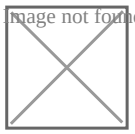

L'INTERVENTION D'UN DÉTECTIVE LORS DE FUITES DE DONNÉES SENSIBLES

Actualité législative publié le **05/09/2018**, vu **2033 fois**, Auteur : AIRP06 DETECTIVES - Detective privé Nice

Chaque entreprise détient des informations stratégiques et économiques propres à son activité. Ces informations ne sont pas toutes confidentielles et il est utile d'identifier celles qui doivent être protégées.

Chaque entreprise détient des informations stratégiques et économiques propres à son activité. Ces informations ne sont pas toutes confidentielles et il est utile d'identifier celles qui doivent être protégées.

Il s'agit des informations relatives au savoir-faire, aux méthodes de conception et de fabrication, aux projets et concepts technologiques. Les fichiers clients et fournisseurs font également partie intégrante des données à protéger.

Toutes les informations financières et commerciales nécessitent une protection sans faille. Dans l'hypothèse d'une fuite de ces informations, l'entreprise court le risque de compromettre sa compétitivité dans un environnement concurrentiel déjà très difficile.

Plus une entreprise investira dans la protection de ses données stratégiques et économiques, plus elle assurera sa pérennité.

LA DÉTENTION DES INFORMATIONS SENSIBLES

Chaque niveau hiérarchique d'une société est détenteur de l'information. En fonction du degré de responsabilité, elle peut être expurgée de façon à renforcer sa protection.

Parfois, c'est l'ensemble du personnel d'une même entreprise qui détient l'information afin de garantir un niveau de performance accru. A contrario, d'autres entreprises ne confèrent ce droit qu'à certains cadres personnellement concernés par la nature de l'information stratégique.

Ces informations sensibles sont généralement stockées sur un serveur central sécurisé et seul le personnel désigné y a accès. D'autres données confidentielles, en support papier, peuvent être stockées dans un coffre de l'entreprise.

En fonction du niveau de confidentialité de ces informations, des habilitations d'accès peuvent être délivrées aux personnes faisant partie du premier cercle autour du responsable de la société.

LA PROTECTION DE L'INFORMATION STRATÉGIQUE ET ÉCONOMIQUE

Protéger les informations sensibles d'une entreprise s'avère relativement compliqué.

90% des entreprises ont été victimes de vol ou de perte de données confidentielles au cours de l'année passée.

La majorité des employés ne mesure pas l'importance de protéger l'information et certains véhiculent des données sensibles entre leur bureau et leur domicile sur des supports numériques.

Le risque de fuite est accentué lorsque l'information sensible circule par voie de courrier électronique ou lorsqu'elle est stockée dans un cloud.

Même sécurisés et cryptés, ces modes de transmission et de stockage restent faillibles.

La principale cause des fuites de données sensibles est d'origine humaine et interne à l'entreprise.

Elle peut être intentionnelle, comme le vol de documents confidentiels, le détournement d'ordinateurs ou de téléphones appartenant à l'entreprise, ou la copie d'informations stratégiques et économiques sur une clé USB.

Les salariés malveillants agissent par vengeance, ou par intérêt, en divulguant ces informations à des concurrents. Ces actes sont qualifiés de vol par le code pénal et celui qui copie frauduleusement des données de l'entreprise sur une clé USB peut être poursuivi en vertu de l'*article 311-1 du CP*.

Dans un arrêt du 28 juin 2017, la Cour de Cassation a confirmé une décision rendue contre un salarié d'un cabinet d'avocats auteur d'un vol de données.

Lorsque la direction d'une entreprise suspecte une fuite d'information sensible, elle peut faire réaliser une enquête afin de confirmer ses doutes. Un enquêteur privé peut effectuer ce type d'investigations. Lorsque ce dernier aura établi la réalité des faits, et éventuellement identifié la source des fuites de données, le responsable de l'entreprise pourra déposer une plainte.

Dans d'autres cas, les fuites de données sont provoquées par des négligences. Une session restée ouverte ou une navigation sur des sites peu fiables favorisent la divulgation de données stratégiques.

Une entreprise consciente de ces risques, sensibilisera son personnel sur les conduites sécuritaires à tenir lors de la consultation et la transmission des informations stratégiques et économiques.

En dehors des risques inhérents au stockage et à la transmission des données par voie numérique, il est important de protéger l'information lorsqu'elle circule oralement au sein de l'entreprise ou à l'occasion de réunions se déroulant à l'extérieur de l'entreprise.

Si toutes les mesures de protection ont été mises en place sur les ordinateurs, les serveurs et le réseau numérique d'une société, il n'en reste pas moins que l'information peut circuler par d'autres voies.

Lors de réunion, des informations sensibles peuvent être évoquées et débattues. Des stratégies

commerciales, financières ou des projets sont abordés. Ces informations sont échangées verbalement et sont susceptibles d'être interceptées.

De récentes affaires de découvertes de micro espion, dans des bureaux ou des salles de réunions, ont fait la une de la presse (un micro dans l'hôtel des All Blacks à Sidney, un micro dissimulé dans le bureau du maire de Ste Maxime, des micros espions dans le bureau de Gérard Larcher, etc…).

Ces méthodes d'espionnage sont de plus en plus fréquentes et permettent à leurs auteurs d'obtenir des informations cruciales sur les projets ou le savoir-faire de leurs concurrents.

Ces fuites de données sont extrêmement préjudiciables aux entreprises qui les subissent.

Pour se prémunir contre tous types de fuites d'informations stratégiques et économiques, il est nécessaire de sécuriser le système informatique de l'entreprise, de sensibiliser le personnel détenteur de l'information aux risques inhérents à la négligence lors du stockage, la transmission et le partage de cette information.

Il est préconisé de faire procéder régulièrement à une détection de micros ou cameras espions dans les locaux de l'entreprise (bureaux, laboratoires, salles de réunions etc…)

Cette opération, communément appelée « dépoussiérage », peut être réalisée par des spécialistes (en général des détectives privés rompus aux techniques de détection de micros et caméras cachés). Elle permet alors à ceux qui détiennent l'information stratégique et économique, de s'exprimer en toute sécurité, sur des sujets sensibles lors de réunions de travail ou à l'occasion d'échanges verbaux dans les locaux de l'entreprise.

©airp06 détectives - Détective privé Nice Cannes Monaco