Espionnage Industriel : Préserver les secret de l'entreprise

Les Espaces à risque

Il rappelle d’abord les espaces à risques, lieux dans lesquels on observe le plus souvent des fuites d’informations sensibles. Les espaces confinés tels que les avions, les trains font partie de ces espaces privilégiés pour écouter les communications. Ces lieux publics sont en effet de véritables mines d’or puisque de nombreux salariés profitent bien souvent de leur temps disponible passé en déplacement pour contacter leurs collaborateurs et causer tel ou tel projet en cours. Il est important pour cela de « prendre l’habitude de faire attention aux personnes qui se trouvent autour de vous » explique Alain Juillet. Dans ces espaces, on peut très bien être entouré de concurrent ou de personnes qui pourraient monnayer les informations communiquées aux interlocuteurs.

Quelles sont les informations sensibles ?

Secrets de fabrication, contrats, business plans, nouveaux produits… Beaucoup d’informations ne doivent pas sortir de l’entreprise et être divulguées. Une information est dite sensible lorsque sa perte ou sa diffusion peut avoir un impact sur le business de l’entreprise, sur sa réputation, ou sur le personnel employé ainsi que sont entourage.

Il peut s’agir d’informations personnelles (par exemple une photocopie de carte d’identité), mais aussi d’informations professionnelles comme une base de donnée « clients », contrats, budgets, stratégies, dont la divulgation peut avoir un impact sur le chiffre d’affaire, la réputation.

Il convient donc pour les entreprises de bien déterminer quelles informations elles doivent protéger, c’est-à-dire quelles sont celles qui peuvent leur porter préjudice en cas de diffusion, et quels en seront les meilleurs moyens de protection.

Il existe des certifications crées par des organismes internationaux et qui ont pour but de rendre les entreprises plus "sures" face aux risques de sécurité et permettent entre autre d'éviter des risques d'espionnage. Par exemple, la certification ISO 27000, ainsi que toutes les normes qui en découlent, est de plus en plus adoptée par les entreprises. Cette certification est obtenue par les entreprises ayant eu des réflexions importantes en matière de sécurité informatique, mais aussi en terme de sécurité des infrastructures et ayant développé des plan de sécurité global à l'entreprise elle-même.

l'IGI 1300 est appliqué à au niveau de l'individu, et permet de d'habilité du personnel travaillant sur des documents confidentiels. Ce type d'habilitation est une source de confiance envers le personnel et constitue une première couche de sécurité.

Que ce soit la certification ISO 27K ou une autre, ces certifications sont indirectement liées à l'espionnage industriel, mais permettent cependant d'éviter de se retrouver dans des situations délicates où des actes malveillants d'espionnages seraient facilité.

Enfin, l’action la plus importante d’une entreprise pour protéger ses secrets reste avant tout la sensibilisation des salariés et du personnel de l’entreprise au enjeux de la sécurité, car ce sont les sources principales, sans avoir forcément de mauvaises intentions mais bien souvent par inadvertance ou mégarde.

Pour en savoir plus...

http://business.lesechos.fr/directions-generales/strategie/espionnage-industriel-apprenez-a-preserver-les-secrets-de-l-entreprise-9449.php