



L'INTELLIGENCE ÉCONOMIQUE À L'ASSAUT DE L'INFORMATION STRATEGIQUE

Attaquer, défendre... Un vocabulaire guerrier pour une discipline qui n'a pourtant rien de barbare. L'Intelligence Économique, c'est d'abord un management de l'information stratégique que toute entreprise a intérêt à mettre en œuvre pour accroître et préserver son business.

► DÉFINITION

L'INTELLIGENCE ÉCONOMIQUE

« L'Intelligence Économique peut être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques. Cette information est celle dont ont besoin les entreprises pour élaborer et mettre en œuvre les tactiques nécessaires à l'atteinte des objectifs par l'entreprise dans le but d'améliorer sa position dans son environnement concurrentiel. »

Rapport Martre, Intelligence économique et stratégie des entreprises (La Documentation Française, Paris, 1994)

Apparu en France il y a 20 ans, le concept d'Intelligence Économique (IE) s'inscrit dans un contexte bien précis, celui de la mondialisation et de l'interconnexion des entreprises. L'apparition d'une véritable société de l'information caractérisée par la surabondance d'informations est un autre facteur à prendre en compte.

« Au début des années 90, ce sont surtout des grands groupes qui mettent en œuvre des actions en matière d'IE, rappelle Franck Guigard, chargé de mission en Intelligence Économique à la CCI de la Drôme.

Aujourd'hui, une entreprise, quelle que soit sa taille et son activité, se doit de faire de l'IE. Ainsi l'IE est une démarche qui concerne aussi bien les PME que les grandes entreprises à partir du moment où elles sont innovantes et évoluent dans un secteur concurrentiel. »

SE DÉFENDRE POUR PROTÉGER SON ENTREPRISE

L'IE doit, dans un premier temps, assurer la sécurité économique de l'entreprise. Cette dernière peut être l'objet de différentes ingérences extérieures : atteintes aux savoir-faire (captation de brevets), atteintes financières, atteintes informatiques, exploitation des failles humaines, etc. S'il est indispensable pour une entreprise d'être tournée vers l'extérieur et de communiquer de l'information, il est tout aussi indispensable d'identifier et de protéger son information stratégique. Ainsi, pour se protéger, elle doit adopter une posture d'IE défensive. Celle-ci se caractérise notamment par la veille "image" qui permet de surveiller la réputation (e-réputation) de l'entreprise, la veille "marché" qui permet de surveiller les données économiques d'une entité. « *La protection du patrimoine physique et informationnel de l'entreprise ainsi que la défense de la propriété intellectuelle sont également des éléments à prendre en compte* », souligne Franck Guigard.

ATTAQUER POUR CONQUÉRIR DES MARCHÉS

La veille stratégique qui peut également être exploitée dans le cadre d'une IE de type offensive, doit, elle, permettre d'identifier de nouveaux débouchés commerciaux, de trouver de nouveaux partenaires, de surveiller la concurrence, etc. La veille économique qui consiste à surveiller et analyser un marché donné, la veille juridique et réglementaire ainsi que la veille technologique sont les principaux axes de recherche et d'analyse. « *On ne peut pas tout surveiller*, souligne Franck Guigard. *La veille doit être mise en place en adéquation avec les actions et les projets stratégiques de l'entreprise.* » Pour mener à bien des opérations de veille défensive et offensive, plusieurs moyens s'offrent aux entreprises. Le principal consiste en l'utilisation et l'exploitation des données sur internet. Mais d'autres sources doivent, elles-aussi, être envisagées : réseaux humains, retours d'expériences des collaborateurs de l'entreprise, conférences, salons, opérations de lobbying.

► TÉMOIGNAGE

Christian SALANON

Responsable nouvelles technologies et sécurité informatique chez Markem-Imaje



« LE MAILLON FAIBLE, C'EST L'ÊTRE HUMAIN. »

Entreprise de référence mondiale dans les systèmes de codage, d'identification et de traçabilité des produits basés sur les technologies jet d'encre, laser et transfert thermique, Markem-Imaje recense 50 000 clients dans le monde.

Filiale du groupe américain Dover, la société possède à Bourg-lès-Valence (Drôme) sa branche de distribution française, sa plate-forme logistique européenne et un centre de R&D. Entreprise mettant en œuvre des technologies de pointe, Markem-Imaje a un besoin vital de sécuriser ses savoir-faire comme le confirme Christian Salanon, responsable nouvelles technologies et sécurité informatique. « *L'intelligence économique est un combat de tous les jours car le nombre d'attaques augmente. Celles-ci visent les données détenues au sein de l'entreprise,*

principalement les données financières et bancaires, et de plus en plus, les données "métiers" de l'entreprise. Nous avons mis en place une véritable veille sécurité pour connaître au plus tôt les menaces afin de nous protéger efficacement. Ceci passe aussi par l'éducation et la sensibilisation des collaborateurs. Le maillon faible dans la sécurité c'est avant tout l'être humain qui, à son insu, va divulguer des informations importantes. Cette année, nous mettons en place un plan de sensibilisation des salariés qui consiste à mesurer leur degré de connaissance des risques. Il y a quelque temps nous avons également mis en place un vaste projet destiné à inventorier toutes nos données et processus pour définir leur degré de sensibilité. La réduction des risques est un combat de tous les jours. »

[EN SAVOIR + : www.markem-imaje.com]

L'INFO C'EST BIEN, L'ANALYSE C'EST MIEUX

« Quand on parle d'Intelligence Économique il est important de se poser la question : que fait-on, une fois réunies, de toutes ces informations ? Car le fondement même de l'IE c'est l'analyse. Sans cela, l'info brute ne vaut rien », insiste Franck Guigard. En effet, la mise en place d'une démarche d'IE doit reposer sur un management et une organisation structurée et doit être construite comme un tout cohérent impliquant l'ensemble des acteurs de l'entreprise. La sensibilisation à toutes ces questions est donc primordiale. L'IE revêt également une autre dimension. Celle-ci doit permettre d'anticiper et d'identifier les scénarii de crise afin de maintenir l'activité et, in fine, de sauvegarder des emplois. Prenons l'exemple d'une entreprise, victime d'une attaque de type "ransomware* ". Comment doit-elle communiquer vis-à-vis de ses clients et/ou fournisseurs ? Quelle sera la réaction de ses partenaires ? Quelles parades préventives aurait-elle dû mettre en place ? Ou encore l'exemple d'une entreprise victime d'un vol ou d'une détérioration de matériel informatique. Quelles sont les fonctions vitales informatisées de l'entreprise qui devront être rétablies prioritairement ? Si le responsable informatique est absent, quelles sont les consignes à appliquer ? Combien de temps avant de restaurer tout le système informatique ? Quelle communication à avoir vis-à-vis de ses partenaires ? « *Il faut comprendre avant d'agir*, explique Franck Guigard. *La question se pose dès lors aux entreprises. À savoir, est-on dans l'anticipation des crises ou bien subissons et réagissons-nous après coup ?* »

* Logiciel malveillant qui prend en otage des données personnelles

L'IE EN CHIFFRES

➤ 1 000

C'est le nombre d'actes hostiles significatifs recensés chaque année à l'encontre des acteurs économiques.

➤ 525 millions de sites web

Existent aujourd'hui dans le monde, dont 155 millions sont actifs (producteurs et diffuseurs de contenu réguliers).

➤ 72% des entreprises

Interrogées dans le cadre d'une enquête de la CCI de la Drôme pratiquent la veille et/ou la recherche d'informations sur internet, 26 % d'entre elles jugent la notion d'intelligence économique abstraite.

Sources : Services de l'État en charge de la sécurité économique, Netcraft, enquête de la CCI Drôme menée en 2014 auprès de 83 entreprises.

➤ TÉMOIGNAGE

Sébastien PAOLOZZI - Gérant CEFT et Prodeval

« AVANT NOUS ÉTIIONS PASSIFS, Désormais nous ATTAQUONS. »



Gérant des deux sociétés CEFT, bureau d'études spécialisé en ingénierie biogaz et méthanisation, et Prodeval, expert en traitement et valorisation du biogaz, implantées sur Rovalatain, Sébastien Paolozzi a mis en place il y a deux ans une stratégie d'intelligence économique offensive.

« Depuis un moment déjà j'étais intéressé par la mise en place d'une veille technologique, mais je ne savais pas vraiment comment m'y prendre. Un pré-diagnostic effectué par la CCI Drôme m'a éclairé sur la mise en place de certaines actions. Aujourd'hui nous avons une personne en interne qui fait de la veille régulière sur les marchés, les secteurs d'activités, les réglementations et plus ponctuellement sur la concurrence. Pour obtenir des informations, c'est finalement assez simple,

nous naviguons sur internet, nous nous abonnons à des flux RSS, des newsletters, etc. Avant nous subissions, nous étions passifs, désormais nous attaquons, nous sommes proactifs et nous anticipons le marché. Nous regardons également ce qui se fait à l'étranger. Toute cette veille et ces informations recueillies influent sur notre R&D. En plus de la veille sur internet, nous enrichissons nos connaissances par notre présence sur des salons et la veille terrain. Maintenant je vois les bénéfices que peut nous apporter une veille régulière. Je sais aussi qu'il faut la faire vivre et évoluer, ainsi je compte développer désormais davantage le suivi des clients et des fournisseurs. »

[EN SAVOIR + :
www.ceft.eu, www.prodeval.eu]



CYBERCRIMINALITÉ : SOMMES-NOUS TOUS MENACÉS ?

L'exemple de la cyberattaque à l'encontre de Sony en fin d'année 2014 a montré au monde entier à quel point toute entreprise, même parmi les plus puissantes, pouvait être vulnérable. Et que la moindre faille de son système d'information pouvait être préjudiciable. À toutes les entreprises qui pensent qu'elles ne risquent rien parce que trop petites, trop locales, trop discrètes... Détrompez-vous ! À partir du moment où vous exploitez des données à caractère stratégique ou des fichiers clients, il y a des risques. Une université rhônalpine en a fait l'expérience avec le vol de 88 000 données étudiantes en ce début d'année. Et savez-vous que le défaut de moyens mis en place pour éviter la diffusion de données personnelles, fait courir un risque pénal à l'organisation responsable ? Jusqu'à 5 ans d'emprisonnement et 300 000 € d'amendes pour négligence ou non déclaration des fichiers à la CNIL.

Comment se protéger ?

La généralisation de l'usage du Cloud Computing amène à devoir respecter quelques précautions quant au stockage de ses données : dans quel pays sont-elles stockées et quelle législation s'applique alors en cas de problème ? Avec quel autre type de données cohabitent-elles ? Comment sont-elles sécurisées chez le prestataire ?... Le maître mot est SÉCURITÉ : attention aux clés USB qui, branchées innocemment sur un poste de travail, peuvent diffuser des virus ou aspirer toutes les données (juice jacking). Tout objet connecté peut être affecté. Évitez de travailler à distance avec des outils personnels. Sécurisez un maximum vos mots de passe. Le plus simple est de s'"auto-googliser" afin de se prendre conscience de l'étendue des données disponibles sur soi et son entreprise sur le web... À partir de là, à chacun de définir ses propres exigences de sécurité et les moyens à mettre en œuvre pour les atteindre.

Extrait d'une conférence intitulée "Intelligence économique, espionnage et cybercriminalité : valoriser la protection de l'information de votre entreprise" organisée en mars 2012 par la CCI Drôme.

SITES UTILES :

- ▶ **L'ANSSI** : www.ssi.gouv.fr/entreprise/bonnes-pratiques
(Agence Nationale de la Sécurité des Systèmes d'Information)
- ▶ **Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques** : www.cert.ssi.gouv.fr
- ▶ **Fuites d'informations** : un guide AFNOR pour les prévenir et s'en protéger : www.afnor.org
- ▶ **Le CLUSIF** : www.clusif.asso.fr
(Club de la Sécurité de l'Information Français)

INTELLIGENCE ÉCONOMIQUE, la CCI Drôme vous forme et vous informe

- > **SENSIBILISATION À :**
 - La démarche d'intelligence économique
 - La propriété industrielle (en partenariat avec l'INPI)
- > **ACCOMPAGNEMENT DE L'INTELLIGENCE ÉCONOMIQUE :**
 - Pré-diagnostic en intelligence économique
- > **FORMATION (INTER/INTRA) :**
 - Recherche d'informations (méthodologie et outils)
 - La veille (méthodologie et outil)
 - La structuration d'un système d'informations
 - Les réseaux sociaux

CONTACT : Franck Guigard,
04 75 75 87 24, f.guigard@drome.cci.fr