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, brevets, plans, procédés de fabrication, codes sources…) ;
- recenser les ressources du système d'information 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 couvrira des aspects variés :

- nomination d'un responsable sécurité et identification des responsabilités dans l'entreprise ;
- classification des informations en fonction de leur degré de sensibilité (rares, vulnérables, stratégiques) ;
- définition des règles d'accès aux bâtiments, aux outils informatiques, à Internet… ;
- rédaction et diffusion de procédures de sécurité quotidiennes ;
- communication des mesures à adopter en cas d'incendie ;
- 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

1. La volonté d'assurer la sécurité économique des entreprises relève d'une **compréhension profonde** et nécessaire des **conditions de la compétitivité,** et de la nécessité de protéger leurs atouts.
2. **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.
3. Les protections relèvent à la fois de la **stratégie juridique** (dépôts de brevets, protection des marques, etc.) et de la **sûreté** (mesures de protection du savoir stratégique à travers les systèmes d'information, sensibilisation des personnels de l'entreprise, observation des pratiques et des comportements des concurrents, etc.). Les entreprises ont également l'obligation légale de **protéger leur personnel ainsi que leur lieu d'implantation et de veiller à ce que les renseignements les concernant soient sécurisés.**
4. 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…** qui peuvent s'avérer vulnérables. Il existe un risque de sabotage, d'altération, d'effacement ou de fraude.
5. La question du **transfert des technologies** revêt une importance capitale : consenti et maîtrisé, il ne pose pas de problème ; en revanche, en cas de captation technologique issue de méthodes indélicates, il peut

se révéler catastrophique pour une entreprise dont le développement repose avant tout sur sa créativité et 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.**

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, sauf à ce que la PME 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. Certaines de questions formulées 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.

➢ **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 en France.

➢ **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 sur 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 !

➢ **Divulgation 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 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'acquérir des licences d'exploitation étrangères afin d'utiliser un procédé de fabrication qu'ils ont eux-mêmes conçu !

➢ **Résultats de la 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 puissance étrangère :** un membre d'un centre de recherche publique alsacien a mené en parallèle des travaux de recherche pour une société étrangère. Ce groupe étranger a déposé deux brevets internationaux 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 l'adresse du 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.

➢ **Mise en place d'un espion informatique dans un téléphone portable :** espion potentiel de choix, le téléphone mérite une attention particulière. 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. 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 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…).

SÉCURISER LE PATRIMOINE ÉCONOMIQUE DE VOTRE ENTREPRISE

Évitez d'être naïf, sans verser dans la paranoïa : soyez vigilants !

L'objectif de la sécurité économique n'est pas de surveiller la terre entière et de se protéger contre tout ce qui est possible et imaginable. Il s'agit d'essayer de comprendre l'environnement de l'entreprise, en particulier les risques et les menaces auxquels elle peut être confrontée, et, à partir de là, de s'organiser de façon proportionnée pour réduire ses vulnérabilités. Mettre en place une démarche de sécurité économique permet avant tout de provoquer une prise de conscience des risques et menaces pour l'entreprise par l'ensemble des collaborateurs et une diminution de l'incertitude pour le chef d'entreprise. Il convient donc d'adopter une attitude pragmatique, réaliste et opérationnelle : un état d'esprit fait à la fois de vigilance et d'ouverture. Que chacun comprenne que protéger son entreprise, c'est protéger son emploi.

Identifiez les menaces

Vous n'êtes pas le seul à rechercher des informations stratégiques sur vos concurrents pour tenter de gagner des parts de marché à leurs dépens. Vous pouvez être la cible de concurrents (voire de partenaires) parfois peu scrupuleux, qui n'hésiteront en tout cas pas à exploiter vos faiblesses ou vos failles de protection. Il est nécessaire que vous preniez régulièrement le temps d'analyser les principales menaces qui peuvent peser sur votre entreprise :

➢ **Actions illicites exploitant les failles de la politique de sûreté :** intrusions, vols, déstabilisation d'individus, piratages ou destructions informatiques, usurpation ou subtilisation d'identités, diffamation…
➢ **Campagne de désinformation** par fausses rumeurs ou accusations non fondées afin de nuire à l'entreprise et à son image.
➢ **Actions licites exploitant des maladresses :** récupération de poubelles, filatures et observations de rencontres de personnes, écoute de conversations dans les lieux publics, bavardages.
➢ **Actions indirectes visant des partenaires privilégiés de l'entreprise :** fournisseurs, intermédiaires, clients, prestataires de services, sous-traitants.
➢ **Exploitation des failles** dans la politique de sûreté ou **imprudences** commises pour s'approprier des éléments faisant partie du patrimoine stratégique de l'entreprise.
➢ **Analyse des sources ouvertes,** c'est-à-dire des informations provenant de l'entreprise elle-même (salons, colloques, interviews, publications, sites internet…). Une astuce pour les identifier précisément peut être de confier à un cabinet d'intelligence économique une mission de recherche… sur sa propre entreprise !
➢ **Manque de prudence** (bavardage, indiscrétions publiques, étalage de sa vie professionnelle sur les réseaux sociaux type Facebook, Viadeo, LinkedIn, Google +…) ; **manque de vigilance** (perte de matériels informatiques, absence de surveillance de prestataires extérieurs intervenant dans l'entreprise…) ; **manque de rigueur** dans l'application des procédures par les collaborateurs (documents emportés à l'étranger, non-respect des mesures de sûreté…).
➢ **Collaborateurs déçus ou achetés** qui, pour des motivations personnelles diverses et variées (vengeance, jalousie, intérêt…), sont amenés, dans l'exercice de leurs fonctions, à commettre des actes peu scrupuleux (détournement de patrimoine, divulgation d'informations ou de contacts…).

Déterminez votre degré d'exposition aux risques informatiques

Posez-vous les bonnes questions :

- Quelle place l'outil informatique occupe-t-il au sein de l'entreprise ?
- Quels sont les services qui utilisent des ordinateurs ?
- Quels types d'informations manipulent-ils ?
- Ces informations sont-elles stratégiques pour le développement de l'entreprise ?
- Quels sont les ordinateurs qui rassemblent des données sensibles ? Celui du comptable ? Celui du responsable des ventes ?
- Les boîtes e-mail de vos représentants commerciaux contiennent-elles des informations stratégiques ?
- Y a-t-il des informations confidentielles sur l'agenda électronique sur votre téléphone ou sur le carnet d'adresses électronique de l'entreprise ?
- Des documents stratégiques sont-ils accessibles sur les serveurs de l'entreprise ?

En fonction des réponses, vous pourrez cartographier l'exposition de votre entreprise à ces risques en signalant :
- les zones de stockage des informations : ordinateurs, disques durs externes, bases de données… ;
- les zones de passage des informations : e-mails, transferts de données

par supports physiques (disques durs, clefs USB…), mise en ligne de documents, travail de groupe en ligne, archives électroniques, téléphones… ;
- le degré d'importance des informations et des zones ;
- les zones de traitement des données : ordinateurs du service comptable, du service des ventes… ;
- les zones de suppression des données : suppression physique (supports jetés) et numérique (e-mails effacés).

Mettez en place des mesures pragmatiques

Certaines informations et certains savoir-faire constituent un **actif immatériel** que l'entreprise doit savoir protéger, de la même manière qu'elle protège ses locaux. Les 10 actifs immatériels identifiés par l'Observatoire de l'immatériel (observatoire-immateriel.com) sont :
- le capital clients ;
- le capital marques ;
- le capital organisationnel ;
- le capital humain ;
- le capital technologique ;
- le capital actionnaires ;
- le capital fournisseurs / partenaires ;
- le capital systèmes d'information ;
- le capital sociétal ;
- le capital naturel ou capital environnemental.

Avant de mettre en place des portiques de sécurité ou de s'équiper en logiciel spécialisé, la protection des informations de l'entreprise passe d'abord par du bon sens :

Soyez discret

Tout le monde sait pertinemment qu'il faut faire attention à ce que l'on dit, et pourtant les trains et les avions demeurent encore des espaces où l'information économique circule trop librement. Les cadres dirigeants s'y laissent aller, dévoilent parfois le nom de leurs clients ou de leurs fournisseurs. D'autres font des confidences à leur voisin sans savoir qu'il travaille pour la concurrence. Le pire, c'est lorsqu'un colloque réunit tous les acteurs d'une filière économique dans une ville : il suffit alors de prendre le bon train ou le bon avion et d'écouter les discussions ! Les langues se délient également trop facilement dans les salons professionnels ou au téléphone.
Pour éviter tout risque, imaginez qu'un directeur de votre principal concurrent voyage à proximité immédiate : vous réaliserez que ce n'est ni le lieu ni le moment d'échanger avec vos collaborateurs sur la stratégie commerciale ou de préparer la négociation qui vous attend à l'arrivée du train. **Sachez que des personnes intéressées par certaines catégories d'informations empruntent systématiquement le TGV Paris-Bruxelles pour écouter les conversations de leurs voisins et capter des informations en lisant les écrans des ordinateurs portables…**

Sensibilisez vos collaborateurs

La majorité des informations sensibles sont transmises par les personnes.

Identifiez les informations sensibles

Puis protégez-les et listez les personnes pouvant y avoir accès.

ORDRE DES EXPERTS-COMPTABLES

mon expert-comptable, je compte sur lui !

BESOIN D'UN FINANCEMENT DE 25.000 EUROS ?

Les experts-comptables
et leurs partenaires bancaires
facilitent votre développement.

- TÉLÉCHARGEZ LES DOSSIERS MODÉLISÉS

www.financement-tpe-pme.com

- CONTACTEZ VOTRE EXPERT-COMPTABLE POUR COMPLETER ET TRANSMETTRE LE DOSSIER À LA BANQUE

BANQUE POPULAIRE

LCL BANQUE ET ASSURANCE

Groupe Crédit du Nord

3 RÉSEAUX BANCAIRES ONT SIGNÉ
AVEC L'ORDRE DES EXPERTS-COMPTABLES POUR
UN ENGAGEMENT DE RÉPONSE SOUS 15 JOURS !

Les chefs d'entreprise ont des solutions pour mettre en œuvre leurs stratégies de croissance

Création, financement, innovation, export... avancez sur votre

e-parcours

Une initiative des Collectivités territoriales et de Cemagid

Anticipez et maîtrisez les échéances de votre entreprise avec

L'Agenda de l'Entreprise

Une initiative des Chambres de Commerce et d'Industrie et de Cemagid

Retrouvez ces applications sur www.comptanoo.com

Cemagid

LA JOINT-VENTURE GROUPAMA-CEGID

Groupama

Toujours là pour moi.

Cegid

gan

CCI DE FRANCE

Les Chambres de Commerce et d'Industrie au service des Territoires et des Entreprises

Création d'entreprise

Formation

Aménagement du territoire

Développement durable

Innovation - Intelligence économique

Culture et patrimoine

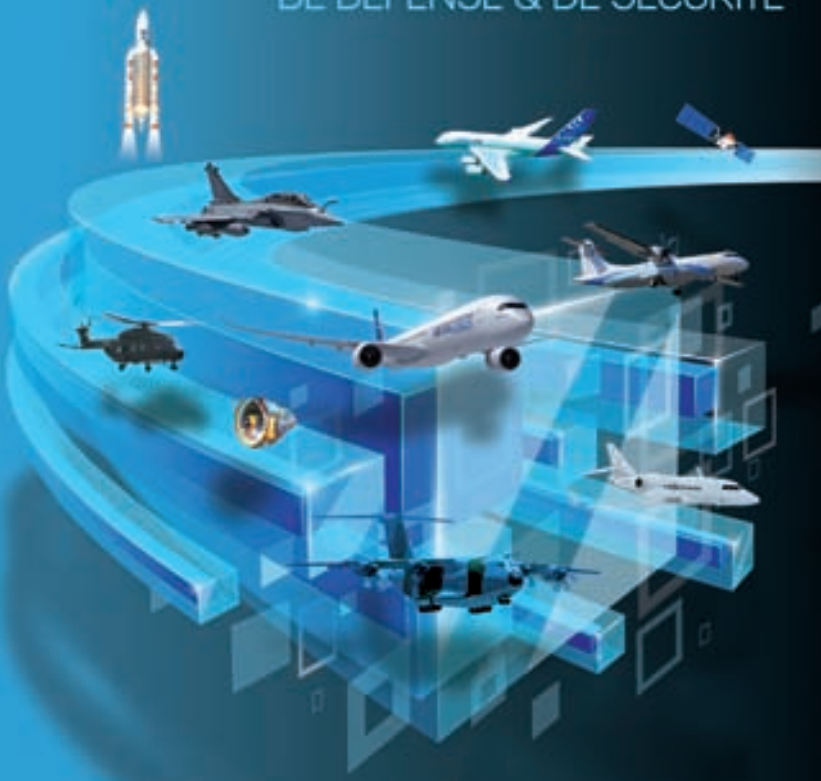
International

Un réseau de plus de 150 CCI,
4 800 élus et 30 000 collaborateurs
dans toute la France pour faire route
avec les entreprises

Retrouvez l'ensemble de nos services sur

www.cci.fr

INDUSTRIE FRANÇAISE AÉRONAUTIQUE, SPATIALE, D'ÉLECTRONIQUE DE DÉFENSE & DE SÉCURITÉ



GIFAS

8, rue Galilée
75116 PARIS
Tél. 01 44 43 17 00
Fax. 01 40 70 91 41
infogifas@gifas.fr

www.gifas.fr

Groupement des Industries Françaises Aéronautiques et Spatiales

Thomas Legrain Conseil

Stratégie - Lobbying - Communication d'influence

CONSEIL EN **STRATEGIE**, **LOBBYING** ET **COMMUNICATION D'INFLUENCE**

NOS OBJECTIFS

- Concevoir et mettre en œuvre votre **stratégie de lobbying** et de **communication d'influence** pour vous aider à jouer un rôle actif dans l'élaboration de la décision publique.
- Vous aider à **anticiper les modifications législatives et réglementaires**.
- Vous accompagner dans la **défense de vos intérêts**, tout en prenant en compte l'intérêt général.
- Mobiliser des expertises et des outils variés autour d'un seul objectif : **accroître votre influence**.

NOTRE MISSION

- Veille législative, réglementaire et politique
- Relations gouvernementales et parlementaires
- Rédaction d'amendements
- Organisation de petits déjeuners thématiques, de dîners-débats, de colloques, de groupes de liaison avec le Parlement...
- Stratégies de communication d'influence
- Élaboration d'argumentaires et d'outils de communication (lettres d'information, dossiers thématiques, blogs, réseaux sociaux...)
- Marketing de soi
- Relations presse
- Prévention et gestion de crise
- Intelligence Economique
- Accompagnement de candidats dans le cadre d'élections professionnelles
- Formation des collaborateurs aux enjeux du lobbying et aux techniques de la communication d'influence

CONTACT

E-mail : **contact@tlconseil.com**
Tél. +33 **(0)1 42 94 93 14** | **Fax** +33 **(0)1 79 73 29 27**
6, avenue Rachel - 75018 Paris
www.thomas-legrain-conseil.com - www.networking-business-club.com
www.legrain2sel.com - www.tlimpression.com

Femmes
Diplômées d'Expertise
Comptable Administrateurs

un réseau influent pour répondre aux besoins des entreprises et promouvoir la marque expert-comptable

La vocation de l'association : proposer des profils d'administratrices aux entreprises de taille intermédiaire, sur tout le territoire.

Créée par le Conseil Supérieur de l'Ordre des Experts-Comptables en réponse à la loi Copé Zimmermann , l'Association des Femmes Diplômées d'Expertise Comptable Administrateurs rassemble 1300 femmes en France. De quoi fournir un vivier à la fois conséquent et qualitatif pour les postes d'administrateurs.

Le réseau est aussi un lieu d'échanges autour d'événements, souvent organisés en présence de personnalités, de défis sportifs ou d'initiatives régionales. Il propose également à ses membres des formations au mandat d'administrateur.

« Les femmes experts-comptables ont un rôle actif à jouer dans une dynamique de gouvernance des entreprises et de compétitivité de l'économie. »

« Les femmes experts-comptables en entreprise ont vocation à rejoindre le réseau pour porter haut la marque expert-comptable. »

Rendez-vous sur le blog
www.femmes-experts-comptables.com

ORDRE DES EXPERTS-COMPTABLES

LE **RESEAU D'INFLUENCE** DES DIRIGEANTS D'ENTREPRISE

NETWORKING
BUSINESS
Club

Le Networking & Business Club a été créé en 2003. L'objectif du club est clair : **établir des liens entre le monde politique et la société civile**, **faire jouer les synergies d'affaires**, **favoriser les échanges et l'entraide**.

Le club compte **280 membres**, dont la moitié appartient à la sphère politique, droite et gauche confondues.

Le temps d'un petit déjeuner, les membres du club échangent avec **une personnalité de premier plan du monde politique ou économique sur les grands enjeux de société qui impactent leurs activités quotidiennes**.

À chaque rencontre, trois temps forts : **un temps d'échange autour d'un petit déjeuner convivial**, **une conférence**, **un débat**.

Ils sont intervenus dans le cadre du club : Xavier Beulin, Président de la FNSEA – Olivier Buquen, Délégué interministériel à l'Intelligence économique – Pierre-André de Chalendar, Directeur général de Saint-Gobain – Bertrand Collomb, Président de Lafarge – Olivier Ferrand, Président de Terra Nova – Xavier Fontanet, Président d'Essilor – Muriel Mayette, Administrateur général de la Comédie Française – Christian Noyer, Gouverneur de la Banque de France – Augustin de Romanet, Directeur général de la Caisse des Dépôts et Consignations – Jean-François Roubaud, Président de la CGPME – Louis Schweitzer, Président d'honneur de Renault – Nicolas de Tavernost, Président du groupe M6 – Laurent Wauquiez, Secrétaire d'État chargé de l'Emploi – Alain Weil, PDG de NextRadio TV...

Soumettre sa candidature pour adhérer au club :
www.networking-business-club.com

ORDRE DES EXPERTS-COMPTABLES

L'ASSURANCE SANTÉ ENTREPRISE : UNE GARANTIE D'ACCÈS À LA PRÉVENTION

- Pour assurer la pérennité des entreprises et maintenir l'emploi
- Pour couvrir les honoraires d'un expert de crise : avocat, expert-comptable…

6 compagnies d'assurance s'associent à cette initiative

en partenariat avec le CIP National

Centre d'information sur la prévention des difficultés des entreprises

www.cip-national.fr

AXA · Cfdp · CHARTIS · Covea Risks · Groupama · HISCOX

TOUT SAVOIR SUR

www.entreprisepreventionsante.com

Téléchargez les fiches d'information
et les conditions générales des contrats d'assurance Santé

Encadrez les stagiaires
Appliquez des conventions strictes, relisez leurs rapports de stage avant leur diffusion.

Sécurisez les systèmes d'information

La plupart des destructions d'informations proviennent de mauvaises manipulations internes sur les ordinateurs, les serveurs ou les téléphones. Tous ces matériels doivent être protégés, afin d'éviter les intrusions d'une part et les maladresses d'autre part.

Protégez les innovations techniques, marques, dessins et modèles – propriété de votre entreprise

La protection de la propriété industrielle s'effectue auprès de l'Institut national de la propriété industrielle (l'INPI).

Protégez l'image et la réputation de votre entreprise et des principaux dirigeants

Assurant notamment une veille sur les forums et les réseaux sociaux. Une rumeur lancée par un concurrent peu scrupuleux peut, en effet, causer de sérieux dommages à l'entreprise. Apprenez à y répondre.

Protégez le patrimoine immatériel

Une TPE-PME doit avoir une **politique de protection de la propriété intellectuelle adaptée.** Elle peut recourir aux principaux outils de protection du patrimoine immatériel de l'entreprise :

- *Dépôts de brevets :* un brevet est un titre de propriété industrielle qui protège une innovation technique pendant 20 ans. En contrepartie, l'innovateur rend publique sa découverte. Ainsi, nul ne peut utiliser une innovation sans l'accord du propriétaire du brevet et moyennant le paiement d'une licence d'utilisation. L'innovation reste confidentielle pendant 18 mois.
- *Protection des dessins et modèles.*
- *Enveloppe Soleau :* faible protection qui permet d'entériner la création d'une idée, d'un concept.
- *Manuel de process :* afin de savoir qui fait quoi et comment.

Face à la **contrefaçon,** il peut être utile de réfléchir, en amont de la phase de développement d'un produit, aux possibilités techniques et juridiques de **réduire les risques de copie.** Des conseils juridiques peuvent être obtenus à ce sujet auprès de la direction générale de l'Union des fabricants (UNIFAB, unifab.com).
Les logos des produits de marques sont ainsi abondamment copiés par des sociétés qui prospèrent dans certains pays peu respectueux des lois régissant la protection de la propriété intellectuelle et des marques. Les sociétés françaises qui travaillent dans l'industrie des produits de luxe en sont les premières victimes et sont obligées de consacrer des budgets très conséquents pour faire respecter leurs marques.

Il est aussi nécessaire de **protéger la documentation interne de l'entreprise.** Les processus de **classement** et d'**archivage** des documents peuvent être plus ou moins sophistiqués et plus ou moins lourds. Même au niveau d'une TPE-PME, le simple fait de se poser sérieusement la question du traitement des courriers, propositions, catalogues et autres documents dans l'entreprise permet au moins de prendre conscience des risques éventuels liés à la circulation de documents stratégiques au sein de l'entreprise, et de mesurer les conséquences d'une éventuelle action nocive

(perte, destruction, vol, copie illicite).
Identifiez les documents confidentiels de votre entreprise avec un marquant spécifique apposé sur la couverture des rapports papier ou avec un logo visible à l'écran sur vos supports numériques. Mettez en place une gestion spécifique de ces documents pour contrôler leur usage et leur diffusion. Ce marquage peut concerner :

- des documents éphémères : brouillons, notes, préparations d'accords ou de négociations… ;
- des documents pérennes : dossiers, plans d'action ou marketing, documentation financière, contrats, accords…

Le marquage ne doit s'appliquer qu'aux documents stratégiques et confidentiels pour l'entreprise. Ces documents doivent être peu nombreux et protégés pour une durée limitée (pensez à sortir de façon régulière les documents dont les restrictions d'accès ne se justifient plus). Les documents protégés peuvent, selon leur importance, faire l'objet de procédures de :

- suivi pour les documents papier : enregistrement, diffusion, inventaire, destruction ;
- traçabilité pour les documents numériques : des marquants permettant de repérer l'origine du document peuvent être insérés dans les fiches caractéristiques ou dans le corps du texte au moyen de mots ou de formules banalisées, apparentes pour le seul rédacteur ;
- conservation : armoires ou coffres avec verrous de sûreté dont les combinaisons doivent être changées régulièrement, installés dans des locaux protégés, d'accès contrôlé, surveillés éventuellement par des dispositifs de vidéosurveillance ou anti-intrusion. Ces mesures doivent être mises en œuvre lors du départ du lieu de travail ;
- destruction : brûlage ou broyage pour les supports papier. Pensez à une attention spéciale à l'utilisation des poubelles en instaurant, par exemple, un circuit particulier pour les documents protégés à détruire, par la mise à disposition de poubelles spécifiques d'une couleur bien repérable.

Sécurisez vos locaux

– Une entreprise ne doit pas être ouverte à tous les vents : un livreur ne doit pas pouvoir s'introduire librement dans une entreprise !
– Un système de badges doit être installé pour sécuriser l'accès aux locaux.
– Les collaborateurs doivent veiller à ne pas laisser d'informations à l'issue de réunions, quel que soit le support (*paperboard,* clé USB…).
– Un collaborateur ne doit pas laisser entrer un inconnu sous prétexte qu'il imagine que cette personne travaille dans un autre service.
– Lors d'un entretien, chaque collaborateur doit penser à fermer les dossiers qui peuvent traîner sur son bureau et sur son ordinateur.
– Un collaborateur doit baliser le circuit de visite de son entreprise, car trop souvent un visiteur peut photographier de manière illicite une maquette ou une machine avec son téléphone portable. Il faut également penser à mettre sous coffre les documents les plus importants (brevet, fichier client…).
– Il faut avoir le réflexe de broyer les documents importants que l'on jette.
Selon la sensibilité des activités de l'entreprise, l'accès à certains locaux (laboratoires, salles de serveurs informatiques, bureaux d'études…) doit faire l'objet de mesures de restriction. Ce dispositif repose sur le principe d'une autorisation d'accès permanente ou temporaire réservée aux seuls collaborateurs qui en ont besoin dans le cadre de leur travail.
Toute intervention d'un sous-traitant à l'intérieur des locaux (entretien d'un photocopieur, travaux d'aménagement des bureaux, réparations diverses…) doit être effectuée sous surveillance constante d'un collaborateur averti. Les règles de protection du patrimoine en matière d'accès

aux locaux, de confidentialité, de manipulation de l'information électronique, de stockage de données doivent être spécifiées contractuellement avec les directions des entreprises intervenantes : sécurité, nettoyage, consultants, auditeurs, transports, maintenance, fournisseurs…, et avec les personnes concernées prises individuellement. Des contrôles fréquents doivent permettre de vérifier la bonne application par le personnel de ces clauses de protection.

Verrouillez vos systèmes d'information

L'informatique peut constituer la faille d'une TPE-PME. Par exemple, lorsqu'un collaborateur travaille sur son ordinateur portable dans le train via le WiFi, il doit être conscient du fait que son travail peut être récupéré par un tiers. Les données confidentielles doivent uniquement être traitées sur des postes de travail non connectés en réseau.
Les dossiers doivent avoir des mots de passe différents et renouvelés régulièrement. Les ordinateurs doivent disposer de logiciels de détection d'erreurs ou d'intrusion. Il faut installer des logiciels de sécurité (antivirus, antispam…) et modifier les configurations et mots de passe du constructeur installés par défaut. Il faut éviter d'autoriser n'importe quel téléchargement sur le réseau de l'entreprise.
Utilisez des dispositions de sauvegarde sûres et redondantes à l'aide de **bases de données centrales** ou de **supports gravés. Dupliquez les données stratégiques** de l'entreprise dans un site différent, en les confiant, par exemple, à une société extérieure spécialisée dans l'archivage informatique.
L'essor de l'informatique a totalement bouleversé la gestion des TPE-PME, tant au niveau des procédés de fabrication, qu'au niveau de la recherche et développement, la prospection ou encore la vente… Si l'ère du numérique constitue une opportunité de transformation pour les entreprises, elle représente aussi un danger dans la mesure où les données sont susceptibles d'être dérobées.

Délimitez l'activité des stagiaires

Délimitez l'activité des stagiaires au sein de l'entreprise dès le début de leur stage. Vérifiez les CV des stagiaires que vous vous apprêtez à recruter. Déterminez qui sera destinataire de leur rapport de stage et vérifiez attentivement qu'il n'y soit pas divulgué d'information confidentielle. Assurez-vous que le stagiaire n'aura pas accès aux informations confidentielles de l'entreprise. Ne lui donnez pas, par exemple, de droits d'accès sur son ordinateur qui lui permettent de prendre connaissance de toutes les informations stockées sur les serveurs de l'entreprise.
Faites-lui signer une clause de confidentialité avant l'entrée dans l'entreprise et assurez-vous qu'il a bien compris à quoi cette clause l'engage. Si vous accueillez un stagiaire étranger dans un laboratoire de recherche et que sa demande de stage spontanée n'est pas liée à une coopération scientifique ou universitaire entre les deux pays, renseignez-vous auprès de l'ambassade de France sur l'organisme d'appartenance du demandeur.
Pendant le stage, veillez au respect par le stagiaire des horaires et des lieux autorisés. Prenez des mesures de surveillance et de contrôle concernant l'accès du stagiaire au réseau informatique, à la téléphonie et à la photocopieuse. Faites-vous communiquer une adresse où le stagiaire peut être joint en cas d'urgence.

Récupérez le badge et les clefs à l'issue du stage et les éventuels codes d'accès que vous lui avez communiqués (accès aux locaux, accès informatique). Si le stagiaire est étranger, assurez-vous qu'il a un visa en règle. Vérifiez que vous avez bien reçu sa convention de stage et que celle-ci a bien été signée par les trois parties (l'entreprise, l'organisme de formation, le stagiaire lui-même).

Définissez une procédure pour les visites

- Définissez une zone protégée interdite à toute personne non autorisée.
- Interdisez que le visiteur entre en relation avec des salariés non préalablement désignés.
- Créez un circuit de visite.
- Instituez le port du badge.
- Ouvrez un registre des visites.
- Accompagnez le visiteur durant l'ensemble de la visite.
- Ouvrez une consigne pour les téléphones portables ou autres appareils permettant des enregistrements photos, vidéos ou sonores.
- Éteignez les ordinateurs, rangez dans des armoires sécurisées les matériels de bureautique portables.
- Formalisez une liste de sujets que personne ne doit évoquer avec les visiteurs.

Formalisez une charte de bonnes pratiques

Il est vivement recommandé de mettre en place dans chaque entreprise, quelle que soit sa taille ou son secteur d'activité, une charte des bonnes pratiques professionnelles – à respecter aussi bien en interne qu'à l'extérieur – qui permet notamment de lister les comportements à adopter pour conserver la confidentialité des informations stratégiques. Elle doit être remise à chaque membre du personnel afin qu'il prenne connaissance et l'applique au quotidien dans son travail. Il y sera fait référence aussi souvent que nécessaire, notamment lors de salons ou de conférences. Voici quelques bonnes pratiques qui peuvent être mises en place dans l'entreprise.

Sécurité dans l'entreprise

➢ Lors d'un recrutement, **vérifier les diplômes et l'expérience professionnelle du candidat pressenti** auprès de sources extérieures (cabinets de recrutement, anciens employeurs, organismes de formation).

➢ **Contractualiser la confidentialité :** des clauses de respect de la confidentialité des données informatiques peuvent être intégrées à des contrats de travail. Par exemple : « M… s'engage à ne pas faire usage des informations recueillies au cours de son travail en dehors de l'entreprise, tant à l'extérieur du lieu physique de travail qu'à l'extérieur du réseau informatique et du matériel informatique propre à l'entreprise. »

– Sélectionner et travailler avec des sous-traitants, des prestataires informatiques, des cabinets d'étude de marché, des cabinets d'audit, des sociétés de traduction, des transporteurs ou encore des sociétés de nettoyage **exclusivement dans un cadre contractuel.**

➢ **Protéger les accès** aux sites et aux immeubles en installant des sas de contrôle, des barreaux aux fenêtres, des dispositifs extérieurs de fermeture…

➢ **Protéger les locaux** en interne à travers la mise en place de codes électroniques ou de moyens d'identification biométrique…

➢ Vérifier le **bon fonctionnement des portes et des fenêtres** des locaux.
➢ **Regrouper et protéger les clefs** donnant accès à tout ou partie des locaux et rangements de l'entreprise.
➢ **Ranger les documents** de travail sensibles sous clé, lors de la pause déjeuner, le soir ou durant le nettoyage des bureaux.
➢ **Nettoyer les bureaux,** effacer les tableaux, retirer les feuilles du *paper-board* après toute réunion.
➢ **Installer des armoires fortes** pour y ranger les documents stratégiques de l'entreprise ainsi que les supports informatiques.
➢ **Nettoyer les disques durs des ordinateurs** avant de les affecter à un autre collaborateur ; effacer toutes les données.
➢ **Broyer les documents sensibles** devenus inutiles, y compris les brouillons. Il faut proscrire l'utilisation de la simple poubelle d'une part et du broyeur « droit » d'autre part. L'idéal est d'avoir un broyeur « croisé ».
➢ **Avant de les jeter, détruire les supports de données** susceptibles de contenir des informations confidentielles qui pourraient être récupérées : lorsqu'un matériel de stockage (disque dur, ordinateur) est supprimé, il faut en empêcher l'usage en détruisant le matériel. Un disque dur même effacé contient encore de nombreuses données. Les boîtes e-mails peuvent aussi contenir de nombreuses informations, même effacées.
➢ **Rester discret sur les mesures de protection** et les dispositifs d'alarme mis en place dans l'entreprise.
➢ **S'assurer que les documents promotionnels, le site internet de l'entreprise ou encore les blogs des collaborateurs ne laissent pas filtrer des renseignements confidentiels** qui pourraient être exploités par des concurrents.
➢ **Apposer une marque de propriété** sur tous les documents que votre entreprise produit.
➢ **Penser à mettre en place une stratégie appropriée de propriété industrielle** pour protéger les innovations, les produits et le savoir-faire de l'entreprise. Penser notamment à protéger le nom de domaine de l'entreprise (déposer au minimum le **.fr** et le **.com** ; si le nom de domaine comprend plusieurs mots, le déposer avec et sans tirets).

Sécurité informatique

➢ **Distinguer les profils utilisateurs** à l'intérieur de l'entreprise et les droits d'accès associés.
➢ **Choisir des mots de passe qui n'évoquent rien a priori,** les renouveler régulièrement et ne les communiquer à personne.
➢ **Se poser la question de savoir combien de personnes dans l'entreprise disposent du mot de passe administrateur** permettant d'accéder au système central de gestion des droits. Il convient de réduire le nombre de titulaires de comptes disposant de privilèges élevés aux seules personnes pour lesquelles ces privilèges sont absolument nécessaires dans l'accomplissement de leur mission. Des listes doivent être tenues à jour pour tous les comptes de ce type, dont évidemment les comptes permettant d'accéder au système central de gestion des droits, qui constituent des cibles de choix pour les attaquants.
➢ **Gérer les mots de passe des ordinateurs.** Il est stratégique de systématiser les droits d'accès et les mots de passe, et de garder les mots de passe confidentiels. Il ne faut pas les écrire sur un post-it que l'on colle sur son ordinateur ! Le mieux est d'utiliser un mot de passe qui n'est pas évident à découvrir et de ne le donner à personne ! Il faut les modifier régulièrement.
➢ **Vérifier que les collaborateurs ne partagent pas un mot de passe entre plusieurs postes.** Le partage de mots de passe entre comptes doit