Protection des secrets commerciaux dans l'entreprise moderne

Quelques suggestions sur comment protéger la confidentialité des informations d'entreprise.

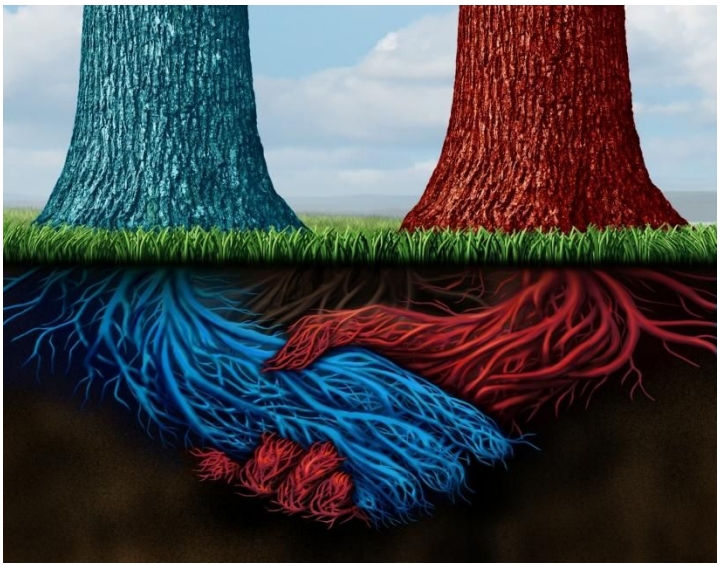
par John EASTWOOD

S'agissant des informations sensibles et confidentielles de votre entreprise, il est important dans un premier temps de s'assurer que vos employés et votre équipe managériale font partie d'une culture de protection. Trop souvent, accords et clauses de confidentialité sont simplement noyés sous une pile de documents officiels signés en hâte lors de l'embauche - avec peu ou pas de discussion ultérieurement.

Et pourtant, les communications regardant les attentes de l'entreprise en matière de confidentialité doivent être exposées clairement, et ce, dès le départ. Des règles et procédures explicites, comprises par tout le monde, doivent notamment être mises en place s'agissant du traitement des informations sensibles et confidentielles.

Typiquement, ces règles peuvent inclure :

- Pas de disques durs privés, clés USB, ordinateurs, etc. utilisés dans les locaux ou dans le cadre des activités de votre entreprise.



- L'accès physique ou électronique à vos secrets commerciaux est restreint à ceux qui en ont réellement besoin.
- Seuls les logiciels autorisés par l'entreprise peuvent être installés, et installés seulement par l'entreprise.
- L'utilisation de logiciels de messagerie privée (email) pour communiquer à partir des ordinateurs de l'entreprise doit être interdit ou restreint.
- Lorsque des documents sont confidentiels, les employés doivent le

signaler (ou utiliser un modèle de document comportant un tel

signalement) en indiquant la nature confidentielle des documents.

- A l'échelle de l'entreprise, une politique en matière de rangement des bureaux doit être entretenue.
- Des mesures de sécurité additionnelles, plus élaborées que de simples mots de passe, peuvent être requises pour accéder aux réseaux de l'entreprise, incluant des logiciels de vérification, des lecteurs d'empreintes digitales, etc...

Quelque soient les règles que vous choisissez d'établir, elles doivent être communiquées de façon claire et sans équivoque aux employés et à l'équipe de direction. Une réunion consacrée à la sécurité, tenue chaque année ou même chaque trimestre avec les employés, constitue un bon moyen de s'assurer que ces derniers savent ce qui est attendu d'eux. Demandes d'autorisation, questionnaires, attestations permettent ici de s'assurer que le personnel ne travaille pas seulement de façon machinale, sans faire véritablement attention.

Les entreprises doivent aussi garder à l'esprit que les informations confidentielles ne se limitent pas aux activités de recherche et développement en cours ou aux formules et procédés de fabrication déposés. Elles comprennent également les données clients, les projets commerciaux, le texte des accords conclus avec les partenaires commerciaux, les données personnelles des employés, les futurs objectifs commerciaux, et beaucoup d'autres éléments susceptibles d'être utilisés par vos concurrents ou partenaires commerciaux.

Quelques autres points à garder à l'esprit sont listés ci-dessous :

1. Suivez de strictes procédures de sortie

Il est crucial d'avoir un plan établi pour faire face au départ d'un membre du personnel. Des modèles de documents spécifiques doivent être préparés pour traiter respectivement des démissions ordinaires, licenciements, licenciements pour mauvaise performance ou pour faute. Les procédures de sortie doivent toujours prendre en compte les informations confidentielles que l'employé(e) pourrait avoir en sa possession, en prévoyant un délai pour la restitution de telles informations et la clôture des accès aux informations confidentielles au sein des systèmes de l'entreprise.

Notamment, le déroulement de la clôture des accès aux emails et aux réseaux informatiques de l'entreprise doit prendre en compte la nature du départ. Dans les cas impliquant un licenciement immédiat pour faute, l'entreprise doit particulièrement prendre soin de ne pas permettre à l'employé(e) d'avoir accès à des systèmes au sein desquels il/elle pourrait tenter de télécharger ou effacer des fichiers, ou de perturber l'activité de l'entreprise de quelque autre façon.

En fonction de la situation, beaucoup d'entreprises auront un système de sécurité présent ou prêt à intervenir si nécessaire au cours du licenciement. Dans certains cas, ce système peut jouer un rôle moteur, en motivant la récupération des cartes d'accès à l'entreprise, des ordinateurs, des smartphones, des clés de voiture, etc. Les effets personnels présents dans le bureau de l'individu peuvent être stockés séparément et envoyés à l'adresse personnelle de l'employé(e) de manière à

éviter un débordement d'émotions ou le rassemblement d'employés curieux.

La stratégie utilisée pour traiter d'un licenciement motivé doit viser une efficacité et finesse maximales afin d'aider à préserver la dignité de toutes les parties impliquées. Un(e) employé(e) licencié(e) sans humiliation publique ou embarras est moins susceptible de chercher à "régler ses comptes" avec son précédent employeur, et davantage susceptible d'écrire un nouveau chapitre de son parcours professionnel.

2. Gardez à l'esprit quelques principes de psychologie

Presque toujours, une motivation d'ordre psychologique sous-tend un comportement fautif tel que le vol ou le détournement de secrets commerciaux. Agissant souvent sous le coup du stress ou de la pression, l'employé(e) s'appropriant une information confidentielle ou la partageant avec d'autres considère le ratio risques/bénéfices comme lui étant favorable.

Le motif peut même être l'amour. Il y a quelques années, nous avons traité d'une affaire impliquant un homme et une femme (mariés mais pas l'un à l'autre) qui entretenaient une liaison tout en travaillant pour des entreprises partenaires. L'équipe informatique de notre client s'est finalement aperçu qu'un des employés de l'entreprise utilisait son compte personnel de messagerie pour envoyer les plans de produits futurs à son amante, qui travaillait pour un distributeur gérant également quelques produits de la concurrence. Il n'en avait retiré aucun bénéfice financier, et l'enquête ultérieure a révélé qu'aucune information n'avait été transmise aux concurrents. Néanmoins et pour quelques mois, il avait pu permettre à son amante d'apparaître, au sein de son entreprise, bien renseignée sur les projets commerciaux et produits à venir d'un de leurs fournisseurs-clés

Dans une autre affaire de licenciement hostile, un cadre supérieur avait été rappelé de l'étranger et informé de son licenciement imminent le premier de deux jours consacrés à la négociation de son départ. A la fin du premier jour des négociations, l'entreprise n'avait pas encore clôturé l'accès du cadre aux systèmes de messagerie et base de données de l'entreprise. L'examen informatique réalisé par la suite devrait révéler que le cadre s'était levé au milieu de la nuit, apparemment incapable de trouver le sommeil, et avait passé le reste de la nuit à télécharger - et tenter de télécharger - une grande quantité d'emails et de données.

Pourquoi ? Sous l'effet du décalage horaire, du stress, vos cadres supérieurs au beau milieu d'une procédure de licenciement n'auront pas forcément toujours les idées claires, par conséquent n'attendez pas d'eux qu'ils prennent nécessairement les bonnes décisions. Suivez une procédure méthodique afin de leur retirer immédiatement l'accès aux informations de votre entreprise.

Particulièrement dans les cas impliquant le licenciement de personnel informatique, il est vital de ne pas donner de préavis, lequel leur donnerait une chance de prendre une revanche rapide et désastreuse. Certains de nos clients

ont ainsi pu rencontrer les situations suivantes :

- Une entreprise d'édition de magazines ayant découvert que chaque article et photographie des 48 pages d'un sujet à venir avaient été supprimés de leurs serveurs une semaine avant de partir à l'impression.

- Une agence de relations publiques dont l'informaticien avait passé ses 24 dernières heures dans les locaux à télécharger des versions piratées de logiciel sur chaque ordinateur. L'ex-employé avait ensuite reporté lesdites "infractions" aux développeurs des logiciels originaux.

- Un employé ayant enregistré, à son nom, des noms de domaine très similaires à celui utilisé par son employeur. Après la résiliation de son contrat de travail, il les avait configurés de telle façon que n'importe qui ouvrant par hasard l'une de ces adresses soit redirigé automatiquement sur le site du principal concurrent de son ex-employeur.

3. Soyez inflexible - pour rester bref

Une fois que la preuve a été rapportée qu'un(e) employé(e) s'est approprié des informations confidentielles, différentes opinions peuvent être exprimées parmi les cadres de l'entreprise et leurs conseillers juridiques quant à la meilleure voie à suivre. Mais il est extrêmement important d'adopter rapidement une position ferme et de la maintenir; sans quoi l'affaire risque de s'éterniser, devenant un fardeau tant financier qu'émotionnel.

L'équipe managériale de l'entreprise pourra vouloir croire que le cadre licencié récemment a simplement copié 30GB de données appartenant à l'entreprise sous l'impulsion d'un désir déplacé de garder un "souvenir" ou "preuve" de son travail. Néanmoins et d'un point de vue juridique, il est essentiel d'agir vite afin de stopper le transfert éventuel de données vers un concurrent ou un partenaire en amont ou aval. Les affaires relatives aux secrets commerciaux sont difficiles. Elles requièrent de la concentration et de la discipline afin d'obtenir une intervention rapide des tribunaux et, si possible, de faire peur à la partie adverse pour la pousser à restituer ou détruire les données en jeu.

Dans ce genre d'affaires, "trop de cuisiniers peuvent gâter la sauce". Il y a quelques années, nous avons regardé une entreprise se contenter de faire "la moyenne" des conseils reçus de plusieurs cabinets d'avocats, gérant l'affaire de façon jamais ferme ni définitive. Balancer entre une approche "sévère" ou plus "souple" ne donne aucun avantage stratégique ou tactique à votre entreprise et ajoute seulement à vos frais juridiques. Pour résoudre le problème, nous avons dû persuader notre client de "repartir à zéro" avec la ferme résolution d'utiliser les options rendues disponibles par le droit pénal taïwanais. Cette décision a rapidement amené la partie adverse à la table des négociations.

Pensez au challenge comme à couper un arbre avec une hache. Vous n'arriverez à rien si vous vous contentez de donner quelques coups gentils dans le tronc en espérant réussir. Dans une affaire relative au secret des affaires, il faut avancer vite

afin de s'assurer que la partie adverse sait que l'enfer pourrait bien se déchaîner si les informations volées ne sont pas restituées. La probabilité d'une intervention efficace des tribunaux ou d'un règlement rapide de l'affaire augmente considérablement si la partie adverse sait que vous êtes prêts à tenir la distance. Par ailleurs, la probabilité d'obtenir de vos employés qu'il respectent vos secrets commerciaux sur le long-terme augmente s'ils savent que vous êtes prêts à être inflexible en la matière.

4. Pensez flexibilité

Le vol ou détournement de vos secrets commerciaux comporte-t-il un aspect pluridisciplinaire qui puisse justifier que d'autres champs juridiques soient pris en compte ?
Bien souvent, les comportements décisifs relatifs au manquement semblent se produire à l'étranger, parfois lors de voyages aux Etats-Unis où le très sévère Economic Espionage Act[1] (Loi sur l'Espionnage Économique) est en vigueur. Un(e) ancien(ne) employé(e) peut trouver ses perspectives d'embauche future considérablement réduites s'il lui est impossible de voyager à l'international ou de rentrer chez lui/elle sans avoir à craindre d'être arrêté(e) à l'aéroport.

5. N'en faites pas trop

En travaillant dans le camp de l'employé(e), nous avons également pu observer que certaines entreprises font l'erreur inverse - porter de fausses accusations de vol de secrets commerciaux sans réel fondement. Les entreprises qui s'empressent de prendre des mesures drastiques contre des employés partant de bonne foi peuvent par la suite se trouver confrontées à des réclamations considérables en responsabilité civile ou pénale.
Compte tenu des sévères sanctions pénales prévues en cas de violation de la Loi taiwanaise sur la protection des informations personnelles (LPIP), il est absolument essentiel que les entreprises assument leur part de responsabilité lorsqu'elles choisissent d'enquêter sur leurs employés.

Dans un cas extrême, l'employé quittant l'entreprise avait volontairement transmis la totalité de ses disques durs personnels à la sécurité d'entreprise dans le cadre d'une dernière vérification sollicitée pour s'assurer qu'il n'emporterait pas avec lui des données sensibles. Les disques durs contenaient l'unique copie de nombreuses années de photos de famille, la totalité de ses informations financières - incluant ses déclarations d'impôts, et de nombreuses autres informations très privées. L'équipe de sécurité de son ancien employeur avait ensuite gardé ces données pendant des mois, copié et conservé le contenu des disques durs (y compris les photos de famille et informations financières) sans avoir son autorisation, et seulement ensuite avait pensé à demander son approbation écrite. L'entreprise a bientôt commencé à rencontrer des problèmes

[1] La Loi américaine sur l'Espionnage Économique (1996) définit l'espionnage économique comme le vol ou le détournement d'un secret commercial avec l'intention ou la certitude qu'une telle infraction bénéficiera un gouvernement étranger, une agence étrangère ou un agent étranger quelconque.

en vertu de la LPIP à cause de ces copies non-nécessaires et non-autorisées de données très privées.

L'entreprise aurait pu faire l'économie d'importants frais de contentieux en se contentant simplement de vérifier les disques durs des employés puis de les leur restituer sans continuer de les copier ou de les conserver au-delà d'un délai raisonnable. Un bon sens du jugement doit être utilisé au moment d'évaluer quels cas poursuivre et quelles méthodes utiliser pour les poursuivre.

6. Faites le rapprochement

Un programme performant de protection des secrets commerciaux sur le lieu de travail doit créer des attentes parmi les employés - attentes relatives à leur propre comportement mais aussi relatives à la détermination de l'entreprise à prendre des contre-mesures fortes lorsque nécessaire. Organiser des sessions de formation sur une base régulière peut être très utile pour construire un environnement conforme, elles doivent cependant être structurées de telle façon que les informations communiquées soient comprises et retenues.

Une fois que vous avez confirmé qu'il existe des preuves solides pour attester de l'existence d'un vol ou de la divulgation de secrets commerciaux, l'entreprise doit agir de manière rapide et décisive afin d'accroître la probabilité d'obtenir de la partie adverse qu'elle fasse machine arrière. Toute demi-mesure sera interprétée, par les tribunaux et par vos partenaires, comme démontrant un manque de résolution et de certitude. Si votre propre enquête vous laisse avec des informations incomplètes s'agissant de ce qu'il s'est passé, considérez avoir recours aux ressources de la police afin qu'une enquête plus poussée soit menée avec l'autorisation des tribunaux.

Néanmoins, s'il n'existe pas de preuve convaincante attestant du vol de vos secrets commerciaux ou s'il existe des signes évidents que votre ex-employé(e) agit de bonne foi, la meilleure chose à faire est de renoncer. Une entreprise ne devrait jamais agir de sa propre initiative ou faire appel à enquêteurs privés d'une façon qui pourrait être considérée comme une violation du droit à la vie privée des employés, dans la mesure où des sanctions lourdes pourraient en résulter.

La version anglaise de cet article est parue originellement dans le magazine Topics de l'AmCham de Taipei (Février 2016). Lien:
https://goo.gl/hHr5pV

Auteur:

John EASTWOOD, Associé
john.eastwood@eigerlaw.com