Votre activité R&D est en plein essor mais vous manquez de moyens financiers.

Vous êtes l'actionnaire majoritaire de votre entreprise. La recherche de nouveaux partenaires financiers peut amener des investisseurs étrangers à prendre part au capital.
Cette opération peut constituer une menace d'atteinte au patrimoine technologique et industriel de votre entreprise.

Fiche 7 : Éviter l'arrivée de fonds hostiles pouvant déstabiliser votre entreprise.

- Rechercher des partenaires financiers « amis ».
- Rechercher des partenariats avec les grandes entreprises.
- S'informer au préalable sur les partenaires potentiels et leurs intentions.
- Contacter le conseiller Chargé de Mission régional à l'Intelligence Économique (CRIÉ) qui vous conseillera sur les organismes financeurs.

Arrivé à la fin de votre parcours professionnel, vous n'avez pas planifié la transmission du patrimoine de l'entreprise.

Les conséquences économiques de l'échec de la transmission d'entreprise peuvent être : perte d'emplois directs et indirects, perte de compétence de métier, déclin économique de la filière…

Fiche 8 : Assurer la transmission du patrimoine de l'entreprise.

- Définir votre stratégie de retraite.
- Préparer votre successeur en vue d'assurer la continuité.
- Rédiger une convention unanime entre les actionnaires qui régira leurs rapports afin d'assurer une transmission harmonieuse du patrimoine.
- Prendre connaissance des moyens légaux et fiscaux pour effectuer la transmission selon vos intentions et vos priorités.
- Préparer à l'avance un «plan de relève».

Vous pensez peut-être que la sécurité est établie une fois pour toute.

Le défaut de contrôle du suivi de la politique établie est dangereux car il peut créer un sentiment de fausse sécurité.

Fiche 9 : Gérer et maintenir la politique de sécurité.

- Les risques liés au changement de personnel.
- La maintenance du système informatique.
- Tester périodiquement le plan de sauvegarde des données de l'entreprise.
- S'assurer du respect des lois et des réglementations.
- Simuler des tentatives d'intrusion surprises.
- Réaliser périodiquement un audit de la politique de sécurité de votre entreprise, afin d'identifier et d'évaluer les insuffisances reliées à la sécurité et d'apporter des améliorations s'il y a lieu.

Sécurité Économique

Dispositif régional

Pour accompagner les entreprises dans leur démarche de protection de l'information stratégique, l'État a mis en place dans la région Rhône Alpes un Comité Régional de Sécurité Économique.
Cette structure est composée des représentants de l'État exerçant des missions régaliennes liées à la sécurité :
Direction Centrale du Renseignement Intérieur (DCRI), Direction de la Protection et de la Sécurité de la Défense (DPSD), Gendarmerie et Chargé de Mission Régional à l'Intelligence Économique (CRIÉ).
Les membres du Comité Régional de Sécurité Économique et leurs représentants départementaux effectuent dans les entreprises des visites de sensibilisation à la Sécurité Économique.

Vos contacts en Rhône Alpes

- CRIÉ : tel 06.73.28.77.99 Email : *pascal.brocard@finances.gouv.fr* *pascal.brocard@direccte.gouv.fr*
- DCRI : tel 04.78.66.84.80
- DPSD : tel 04.37.27.35.28
- GENDARMERIE : tel 04.37.56.21.11

Pour en savoir plus….

- *www.intelligence-economique.gouv.fr*
  site du Haut Responsable à l'Intelligence Économique (HRIÉ)
- *www.ssi.gouv.fr*
  serveur thématique sécurité des systèmes d'information
- *www.clusir-rha.fr*
  site du club sécurité des systèmes d'information en Rhône-Alpes
- *www.inpi.fr*
  site d'information sur la propriété industrielle

Service de coordination à l'intelligence économique

Réalisation : Pascal Brocard (Chargé de Mission régional à l'Intelligence Économique).

Sécurité Économique

La sécurité économique peut se définir comme l'ensemble des moyens actifs et passifs pour assurer la sauvegarde du patrimoine informationnel de l'entreprise ainsi que ses activités.

Quel sont les risques ?

- Vols d'informations (savoir-faire, secrets de fabrique, secrets des affaires…).
- Pertes d'information et de données après sinistre.
- Intrusions du système informatique et utilisation de ressources système.
- Mise hors service des ressources informatiques.
- Tentatives de déstabilisation.
- Risque financier par prise de participation de capitaux extérieurs.
- Mise en cause au plan légal.

A quels niveaux doit-elle s'exercer ?

- Auprès des personnes qui détiennent des informations stratégiques ou qui peuvent les utiliser ou les répandre plus ou moins consciemment.
- Sur les supports matériels sur lesquels les données sont enregistrées (papier, disques gravés, disques durs, clés USB…).
- Dans les établissements où elles sont créées, détenues, utilisées.
- Dans les télécommunications au sens large, lorsque les informations circulent (voie postale, Internet, téléphones portables…).

Votre entreprise est-elle concernée ?

- Votre entreprise stocke sur ses systèmes des données confidentielles et stratégiques pour son développement ?
- Vous développez des produits issus de technologies innovantes ?
- Vous êtes jeune créateur d'entreprise en recherche de financement ?
- Vous recherchez des financements pour développer votre activité R&D?
- Vous échangez, via Internet, des données importantes avec vos clients ou partenaires ?
- Votre entreprise présente ses activités sur les salons professionnels ?
- Vos collaborateurs sont équipés de moyens mobiles de présentation et de communication (portables, clés USB, assistants, …) ?
- Vous recevez des visiteurs extérieurs et des stagiaires dans votre entreprise ?

Si vous avez répondu OUI à au moins une de ces questions, vous êtes concerné par ce guide.

Sécurité Économique

Quelques méthodes simples et facilement applicables

Vous n'avez pas identifié vos informations stratégiques et les risques et menaces qui pèsent sur l'entreprise. L'entreprise ne dispose pas d'une documentation générale sur sa sécurité (objectifs, organisation, moyens, procédures de mise à jour…). Votre sécurité n'est pas abordée comme un projet appelé « politique de sécurité ».	**Fiche 1 : Bâtir une politique de sécurité.** ► Faire l'inventaire du patrimoine informationnel à protéger. ► Classifier et repérer les documents en fonction de leur niveau de confidentialité. ► Sensibiliser vos salariés à la valeur des informations et au respect des règles de base. ► Bâtir la politique de sécurité .
Votre entreprise n'a pas mis en place des principes simples de sécurité passive. Nombreux sont les incidents de sécurité qui peuvent intervenir : vol d'un bien, sabotage de matériel informatique, indiscrétion dans un micro-ordinateur au cours d'une absence…	**Fiche 2 : Protéger vos locaux.** ► Mettre en place un système de contrôle d'accès administré (badges, portiques, sas, serrures,…). ► Contrôler l'entrée et la sortie des véhicules dans l'enceinte de votre structure. ► Acquérir des réflexes simples : fermeture des portes et fenêtres, déclaration de pertes de clés ou de badges, dissimulation du clavier lors de l'utilisation d'un digicode… ► Contrôler l'introduction et la sortie de documents, matériels informatiques, électroniques ou de télécommunication. ► Engager du personnel formé et dédié à la protection de vos locaux (hôte ou hôtesse d'accueil, agents de surveillance…). ► Disposer d'un plan d'intervention suite au déclenchement d'une alarme et/ou la détection d'une intrusion.
Vos données sensibles ne sont pas protégées. En partageant ainsi ses informations (innovations, travaux de R&D, orientations stratégiques, ses plans marketing, etc.), votre entreprise accroît potentiellement sa vulnérabilité. Il est impératif de concilier la nécessité d'exposer des informations, et l'obligation de protéger certaines d'entre elles en fonction de leur niveau de sensibilité.	**Fiche 3 : Protéger vos données** ► Archivage des informations en lieu sûr et protection contre les intrusions, les incendies, les inondations… ► Contractualiser ses relations partenaires (fournisseurs, sous-traitants…). ► Contrôler l'accès des visiteurs (badges) et déterminer à l'avance le circuit de visite. ► Faire intervenir les entreprises de nettoyage en présence de vos salariés. ► Utiliser un déchiqueteur pour les documents (papiers, CD-ROM). ► Définir une stratégie appropriée pour protéger vos innovations, produits ou savoir-faire (secret industriel, brevet).

Sécurité Économique

Vous n'avez pas associé certains de vos collaborateurs à votre projet «politique de sécurité». Les risques et menaces proviennent d'abord des ressources internes à l'entreprise : collaborateurs et stagiaires sont à l'origine de 2/3 des actes de malveillance.	**Fiche 4 : Sensibiliser vos salariés** ► Présenter les enjeux de sécurité, principes et règles de la sécurité de l'entreprise. ► Définir le comportement à adopter à l'extérieur de l'entreprise (salon, restaurant, hôtel, transports en commun). ► Déterminer un périmètre d'accès aux informations en fonction du niveau de responsabilité du salarié. ► Insérer des clauses spécifiques de confidentialité dans le contrat de travail ou la convention de stage.
Vous n'avez pas mis en place une politique de sécurité des systèmes d'information. A défaut d'une bonne gestion des moyens d'identification et de sécurisation des échanges informatiques, vos données sensibles (comptabilité, fichiers clients, brevets, plan…) peuvent être accessibles par des personnes non autorisées ayant accès au réseau en interne ou en externe.	**Fiche 5 : Mettre en oeuvre des moyens appropriés à la confidentialité des données.** ► Réaliser un audit de sécurité des systèmes d'information. ► Contrôler l'accès aux données et applications (identification et mot de passe). ► Procéder régulièrement à la mise à jour du système de protection (antivirus, firewall). ► Mettre en place des solutions d'échanges électroniques sécurisées : outils de chiffrement intégrés à la messagerie électronique ou espace web sécurisé, certificats de signature électronique. ► Stocker les informations confidentielles sur un poste non connecté au réseau.
Vous n'avez pas prévu de reprise d'activité après un sinistre éventuel. Votre entreprise n'a pas mis en place un plan de continuité et de relève des services et de sauvegarde des données et des applications de l'entreprise. Plus de la moitié des sociétés ayant connu un sinistre majeur de leur système d'information ont cessé leur activité dans les deux ans qui ont suivi.	**Fiche 6 : Prendre des dispositions en cas de crise.** ► Prévoir la sauvegarde dupliquée des données sensibles sur un serveur distant géographiquement de l'entreprise. ► Établir un plan de secours opérationnel pour réagir face à des situations liées à l'activité industrielle ou la menace environnementale. ► Prévoir un contrat d'assurances solide pour couvrir les éventuels coûts en cas d'atteinte aux biens matériels ou aux personnes. ► Assurer la pérennité de l'entreprise en cas de difficultés financières ou de tentatives de rachats hostiles.