que, pour une entreprise et ses dirigeants, la maîtrise de leur réputation numérique doit être une préoccupation majeure. Oui, vous êtes concerné ! Votre entreprise court le risque de voir sa marque associée à des valeurs non souhaitées ou à des comportements répréhensibles. La divulgation d'informations peut desservir les intérêts de vos clients, fournisseurs, distributeurs et autres partenaires commerciaux. Pour anticiper les risques d'atteinte à l'image de votre entreprise, vous devez développer et mettre en œuvre une véritable politique de gestion de votre réputation numérique :

- **protégez** le nom de domaine associé à votre propre nom (prénom-nom.fr et .com et prénomnom.fr et .com mais aussi si possible nom.fr et .com) ;
- protégez les marques et les noms de domaine de votre entreprise. En premier lieu, il faut protéger ses marques en les enregistrant auprès de l'INPI (Institut national de la propriété industrielle), éventuellement sous plusieurs formes (nominative et figurative), et étendre la protection à plusieurs pays, au cas où votre entreprise aurait une activité commerciale à l'international (marque communautaire ou internationale) ;
- **formalisez** une stratégie de communication et de veille de l'e-réputation. Votre entreprise doit communiquer sur sa marque, ses produits et services de manière régulière et adaptée aux nouveaux usages d'Internet, par exemple en animant une communauté d'internautes, en dialoguant avec ses clients via la plate-forme Internet collaborative de la société, ou via une page entreprise sur un réseau social (Facebook, LinkedIn, Viadeo...) ;
- les salariés s'expriment de plus en plus sur Internet à propos de leur employeur ; **sensibilisez** les salariés de votre entreprise à la question de l'« e-réputation » :
 - mise en place d'une charte Internet complète et à jour,
 - proposition de formations sur les bonnes pratiques d'utilisation des outils de communication électronique (e-mail, blogs, réseaux sociaux...), ainsi que sur l'exercice de la liberté d'expression et ses limites.

LES PIÈGES À ÉVITER

1. Voir la compétition économique comme un sport individuel

Penser l'entreprise comme un système fermé et analyser ses problèmes par rapport à sa structure interne, sans prendre en compte la globalité de son environnement, est voué à l'échec. Il faut jouer collectif, en interne et en externe.

2. Croire que tous les coups sont permis

L'intelligence économique obéit à des règles et à une éthique.

3. Penser qu'on est plus influent en multipliant les contacts

500 amis, 10 000 contacts, une présence sur tous les réseaux sociaux ne font pas un réseau... mais sont autant d'occasions de divulguer une information ou de perdre le contrôle de votre réputation.

4. Miser sur le héros solitaire ou l'homme providentiel

Ceux qui mettent en place dans l'entreprise la démarche d'intelligence économique ne doivent pas agir seuls mais en réseau. Sensibilisez vos équipes sur le fait que l'IE va permettre à votre entreprise d'obtenir un avantage concurrentiel tout en protégeant ses savoirs. Tout comme les crises, les besoins d'informations critiques peuvent survenir à tout moment. L'intelligence économique se fait donc au quotidien, en mobilisant d'une part l'ensemble de l'organisation et, d'autre part, ses réseaux relationnels extérieurs (dans les organisations professionnelles, dans les organismes de normalisation...).

5. Croire que l'IE vous rendra plus intelligent...

La vocation de l'IE consiste à diminuer l'incertitude et à augmenter votre capacité d'adaptation, ce qui contribuera à vous rendre plus influent. Ce qui est déjà beaucoup !

NORMALISATION INTERNATIONALE ET STRATÉGIE D'INFLUENCE

Aujourd'hui, plus de 80 % des normes concernant des entreprises françaises sont décidées au sein d'enceintes internationales. Les normes européennes ou internationales sont un enjeu de plus en plus important pour la compétitivité des entreprises et le développement de leurs marchés à l'export. Ainsi, selon l'AFNOR (dont la fonction est précisément de représenter les intérêts français dans les instances européennes et internationales d'élaboration et de diffusion des normes), la normalisation contribue directement à la croissance des économies dans des pourcentages de l'ordre de 0,8 %.

Cet axe de développement des entreprises, a priori très technique, est donc fondamental. Il permet à l'industrie et aux services innovants de maintenir ou de gagner des avantages concurrentiels dans la compétition internationale. Outre les avantages évidents liés au respect des normes (réduction des risques juridiques, confiance du client, accès à davantage de marchés), la normalisation est une véritable arme économique : participer à l'élaboration de la norme permet de ne plus la subir, mais de l'anticiper ! Une participation aux comités de normalisation permet aux entreprises impliquées de repérer les nouvelles technologies innovantes, de détecter, voire d'orienter

les nouvelles exigences du marché dans tel ou tel secteur, ce qui génère un avantage compétitif indéniable. Si les processus de préparation des normes sont ouverts, ils peuvent constituer un instrument redoutable au profit d'entreprises leaders sur un marché, tentées de préserver leur avance en freinant certains travaux ou, au contraire, de jouer de leur influence pour y intégrer des éléments favorables à leurs intérêts.

Pour être autorisé à commercialiser un produit sur un marché, il est nécessaire que ce dernier réponde aux normes en vigueur dans le pays. Dans ce cadre, les entreprises ont tout intérêt à mener directement ou indirectement, seules ou le plus souvent dans le cadre d'un réseau professionnel ou de groupements d'entreprises, des actions d'influence auprès des organismes de normalisation.

Plusieurs exemples récents de standards montrent à quel point la politique d'influence et l'intelligence économique peuvent constituer un élément crucial en faveur des normes qu'il s'agit de promouvoir. Ainsi, le succès de la norme européenne GSM illustre une politique française d'influence réussie grâce à l'unité et la coordination des entreprises françaises. Il en est de même en matière de systèmes antifoudre : l'action d'influence menée par une PME française porteuse d'une technologie de rupture a permis de contrer l'offensive de gros acteurs étrangers du secteur, qui visait à bloquer l'adoption de normes validant cette technologie.

À l'inverse, certains échecs rencontrés par le passé stigmatisent les types de comportements à prévenir et à corriger : le manque de réactivité, l'absence de participation aux enceintes informelles, les profils inadaptés d'experts participant aux groupes de travail et l'absence de circulation de l'information au bénéfice des utilisateurs et des entreprises concernées en France.

Ces expériences démontrent la nécessité d'une action volontariste et soutenue pour renforcer les conditions d'une réelle stratégie d'influence française dans les enceintes de normalisation. En la matière, l'État contribue à l'accompagnement des entreprises, notamment via des aides au financement (crédit impôt normalisation, programme de soutien du ministère de l'Économie à la participation de certains groupements de PME à des travaux européens ou internationaux de normalisation).

LA SÉCURITÉ ÉCONOMIQUE

EN QUOI LES ENTREPRISES SONT-ELLES DIRECTEMENT CONCERNÉES ?

Les entreprises et les établissements de recherche français exercent leurs activités dans le cadre d'une économie mondialisée, ouverte, dont l'intensité concurrentielle est croissante et qui compte, avec les pays émergents, de nouveaux acteurs puissants. Cette ouverture et cette concurrence sont porteuses de croissance, et donc positives pour l'économie française : de nombreuses entreprises françaises sont, en effet, leaders européens ou mondiaux dans leurs secteurs, se développent et réalisent des acquisitions hors de France. Pour autant, cette ouverture nécessaire comporte un certain nombre de risques pour les entreprises, les établissements de recherche et globalement pour l'économie française. Il est donc indispensable d'identifier et de prévenir ces menaces. La sécurité économique vise avant tout trois objectifs :

- **l'identification et l'analyse des menaces** dont les entreprises françaises sont la cible ;
- **la protection des entreprises et des établissements de recherche**, quels que soient leur taille ou le secteur d'activité dans lequel ils évoluent. En effet, toute entreprise est susceptible de faire l'objet d'attaques, à partir du moment où elle est innovante et évolue dans un secteur concurrentiel. Il en va de même pour les établissements de recherche ;
- **la diffusion d'une culture de la sécurité du patrimoine matériel et immatériel** au sein de l'ensemble des entreprises, grands groupes comme PME, et des établissements de recherche.

Pour la PME, la sécurité économique recouvre des réalités très variées, souvent complexes et imbriquées. Il est clair qu'en ce domaine il n'existe pas de risque zéro : tout l'enjeu pour l'entreprise est donc de réduire les risques à un niveau de vigilance qui n'entrave pas son fonctionnement.

La première étape consiste à repérer les informations stratégiques de l'entreprise ainsi que les risques associés. Il faut donc :

- faire l'inventaire de toutes ses informations sensibles ou confidentielles (plan stratégique, études de concurrence, fichiers clients et prospects, liste des fournisseurs, contrats, données comptables, paie, dossiers du personnel, organigramme détaillé de l'entreprise, inventions brevetables, plans, procédés de fabrication, concepts innovants, créations, codes sources...);
- recenser les supports sur lesquels reposent les informations de l'entreprise (ordinateurs fixes et portables, accès à Internet, messageries électroniques, logiciels, clefs USB, WiFi, Bluetooth, téléphones fixes et portables, télécopieurs, photocopieurs, armoires et locaux d'archivage...).

Il faut aussi prendre conscience des menaces qui pèsent sur votre entreprise : vols d'informations, de savoir-faire et de secrets de fabrication, contrefaçons et atteintes à la propriété intellectuelle, pertes de données après un sinistre ou une erreur de manipulation, intrusions dans le système informatique, mises hors service des ressources informatiques, débauchage de salariés, risque financier par prise de capitaux extérieurs, mises en cause au plan légal et actions de justice, atteintes à l'image de marque et à la réputation. Toutes les entreprises sont concernées, il ne faut pas se croire à l'abri sous prétexte qu'on est une TPE-PME ou que son secteur est peu concurrentiel. Ainsi, le chef d'entreprise et ses collaborateurs seront-ils en mesure d'adopter et d'adapter au quotidien des règles de conduite simples.

Par-delà les bonnes pratiques, relativement faciles à mettre en place, il est possible de **bâtir une politique de sécurité globale**, qui prendra en compte les étapes du cycle de vie de l'information (acquisition, création, communication, stockage, mise à jour, destruction) et qui couvrira des aspects variés :

- **nomination d'un responsable sécurité** et identification des responsabilités dans l'entreprise ;
- **qualification des informations** en fonction de leur niveau de sensibilité (ouvertes, restreintes, confidentielles, etc.) ;
- **consultation d'un avocat** pour organiser sa propriété intellectuelle et pour rédiger les clauses contractuelles indispensables (en particulier les clauses de confidentialité dans les contrats de travail et de prestation de services) ;
- **définition des règles d'accès** aux bâtiments, aux outils informatiques, à Internet... ;
- **rédaction et diffusion de procédures de sécurité** à appliquer au quotidien ;
- **rédaction et diffusion d'une charte** précisant les usages autorisés des équipements informatiques ainsi que des supports de communication ;
- **gestion des risques** et politique d'assurances ;
- **organisation d'une cellule de crise et d'un plan de continuité d'activité.**

Bien sûr, le chef d'entreprise veillera à adapter cette politique à la taille de son entreprise et à sa situation, et à ne protéger que ce qui doit l'être : il ne s'agit pas de tout verrouiller, mais d'être vigilant sur l'essentiel ! Il veillera particulièrement au facteur humain : en effet, il est essentiel d'obtenir l'appui de l'ensemble des collaborateurs à travers des actions de sensibilisation et de formation. Enfin, cette politique de sécurité devra impérativement s'inscrire dans le temps, malgré les changements de personnes, d'équipements ou d'organisation.

LE CONCEPT DE SÉCURITÉ ÉCONOMIQUE EN CINQ POINTS

Assurer la sécurité économique des entreprises est une nécessité absolue afin de préserver leur compétitivité dans un contexte très concurrentiel.

1. **Toutes les entreprises possèdent des informations importantes et un savoir-faire** qui doivent être protégés d'une manière ou d'une autre : procédés, objets, documents, données ou fichiers de nature commerciale, industrielle, financière, scientifique, technique ou stratégique, sans caractère public. La perte ou la divulgation de ces informations peuvent être lourdes de conséquences, notamment en termes d'image, de chiffre d'affaires ou de parts de marché.
2. Les protections relèvent à la fois de la **stratégie juridique** (dépôts de brevets, protection des marques et des modèles, preuves des créations protégées par le droit d'auteur, contrats, etc.) et de la **sûreté** (mesures de protection du savoir stratégique à travers les systèmes d'information, sensibilisation des personnels de l'entreprise). Les entreprises ont également l'obligation légale de protéger leur personnel ainsi que leur lieu d'implantation et de veiller à ce que les informations les concernant soient sécurisés.
3. Avec le développement du commerce électronique et l'**utilisation croissante d'Internet**, de plus en plus d'informations sont partagées par les partenaires commerciaux, et stockées partout dans le monde sur des serveurs (cloud computing, etc.) qui peuvent s'avérer vulnérables. Il existe un risque de sabotage, d'altération, d'effacement ou de fraude.

4. La question du **transfert des technologies** revêt une importance capitale : consenti et maîtrisé, il ne pose pas de problème et doit faire l'objet d'un contrat qui en fixe les limites ; en revanche, en cas de captation technologique issue de méthodes indécrites, il peut se révéler catastrophique pour une entreprise dont le développement repose avant tout sur sa créativité et sur son potentiel de recherche et développement. En tout état de cause, tant que la créativité et l'innovation n'ont pas été protégées par des brevets ou des dépôts de marque, l'entreprise doit mettre en place des **procédures de confidentialité**.
5. Protéger est un réflexe qui s'apprend.

MENACES : DES CAS RÉELS

Chaque année, près de 1 000 atteintes économiques sont recensées par les services de l'État en charge de la sécurité des entreprises (Direction centrale du renseignement intérieur, Gendarmerie nationale et Direction de la protection et de la sécurité de la défense nationale). Ces atteintes économiques visent à capter tout ou partie du patrimoine économique et scientifique d'une entreprise et/ou à endommager, saboter, voire détruire ce patrimoine. Si le piratage informatique en est la forme la plus connue, ces attaques peuvent être extrêmement variées.

Atteintes financières

La manière la plus simple de capter le savoir-faire d'un concurrent, voire de l'éliminer, est bien souvent de le racheter. Certains acteurs peu scrupuleux s'affranchissent parfois des règles du marché pour racheter sous la contrainte.

➤ **Chantage à l'approvisionnement** : une PME a développé une technologie innovante dans le domaine du traitement de surfaces. Elle s'est efforcée de protéger au mieux ses innovations : elle a déposé plusieurs brevets, elle a imposé à tous les collaborateurs le respect d'une clause de confidentialité. Et pourtant, cette PME a fait l'objet d'une manœuvre offensive de la part de son principal concurrent étranger : dans un premier temps, il a fait racheter par une de ses filiales le principal fournisseur d'un produit indispensable à la PME ; dans un second temps, il a menacé la PME de ne plus lui livrer le matériel indispensable à la mise en œuvre de sa technologie, à moins que la PME ne lui cède 51 % de son capital... ! Il a fallu l'intervention des pouvoirs publics pour que la situation soit réglée.

Intrusions consenties

Un nombre très important d'atteintes économiques sont le fait de personnes extérieures à l'entreprise, mais qui ont obtenu l'autorisation d'y pénétrer (stagiaires, auditeurs, délégations étrangères...).

➤ **Comportement intrusif d'une délégation étrangère** : un grand groupe étranger a envoyé une délégation visiter l'atelier de production d'une PME de la région Rhône-Alpes. Alors qu'ils n'avaient au préalable sollicité aucune autorisation de la part de l'entreprise, les visiteurs ont sorti des appareils photos et pris de nombreux clichés, notamment de la chaîne de fabrication... !

➤ **Questionnaire ouvertement intrusif d'un stagiaire** : un stagiaire d'une école de commerce a adressé un questionnaire particulièrement indiscret à

plus de cinq cents professionnels d'un secteur technologique, dans le cadre de son stage de recherche post-doctorat. Il s'est abstenu de soumettre à son directeur de laboratoire le questionnaire avant diffusion. Or certaines questions étaient ouvertement intrusives (montant du pourcentage de R&D investi dans le total des ventes de l'entreprise au cours des trois dernières années, part des revenus tirés des licences et des brevets, etc.). Il est rare que les atteintes au secret des affaires soient menées de manière aussi frontale et en direction d'un public aussi large, mais cela peut arriver.

MENACES : DES CAS RÉELS

➤ **Appropriation de travaux de recherche par un jeune doctorant étranger :**

un doctorant a effectué un stage pratique dans un laboratoire public du Gard. Après avoir sollicité l'obtention d'informations scientifiques complémentaires, il a rédigé un article pour un journal scientifique étranger, décrivant les chercheurs français comme de simples collaborateurs.

➤ **Communication des résultats de thèse d'un étudiant étranger avant soutenance :**

un étudiant en troisième année de thèse au sein d'un laboratoire public de recherche de Midi-Pyrénées a présenté ses travaux à l'association des scientifiques et ingénieurs de son pays en France sans accord préalable de son laboratoire français.

➤ **Captation d'information stratégique via un simple appel téléphonique :**

le concurrent d'une PME française est parvenu à obtenir des informations stratégiques (molécule utilisée dans un médicament), au « bluff », en passant plusieurs appels téléphoniques à divers interlocuteurs au sein du laboratoire. Il a obtenu l'information en une demi-journée.

➤ **Audit intrusif sur des informations techniques concernant des matériels destinés à un pays tiers :**

au cours d'un audit sur une entreprise de Bourgogne, un responsable étranger est venu observer la production du site dans le cadre d'une vente au profit du groupe étranger. Il a été surpris en train de recopier indûment des informations techniques relatives à un produit destiné à un pays tiers.

➤ **Audit intrusif sous couvert d'un audit financier :**

sous couvert d'un audit financier, une société a cherché à capter les informations stratégiques d'une PME française. Prétextant attendre de cette PME qu'elle justifie le prix de vente de ses produits par un détail précis des coûts de production, un de ses clients étrangers a souhaité envoyer sur le site de l'usine des « auditeurs qualifiés » afin d'examiner tous les coûts de production... !

➤ **Tentative de captation d'informations stratégiques par un cabinet étranger de conseil en investissements :**

un cabinet spécialisé dans le conseil en développement industriel auprès des entreprises et des investisseurs cible des sociétés innovantes en pleine phase de croissance, évoluant dans des secteurs stratégiques. Ce cabinet a une réputation internationale dans le domaine des études de marché. Afin d'évaluer les potentialités de marchés, il adresse des questionnaires très précis concernant les conclusions que les entreprises françaises tirent de leurs travaux, leurs applications futures, leur analyse du marché actuel ainsi que leurs attentes.

➤ **Mise en ligne d'informations confidentielles sur un blog :**

l'informaticien d'une PME avait décidé de tenir un journal professionnel qu'il avait mis en ligne sur son blog. Son site personnel dévoilait ainsi une véritable chronique de la vie de son entreprise. Un informaticien d'une entreprise concurrente, fin psychologue, a procédé à une opération d'approche de

l'auteur du blog. En usant de flatterie, il a réussi peu à peu à créer un lien régulier au point de soutirer insidieusement des informations techniques, à tel point que l'auteur du blog finit par divulguer des informations qui devaient logiquement rester confidentielles...

> **Mise en ligne sur Internet de rapports de stage contenant des informations sensibles :** plusieurs sites internet proposent, moyennant un prix modique, un accès en ligne à divers rapports de stage réalisés par des étudiants accueillis dans des entreprises. On trouve sur ces sites des rapports qui portent sur la conception et la réalisation de la carte électronique d'un dispositif aéronautique sensible, la création de pages web sur l'espace Intranet « sécurité » d'un major énergétique français !

> **Divulgaration d'informations stratégiques lors de l'utilisation d'un traducteur en ligne :** des informations stratégiques pour une PME ont été divulguées lorsqu'un collaborateur de l'entreprise a copié-collé des textes sensibles dans un traducteur en ligne. Ces informations ont alors été captées par des tiers, concurrents de l'entreprise. Le collaborateur n'avait pas à l'esprit le fait que tout ce qui passe sur Internet peut être lu !

Atteintes au savoir-faire

> **Dépôt de brevet à l'international similaire à des travaux français :** quatre partenaires académiques et un industriel français collaborent dans un programme de recherche international basé en France. Les chercheurs français découvrent qu'une équipe étrangère associée à un de leurs partenaires a déposé deux brevets présentant de fortes similitudes avec leurs propres travaux. Si l'action visant à invalider les deux brevets étrangers n'avait pas été menée, les scientifiques français se trouveraient contraints d'acquiescer des licences d'exploitation étrangères afin d'utiliser un procédé de fabrication qu'ils ont eux-mêmes conçu !

> **Résultats de recherche d'une PME française brevetés à l'étranger par un post-doctorant :** le centre de recherche d'une PME française a accueilli un médecin étranger dans le cadre de sa thèse et de son post-doctorat. Un premier brevet, limité aux essais en laboratoire, a été déposé par la PME, mentionnant ce chercheur en tant que co-inventeur. Dès son retour dans son pays, ce dernier a fait breveter les applications thérapeutiques, prenant ainsi de vitesse la PME française et empêchant toute extension internationale du brevet français initial. La poursuite des travaux scientifiques de l'équipe française est aujourd'hui conditionnée au bon vouloir de son ancien thésard, qui est juridiquement propriétaire des potentialités thérapeutiques de l'invention de la PME française... !

> **Livraison d'informations à une entreprise étrangère :** un membre d'un centre de recherche public alsacien a mené en parallèle des travaux de recherche pour une société étrangère. Ce groupe étranger a déposé deux demandes internationales de brevet au sujet de ces recherches, mentionnant le nom de ce chercheur, mais pas les structures françaises de recherche auxquelles il appartenait.

> **Transfert massif de données à l'étranger :** un post-doctorant étranger, travaillant dans une unité de recherche mixte, a transféré pendant 3 ans par e-mail l'ensemble des données relatives aux travaux du centre vers son université d'origine, en dehors de tout cadre de coopération. Le centre de recherche devra procéder à une indispensable veille pour revendiquer la paternité des travaux de ses laboratoires si des brevets venaient à être déposés par l'université d'origine du doctorant.

➤ **Concurrence d'un actionnaire avec une de ses participations:** une grande entreprise étrangère, actionnaire et fournisseur d'une entreprise d'Isère, a obtenu des renseignements techniques lors de réunions de travail. La société française a constaté la présence sur le marché de deux produits de la marque étrangère, concurrençant directement les siens et basés sur la même technologie. La société étrangère a contraint l'entreprise française à entamer une phase de négociations afin de la forcer à racheter les concepts!

Intrusions informatiques

➤ **Attaque du système informatique d'une TPE par un virus:** l'informaticien d'une TPE était très fier de son parc informatique. Seul imprévu de taille : l'intrusion d'un virus via Internet. Un mail anodin, une fois ouvert, libéra le virus qui contamina tout le système informatique de la TPE au point de le rendre inopérant : plus aucune démarche ne pouvait être effectuée, les postes informatiques étaient inutilisables. Par souci d'économie, l'informaticien n'avait pas cru bon de renouveler les mises à jour des antivirus – il regretta amèrement son choix. En effet, cela entraîna des coûts d'immobilisation pour l'entreprise, ce à quoi s'ajoutèrent les coûts de restauration des systèmes et de récupération des données. Au final, l'entreprise dut payer une lourde facture pour remettre en service son informatique, sans compter les pertes commerciales provoquées par l'interruption de la gestion des commandes...

➤ **Cybersquatting par un concurrent européen:** une entreprise de Haute-Marne a constaté le détournement des noms de domaines en .eu du site internet de sa société. Les internautes étaient automatiquement redirigés vers le site internet d'un concurrent direct étranger. L'entreprise française a dû faire assigner la société étrangère devant le tribunal de commerce local pour concurrence déloyale.

➤ **Attaques massives du réseau informatique d'une entreprise:** une société rhodanienne, retenue par une entreprise étrangère au terme d'une mise en concurrence internationale, devait transmettre gracieusement ses procédés de fabrication pour pouvoir signer le contrat commercial. À la suite de son refus d'obtempérer, son réseau informatique a subi plus de 20 000 attaques!

➤ **Vol de données numériques sensibles à l'étranger:** le directeur scientifique d'une PME française a été invité à visiter une nouvelle structure de recherche à l'étranger. Avant de pénétrer dans le laboratoire, il a été contraint de déposer, dans une salle de réunion sans surveillance, son ordinateur portable. Ce dernier contenait des données hautement stratégiques et a manifestement subi une intrusion...

➤ **Attaque du réseau informatique d'une entreprise par un ancien employé:** une entreprise française a licencié son ingénieur système et administrateur du réseau. À peine un mois plus tard, elle a subi une série d'attaques informatiques nocturnes aux conséquences majeures. Pendant deux semaines, l'entreprise a subi un déficit d'image, ne pouvant plus communiquer que par téléphone ou par fax avec ses partenaires. Les dirigeants ont très rapidement fait appel aux services d'un cabinet de sécurité informatique pour identifier l'auteur des faits. Il s'agissait bien de l'ancien cadre licencié, qui s'était connecté sur le réseau local de l'entreprise, muni de droits d'accès empruntés à un collègue et en utilisant une connexion accessible depuis un point d'accès asiatique.

> **Interception des communications d'un dirigeant de PME:** le dirigeant d'une PME innovante avait fait réparer son téléphone portable. Deux mois après, il a eu des doutes sur la confidentialité de ses conversations téléphoniques. Autre fait surprenant, la batterie de son téléphone se déchargeait particulièrement vite, ce qui peut s'expliquer par une mise sur écoute. En apportant son téléphone chez son opérateur, on lui annonça que lors de la réparation de son téléphone, un espion informatique avait été introduit.

Atteintes physiques sur sites

> **Sécurité physique d'un site négligée:** une société classée Établissement à régime restrictif (ERR) en raison de la sensibilité d'une partie de sa production a réduit ses coûts de fonctionnement dans le domaine de sa sécurité physique. Le niveau global de sécurité de l'entreprise a naturellement été impacté par une telle décision, ce qui a largement facilité la réalisation d'un vol. Les conditions de réalisation de ce vol rappellent que les dépenses de sécurité doivent être considérées non comme une charge, mais comme un investissement au service de la pérennité de l'entreprise.

Désorganisation et fragilisation

> **Méthodes de veille technologique déloyales:** une PME d'Île-de-France a fait l'objet d'une procédure contentieuse initiée par un concurrent étranger qui s'est dit victime de contrefaçons. Un huissier, accompagné de deux membres d'un cabinet de conseil en propriété intellectuelle, a souhaité procéder à une saisie des « supposées contrefaçons » dans l'entreprise française, afin de contraindre cette dernière à dévoiler les détails de ce qui constitue son avance technologique...!

> **Imposition de clauses intrusives à un distributeur français:** une société alsacienne est mandataire exclusif d'un groupe étranger pour plusieurs pays d'Europe. Elle s'est vue proposer un nouveau contrat commercial, rédigé en anglais et non régi par les lois françaises, dont une clause particulièrement intrusive mentionnait un accès total et permanent aux comptes détaillés de l'entreprise française. Réalisant près de 70 % de son activité grâce au partenariat exclusif qu'elle entretient avec ce groupe étranger, la société française n'a eu d'autre choix que de signer ce nouveau contrat!

> **Contrefaçon d'innovations par un partenaire commercial:** réalisant 90 % de son chiffre d'affaires à l'international, une société française du Finistère a développé un partenariat commercial avec une société étrangère. La société bretonne a constaté quelque temps après que son partenaire vendait des machines en tous points identiques aux siennes. Cela s'est produit dès lors que le prototype de l'application contrefaite a été fabriqué dans un pays tiers, sans aucune forme de protection juridique de la propriété intellectuelle. La société a imaginé que ses quelques rivaux étaient dignes de confiance...!

Atteintes à la réputation

> **Campagne calomnieuse à l'encontre du produit d'un concurrent:** une société étrangère, concurrente d'un petit laboratoire pharmaceutique français, a mandaté un cabinet peu scrupuleux pour mener une véritable campagne de désinformation sur un produit fabriqué par le laboratoire.

Pour réaliser sa mission, le cabinet avait élaboré un faux rapport d'étude d'infectiologie, prétendument scientifique, portant sur ledit produit et l'avait largement diffusé auprès des acteurs du marché concerné (cliniques, hôpitaux et personnel scientifique). En outre, la rumeur a été abondamment relayée et alimentée sur Internet. L'affaire s'est bien terminée, puisque le laboratoire français a racheté son concurrent et fait condamner au pénal les auteurs du pseudo-rapport pour faux et usage de faux.

Risques liés à des personnes clefs

> **Débauchage massif de cadres par un concurrent étranger:** une société étrangère souhaitait acquérir une PME du sud de la France. Les actionnaires ont suggéré de procéder à un audit. Quelques semaines plus tard, quatre cadres ont été débauchés par le concurrent étranger et ils lui ont apporté des informations stratégiques (fichiers clients, stratégie tarifaire, innovations...).

> **Débauchage d'un ancien salarié par un concurrent:** une PME leader mondial dans son secteur a vu l'un de ses anciens salariés, parti à la retraite, être embauché comme consultant par son principal concurrent. Le concurrent a pu obtenir des informations stratégiques (nom du fournisseur exclusif, lieu de fabrication de la matière première nécessaire...).

À QUELS SERVICES DE L'ÉTAT S'ADRESSER EN CAS DE PROBLÈME ?

Les entreprises victimes d'agressions économiques doivent avertir au plus tôt les services compétents de l'État, afin que ceux-ci puissent les soutenir de la manière la plus efficace possible. En dehors de toute agression, ces services peuvent également vous conseiller sur les bonnes pratiques à mettre en œuvre et réaliser un audit au sein de votre entreprise.

Gendarmerie nationale

- Vous êtes victime d'un vol, d'une extorsion.
- Vous vous sentez exposé, vulnérable.

Direction centrale du renseignement intérieur (DCRI)

- Vous souhaitez être sensibilisé à la protection de vos informations et savoir-faire.
- Vous pensez être la cible d'ingérences étrangères.
- Vous êtes confronté à une menace spécifique (atteinte à la réputation...).

Direction de la protection et de la sécurité de la défense (DPSP) pour les entreprises de ce secteur

- Vous devez élaborer des mesures de protection de vos installations.

- Vous désirez une sensibilisation ou un soutien en matière de protection du patrimoine industriel.

L'agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de sécurité des systèmes d'information. Elle informe régulièrement le public sur les menaces, notamment via ses sites internet.

Les observatoires zonaux de la SSI (OZSSI) sont les interlocuteurs locaux des entreprises en la matière. Ils favorisent les échanges entre les acteurs locaux et peuvent si besoin faire remonter des informations à l'ANSSI.

LES PIÈGES À ÉVITER

SÉCURITÉ ÉCONOMIQUE : LA DCRI ET LA GENDARMERIE NATIONALE PEUVENT VOUS AIDER À DÉTECTER VOS VULNÉRABILITÉS

La DCRI est fortement impliquée dans la prévention des ingérences à l'encontre des institutions et des entreprises qui constituent le tissu économique national. À ce titre, elle dispose d'une forte expertise dans le domaine de la protection physique et économique des entreprises, historiquement liée à sa mission réglementaire de protection des locaux abritants des secrets de la Défense nationale.

Cette compétence s'est étendue à un rôle d'audit et de conseil proposés aux sociétés soucieuses de protéger leur patrimoine économique et de préserver leur compétitivité. Sur sollicitation, des intervenants experts se déplacent dans les entreprises, de la PMI jusqu'aux grands groupes du CAC40, identifiées comme exposées à des risques objectifs d'atteinte. Ils évaluent les vulnérabilités des sites. Clôtures, portails, portes, serrures, coffres-forts, contrôle d'accès, détection alarme, vidéosurveillance, organisation et procédures de sûreté : les spécialistes de la DCRI proposent des solutions pragmatiques et adaptées aux chefs d'entreprise.

La Gendarmerie nationale, présente sur l'ensemble du territoire national, peut également apporter son expertise aux entreprises en matière de sécurité économique par le biais de « diagnostics de vulnérabilité ». Ces bilans permettent aux entreprises d'être sensibilisées sur les éventuelles défaillances pouvant survenir au sein de leurs structures. Les audits de la DCRI et les diagnostics de vulnérabilité de la Gendarmerie nationale sont réalisés sans contrepartie financière.

LES PIÈGES À ÉVITER

1. Se rendre à l'étranger avec des informations confidentielles dans son ordinateur. Si votre ordinateur est saisi durant un passage à la douane d'un pays, puis vous est rendu dans les cinq minutes, il peut avoir été copié de fond en comble.

2. Laisser dans sa chambre d'hôtel des informations confidentielles. Il est possible que la chambre, bagages et coffre-fort compris, soit « visitée » en votre absence.

3. Parler de vos projets en cours lors d'un entretien d'embauche. Certaines entreprises rédigent des actions sur mesure et font passer de faux entretiens uniquement pour obtenir de l'information.

4. Laisser des documents sur une imprimante ou un photocopieur partagés. Vous devez toujours penser à reprendre l'ensemble des documents, originaux ou copies, quitte à en détruire certains plus tard.

5. Parler de son entreprise et des projets dont on a la charge en dehors de l'entreprise. Vous devez absolument éviter de parler de votre entreprise à l'extérieur, notamment lors des pauses cigarettes, durant un *afterwork*, au restaurant ou dans un train : autant de lieux où il est très facile pour des concurrents d'ouvrir grand leurs oreilles.

6. Ne pas connaître précisément les collaborateurs qui ont les droits d'accès à la messagerie du dirigeant de l'entreprise. Les accès messageries doivent faire l'objet d'une surveillance régulière.

7. Penser qu'une intrusion dans le système informatique d'une entreprise n'arrive qu'aux autres et qu'il n'est donc pas forcément utile de s'y préparer. Une intrusion d'ampleur dans un système d'information est une crise. Chaque heure qui passe peut notamment signifier la fuite d'informations confidentielles avec, dans certains cas, leur publication à des fins de déstabilisation. Des risques de suspension de l'activité de l'entreprise sont aussi à prévoir. Un plan de réponse spécifique doit donc exister.

8. En cas d'intrusion sur un poste informatique, ne faire vérifier que le poste concerné. La recherche d'éventuelles autres traces d'intrusion sur votre système informatique est indispensable après la découverte d'une intrusion. Généralement, les attaquants s'ouvrent de multiples portes d'entrées dans le système.

9. Vérifier la taille des fichiers qui sortent du système d'information de l'entreprise, les jours et les horaires de sortie, les destinataires. L'analyse des journaux d'événements permet de repérer les activités inhabituelles et de détecter d'éventuels signes d'intrusion. Les journaux d'événements doivent être activés, configurés et centralisés pour permettre cette analyse.

10. Cliquer de manière automatique sur des liens placés dans les e-mails que vous recevez. Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur.

11. Ouvrir mécaniquement les pièces jointes dans les e-mails que vous recevez. Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux e-mails. Pour vous protéger, n'ouvrez jamais les pièces jointes dont les extensions sont les suivantes : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk. À l'inverse, quand vous envoyez des fichiers en pièces jointes, privilégiez le format le plus « inerte » possible, comme RTF ou PDF. Cela limite les risques de fuites d'informations.

12. Ouvrir les e-mails non sollicités ou d'origine inconnue. Même si l'objet ou la pièce jointe semble intéressant, méfiez-vous de toute pièce jointe à un courriel non sollicité. Désactivez les fonctions de script (par exemple JavaScript, ActiveX...) dans les programmes de messagerie électronique tels qu'Outlook.

13. Répondre à des inconnus sur Internet. Vous ne devez pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans un mail et encore moins répondre à un inconnu sans un minimum de précaution. Si un doute subsiste sur un message, prenez le temps de le confirmer en téléphonant à l'expéditeur.

- QUESTIONNAIRES

FAITES VOTRE AUTODIAGNOSTIC

La veille

Faites votre autodiagnostic en ligne sur experts-comptables.fr espace « Développement économique », rubrique « Intelligence économique ».

Suivez-vous régulièrement :

1 L'environnement économique du secteur d'activité de votre entreprise ?	Oui	Non
2 La législation et la réglementation s'appliquant à l'entreprise ?	Oui	Non
3 Les tendances et les évolutions prévisibles du marché ?	Oui	Non
4 L'évolution prévisible du coût de vos matières premières ?	Oui	Non
5 L'évolution des besoins et des attentes de vos clients ?	Oui	Non
6 Vos concurrents (nouveaux produits, projet de délocalisation, croissance externe) ?	Oui	Non
7 Vos fournisseurs (santé financière, principaux clients) ?	Oui	Non
8 L'image de votre entreprise (dans la presse –y compris à l'international –, sur Internet : réseaux sociaux, forums, blogs...)?	Oui	Non
9 L'action des associations, des « think tanks », des ONG s'intéressant à votre secteur d'activité ou à votre entreprise ?	Oui	Non
10 Avez-vous recensé les sources d'informations internes et savez-vous les valoriser et les exploiter (savoir-faire du personnel, rapports du service après vente, rapport d'étonnement concurrentiel) ?	Oui	Non
11 Avez-vous mis en place un dispositif de collecte de l'information (Internet, abonnement à des bases de données, réseaux humains) ou vous appuyez-vous sur des prestataires extérieurs (recherche de données, réalisation d'études...)?	Oui	Non
12 Développez-vous des partenariats avec des entreprises proches géographique-ment et/ou en termes de secteur d'activité (échange d'informations, participation collective à des salons) ?	Oui	Non
13 Avez-vous identifié les opportunités de développement à l'international pour votre entreprise ?	Oui	Non
14 Bénéficiez-vous d'un accompagnement à l'international (réseau des CCI, Ubi-france, conseillers du commerce extérieur de la France, agences de développement régional) ?	Oui	Non
15 Avez-vous une politique active dans les domaines technologiques et de la propriété industrielle (veille et recherche sur les bases de données de brevets, évaluation des risques de contrefaçons) ?	Oui	Non

Résultats sur 15

Moins de 7 « oui » : une action de veille vous donnerait un avantage concurrentiel.

De 7 à 12 : les efforts que vous effectuerez dans ce domaine permettront une meilleure réactivité de votre entreprise.

Plus de 12 : la veille que vous avez mise en place dans l'entreprise, bien que perfectible, est de bonne qualité.

Quel que soit votre résultat, n'hésitez pas à contacter votre expert-comptable. Grâce à l'outil « Indicateurs de Croissance et de Vulnérabilité » développé par le Conseil supérieur de l'Ordre des experts-comptables, il pourra vous aider à identifier les points faibles de votre entreprise ainsi que les opportunités de développement, et vous accompagner dans la mise en œuvre d'un plan d'actions (voir plus loin « Un travail en réseau »). Vous pouvez également prendre contact avec le Chargé de mission régional à l'intelligence économique (CRIE) de votre région.

FAITES VOTRE AUTODIAGNOSTIC

L'influence et la compétitivité

1	Disposez-vous d'indicateurs précis pour évaluer la compétitivité de votre entreprise ?	Oui	Non
2	Cherchez-vous à créer, entretenir ou participer à des réseaux hors de votre entreprise afin de disposer de sources et de moyens de diffusion d'informations utiles et diversifiés (amicales de dirigeants, associations d'anciens élèves, clubs de réflexion, chambres consulaires, administrations, pôles de compétitivité, centres techniques industriels) ?	Oui	Non
3	L'entreprise adhère-t-elle à des associations professionnelles permettant de faire entendre sa voix ?	Oui	Non
4	L'entreprise conduit-elle ou participe-t-elle à des actions à caractère sociétal (adhésion à des associations sportives, culturelles, humanitaires) ?	Oui	Non
5	Menez-vous des actions d'influence pour préserver et renforcer les intérêts de votre entreprise (organismes de normalisation, décideurs publics locaux, ministères, ONG) ?	Oui	Non
6	Avez-vous une politique de communication pour promouvoir votre entreprise et faire valoir les performances de ses produits, particulièrement les produits innovants ?	Oui	Non
7	Avez-vous une stratégie de communication via le Web2.0 (participation de votre entreprise à des blogs, forums, réseaux sociaux) ?	Oui	Non
8	Votre entreprise a-t-elle les moyens de rétablir sa réputation sur Internet en cas d'attaque ?	Oui	Non
9	Êtes-vous prêt à faire appel à un cabinet de lobbying pour défendre et promouvoir votre entreprise ?	Oui	Non

Résultats sur 9

Moins de 4 « oui » : la mise en œuvre d'actions d'influence permettrait d'améliorer la performance et la compétitivité de votre entreprise.

De 4 à 7 : même si vos produits sont de qualité, vous risquez à terme de rencontrer des difficultés pour les vendre comme vous le souhaitez.

Plus de 7 : vous avez un bon positionnement pour mener des actions d'influence.

Quel que soit votre résultat, n'hésitez pas à contacter votre expert-comptable si vous souhaitez qu'il vous oriente vers un spécialiste du lobbying et de la communication d'influence qui pourra vous accompagner dans la

mise en place d'un plan d'actions. Vous pouvez également prendre contact avec le Chargé de mission régional à l'intelligence économique (CRIE) de votre région

La capitalisation et la préservation du patrimoine immatériel

FAITES VOTRE AUTODIAGNOSTIC

1	Les éléments sensibles de votre entreprise sont-ils bien identifiés (savoir-faire, innovations, mémoire de l'entreprise, annuaire des compétences) ?	Oui	Non
2	Veillez-vous à les protéger ?	Oui	Non
3	Avant de lancer un projet important, traitez-vous les aspects relatifs à la sécurité des informations ? Qui sera informé ? Comment circuleront et seront conservées les informations ? Quelle politique de communication sera associée au projet ? Rédigez-vous systématiquement des manuels de procédures ?	Oui	Non
4	Certaines de vos informations sensibles sont-elles protégées par des contrats d'assurances et/ou des moyens juridiques liés à la propriété intellectuelle (brevets, dépôts de marques, de modèles...) ?	Oui	Non
5	Vos inventions sont-elles protégées ?	Oui	Non
6	Avez-vous formalisé une procédure d'habilitation pour l'accès aux données sensibles de l'entreprise ?	Oui	Non
7	Existe-t-il des consignes claires de rangement et d'archivage des documents sensibles ?	Oui	Non
8	Existe-t-il des consignes claires de destruction des documents sensibles ?	Oui	Non
9	Disposez-vous de locaux ou de mobilier sécurisés pour ranger vos documents sensibles ?	Oui	Non
10	Le système d'information de votre entreprise est-il sécurisé ?	Oui	Non
11	Insérez-vous des clauses de confidentialité dans les contrats de travail du personnel ?	Oui	Non
12	Les informations diffusées lors des congrès, salons et foires expositions sont-elles maîtrisées ?	Oui	Non
13	Contrôlez-vous la sensibilité des informations contenues dans vos supports de communication (documents de promotion, site web, lettre d'information) ?	Oui	Non
14	La somme des informations qui peuvent être recueillies légalement (information ouverte) peut-elle mettre en péril la compétitivité de l'entreprise ?	Oui	Non

Résultats sur 14

Moins de 7 « oui » : votre entreprise est confrontée à un risque bien réel de divulgation de son savoir ou de son savoir-faire.

De 7 à 11 : la protection du patrimoine de votre entreprise peut être accrue par la mise en place de solutions simples.

Plus de 11 : vous avez le souci de protéger le patrimoine immatériel de votre entreprise.

Quel que soit votre résultat, n'hésitez pas à contacter votre expert-comptable qui pourra vous orienter vers un spécialiste de la protection du patrimoine immatériel capable de vous accompagner dans la mise en place d'un plan d'actions. Vous pouvez également prendre contact avec le Chargé de mission régional à l'intelligence économique (CRIE) de votre région