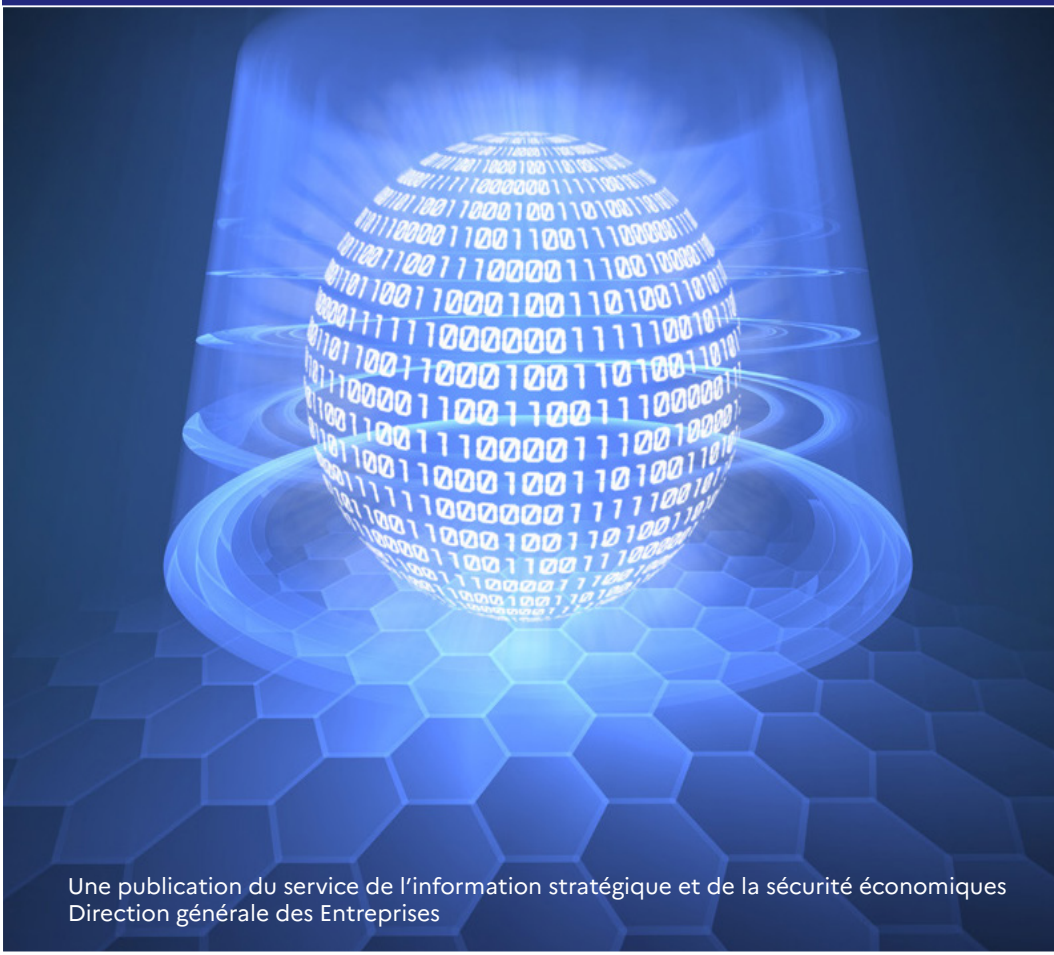
MINISTÈRE
DE L'ÉCONOMIE
DES FINANCES
ET DE LA RELANCE

Liberté
Égalité
Fraternité

LA SÉCURITÉ ÉCONOMIQUE AU QUOTIDIEN

En 26 fiches pratiques



Une publication du service de l'information stratégique et de la sécurité économiques
Direction générale des Entreprises

Couverture : © Pobytov

ISBN : 978-2-11-15 645-7 (en ligne)

DGE - Bat. Siéyès - 61 Bd Vincent Auriol 75703 Paris Cedex 13

Édition : juillet 2021

AVANT-PROPOS


© Sircom-Bercy

J'ai le plaisir de vous présenter aujourd'hui « La sécurité économique au quotidien, en 26 fiches pratiques », coordonné par le service de l'information stratégique et de la sécurité économiques (Sisse) du ministère de l'Économie, des Finances et de la Relance.

Ces fiches pédagogiques sont destinées à guider les dirigeants d'entreprises, les chefs de laboratoires de recherche, mais aussi les responsables d'administrations, dans la mise en œuvre des bons réflexes face aux nouvelles menaces auxquelles ils font face.

Depuis 2014, année de publication des premières fiches, les risques sur la sécurité économique de nos entreprises se sont à la fois intensifiés et diversifiés.

En particulier, l'importance croissante des technologies numériques dans la compétition économique crée non seulement des opportunités, mais aussi des nouvelles vulnérabilités, particulièrement pour les données, qui sont au cœur de votre activité. La protection des informations doit être une priorité partagée à chaque instant par l'ensemble des collaborateurs d'une entreprise, d'un laboratoire ou d'une administration.

De même l'usage accru du droit comme instrument de puissance économique, notamment à travers l'extraterritorialité des législations étrangères, participe de ce contexte nouveau.

C'est pourquoi il nous a semblé essentiel de sensibiliser à nouveau l'ensemble des entreprises françaises avec une approche aussi concrète et vivante que possible.

Je vous invite à faire de ces fiches pratiques un outil d'accompagnement de tous les jours, pour chacune et chacun d'entre vous.

C'est un prolongement indispensable à l'effort engagé actuellement par l'État pour renforcer la politique publique de sécurité économique, à travers la mission que j'ai confié au commissaire à l'information stratégique et à la sécurité économiques et au service qui lui est attaché, le Sisse. La sécurité économique est l'affaire de chacun !

Bruno Le Maire,
Ministre de l'Économie des Finances
et de la Relance

ÉDITORIAL

DU DIRECTEUR GÉNÉRAL DES ENTREPRISES, COMMISSAIRE À L'INFORMATION STRATÉGIQUE ET À LA SÉCURITÉ ÉCONOMIQUES

© A. Salesse - Sircom

La sécurité des entreprises et la protection de leurs informations stratégiques font partie intégrante de la politique économique et industrielle du Gouvernement.

En tant que commissaire à l'information stratégique et à la sécurité économiques auprès du ministre de l'Économie, des Finances et de la Relance, j'ai le plaisir de mettre à votre disposition ce nouvel outil pratique, accessible à toutes et à tous, qui, je l'espère, vous guidera efficacement dans la protection de votre entreprise, de son savoir-faire et de son patrimoine informationnel.

Les équipes du Sisse, qui y ont travaillé depuis de nombreux mois avec le concours de nombreuses administrations, se sont attelées à couvrir l'ensemble des sujets qui intéressent la sécurité économique de l'entreprise au sens large, avec l'objectif d'être le plus pratique possible.

Les 26 fiches abordent ainsi, sous une forme concrète et vivante, de très nombreux cas de figure tirés de l'expérience et proposent des idées et des outils pour y répondre, à la fois au niveau de l'organisation, du comportement des collaborateurs, et des mesures techniques.

La sécurité économique n'est pas seulement une politique impulsée par l'État. C'est une entreprise collective que l'ensemble des acteurs du tissu économique français doit pouvoir s'approprier, à la fois pour protéger ses propres intérêts, mais aussi pour servir le bien commun.

Je forme le vœu que ces 26 fiches de sécurité économique y contribuent le plus directement possible et deviennent pour vous une référence utile et un réflexe au quotidien.

Thomas Courbe,
Commissaire à l'information stratégique
et à la sécurité économiques

SOMMAIRE

PRÉSENTATION

DU SERVICE DE L'INFORMATION STRATÉGIQUE ET DE LA SÉCURITÉ ÉCONOMIQUE

Le Service de l'information stratégique et de la sécurité économiques (Sisse) coordonne la politique de sécurité économique de l'État. Des réformes d'ampleur, engagées depuis deux ans en matière de gouvernance de la politique de sécurité économique (PSE), ont permis d'établir une liste nationale (confidentielle) d'entreprises stratégiques et de technologies critiques à protéger en priorité et de mettre en place des organes de gouvernance. À ce titre, le Sisse coordonne la surveillance et l'action des différents ministères qui travaillent à la protection de ces actifs stratégiques pour la nation et oriente les services de renseignement.

Concrètement, lorsqu'une menace économique étrangère est mise au jour (un raid capitalistique hostile contre une pépite par exemple), celle-ci est enregistrée, cotée, caractérisée, partagée, et traitée. Le Sisse organise la coopération entre les acteurs du dossier pour s'assurer que des mesures efficaces sont prises pour faire cesser la menace lorsqu'il le faut pour préserver notre souveraineté économique. Le Sisse s'appuie sur un réseau territorial de 21 délégués à l'information stratégique et à la sécurité économiques (Disse), présents dans toutes les régions françaises, qui jouent un rôle clef dans la détection d'alertes de terrain sur les entreprises stratégiques et technologies critiques de la région.

La politique de sécurité économique bénéficie du renforcement du contrôle des investissements étrangers (IEF) qui permet à l'État de mieux contrôler, voire dans certains cas, de s'opposer à des rachats dans des secteurs jugés stratégiques. La liste des activités stratégiques couvertes par le contrôle des IEF s'est élargie en deux vagues successives depuis 2019, avec notamment l'inclusion des biotechnologies en avril 2020 en réponse à la crise sanitaire. Outre la détection précoce des manifestations d'intérêts étrangers pour des entreprises stratégiques, le Sisse est également chargé de coordonner le suivi du respect des engagements imposés aux investisseurs étrangers sur certaines transactions.

Le Sisse veille aussi à la bonne application de la loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères. Il est le référent des entreprises et des professions du droit confrontées à des demandes d'information potentiellement sensibles de la part d'autorités étrangères.

Le Sisse s'occupe aussi de sensibiliser les entreprises françaises, en particulier les PME, TPE, start-up, sur les bons réflexes en matière de sécurité économique. Ce guide pédagogique, téléchargeable sur le site du Sisse, est republié en 2021 pour que tous les acteurs économiques utilisent et pratiquent, La sécurité économique au quotidien en 26 fiches pratiques.

Remerciements

Le Sisse remercie tous les acteurs, publics, parapublics et privés ayant participé, dès 2014, à la rédaction de ces fiches de sécurité économique.

SÉCURITÉ ÉCONOMIQUE GLOBALE

Définition & enjeux
La sécurité économique globale : de quoi parle-t-on ? Quels sont les enjeux ? Pourquoi la pratiquer ?

Les règles et les outils de la compétition économique changent et voient l'émergence de nouveaux acteurs qui bousculent les schémas concurrentiels traditionnels et recomposent les équilibres et les rapports de forces économiques.

Les nouveaux avantages concurrentiels déployés par ces acteurs résultent de stratégies politiques et économiques visant la conquête de marchés, grâce à des leviers jusqu'ici pas ou peu considérés comme stratégiques. L'usage offensif du droit en soutien au développement international en est une des illustrations, notamment au travers des procédures extraterritoriales de conformité.

Dans ce contexte de compétition exacerbée et d'asymétrie des rapports de forces entre pays et entre entreprises, **le premier acteur à adopter un positionnement stratégique**, permettant de placer ses entreprises ou son activité sur les marchés clés de demain, **bénéficiera d'un avantage compétitif majeur.**

Il devient donc d'autant plus important de protéger les atouts économiques, technologiques et scientifiques français, afin de **réduire les risques qu'ils soient captés et exploités** par des acteurs étrangers.

La sécurité économique s'adapte en fonction des enjeux propres à chaque acteur. Pourtant, force est de constater qu'aujourd'hui elle est abordée de façon disparate par les acteurs publics et privés. Dans ce contexte, elle doit devenir un **outil de différenciation positive, un levier au service de la compétitivité** et ne plus être perçue comme une contrainte pesant sur l'entreprise.

La sécurité économique consiste en l'analyse et la réduction des risques extra-financiers pesant sur l'entreprise : la non-conformité, les risques de réputation, de fuites de données stratégiques ou encore d'usage du numérique à des fins malveillantes et, bien évidemment, les risques pesant sur la sûreté et la sécurité des personnes et des biens.

Bien que prise en compte par de nombreuses entreprises, l'évolution de son périmètre, des cadres juridiques applicables et des outils concrets pouvant être mis en place, justifient un partage et des recommandations.

Enfin, la sécurité économique est l'affaire de l'ensemble de l'organisation, du dirigeant jusqu'à l'employé. **Tous doivent être impliqués** et conscients que chacun, en fonction de son rôle, concourt à la sécurité économique de son entreprise, qu'il s'agisse d'un grand groupe, d'une start-up, d'une petite et moyenne entreprise (PME), d'une entreprise de taille intermédiaire (ETI) mais aussi d'un organisme de recherche.

MODE D'EMPLOI

Comment aborder ce recueil de fiches ?

Ces fiches s'adressent à un public très large. Toutes les entreprises quelle que soit leur taille, les organismes de recherche et les administrations sont regroupés sous le terme générique « d'entreprise », qui ne recouvre qu'imparfaitement la réalité de nombreuses structures concernées par la sécurité économique, notion d'entité ou d'établissement au sens large.

Chaque thématique est traitée sous différents angles afin de tenir compte de tous les aspects de la vie de « l'entreprise ».

Ainsi, selon les thèmes, les différentes préconisations sont regroupées autour de trois rubriques principales :

- des recommandations d'ordre « ORGANISATIONNEL» qui s'adressent, de prime abord, aux managers,
- des recommandations d'ordre «TECHNIQUE» qui s'adressent principalement aux responsables de la sécurité des systèmes d'information, des locaux ou de la logistique, mais aussi parfois à chaque employé qui peut appliquer lui-même certaines prescriptions très simples,
- et enfin des recommandations d'ordre « COMPORTEMENTAL» qui s'adressent à tout un chacun, quel que soit son niveau dans la hiérarchie et son poste de travail.

Pour une plus grande clarté et afin de permettre aux lecteurs d'accéder rapidement à l'information recherchée, nous avons regroupé les fiches en sept familles qui sont :

A – PENSER LA SÉCURITÉ ÉCONOMIQUE

B – DANS L'ENTREPRISE

C – PROTÉGER SON PATRIMOINE

D – LA CONDUITE DES AFFAIRES

E – LE NUMÉRIQUE

F – COMMUNIQUER

G – À L'EXTÉRIEUR DE L'ENTREPRISE

Dans chaque fiche il est possible d'approfondir une notion grâce aux rubriques, « Mots-clés *» et «* Pour aller plus loin *». La première rubrique précise termes ou notions abordés dans la fiche. La seconde propose un accès rapide à des compléments sur le sujet, grâce à des liens hypertextes.*

A1. Mener une politique de sécurité économique au sein de l'entreprise

La sécurité économique au sein d'une entreprise ou d'un établissement ne peut se résumer à des mesures techniques ou organisationnelles ponctuelles. Pour être pleinement efficace, elle suppose la mise en œuvre d'une véritable politique indispensable à la préservation de ses intérêts, de ses savoir-faire et de son capital informationnel. Cette politique implique l'ensemble des personnels par le biais d'une stratégie de management globale adaptée au fonctionnement de chaque entité.

ORGANISATIONNEL

➤ Identifier les risques, les menaces et les vulnérabilités de l'entreprise *via* un diagnostic général.

➤ Affecter des moyens (humains, financiers, matériels, etc.) adaptés à la mise en œuvre d'une politique de sécurité économique rigoureuse. Nommer un, ou des responsables, en charge de la sûreté et de la sécurité des systèmes d'information.

➤ Impliquer l'ensemble des métiers à travers des procédures dédiées et des mises à jour.

➤ Définir et prioriser les objectifs. Suivre régulièrement leurs réalisations au travers d'audits et de tableaux de bord.

➤ Mettre à disposition de l'ensemble du personnel, des supports de communication destinés à la sensibilisation interne (intranet, plaquettes de communication, notes de service, etc.). Ceux-ci doivent être simples, accessibles à tous et actualisés régulièrement.

➤ Mettre en place des actions de sensibilisation et de formation adaptées à chaque service ou corps de métiers de l'entreprise.

➤ Organiser un dialogue régulier sur les problématiques de sécurité, tant horizontalement que verticalement. En fonction des ressources, constituer un comité « sécurité économique » au sein de l'entreprise, réunissant les responsables sûreté/intelligence économique et les cadres dirigeants. Planifier la réunion de ce comité sur une base régulière afin d'échanger/rendre compte/discuter des sujets se rapportant à la sécurité de l'entreprise.

➤ Évaluer dans quelle mesure l'entreprise peut bénéficier de l'aide proposée par l'État dans le cadre de dispositifs réglementaires type **protection du potentiel scientifique et technique de la nation** (PPST) (cf. annexe 3). Contacter sans hésiter, les services étatiques de sécurité économique (cf. annexe Contacts utiles) chaque fois qu'une situation apparait anormale.

COMPORTEMENTAL

➤ Se rendre accessible et rester à l'écoute sur toutes les questions de sécurité économique et remarques formulées par les équipes.

➤ Ne jamais sous-estimer l'importance d'un fait inhabituel ou d'un incident de sécurité et ne pas hésiter à le signaler, de préférence par écrit au responsable de la sécurité (cf. annexe 1).

Mots clés

Le rapport d'étonnement : compte rendu à adresser au responsable sûreté de l'entreprise relatant toute situation anormale ou inhabituelle (lors d'un déplacement ou au sein/aux abords de l'entreprise). L'ensemble de ces rapports permettra au responsable sûreté de disposer d'une vision générale des vulnérabilités de son entreprise afin d'adapter la politique de sécurité en lien avec les autorités.

Pour aller plus loin

- Le rapport d'étonnement, cf. annexe 1
- Le dispositif de PPST, cf. annexe 3

A2. Mettre en place un processus de veille au profit de la sécurité économique

La bonne information, diffusée au bon moment et à la bonne personne, concourt à renforcer la sécurité économique de l'entreprise. Elle lui permet d'anticiper les évolutions de son environnement afin de s'y adapter. La veille informationnelle permet de suivre l'apparition d'un nouveau cadre réglementaire, la parution d'appels d'offres ou l'émergence de nouveaux concurrents, mais aussi d'identifier les risques pesant sur l'activité de l'entreprise, comme la défaillance d'un fournisseur clé. Trop souvent réalisée de manière informelle, la veille doit impliquer l'ensemble du personnel, de la direction jusqu'aux salariés, et s'inscrire dans une démarche structurée.

ORGANISATIONNEL

Connaître son capital-information déjà disponible

➤ L'entreprise dispose déjà bien souvent de nombreuses informations, pas ou peu exploitées. Elles constituent pourtant la **première source** d'informations utiles à la décision.

Identifier précisément son besoin en information

➤ Face à la quantité de données disponibles, vouloir « tout connaître sur tout » est le meilleur moyen de ne rien savoir. **Prioriser ses besoins** est donc nécessaire.

➤ Afin d'obtenir les informations les plus pertinentes, il est recommandé d'exprimer le plus **précisément** possible son besoin (thèmes et axes de recherche précis).

➤ Penser à surveiller les **acteurs clés** du sujet (grands groupes, PME, influenceurs, opposants, etc.).

➤ Définir l'**échelle géographique** de recherche (locale, régionale, nationale, européenne, internationale).

S'organiser

➤ Penser une organisation interne prenant en compte toutes les étapes du cycle de l'information :

- qui collecte l'information ?
- qui l'analyse ?
- qui la diffuse et à qui ?
- à quelle régularité et sous quelle forme ?

TECHNIQUE

➤ Se doter d'**outils** de veille adaptés à la taille de l'entreprise et à ses besoins, qu'ils soient gratuits ou payants.

➤ **Diversifier ses sources** d'informations, en recourant notamment à divers moteurs de recherche, sans oublier les blogs, les forums et les réseaux sociaux.

COMPORTEMENTAL

➤ La veille est avant tout un **état d'esprit** : il s'agit d'être en alerte permanente sur les sujets intéressants l'entreprise afin de capter, de transmettre et d'analyser toute information utile.

➤ Capitaliser les connaissances issues du terrain : une **démarche collaborative** doit permettre à l'ensemble du personnel de pouvoir contribuer à la veille.

A3. Identifier l'information stratégique à protéger

Tout entreprise dispose d'une quantité d'informations conséquente, qu'elles soient produites en interne ou émanant de tiers (fournisseurs, clients, partenaires financiers, etc.). Elles ne peuvent bien évidemment pas être protégées toutes de la même façon, au risque de paralyser l'activité de l'entreprise. Une analyse précise des risques est donc un préalable indispensable pour identifier les informations qui sont véritablement stratégiques.

ORGANISATIONNEL

En concertation avec l'ensemble des directions de l'établissement :

➤ Collationner l'ensemble des informations détenues ;

➤ Identifier la sensibilité des informations en fonction du préjudice qu'engendreraient leur divulgation, leur perte ou leur destruction pour la vie de l'entreprise (impact faible, moyen, fort – cf. grille *infra*).

Exemples de questionnement

La perte, la destruction ou la divulgation de cette information est-elle de nature à engendrer … :
… un dommage pour l'activité de la structure ou le déroulement d'un projet ?
… un impact financier ou technique ?
… un impact sur le personnel ?
… un impact en matière d'image et de réputation ?
… une incidence sur la confiance des actionnaires ou des banques ?
… une perte de confiance d'un client ou d'un partenaire important ? Etc.

➤ Évaluer l'occurrence de réalisation du risque, tout en appréciant en particulier s'il s'agit de risques humains et/ou techniques.

Exemple de questionnement

Qui, en interne ou en externe, a accès à cette information ?
Les droits d'accès à l'information sont-ils régis (très limités, restreints, libres) ?
Comment cette information est-elle conservée ? Une sauvegarde régulière est-elle prévue ?
L'information doit-elle être transportée sur un support numérique ou autre ?
Comment les échanges d'informations sont-ils opérés ?
Etc.

➤ Agréger les résultats obtenus dans un outil d'analyse, comme par exemple un tableau de criticité.

Exemple de grille de criticité :

			IMPACT				
			Catastrophique	Majeur	Modéré	Mineur	Insignifiant
			5	4	3	2	1
Probabilité d'occurence	Très forte	5					
	Forte	4					
	Moyenne	3					
	Faible	2					
	Très faible	1					

➤ En fonction du classement obtenu, appliquer des mesures de protection adaptées et établir une politique de gestion de l'information (accès, diffusion, reproduction, archivage, destruction, etc.). Les informations les plus critiques doivent toujours faire l'objet d'une protection renforcée.

➤ Une information identifiée comme stratégique à un moment donné ne le reste pas forcément, ce qui doit pousser à réitérer périodiquement la démarche.

Au-delà de la seule information stratégique à protéger, cette démarche peut s'appliquer pour l'ensemble des informations nécessaires à la bonne continuité de l'activité de l'entreprise en cas de sinistres (incendie, inondation, catastrophe naturelle, etc.).

Pour aller plus loin

Le *Cloud Act* : conséquences en matière de sécurité économique et juridique

La loi américaine du 23 mars 2018, dite « *Cloud Act* », visant à clarifier l'usage des données hébergées par des opérateurs américains hors du territoire des États-Unis en matière judiciaire, soulève des risques quant à la protection des données des entreprises françaises recourant à des fournisseurs de services numériques soumis à la juridiction américaine. Sur réquisition, hors de toute convention d'entraide judiciaire internationale, elle permet aux autorités américaines d'exiger, de la part des hébergeurs et opérateurs du numérique américains la communication des données qu'ils abritent, quel que soit le lieu où ces données sont localisées dans le monde. Cette loi facilite ainsi l'accès des autorités précitées aux données des utilisateurs européens, qu'elles soient ou non dans le *cloud*, sans que ni les utilisateurs concernés ni les autorités compétentes des pays où ils sont établis n'aient à en être informés. Cette loi présente, dès lors, des risques potentiels, à la fois en matière de protection des données personnelles des citoyens européens et de données sensibles des entreprises.

L'entreprise doit prendre en compte ce risque lorsqu'elle fait appel à un fournisseur américain de services de communications électroniques soumis aux obligations du *Cloud Act*.

B1. Protéger ses locaux

S'il paraît évident de fermer la porte de son domicile, il est tout aussi indispensable de veiller à ce que seules les personnes dûment autorisées entrent et sortent de l'entreprise que l'on dirige ou dans laquelle on travaille.

ORGANISATIONNEL

➤ Désigner un responsable sûreté, connu de l'ensemble des salariés, chargé de la rédaction des procédures et du contrôle de la mise en œuvre.

➤ Prendre en compte les risques liés à l'environnement immédiat : le voisinage, les bâtiments adjacents, etc.

➤ Identifier les flux d'entrées et de sorties au sein de l'entreprise (personnes, informations, marchandises, fluides/énergies, etc.).

➤ Hiérarchiser les zones à protéger en fonction des risques, des acteurs, du fonctionnement de l'entreprise, et adapter les mesures de sécurité en conséquence. Eviter de placer les zones les plus sensibles dans des locaux trop vulnérables.

➤ Réglementer l'accès aux différentes zones en fonction des nécessités réelles de chacun.

➤ Établir un journal des incidents, des reports et alertes.

➤ Sensibiliser régulièrement les personnels aux règles de sécurité du site et prévoir les formations adaptées en y associant les sociétés prestataires de services et les partenaires aux dispositifs internes de protection des locaux.

➤ Évaluer périodiquement la performance du système de contrôle d'accès : audits internes, exercices, tests d'intrusion, vérification des délais d'intervention, etc.

➤ Centraliser les systèmes de sûreté (contrôle d'accès, détection d'intrusion, vidéo surveillance) au sein du poste central de sécurité sous la supervision du responsable de la sûreté.

➤ Prévoir une gestion rigoureuse des clés et badges d'accès.

Les moyens de protection mécaniques

TECHNIQUE

➤ Délimiter le périmètre de l'entreprise en utilisant une signalétique appropriée (panneau de l'entreprise, propriété privée, etc.).

➤ Organiser, en fonction des possibilités, une protection graduée multipliant les obstacles :
- prévoir une clôture d'enceinte adaptée aux risques (hauteur, épaisseur, etc.). Utiliser la végétation comme barrière naturelle si le site le permet (haie-vive, aubépine, etc.) ;
- équiper le site et ses abords d'un système d'éclairage dissuasif ;
- veiller au niveau de sécurité des ouvertures (portes, fenêtres et volets) afin de limiter tout risque d'intrusion ;
- instaurer un système de contrôle d'accès adapté. Opter pour un système qui prendra en considération la nature des activités menées et préservera la fluidité des flux : humains, marchandises et véhicules.

Les moyens de protection logiques

TECHNIQUE

➤ Prévoir un système de détection des intrusions, périphérique, périmétrique et volumétrique (barrières anti-instrusion, hyperfréquence, etc.). Au besoin, associer au système anti-intrusion une vidéosurveillance couplée, *en veillant à respecter la législation en vigueur concernant son utilisation.*

➤ En fonction du besoin, prévoir un gardiennage éventuellement associé au système de vidéosurveillance.

COMPORTEMENTAL

➤ Alerter immédiatement le responsable sûreté de tout problème ou événement inhabituel survenu sur le site.

Pour aller plus loin

Le réseau des référents sûreté

Les référents sûreté sont des gendarmes ou des policiers ayant suivi une formation spécifique. Ils sont en mesure de vous apporter, gratuitement, des conseils sur les plans législatif, matériel ou humain, abordant de la sorte les dispositifs envisagés pour diminuer le passage à l'acte.

B2. Accueillir et encadrer du personnel temporaire

L'accueil de personnels temporaires (stagiaire, intérimaire, prestataire, etc.) fait partie du quotidien de la vie de l'entreprise. Néanmoins, ils peuvent être les cibles ou les auteurs d'une malveillance. Ainsi, une attention particulière doit être portée à leur encadrement et à leur accès à l'information.

ORGANISATIONNEL

➤ Mettre en place un processus amont visant à bien connaître le parcours du futur personnel temporaire avant qu'il n'arrive.

➤ Avant acceptation du contrat, faire en sorte que les informations relatives à la mission du personnel temporaire soient bien partagées par tous les services concernés (RH, SSI, sécurité, administratif, opérationnel).

➤ Désigner en interne une personne qui sera responsable de l'encadrement du personnel temporaire tout au long de son séjour dans l'entreprise.

➤ Tenir à jour un répertoire des personnels non permanents. Peuvent notamment y être précisées les données suivantes :

- nom et prénom, date et lieu de naissance, adresse,
- références de la CNI pour un ressortissant français, du titre de séjour et du passeport pour un étranger,
- nom du responsable de l'encadrement,
- nom de l'accueillant (si différent du responsable de l'encadrement),
- date de début et de fin de contrat ou de convention,
- objet de la mission ou thématique(s) abordée(s),
- autorisations d'accès géographiques et informationnels.

➤ **Prévoir dans le contrat** ou la convention **une clause de confidentialité** spécifiant expressément l'interdiction formelle de toute diffusion d'informations relatives à l'entreprise ou à ses activités, sans l'accord express de celui-ci.

➤ Sensibiliser le personnel temporaire dès son arrivée aux mesures de sécurité exigées par l'entreprise. **Lui faire signer le règlement intérieur et la charte informatique**.

➤ Imposer le port d'un badge spécifique et apparent pour les personnels temporaires.

➤ Apporter une attention particulière aux informations figurant dans les documents produits par les personnels temporaires (rapport de stage, mémoire, livrable, etc.).

➤ Saisir rapidement les services de police ou de gendarmerie compétents en cas de malveillance suspectée. Ne pas essayer de gérer la situation uniquement en interne.

➤ Suivre le parcours des stagiaires durant quelques mois après leur départ.

TECHNIQUE

➤ N'autoriser l'accès aux systèmes d'information qu'à partir d'équipements fournis par l'entreprise, et à l'aide d'un identifiant strictement personnel et tracé.

➤ Limiter l'accès aux ressources informatiques et aux informations strictement nécessaires et en relation directe avec leur sujet de travail.

➤ Clôturer les comptes informatiques des personnels temporaires immédiatement après la fin de leur contrat pour l'entreprise.

➤ En présence de personnel temporaire, n'évoquer que des sujets se rapportant à leur mission.

COMPORTEMENTAL

➤ En cas de non-respect des règles encadrant leur présence dans l'entreprise, alerter sans délai les responsables de l'encadrement et de la sécurité.

B3. Encadrer des visiteurs

Si toute entreprise se doit d'assurer un accueil de qualité pour ses visiteurs (délégations, clients, prestataires, partenaires d'affaires, livreurs..), des règles de sécurité élémentaire doivent toutefois être mises en œuvre.

ORGANISATIONNEL

➤ Impliquer l'ensemble du personnel lors de visites sensibles. Demander à chacun un regain de vigilance.

➤ Adopter des schémas de sécurité conformes à l'objet/la nature de la visite ou du visiteur.

➤ Connaître avant même la visite, l'identité, les coordonnées et la fonction des visiteurs. N'accepter que ceux qui se sont déclarés.

➤ Élaborer formellement une procédure d'accueil des visiteurs quels qu'ils soient. S'assurer que l'ensemble du personnel en a connaissance et la met en œuvre.

➤ Vérifier l'identité des visiteurs à leur arrivée dans l'entreprise. En échange d'un document d'identité, remettre un badge d'accès spécifique, ou un autre signe distinctif, et rendre obligatoire son port apparent.

➤ Prévoir des lieux spécifiquement dédiés à leur accueil (stationnement et réception).

➤ Notifier, si possible dans la langue des visiteurs, les engagements de confidentialité propres à la visite.

➤ Définir un parcours de visite (**circuit de notoriété**) excluant les zones les plus confidentielles.

➤ Définir précisément les informations qui pourront être évoquées au cours de la visite.

➤ Accompagner les visiteurs, dans la mesure du possible en permanence, de leur arrivée à leur départ.

➤ Enregistrer les horaires d'entrées et de sorties des visiteurs et en conserver la trace plusieurs semaines.

➤ Encadrer strictement l'utilisation d'outils numériques (smartphones, appareils photo, lunettes ou montres connectées, clés USB, etc.).

TECHNIQUE

➤ Prévoir un ordinateur dédié, non connecté au réseau, permettant de recevoir les supports amovibles des visiteurs.

COMPORTEMENTAL

➤ Ne pas hésiter à questionner un visiteur non accompagné semblant chercher son chemin et le raccompagner vers son groupe ou son responsable.

➤ Être vigilant aux questionnements trop intrusifs dont pourraient faire preuve certains visiteurs.

➤ Rendre compte immédiatement de tout problème ou événement inattendu survenu lors de la visite.

Mots clés

Circuit de notoriété : circuit préétabli permettant de faire visiter une entreprise, d'en donner une image concrète et valorisante tout en évitant les locaux sensibles.

C1. Protéger son savoir et ses idées

Encore trop souvent négligée, la protection du savoir, du savoir-faire et des idées constitue pourtant un investissement souvent déterminant pour le développement et parfois pour la vie de l'entreprise ou de l'organisme de recherche. De nombreux outils juridiques sont pourtant mis à disposition pour protéger le patrimoine intellectuel des personnes physiques et morales.

ORGANISATIONNEL

Comment protéger son savoir et ses idées ?

➤ Identifier, parmi les différents titres de propriété intellectuelle (**brevets, marques, dessins et modèles, droits d'auteur,** etc.) ceux qui sont les mieux adaptés pour protéger et valoriser ses innovations, ses produits ou ses créations immatérielles.

➤ Avant de déposer une marque, un dessin et modèle ou un brevet, vérifier auprès de l'**Institut national de la propriété industrielle (Inpi)** la disponibilité du droit à protéger (recherches d'antériorité) pour s'assurer du caractère nouveau de la création. Examiner la nécessité de se faire assister d'un conseil en propriété intellectuelle.

➤ Identifier les marchés (national, communautaire, international), présents et futurs, sur lesquels protéger ses droits. Si des droits sont présents à l'international, se renseigner auprès du réseau d'experts à l'international (Douanes, Inpi, Business France, **conseillers du commerce extérieur**, CCI Innovation, etc.).

➤ Enregistrer ses droits auprès des offices compétents (Inpi, l'**Office de l'Union européenne pour la propriété intellectuelle, EUIPO** ; l'**Office européen des brevets, OEB** ; l'**Organisation mondiale de la propriété intellectuelle, Ompi**).

➤ Faire enregistrer les noms de domaine liés aux titres et à l'activité commerciale auprès de l'**Agence française pour le nommage sur internet en coopération (Afnic)**.

Quelles démarches adopter pour se prémunir de la contrefaçon ?

➤ Mettre en place une veille, notamment sur internet, afin de détecter et de se prémunir des **contrefaçons**.

➤ Déposer une demande d'intervention auprès des Douanes qui permettra de mettre en retenue des marchandises suspectées d'être contrefaisantes et d'alerter le propriétaire du droit. Cette demande gratuite est valable un an renouvelable.

➤ Protéger ses créations par une confidentialité stricte des documents relatifs aux droits et aux produits : signature de clauses de confidentialité, protection physique et numérique des documents, etc.

➤ Faire immédiatement opposition auprès de l'Inpi, ou de tout autre office compétent, dès qu'une personne dépose un droit déjà détenu par l'entreprise. Examiner sans délai la nécessité de se faire assister d'un avocat ou d'un conseil en propriété intellectuelle.

Quelle attitude adopter en cas de contrefaçon ?

➤ Mettre en demeure le contrefacteur de cesser les actes de contrefaçon en lui envoyant un courrier lui rappelant ce qu'il encourt à enfreindre les droits de propriété intellectuelle en question.

➤ Communiquer aux autorités compétentes, en particulier aux Douanes, les informations dont dispose l'entreprise sur la contrefaçon : circuit de fraude, identité des contrefacteurs, caractéristiques des marchandises contrefaites, etc.

➤ Ne pas hésiter à intenter une action en justice, devant les juridictions civiles ou pénales, contre le présumé contrefacteur afin de faire cesser l'infraction et d'obtenir des dommages et intérêts.

Mots clés

Brevet : le brevet protège temporairement une innovation technique et industrielle. Pour être brevetable, une invention doit être nouvelle, sa conception doit être inventive et susceptible d'une application industrielle. **Attention**, il n'est pas possible de protéger une idée par un brevet, seuls les moyens techniques mis en œuvre pour la concrétiser le seront.

Marque : au sens de la propriété intellectuelle, la marque est un « signe » servant à distinguer précisément vos produits, ou services, de ceux de vos concurrents. Elle peut être notamment sonore, figurative, tridimensionnelle et même olfactive.

Dessins et modèles : l'apparence des produits peut être protégée au titre des « dessins et modèles », selon qu'elle matérialise un assemblage de lignes et de couleurs en deux dimensions (dessins) ou une forme modélisée en trois dimensions (modèles).

Droit d'auteur : le droit d'auteur est un droit de propriété exclusif acquis sans formalité d'enregistrement dès sa création sur toutes les œuvres de l'esprit quels que soient leur genre (littéraire, musical, scientifique et technique) et leur mode d'expression.

Contrefaçon : la contrefaçon est l'utilisation sans autorisation d'un droit de propriété intellectuelle.

Les droits de propriété intellectuelle couvrent principalement :

- la propriété industrielle> marques, dessins et modèles, brevets ;

- la propriété littéraire et artistique > droit d'auteur et droits voisins du droit d'auteur.

Inpi : l'Institut national de la propriété industrielle, établissement public placé sous la tutelle des ministères Économiques et Financiers, est l'organisme compétent pour la délivrance des titres de propriété industrielle nationaux (marques, brevets, dessins et modèles).

EUIPO : l'Office de l'Union européenne pour la propriété intellectuelle est l'agence de l'Union européenne compétente pour l'enregistrement des marques et des dessins ou modèles valables dans les pays de l'UE.

OEB : l'Office européen des brevets offre aux inventeurs une procédure uniforme de demande de brevet, leur permettant d'obtenir une protection par brevet dans un maximum de 40 pays européens.

Ompi : l'Organisation mondiale de la propriété intellectuelle permet d'enregistrer ses marques, dessins et modèles à l'échelle internationale.

Afnic : l'Association française pour le nommage internet en coopération est une association loi 1901 en charge de la gestion des extensions françaises d'internet.

C1. Protéger son savoir et ses idées

Pour aller plus loin

➤ **Institut national de la propriété industrielle (Inpi)**

Guide Protéger ses créations

➤ **Comité national anti-contrefaçon (Cnac)**

Ce comité regroupe tous les partenaires publics et privés impliqués dans la lutte anti-contrefaçon.

➤ **Union des fabricants (Unifab)**

Créée en 1872, l'Union des fabricants regroupe plus de 200 entreprises ainsi que des fédérations professionnelles. Elle promeut la protection internationale de la propriété intellectuelle et lutte contre la contrefaçon en menant des opérations de lobbying, de formation et de sensibilisation.

➤ **Direction générale des Entreprises**

Boîte à outils des PME

Guide contrefaçon PME

➤ **Dispositif France - PME sans contrefaçons**

« France - PME sans contrefaçons », piloté par le Comité national des conseillers du commerce extérieur de la France (CNCCEF), le dispositif a vocation à soutenir les PME françaises dans leur stratégie anti-contrefaçon à l'export.

Les PME, victimes de contrefaçons ou susceptibles de l'être, peuvent saisir la commission technique nationale « France - PME sans contrefaçons » afin de :

- bénéficier gratuitement d'audits confidentiels et d'un accompagnement personnalisé,
- être orientées vers les bons interlocuteurs publics et privés de la lutte contre la contrefaçon.

Guide du dispositif France – PME sans contrefaçons

➤ **Direction générale de la Concurrence, de la consommation et de la répression des fraudes** (DGCCRF)

C2. Éviter ou gérer la perte d'une compétence clé

La seule ressource véritablement durable de toute organisation est l'humain. De par leur valeur, les compétences clés peuvent faire l'objet de convoitises de la part de concurrents plus ou moins loyaux. La perte de ses compétences pouvant avoir des conséquences irrémédiables, il convient de mettre en place des mesures préventives mais aussi réactives pour limiter l'exposition de l'entreprise.

ORGANISATIONNEL

Anticiper et préserver les compétences clés

➤ Cartographier les compétences clés en anticipant la stratégie de développement de l'entreprise et les perspectives du marché.

➤ Développer une veille sur les offres d'emploi du secteur, notamment de la concurrence, ainsi que sur le climat social interne.

➤ Garder à l'esprit que le cloisonnement des missions, des activités et des compétences internes accroît les risques de départ.

➤ Favoriser, par la formation interne, le partage des bonnes pratiques et des compétences.

➤ Établir en amont les schémas d'intervention en cas de vacance d'un poste (personnes relais, délégations de décision, de signature, etc.).

➤ Fidéliser les compétences clés par une politique de gestion des ressources humaines personnalisée (motivation, intéressement, actionnariat, etc.). Profiter notamment des entretiens annuels afin de réévaluer les salaires/primes, les conditions de travail, les projets souhaités, les qualifications, les avantages, etc.

Sur le plan juridique

➤ Garder à l'esprit que le dépôt d'un brevet peut renseigner sur l'existence d'une compétence-clé. Etablir une stratégie interne en matière de propriété intellectuelle et, le cas échéant, se rapprocher d'un cabinet spécialisé.

➤ Formaliser dans les contrats de travail des clauses de confidentialité (durée, champs d'application, etc.), de loyauté (non-concurrence clairement définie dans le temps, l'espace géographique et la contrepartie financière, afin d'éviter son annulation), de dédit-formation (remboursement de la formation par le collaborateur). Veiller à harmoniser ces clauses pour l'ensemble de l'entreprise.

➤ Souscrire, le cas échéant, pour une compétence rare, une police d'assurance « personne clé » ; penser à son adaptation et à son renouvellement.

Agir face à la perte

Réactions à l'annonce du départ

➤ Analyser immédiatement l'impact potentiel de la perte subie en termes d'image et/ou de pertes d'informations stratégiques.

➤ Sécuriser le départ pour que le préavis ne soit pas source de problèmes pour l'entreprise : procédures informatiques, documents officiels, badges d'accès, clefs, téléphones, etc.

➤ Rappeler à l'intéressé le cadre contractuel dans lequel il se situe et, en particulier, les contraintes le liant par des clauses spécifiques.

Après le départ

➤ Mesurer l'impact de la perte subie : quel concurrent a bénéficié de la compétence-clé ? Y a-t-il eu des divulgations sur le savoir-faire de l'entreprise ? Les clauses ont-elles été respectées par le collaborateur et l'entreprise ? etc.

➤ En interne, identifier précisément le « manque » observé et déterminer rapidement l'organisation permettant d'y pallier aux mieux en attendant un éventuel recrutement externe.

➤ Effectuer un retour d'expérience avec les collègues, les supérieurs et la DRH pour comprendre les raisons de cette perte de compétence-clé et mettre en place les mesures correctives nécessaires.

C3. Gérer ses archives et ses rejets

Les archives et les rejets de l'entreprise peuvent renseigner des concurrents, ou des acteurs malveillants à la recherche d'informations techniques, commerciales et même privées. Il convient d'y accorder une attention particulière.

Archives papiers et numériques

ORGANISATIONNEL

➤ Mettre en place une solution de suivi, un plan de classement et d'archivage spécifique pour les supports d'information dont le contenu est stratégique.

➤ Former les collaborateurs à une gestion précise (sauvegarde, niveau de sensibilité, durée de vie, etc.) des documents qu'ils créent (notes manuscrites, courriers électroniques, fichiers numériques, bordereaux, etc.).

➤ Mettre en place une procédure de traçabilité de la consultation des différentes formes d'archives.

➤ En cas d'externalisation des archives numériques, encadrer strictement le contrat avec le prestataire.

➤ Insérer dans les contrats de location de matériels informatiques (serveur, unité centrale, imprimante multifonction, télécopieur, etc.) des clauses spécifiques prévoyant la conservation des disques durs ou leur destruction sécurisée.

➤ Fournir et gérer les supports d'archivage amovibles vérifiés, notamment dans le cadre du télétravail (clé USB, disque dur externe, etc.). Interdire tout support d'archivage privé.

TECHNIQUE

➤ Conserver les archives papier et numériques dans des locaux sécurisés et adaptés (restriction d'accès, protection contre les sinistres, etc.).

➤ Archiver les données stratégiques avec des précautions particulières (coffre-fort, chiffrement, etc.).

➤ Tester régulièrement l'intégrité des documents numériques archivés.

Déchets matériels et numériques

ORGANISATIONNEL

➤ Définir une politique interne de gestion des déchets professionnels, y compris dans le cadre du télétravail.

➤ Sensibiliser les collaborateurs au fait qu'une simple suppression des données ne constitue pas une réelle destruction.

➤ Sélectionner ses prestataires extérieurs en charge de l'évacuation des déchets sur des critères de fiabilité et de sûreté.

➤ Identifier précisément les personnes physiques en charge de l'évacuation des déchets (ménage, etc.). Faire respecter l'obligation du port du badge apparent.

TECHNIQUE

➤ Mettre à disposition un broyeur à coupe croisée pour détruire de manière sécurisée les documents sensibles (papiers, CD, DVD, etc.).

➤ Installer sur chaque poste de travail un logiciel d'effacement sécurisé.

➤ Détruire ou effacer de façon sécurisée les mémoires internes des équipements informatiques en fin de vie ou en fin de contrat (imprimante, fax, photocopieur, etc.).

➤ Détruire de façon sécurisée les prototypes et résidus de matériaux innovants mis au rebut afin d'empêcher toute récupération à des fins de rétro-ingénierie.

Pour aller plus loin

Agence nationale de la sécurité des systèmes d'information (Anssi)

Liste de produits certifiés d'effacement de données et de stockage sécurisé

D1. Sécuriser ses flux de marchandises

Maîtriser ses flux de marchandises permet de préserver ses atouts industriels tout en participant à la sécurisation de l'ensemble de la chaîne logistique.

Sécuriser ses flux de marchandises entrants

ORGANISATIONNEL

➤ Identifier tous les acteurs de la chaîne d'approvisionnement, du fournisseur au transporteur final, en passant par l'ensemble des prestataires intermédiaires : acheteur, assureur, affréteur et transitaire, compagnie maritime/aérienne, stockeur, représentant en douane enregistré, etc.

➤ Maîtriser, dans la mesure du possible, cette chaîne en organisant le pré-acheminement (recours à des *Incoterms* spécifiques) ou en s'assurant que son fournisseur fasse appel à des prestataires fiables (titulaire d'une autorisation d'**opérateur économique agréé**, par exemple).

➤ Développer une politique interne exigeante dans le choix des fournisseurs, des prestataires de transport et des autres prestataires : privilégier des partenaires connus et fiables, vérifier leur solvabilité, établir des cahiers des charges stricts, etc.

➤ Mettre en place des procédures de contrôle du transport entrant, permettant une traçabilité réelle, à chaque étape de l'acheminement des marchandises : calendrier prévisionnel des arrivées, procédure de traitement des arrivées de marchandises imprévues, contrôle de concordance, marchandise attendue/réceptionnée, etc.

➤ Prévoir un filtrage à l'entrée de l'entreprise (poste de garde, service de réception, etc.) permettant le contrôle du bien-fondé de la livraison, de l'identité du transporteur, et l'orientation vers l'aire de réception du fret.

➤ Sensibiliser l'ensemble du personnel à tout mouvement inhabituel de marchandise.

Garantir l'intégrité des unités de fret au sein de l'entreprise

➤ Délimiter précisément des aires sécurisées de réception : quais de déchargement et zones de stockage des unités de fret.

➤ Limiter l'accès à ces zones aux seuls personnels et entreprises externes autorisés et sensibilisés aux enjeux liés à la sécurité/sûreté (notes internes, protocole de transport).

➤ Vérifier l'intégrité des unités de fret à réception : scellés commerciaux intacts, intégrité physique du moyen de transport.

➤ Contrôler l'état des marchandises : qualité/quantité.

➤ Procéder à la vérification systématique des documents de transport (cohérence, lisibilité, etc.).

➤ Enregistrer précisément tous les problèmes relevés afin de mettre en place des mesures correctives.

Sécuriser le stockage des marchandises

➤ Privilégier le stockage en intérieur, surtout si la marchandise est de forte valeur ou susceptible d'attiser la convoitise. En cas de stockage extérieur, désigner une aire de stockage bénéficiant d'un éclairage adapté, si possible sous surveillance vidéo et éloignée des entrées et enceintes de la société. Dissimuler la nature des marchandises, par exemple sous une bâche.

➤ Limiter strictement l'accès à la zone de stockage aux seules personnes autorisées.

➤ Mettre en œuvre des contrôles internes : procédures d'inventaire régulier, enquête sur les irrégularités, mesures correctives, etc.

TECHNIQUE

➤ Mettre en place un système de surveillance proportionné aux risques liés à la nature de la marchandise.

Protéger sa zone de production de marchandises

ORGANISATIONNEL

➤ Définir une procédure régissant l'accès afin de garantir la sécurité et la sûreté des processus de production.

➤ Sensibiliser le personnel de production au respect de cette procédure.

TECHNIQUE

➤ Mettre en place un système de surveillance proportionnel aux risques liés à la préservation du secret industriel.

Sécuriser ses flux de marchandises sortants

ORGANISATIONNEL

➤ Formaliser des procédures de contrôle du transport sortant.

➤ Délimiter précisément des aires de chargement : quais de chargement, zones de stockage des unités de fret.

➤ Mettre en place une procédure de chargement des marchandises (seul le personnel de la société est autorisé à charger et non le chauffeur du camion, par exemple) avec un contrôle de cohérence des marchandises chargées.

➤ Vérifier la nécessité ou non d'une licence d'exportation : biens à double usage.

➤ Limiter strictement l'accès à la zone de chargement aux seules personnes autorisées.

➤ Vérifier l'existence ou non de sanctions commerciales à l'encontre du pays de destination (cf. cartographie du suivi des sanctions économiques et financières).

TECHNIQUE

➤ Apposer des scellés sur les marchandises sortantes. Stocker ces scellés dans un emplacement sécurisé et tenir un registre de suivi de ce stock.

Comment sécuriser les acheminements ?

ORGANISATIONNEL

➤ Sélectionner ses partenaires commerciaux selon des critères de fiabilité : procédure d'identification, encadrement du recours à la sous-traitance, etc.

➤ Maîtriser, dans la mesure du possible, l'acheminement : soit en choisissant des *Incoterms*

D1. Sécuriser ses flux de marchandises

spécifiques, soit en sensibilisant l'acheteur sur la nécessité de recourir à des prestataires fiables.

➤ Prévoir un suivi des prestataires en matière de sûreté : choix de prestataires agréés, signature de **déclaration de sûreté**, intégration d'une clause de sûreté dans les contrats avec les prestataires réguliers, audits des prestataires, etc.

Mots clés

Opérateur économique agréé (OEA) : la certification OEA atteste le respect de plusieurs critères liés à la gestion de la réglementation douanière et à la prise en compte des risques de sécurité/sûreté. Il existe trois types d'autorisation : OEA Simplifications douanières (OEAC) ; OEA Sécurité/Sûreté (OEAS) ; OEA Simplifications douanières et Sécurité/Sûreté (OEAF) peuvent être combinées. Les entreprises titulaires de l'autorisation OEAS et OEAF ont démontré une prise en compte renforcée des risques liés à la sécurité et à la sûreté. Toutes les entreprises européennes intégrant la chaine logistique internationale (fabricants, exportateurs, importateurs, transporteurs, stockeurs, représentants en douanes enregistrés, etc.) sont éligibles à l'autorisation OEA.

Incoterms **:** « *International Commercial Terms* » ou Conditions internationales de vente. Le but des *Incoterms* est de définir les obligations du vendeur et de l'acheteur lors d'une transaction commerciale, le plus souvent internationale, mais qui peut également s'établir entre des opérateurs nationaux ou communautaires. Ils concernent essentiellement les obligations des parties à un contrat de vente, relatives à la livraison de la marchandise vendue, à la répartition des frais et aux risques liés à cette marchandise, ainsi que la charge des formalités d'export et d'import.

Déclaration de sûreté : document permettant à une société titulaire d'une autorisation OEA d'encadrer juridiquement les prestations réalisées par un prestataire pour son compte.

Biens à double usage (BDU) : par biens à double usage on entend, « les produits, y compris les logiciels et les technologies (ainsi que la transmission de logiciels ou de technologies, par voie électronique, par télécopieur ou par téléphone vers une destination située en dehors de l'Union européenne) susceptibles d'avoir une utilisation tant civile que militaire ». Ils sont repris dans une liste annexée au règlement européen qui définit le cadre juridique applicable en la matière. Ce sont des biens sensibles qui, dans la plupart des cas, sont destinés à des applications civiles, mais qui peuvent être utilisés à des fins militaires ou qui pourraient sensiblement renforcer les capacités militaires des pays qui les acquièrent.

Pour aller plus loin

➤ Douane
- En savoir plus sur le statut d'opérateur économique agréé et déposer sa demande
- Guide sur les exportations de biens et technologies à double usage
- Informations pratiques sur les Incoterms
- Restrictions commerciales à l'encontre de certains pays

➤ Direction générale des Entreprises (DGE)

Service des biens à double usage (SDBU)

D2. Protéger juridiquement son entreprise

De plus en plus d'acteurs économiques utilisent les failles du droit positif pour déstabiliser leurs concurrents. Penser la protection juridique de son entreprise permet d'entraver les manœuvres hostiles et donc de limiter ce risque.

ORGANISATIONNEL

➤ Faire vérifier par un expert que les activités de l'entreprise sont suffisamment protégées sur le plan juridique : conditions générales de vente, contrats de travail, droits de propriété intellectuelle.

➤ Se méfier des modèles de statuts et de contrats en libre accès sur internet. Ils ne protègent l'entreprise que de façon imparfaite, soit parce qu'inadaptés à la situation réelle, soit parce que la rupture des liens contractuels n'a pas été valablement envisagée.

➤ Prévoir **des clauses de confidentialité** dans les contrats de travail des collaborateurs, des intérimaires et dans les conventions de stages.

➤ Prévoir des **clauses de non-concurrence** dans les contrats de travail des personnes occupant des postes clés.

➤ Prévoir des **clauses spécifiques pour le partage d'information** et la confidentialité dans les contrats avec les fournisseurs, les sous-traitants et les distributeurs.

➤ Prévoir des **clauses de non-débauchage** pour les collaborateurs avec lesquels ils sont en contact.

➤ Vérifier, dans les contrats avec des tiers, les clauses liées au règlement des litiges : veiller à bien choisir le tribunal compétent ; prévoir des clauses de médiation et/ou d'arbitrage adaptées aux enjeux.

➤ Veiller à faire protéger juridiquement par un expert tous les éléments immatériels de l'entreprise qui sont susceptibles de faire l'objet de contrefaçons ou d'usurpation : nom de la société, nom de domaine, marque, modèle, brevet, etc.

➤ En cas d'inquiétude ou d'incident avéré, prendre rapidement contact avec son avocat ou son conseil juridique et, si nécessaire, avec les services compétents de l'État. Ne pas hésiter à agir en justice, notamment en cas de faux procès, faux appels d'offres, faux brevets, etc., paraissant uniquement destinés à recueillir de l'information.

➤ Intégrer les conséquences juridiques potentielles de la transformation numérique de l'entreprise (comme le recours au *Cloud Computing*, cf. Annexe sur le *Cloud Act*).

➤ Actualiser les contrats et les protections juridiques de l'entreprise au gré des évolutions législatives et de la vie de l'entreprise.

Mots clés

Clause de confidentialité : article d'un contrat qui garantit la non-divulgation à des tiers d'informations dont la ou les personne(s) aurai(en)t connaissance de par ses (leurs) fonctions. Peut s'appliquer à un salarié ou à un partenaire : fournisseur, distributeur, société en *joint-venture* ou distributeur.

Clause de non-concurrence : clause permettant à un employeur de se prémunir contre la concurrence que pourrait lui faire un salarié à l'expiration du contrat de travail.

Clause spécifique pour le partage d'information : la clause de partage d'information définit les modalités du partage et établit les règles de coopération entre l'entreprise et les tiers avec lesquels elle est en affaires en matière d'information. Elle vise à s'assurer que les informations nécessaires et suffisantes ont bien été portées à la connaissance du tiers, notamment pour l'exécution de sa mission, ou, à l'inverse, que certaines informations liées à la réalisation d'une mission seront bien intégrées, en toute transparence, aux rapports, au suivi, aux bilans.

Clause de non-débauchage : cette clause interdit à la société qui signe le contrat de débaucher l'employé missionné, sous peine de verser un dédit financier plus ou moins important à son client, partenaire, etc. Elle est aussi appelée **clause de non-sollicitation**.

La loi n° 68-678 du 26 juillet 1968 dite « loi de blocage » : ce texte encadre les demandes de communication d'informations économiques sensibles émises par des personnes étrangères, physiques ou morales, auprès d'entreprises françaises. Ces requêtes, après saisine préalable des autorités administratives françaises, sont réorientées vers les mécanismes de coopération internationale. Cet outil législatif vise à éviter deux dérives, la première tenant à la portée extraterritoriale de lois étrangères, la seconde relative aux contournements des accords d'entraide judiciaire internationale lors de requêtes d'information à fin de preuves. Elle permet de protéger les informations détenues par les entreprises françaises dont la divulgation porterait atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public. Elle peut enfin, entraîner des sanctions pénales en cas de non-respect de l'interdiction de communication en dehors des mécanismes de coopération (édictée aux articles 1er et 1er bis de la loi).

Bien que s'appuyant sur une jurisprudence jusqu'à présent encore réduite, la « loi de blocage » est utilisée par les entreprises afin de limiter les risques de perte totale de maitrise des données les plus sensibles, lors de requêtes d'autorités étrangères.

Le Sisse a pour mission, sur la base du décret n° 2019-206 du 20 mars 2019 relatif à la gouvernance de la politique de sécurité économique, en lien avec les ministères concernés, de veiller à l'application des dispositions de la loi du 26 juillet 1968 par les personnes qui y sont assujetties, sous réserve des compétences attribuées par la loi en cette matière à une autre autorité et, le cas échéant, en lien avec celle-ci.

Pour aller plus loin

➤ Institut national de la propriété industrielle (Inpi) :
Comment protéger quoi ?

D3. Sécuriser ses relations commerciales

La construction de relations commerciales avec des partenaires extérieurs (financeurs, clients, fournisseurs, prestataires, etc.) fait partie de la vie quotidienne de l'entreprise. Ces relations constituent néanmoins des actes dont les conséquences peuvent être gravement préjudiciables s'ils ne sont pas réalisés avec la vigilance et la rigueur nécessaires.

ORGANISATIONNEL

➤ Mettre en place une veille sur ses principaux fournisseurs, distributeurs et clients (actualités commerciales, évolution du management, difficultés financières, etc.).

➤ À l'occasion des appels d'offre entrants/sortants, ne diffuser que les informations strictement nécessaires et, au besoin, protéger celles-ci par des clauses de propriété intellectuelle et de confidentialité.

➤ Adapter ses conditions générales de vente en fonction du type de clientèle (particuliers, professionnels).

➤ Éviter d'utiliser des modèles de contrats préétablis, souvent mal adaptés à la spécificité de la relation.

➤ Dans le cas des contrats exports, rédiger le contrat dans une langue parfaitement maîtrisée. Ne pas hésiter à se faire assister par un organisme spécialisé, par un interprète et par un juriste spécialiste du droit local.

➤ Inclure dans les contrats des clauses d'arbitrage et/ou de médiation (cette dernière étant obligatoire dans les contrats de consommation).

➤ Analyser avec attention les enjeux liés au choix de la juridiction compétente.

➤ Prévoir dans les contrats avec les fournisseurs, les distributeurs, les partenaires, des clauses expresses relatives :

- aux échanges d'information et de confidentialité (personnes habilitées, responsabilités respectives, stockage et destruction des informations, etc.) ;
- au non-débauchage de personnel ;
- au respect des législations applicables : emploi des mineurs, marchandage, corruption, etc. ;
- à l'échantillonnage, au prototypage ;
- à la non-concurrence, si la clause est justifiée, proportionnée et limitée, ainsi qu'à l'obligation de signaler toute relation nouvelle avec un concurrent ;
- aux pénalités en cas de rupture d'approvisionnement, de non-respect des délais de livraison et de défaut de qualité ;
- à l'aménagement de la responsabilité des parties.

➤ Attendre, pour verser le premier acompte, que le contrat soit validé et signé par les personnes mandatées.

➤ Respecter rigoureusement la procédure interne de vérification pour toute opération engageant les finances de l'entreprise.

➤ Demander une confirmation écrite pour tout acte engageant l'entreprise et ses partenaires. Confirmer chaque échange ou entrevue par un courriel, un reçu ou un fax à l'en-tête de l'entreprise.

➤ Ne jamais traiter avec des subordonnés du partenaire, ou du prestataire, sans avoir vérifié leur mandat.

➤ Veiller à ce que tous les exemplaires « originaux » des contrats soient numérotés, signés et paraphés. Ne laisser aucune page blanche, aucun blanc, signe ou rature sur les documents. Veiller à ce que chaque partie valide les corrections.

➤ Limiter le nombre de personnes impliquées dans les nouveaux projets, en externe (fournisseurs, distributeurs, etc.) comme en interne, tant que les clauses de confidentialité ne sont pas signées.

TECHNIQUE

➤ Utiliser des salles de réunion plutôt que des bureaux pour les échanges ou séances de travail avec les clients, partenaires et/ou fournisseurs.

➤ Utiliser des équipements informatiques dédiés et « conditionnés » (PC, clef USB, etc.) lors des réunions avec les clients, partenaires et/ou fournisseurs.

D4. Sécuriser son recours aux modes de financements extérieurs

La levée de fonds est une étape importante dans la vie d'un acteur économique mais peut néanmoins comporter des risques de perte d'informations stratégiques, notamment en cas de recours à des plateformes de financement en ligne. Afin de conserver le contrôle sur la gouvernance de son entreprise il s'agit donc d'adopter les bons réflexes.

ORGANISATIONNEL

➤ Définir son besoin en financement, en accord avec la stratégie de l'entreprise. Un besoin à court terme ne doit pas remettre en cause des choix stratégiques.

➤ S'assurer de la bonne réputation des investisseurs contactés, en vérifiant leurs comportements lors d'opérations financières précédentes, en les questionnant sur leur connaissance du secteur d'activité ainsi que sur leurs liens avec la concurrence.

➤ En cas de recours au financement participatif ou en ligne, s'assurer de la probité de la plateforme choisie (réputation, conditions générales d'utilisation, etc.)

➤ Éviter d'entrer en négociation avec des acteurs dont l'étude des investissements passés met en lumière des intentions hostiles pouvant remettre en cause la stratégie de l'entreprise ainsi que sa gouvernance.

➤ Maîtriser sa communication en ne transmettant aucune information stratégique durant les premiers échanges jusqu'à la signature par l'investisseur d'une **lettre d'intention** accompagnée d'un accord de confidentialité.

➤ Limiter dans le temps la période d'investigation et encadrer l'accès des auditeurs au système d'information interne ainsi qu'aux données de l'entreprise. Ne pas hésiter à lister les informations qui leur sont transmises.

➤ Désigner les salariés impliqués dans les négociations. Selon leurs contrats de travail, prévoir de leur faire signer un accord de confidentialité et de leur rappeler les risques potentiels de divulgation d'informations stratégiques.

➤ Porter une attention particulière aux clauses et dispositions statutaires qui, en cas de différend, pourraient être exploitées : droits de vote, nomination et révocation des dirigeants et administrateurs, minorité de blocage, accès et convocation aux assemblées générales, etc.

➤ Rester toujours maître de la décision quant au choix de l'investisseur, sans se laisser influencer.

Mots clés

La lettre d'intention : lettre formalisant la proposition d'un investisseur à l'attention de l'entreprise cible à l'issue des négociations et des audits, précisant le cadre des échanges à venir. Encadrée par le Code civil depuis 2006, elle est non contraignante et à durée limitée mais a force probatoire en cas de différend entre les parties.

D5. Les escroqueries dites « au président » ou Fovi

Depuis quelques années, les escroqueries aux faux ordres de virement (Fovi), dites également au président, se multiplient, faisant de nombreuses victimes parmi les entreprises. Les services de l'État, les collectivités locales et les établissements publics de santé sont également concernés. Outre le préjudice financier direct, les conséquences peuvent être dramatiques pour la poursuite de l'activité.

Le mode opératoire

Le but d'un Fovi est d'obtenir la réalisation d'un virement, souvent à l'international, au profit de l'escroc. En général, le mode opératoire revêt les caractéristiques suivantes : l'escroc se fait passer pour le président de l'entreprise lors d'un contact téléphonique ou par courriel avec les services comptables ; il crédibilise sa demande et met en confiance la victime grâce à de l'**ingénierie sociale** ; il utilise des ressorts psychologiques visant à abolir le discernement de la victime pour lui faire prendre des décisions sous le coup de l'urgence et de la confidentialité.

Se prémunir

ORGANISATIONNEL

- Sensibiliser régulièrement tout le personnel (y compris les stagiaires, les nouveaux arrivants, les saisonniers, les prestataires, etc.) à ce type d'escroquerie.
- Expliquer les principales vulnérabilités associées à l'usage des réseaux sociaux et la nécessité de ne pas mettre en avant des informations qui pourraient être utilisées dans le cadre d'un Fovi (déplacements de la direction, organigramme trop détaillé, informations comptables, etc.).
- Mettre en place des procédures de vérifications et de signatures multiples pour les paiements internationaux.

TECHNIQUE

- Maintenir à jour le système de sécurité informatique.

COMPORTEMENTAL

- Respecter les procédures mises en place malgré les pressions d'un interlocuteur souhaitant un paiement dans l'urgence.
- Exiger une sollicitation écrite via un courriel professionnel afin de pouvoir la vérifier. Faire de même avec un numéro de téléphone fixe.
- Être attentif aux demandes inhabituelles de transmission de nouvelles coordonnées bancaires et, plus largement, faire remonter toute information jugée inquiétante.
- Redoubler de vigilance sur les périodes de congés scolaires, les jours fériés, les vendredis soir, les week-ends et les périodes de remplacement.
- Se rapprocher de son organisme bancaire et suivre les procédures indiquées.

Conduite à tenir en cas d'escroquerie

COMPORTEMENTAL

➤ Identifier immédiatement les virements exécutés, les mandats de paiement ou les demandes de paiement en instance ou à venir concernés.

➤ Demander le blocage des coordonnées bancaires frauduleuses dans les applications métiers.

➤ Si le paiement n'est pas encore intervenu, suspendre le mandat ou la demande de paiement.

➤ Si le paiement est déjà intervenu, demander le blocage ou le retour des fonds auprès de l'instance bancaire.

➤ Déposer plainte auprès des services de police et de gendarmerie, en apportant un maximum d'éléments (références des virements, coordonnées des personnes contactées). Un dépôt de plainte rapide permet d'optimiser les chances de récupérer les fonds versés.

Escroqueries similaires

➤ La fraude au « changement de RIB » : l'escroc s'adresse aux services de comptabilité d'une entreprise en se faisant passer pour un fournisseur. Il demande ensuite le règlement de factures sur un compte bancaire autre que le compte habituel.

➤ La fraude au « faux technicien » : l'escroc se présente comme un technicien informatique venant réaliser une opération de maintenance sur l'outil de gestion des comptes et virements.

➤ La fraude « au faux ministre » : cette escroquerie consiste à atteindre un dirigeant, en usurpant l'identité d'un ministre, pour le convaincre de virer des fonds à l'étranger en vue de mener des actions de lutte contre le terrorisme ou de libération d'otages.

Mots clés

Ingénierie sociale : recueil d'informations sur une cible basé sur l'étude de l'environnement personnel et/ou professionnel, à partir notamment des informations publiées sur les réseaux sociaux.

Escroquerie : l'escroquerie est le fait de tromper une personne physique ou morale afin de l'inciter à remettre des fonds, des valeurs, des services ou un bien quelconque (délit puni de cinq ans d'emprisonnement et de 375 000 € d'amende - article 313-1 du Code pénal).

Pour aller plus loin

➤ Fédération des banques françaises (FBF)
- Consignes de prévention indispensables pour éviter les escroqueries aux faux ordres de virement internationaux (Fovi)
- Guide sécurité de la FBF « Ordres de virement des entreprises – 9 réflexes sécurité »

➤ Ministère de l'intérieur – OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication)

Portail officiel de signalement des contenus illicites de l'Internet :

https://www.internet-signalement.gouv.fr

D6. Se prémunir des risques générés par les procédures de conformité (*compliance*)

La multiplication des réglementations juridiques et le renforcement de la culture de l'éthique ont conduit à la naissance d'une nouvelle matière mêlant management et droit : la **conformité** ou *compliance*. Celle-ci a vocation à toucher tout le droit de l'entreprise. Et si elle peut paraître abstraite de prime abord, elle est bien concrète en ce qu'elle permet de gérer au mieux les risques de sécurité économique générés par l'activité de l'entreprise. En effet, l'essor de la conformité touche toutes les entreprises et toutes les branches du droit intéressant leurs activités. De manière générale, la conformité porte sur : la corruption, la fraude et le blanchiment, les pratiques anticoncurrentielles, les sanctions économiques (par exemple le contournement des embargos), la responsabilité sociale et environnementale des entreprises, la protection des données numériques, sans que cette liste soit limitative.

Le prononcé des sanctions est tout particulièrement important pour la sécurité économique des entreprises. En effet, un grand nombre d'États mettent en place des dispositifs de sanctions à portée **extraterritoriale** (les lois américaine et britannique telles que par exemple le *Foreign Corrupt Practice Act* et le *UK Bribery Act*) pouvant sanctionner très lourdement des entreprises étrangères n'opérant pas sur leur territoire, notamment avec des amendes transactionnelles (comme les accords tel le **DPA** et **NPA**). Toutes les établissements, quelle que soit leur taille, étant concernés par ces dispositifs, doivent connaitre leur existence tant les conséquences peuvent être désastreuses. Pertes financières, perte de savoir-faire matériel et immatériel, perte de données stratégiques, dommage réputationnel, sanctions de mise en conformité avec imposition d'un **monitoring**, autant de risques pour la sécurité économique qu'une bonne compréhension de la *compliance* doit prévenir.

Prévenir, grâce à des procédures internes

ORGANISATIONNEL

➤ **Nommer un** *responsable conformité*, qualifié et hiérarchiquement indépendant de la direction, qui coordonne les actions de prévention, de contrôle et de correction.

➤ **Rédiger une charte éthique** encadrant les comportements du personnel et la faire signer par tous.

➤ **Développer une veille** dédiée à l'activité législative et normative concernant l'activité de l'entreprise et son implantation géographique.

➤ **Sensibiliser** régulièrement les dirigeants comme les salariés aux bons comportements à adopter ainsi qu'aux risques encourus, tant pour l'entreprise que pour eux-mêmes, notamment en rappelant le cadre juridique s'appliquant aux cadeaux d'affaires.

➤ **Mettre en place un dispositif d'alerte** afin que le personnel puisse signaler au *responsable conformité* toute situation à risque ou suspecte. Les salariés doivent être informés de son existence et de la garantie d'anonymat qui leur est légalement accordée.

Contrôler son organisation

ORGANISATIONNEL

➤ **Vérifier systématiquement l'honorabilité** des partenaires et des tiers externes en se demandant si des éléments sont susceptibles de remettre en cause leur « bonne réputation » (sanctions, conflits d'intérêts, rumeurs défavorables, etc.) ?

➤ **Contrôler continuellement la conformité de son activité** aux normes juridiques, environnementales et éthiques applicables à l'entreprise et à ses implantations.

➤ Dresser **une cartographie des risques**, présentant des schémas de réponses concrets pour chacun d'eux et adaptés à la taille de l'entreprise et à son contexte local.

➤ **Conduire des audits** pour identifier et corriger les failles organisationnelles, comportementales et techniques pouvant motiver une procédure d'incrimination.

➤ En cas d'audits externes, veiller à **limiter les risques d'exposition du patrimoine informationnel de l'entreprise** : délimiter l'accès des sociétés étrangères aux ressources numériques, exiger la signature d'un accord de confidentialité et imposer le suivi de l'audit par un juriste interne.

TECHNIQUE

➤ Veiller, dans la mesure du possible, à héberger et gérer les données propres au travers de solutions nationales agréées par l'Anssi.

Mots clés

Conformité (*compliance*) : ensemble des processus qui permet d'assurer la conformité des comportements de l'entreprise, de ses dirigeants et de ses salariés aux normes juridiques et éthiques qui leur sont applicables.

Extraterritorialité : principe de droit international visant à laisser s'exercer dans un État l'autorité juridique d'un autre État.

Foreign Corrupt Practice Act (FCPA) & UK Bribery Act : lois, respectivement des États-Unis et du Royaume-Uni, visant à sanctionner les actes de corruption. De portée extraterritoriale, ces législations peuvent s'appliquer à des acteurs étrangers ayant un lien quelconque avec l'État en question (États-Unis ou Royaume Uni selon la loi).

Deferred Prosecution Act (DPA) : accord passé avec les autorités américaines ou britanniques par lequel une société, objet d'enquête pour corruption ou fraude, accepte de s'acquitter de sanctions financières, de reconnaître les faits et de se soumettre à un contrôle afin d'empêcher de futures infractions, en contrepartie de l'extinction des poursuites à son encontre.

Non Prosecution Agreement (NPA) : négociation extra-judiciaire proposée à un établissement contre lequel il y a des soupçons de conduite déviante, mais contre lequel les autorités n'ont pas encore lancé de poursuites pénales.

Monitoring : technique visant à évaluer et contrôler le respect des engagements pris par une entreprise dans le cadre d'une transaction judiciaire (DPA ou NPA). Il peut être imposé à l'entreprise ou choisi par elle et est toujours financé par l'entreprise.

Monitor : personne désignée afin d'évaluer le respect des engagements pris par l'entreprise, son mandat est négocié entre l'entreprise et l'autorité de poursuite. Elle peut avoir accès à la quasi-intégralité des données de l'entreprise et peut potentiellement représenter un risque pour la sécurité économique de l'entreprise.

D6. Se prémunir des risques générés par les procédures de conformité

Pour aller plus loin

Toutes concernées, les établissements doivent avoir conscience de la réglementation et notamment :

- la loi « Sapin II » sur la lutte anticorruption (annexe 2) ;
- le Règlement général sur la protection des données à caractère personnel (RGPD) expliqué sur le site de la Cnil.

- Anssi

Liste de produits certifiés de stockage sécurisé

E1. Protéger son poste de travail

Si les systèmes d'information numériques sont désormais totalement indispensables à tous les acteurs économiques, l'attention portée à leur sécurité au quotidien par leurs utilisateurs reste bien insuffisante. Les négligences sur les postes de travail exposent l'entreprise à de graves problèmes susceptibles de compromette son activité.

ORGANISATIONNEL

➤ Définir et faire appliquer une politique de choix de **mots de passe robustes**, difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne :

- au minimum 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) ;
- aucun lien direct avec la personne : éviter les noms, dates de naissance, etc. ;
- absents des dictionnaires.

➤ Définir un mot de passe unique et personnel pour chaque usage. Les mots de passe protégeant des contenus sensibles (banque, messagerie, etc.) ne doivent en aucun cas être réutilisés.

TECHNIQUE

➤ Mettre régulièrement à jour le **système d'exploitation** et les logiciels.

➤ Télécharger les installateurs de logiciels uniquement depuis les sites de leurs éditeurs et vérifier leur authenticité avant toute installation.

➤ N'installer que le strict nécessaire sur les postes de travail. En particulier, limiter les logiciels installés et les modules optionnels pour les navigateurs.

➤ Utiliser un **pare-feu** local et un **anti-virus**.

➤ Utiliser un gestionnaire de mot de passe pour leur stockage. Choisir pour ce gestionnaire un **mot de passe robuste**.

➤ Désactiver les exécutions automatiques.

➤ Chiffrer les partitions où sont stockées les données utilisateur.

➤ Désactiver les ports USB non utilisés pour la connexion des périphériques.

➤ Protéger l'accès aux informations sensibles à l'aide d'un système de contrôle d'accès adapté. Pour les informations les plus critiques, privilégier des systèmes basés sur la cryptographie comme des conteneurs chiffrés.

➤ Effectuer régulièrement des sauvegardes de données. Elles permettent de retrouver les données après une attaque (avec un rançongiciel, par exemple) ou un sinistre (incendie, inondation, etc.). Ces sauvegardes sont à appliquer en priorité aux données sensibles. Le moyen le plus sûr, mais aussi le plus simple, consiste à stocker, de manière sécurisée et dans un endroit distinct, une copie de ses sauvegardes sur un support déconnecté comme par exemple un disque dur amovible. Pour les entités plus larges où une telle solution n'est pas envisageable de manière générale, elle pourra être réservée aux données les plus sensibles.

COMPORTEMENTAL

➤ Face à un courriel suspect :
- ne jamais ouvrir les pièces jointes provenant de destinataires inconnus ou dont le sujet ou le format paraissent incohérents avec les messages habituellement reçus ;
- si des liens figurent dans le corps du courriel, vérifier l'adresse pointée par le lien avant de cliquer ;
- ne jamais répondre par courriel à une demande d'informations personnelles, confidentielles ou bancaires ;
- ne pas ouvrir ni relayer des chaînes de courriels ou des appels à solidarité suspects ;
- ne pas prendre de décisions importantes (comme un virement bancaire) sur la base d'un courrier seul.

➤ Utiliser un compte qui ne bénéficie pas des **droits** « **administrateur** » pour les tâches quotidiennes (navigation internet, usage de suites bureautiques, consultation de messagerie, etc.).

Mots clés

Mot de passe robuste : la robustesse d'un mot de passe dépend en général, d'abord de sa complexité, mais également de divers autres paramètres. Choisir des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Système d'exploitation : programme assurant la gestion de l'ordinateur et de ses périphériques.

Pare-feu : dispositif informatique qui filtre les flux d'informations entre le réseau interne et le réseau externe de l'organisme en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur.

Anti-virus : logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.

Droits « administrateur » : faculté d'effectuer des modifications touchant la configuration du poste de travail (modifier des paramètres de sécurité, installer des logiciels, etc.).

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)
- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Recommandations de sécurité relatives aux mots de passe

➤ Service du haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance
- Mémento cybersécurité pour le créateur d'entreprise
- Mémento cybersécurité pour le dirigeant d'entreprise

E2. Protéger et gérer l'accès au système d'information

Le réseau informatique d'un acteur économique est désormais la principale porte d'entrée pour l'accès à l'information. Sa sécurité peut s'avérer vitale pour l'entreprise et elle se mesure à l'aune de son maillon le plus faible. Chacun à son poste doit donc être pleinement mobilisé.

ORGANISATIONNEL

➤ Tenir à jour la liste précise de tous les équipements informatiques de l'entreprise qui peuvent se connecter au réseau (postes utilisateurs, serveurs, imprimantes, photocopieurs, etc.).

➤ Identifier nommément chaque utilisateur, supprimer minutieusement les comptes anonymes et génériques.

➤ Attribuer des droits d'accès (répertoires, calendriers, etc.) de façon graduée et adaptée strictement aux besoins. Actualiser ces droits lors des arrivées, des départs et des mouvements internes.

➤ Dédier les comptes d'administration à ces seules tâches.

➤ Limiter drastiquement le nombre d'utilisateurs disposant de **droits administrateurs**.

➤ S'assurer de la suppression effective des droits d'accès au système d'information lors du départ d'un collaborateur ou d'un personnel temporaire.

TECHNIQUE

➤ Privilégier une connexion au réseau par câble plutôt que par Wifi.

➤ Mettre en place une passerelle d'accès à internet sécurisée à travers par exemple la mise en place d'un **pare-feu**.

➤ Cloisonner les différents services au sein du réseau. En particulier, isoler les services exposés sur internet du reste du système d'information.

➤ Si le Wifi est utilisé, sécuriser l'accès en suivant les recommandations de l'Anssi.

➤ Vérifier qu'aucun équipement connecté au réseau interne ne puisse être administré via internet. Limiter, si possible, la télémaintenance. Cloisonner les fonctions d'administration du reste du système d'information.

➤ Ne pas laisser de prises d'accès physique au réseau interne accessibles à tous (salle d'attente, salle de réunion, etc.).

➤ Renouveler régulièrement les identifiants et mots de passe configurés sur tous les équipements (imprimantes, serveurs, etc.).

Mots clés

Droits administrateurs : faculté d'effectuer des modifications affectant tous les utilisateurs (modifier des paramètres de sécurité, installer des logiciels, etc.).

Pare-feu (*firewall)* : logiciel et/ou matériel protégeant un équipement ou un réseau informatique en contrôlant les entrées et sorties selon des règles définies par son administrateur.

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)

- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Sécuriser les accès Wi-Fi

➤ Service du Haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance

- Mémento cybersécurité pour le créateur d'entreprise
- Mémento cybersécurité pour le dirigeant d'entreprise

E3. Utiliser des supports amovibles de façon sécurisée

Le support amovible, s'il permet de transporter facilement des données, peut être compromis par un logiciel malveillant susceptible d'agir sur la machine ou le réseau auquel il sera connecté. La perte d'un support amovible signifie, bien évidemment, la perte des informations qu'il contient.

ORGANISATIONNEL

- Interdire la connexion, à des postes reliés au système d'information de l'entreprise, d'équipements et de supports amovibles personnels (clés USB, disques durs externes, lecteurs MP3, etc.).
- Sensibiliser les collaborateurs, notamment au moyen de la charte informatique, à cette règle importante souvent perçue comme une contrainte.

TECHNIQUE

- Désactiver l'exécution automatique des périphériques.

COMPORTEMENTAL

- En cas d'utilisation d'un support amovible, par exemple pour échanger des données sensibles, choisir un support réservé à cet usage.
- Avant de l'utiliser, analyser avec un outil adapté, tout support amovible qui a été connecté à l'extérieur du réseau de l'entreprise.
- **Chiffrer** les supports amovibles pour limiter tout risque de fuite d'information en cas de perte ou de vol.
- Ne pas prêter ses supports amovibles. Ne pas les laisser accessibles sans surveillance.

Mots clés

Chiffrement : procédé de cryptographie grâce auquel on rend la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)
- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Passeport de conseils aux voyageurs
- Guide d'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques
- Liste de logiciels de chiffrement que vous pouvez utiliser en toute confiance

➤ Service du Haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance
- Mémento cybersécurité pour le créateur d'entreprise
- Mémento cybersécurité pour le dirigeant d'entreprise

E4. Sécuriser le télétravail

Si les appareils nomades sont appréciés et utiles parce qu'ils simplifient souvent les tâches quotidiennes des acteurs économiques, leur usage expose cependant l'entreprise et ses partenaires à des risques nouveaux de perte ou de captation d'informations stratégiques qu'il est nécessaire de bien maîtriser en prenant certaines précautions élémentaires.

ORGANISATIONNEL

➤ Penser une politique de mise à disposition d'outils nomades maîtrisée afin d'éviter les écueils d'un recours au BYOD (*Bring your Own Device*) non contrôlé.

➤ Veiller à ce que personne dans l'entreprise n'utilise son appareil nomade personnel (ordinateurs portables, smartphones, tablettes) à des fins professionnelles, sans accord ni contrôle. Cette règle est souvent perçue comme une contrainte forte, notamment par l'encadrement supérieur ; elle est cependant d'une importance particulière.

COMPORTEMENTAL

➤ Désactiver la connexion automatique des appareils nomades aux points d'accès Wifi ouverts.

➤ Désactiver le *bluetooth* lorsqu'il n'est pas utilisé.

➤ En plus du code PIN protégeant la carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès au smartphone ou à la tablette et les configurer pour qu'ils se verrouillent automatiquement après un court moment d'inactivité.

➤ Chiffrer les données les plus sensibles à l'aide d'un logiciel ou d'une application dédié.

➤ N'installer que les applications nécessaires et vérifier à quelles données elles permettent l'accès avant de les télécharger sur l'appareil nomade (informations géographiques, contacts, appels téléphoniques, etc.). Éviter d'installer les applications demandant l'accès à des données qui ne sont pas strictement nécessaires au fonctionnement de l'appareil nomade.

➤ Effectuer des sauvegardes régulières des contenus sur un support externe pour pouvoir les conserver en cas de restauration de l'appareil dans son état initial.

➤ Être très attentif à ne pas se séparer des appareils nomades qui peuvent contenir des informations sensibles ou permettre d'accéder au réseau de l'entreprise.

Mots clés

Chiffrement : procédé de cryptographie grâce auquel on rend la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

***BYOD* ou AVEC** : *Bring your Own Device* ou « Apporter votre équipement personnel de communication » est la politique d'entreprise qui admet ou préconise l'utilisation d'équipements de communication personnels à des fins professionnelles.

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)

- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Recommandations de sécurité relatives aux mots de passe
- Liste de logiciels de chiffrement que vous pouvez utiliser en toute confiance
- Passeport de conseils aux voyageurs

➤ Service du Haut fonctionnaire de défense et de sécurité (SHFDS) du ministère de l'Économie, des Finances et de la Relance

- Mémento cybersécurité pour le créateur d'entreprise
- Mémento cybersécurité pour le dirigeant d'entreprise

E5. Maîtriser l'externalisation informatique

L'externalisation informatique (dite aussi « infogérance ») peut parfois permettre de pallier l'absence d'une compétence en interne. Elle présente néanmoins des risques pour les données et les systèmes d'information, qu'il convient de connaître et de maîtriser.

ORGANISATIONNEL

➤ Déterminer, en fonction de la nature de l'entreprise, ses besoins précis en externalisation informatique (***Cloud Computing***, plateforme logicielle à distance, etc.).

➤ Hiérarchiser les objectifs de sécurité de l'entreprise (disponibilité du site internet, hébergement sur des serveurs dédiés, etc.) et, lors des appels d'offres, les intégrer dans le cahier des charges par des clauses détaillées.

➤ Demander explicitement aux prestataires répondant aux appels d'offres un **Plan d'assurance sécurité (Pas)**.

➤ Afin de limiter les risques liés à la perte de maîtrise des systèmes d'information, aux interventions à distance et à l'hébergement mutualisé (lorsque les données de plusieurs entreprises sont hébergées sur le même serveur physique), faire analyser le contrat par des spécialistes (techniques et juridiques).

➤ Il existe des risques spécifiques liés au ***Cloud Computing***, ou **informatique en nuage** : risques pour la confidentialité des données, risques juridiques liés à l'incertitude sur la localisation des données, risques liés à la perte de maîtrise du système d'information, risques liés à l'irréversibilité des contrats. Les contrats proposés dans le cadre des offres génériques ne cadrent généralement ces risques que de façon très insuffisante. Rédiger, en liaison avec des spécialistes (techniques et juridiques), des contrats personnalisés et appropriés aux enjeux de l'entreprise.

➤ Privilégier les services de *Cloud Computing* ayant reçu un label de confiance comme «SecNumCloud » de l'Anssi.

Mots clés

Infogérance : externalisation appliquée au domaine des systèmes d'information.

Informatique en nuage (*Cloud Computing*) : mode de traitement des données d'un client dont l'exploitation s'effectue par internet, sous la forme de services fournis par un prestataire. Dans ce cas de figure, l'emplacement et le fonctionnement du nuage ne sont pas nécessairement portés à la connaissance des clients.

Plan d'assurance sécurité (Pas) : document contractuel garantissant le respect des exigences de sécurité. Le guide édité par l'Anssi propose un canevas pour la rédaction des objectifs de sécurité devant figurer dans le Pas.

Anssi : Agence nationale de la sécurité des systèmes d'information.

Pour aller plus loin

Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques

- Annexe 6

E6. Se protéger contre les « rançongiciels »

Le terme « rançongiciel » (ou *ransomware* en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant visant à obtenir le paiement d'une rançon. Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données (fichiers clients, comptabilité, factures, devis, plans, photographies, messages, etc.), en les chiffrant, puis lui donner les instructions utiles au paiement de la rançon. Lorsqu'un rançongiciel infecte un poste de travail, le plus souvent (mais pas nécessairement) par l'envoi d'un courrier électronique piégé, l'infection est dès lors susceptible de s'étendre au reste du système d'information (serveurs, ordinateurs, téléphonie, systèmes industriels, etc.).

ORGANISATIONNEL

➤ **Effectuer des sauvegardes de données régulières**

Les sauvegardes constituent la meilleure parade contre les rançongiciels. Effectuées régulièrement, elles permettent de retrouver ses données si une telle attaque survient. Ces sauvegardes sont à appliquer en priorité aux données sensibles, aux serveurs et aux applications métiers dont la paralysie serait très néfaste pour l'activité de l'entité.

Enfin, le moyen le plus sûr, mais aussi le plus simple, de protéger ses données consiste à stocker une copie de ses sauvegardes sur un support déconnecté comme par exemple un disque dur amovible. Pour les entités plus larges où une telle solution n'est pas envisageable de manière générale, elle pourra être réservée aux données les plus sensibles. De la même manière, si le stockage des données est externalisé (i.e. sur le cloud), il est essentiel de se déconnecter à l'issue de chaque sauvegarde.

➤ **Ne pas payer les rançons !**

Accepter le paiement de la rançon entretient d'une part le système frauduleux et, d'autre part, ne garantit en rien la récupération de ses données. Il est en revanche conseillé de porter plainte auprès des services de police ou gendarmerie spécialisés.

TECHNIQUE

➤ **Assurer la mise à jour automatique de tous ses logiciels et applications**

Les rançongiciels utilisent les vulnérabilités des programmes pour se propager. Mettre à jour l'intégralité de ses logiciels et applications limite leur risque de propagation au sein du système d'information.

➤ **Créer et se servir d'un compte « utilisateur »**

Par défaut, la plupart des personnes bénéficient sur leur ordinateur de « droits **administrateur** ». Une telle élévation de droits fait courir le risque, en cas d'attaque, de faciliter la propagation du rançongiciel de l'ordinateur au reste du système. Créer et utiliser un compte « utilisateur » permet au contraire de ralentir ces attaques ou d'en limiter les effets.

➤ **Renforcer la configuration des logiciels bureautiques ou manipulant des données issues d'internet**

Restreindre l'autorisation des macros dans les suites bureautiques permet d'éviter la réalisation de tâches automatisées. Si un logiciel lambda demande de les activer à l'issue de l'exécution d'un document inconnu, il convient de toujours répondre « non ».

COMPORTEMENTAL

➤ **Ne pas ouvrir les messages dont l'origine ou la forme semblent douteuses**

Les courriers électroniques suspects (fautes d'orthographe ou de frappe, langage inapproprié, mauvaise résolution graphique ou déformation des images, etc.), peuvent contenir des liens ou des pièces jointes qui, par un simple clic, sont susceptibles de permettre l'exécution d'un programme malveillant sur le système. Au moindre doute, mieux vaut privilégier l'accès au site internet dont il est fait mention dans le message en tapant directement l'adresse dans la barre de recherche.

Pour tromper la vigilance de l'utilisateur, certains de ces courriers électroniques vont parfois plus loin en adressant à ce dernier un contenu personnalisé qui fera écho à son environnement familier. On parle alors de « hameçonnage ciblé » (*spear phishing* en anglais).

Mots clés

Chiffrement : procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'information impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

Droits « administrateur » : faculté d'effectuer des modifications affectant la configuration du poste de travail (modifier des paramètres de sécurité, installer des logiciels, etc.).

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)

- Guide des bonnes pratiques de l'informatique
- Note d'information du CERT-FR relative à la protection contre les rançongiciels
- Initiative pour aider les victimes de rançongiciels à récupérer leurs données chiffrées sans avoir à payer de rançons aux délinquants
- Fédération EBEN, Alerte aux rançongiciels – Vos données en otage contre de l'argent, flyer

Plateforme cybermalveillance.gouv.fr

- Fiche réflexe - Les rançongiciels (ransomware)

F1. Maîtriser sa communication au quotidien et son e-réputation

Une communication non maitrisée peut entraîner une fuite d'informations stratégiques préjudiciable pour l'entreprise. Il est donc toujours nécessaire de bien évaluer la sensibilité des informations qui sont communiquées, que ce soit sur le plan professionnel ou personnel.

ORGANISATIONNEL

➤ Une communication professionnelle doit être centralisée et maîtrisée :

- demander à tous les employés de l'entreprise de faire valider, préalablement et systématiquement, auprès de la direction ou de la personne chargée de la communication, tout contact avec un journaliste, un analyste financier, le rédacteur d'un rapport ou d'un livre, etc ;
- toujours se demander si les interlocuteurs et les questions sont légitimes, et s'assurer qu'ils s'inscrivent dans la stratégie de communication. Si possible, demander que soit communiquée à l'avance la liste des questions qui vont être posées et bien s'assurer de pouvoir relire la publication avant parution ;
- peser précisément les conséquences, positives mais aussi négatives, de ce qui peut être dit ou écrit sur la base des informations communiquées.

➤ Préparer avec minutie ce qui sera dit lors des événements à l'extérieur (salons professionnels, lancement de produits, colloques, etc.). Identifier les informations sensibles qui doivent rester confidentielles et ne communiquer que ce qui est utile commercialement.

➤ Sur les supports de communication (cartes de visite, signature électronique, etc.), n'indiquer que les coordonnées strictement nécessaires à la relation professionnelle.

➤ Sensibiliser les collaborateurs aux risques des sollicitations urgentes, inhabituelles et ne respectant pas les procédures. Cela peut cacher une manœuvre visant à s'approprier indûment une information ou de l'argent (demande de virement en urgence, etc.).

➤ Mettre en place préalablement une procédure d'urgence, validée par l'entreprise, pour ce type de situations et exiger qu'elle soit respectée en toutes circonstances.

➤ S'assurer de la légitimité des démarches d'audits ou de contrôle :

- vérifier l'identité des intervenants en demandant à voir leur carte professionnelle ;
- s'assurer qu'ils sont bien mandatés par les administrations ou organismes de contrôle auxquels ils prétendent appartenir ;
- exiger une lettre de mission.

➤ Une communication maîtrisée passe également par une attention particulière portée à l'e-réputation de l'entreprise :

- procéder à une veille régulière sur les principaux réseaux sociaux afin de réagir rapidement en cas de publication d'informations sensibles susceptibles d'altérer la réputation de l'entreprise ou de ses salariés, mais aussi afin d'identifier très tôt les informations susceptibles de mettre à mal les actifs de l'entreprise. Le cas échéant, se rapprocher de son conseiller juridique et/ou des services de l'État ;
- mettre également en place une veille rigoureuse sur les noms de la société, de ses dirigeants et des marques afin de pouvoir réagir rapidement contre les dénigrements, les « **cybersquats** » ou toute autre action à l'encontre de l'entreprise ;

- désigner un animateur de réseaux (*community manager*) qui suivra rigoureusement les évolutions techniques du réseau social - sécurité, confidentialité, etc.

Avant toute communication, bien veiller à effectuer une analyse de risques tenant compte des informations à communiquer, du processus de validation avant diffusion, du suivi des commentaires (ou posts), du rythme de publication. Il convient d'être très attentif à la cohérence et à l'intégrité des messages de communication externe, eu égard aux réalités de l'entreprise.

COMPORTEMENTAL

➤ Toujours vérifier l'identité et la légitimité de l'émetteur avant de répondre à un questionnaire, notamment par courriel.

➤ Rester bref et évasif avec des interlocuteurs trop insistants (certains pratiquent habilement l'**élicitation**). Ne donner que des réponses générales.

➤ Rester lucide et sur la réserve lorsqu'on vous promet des gains exceptionnels ou qu'on évoque des risques dramatiques pour l'entreprise.

➤ Ne pas se laisser dominer par quelqu'un qui se targue d'être un expert et semble connaître beaucoup de monde (*name dropping*), en particulier les personnes qui font autorité. Ne jamais se sentir contraint de raconter les détails de l'activité de l'entreprise à une personne dont le statut, la fonction ou l'expertise supposée semblent dignes de confiance.

➤ Ne pas se laisser impressionner par quelqu'un qui fait des confidences, se montre alarmiste ou pressant.

➤ Ne pas sur-réagir aux critiques ou aux mises en cause qui concernent l'entreprise : solidité financière, qualité de l'activité, concurrents, etc.

➤ Si vous pensez être victime d'une action intrusive, récupérez autant d'informations que possible (numéro de téléphone, numéro de voiture, courriel, carte de visite, questionnaire, etc.).

Mots clés

Élicitation : technique de communication, intrusive mais pas illégale, qui consiste à manipuler son interlocuteur en usant de ressorts psychologiques (reconnaissance, séduction, amitié feinte, etc.) afin d'obtenir de sa part des informations qu'il n'aurait pas spontanément délivrées. Elle repose souvent sur une étude préalable de l'environnement personnel et/ou professionnel de la cible, dite ingénierie sociale.

***Name-dropping* :** action qui consiste à évoquer avec son interlocuteur des noms de personnes qui font autorité dans leur domaine, en laissant entendre qu'on les connaît parfaitement.

Cybersquat : acte qui consiste à déposer un nom de domaine en usurpant le nom de l'entreprise ou celui de ses marques (nasa.com était un site pornographique alors que le site officiel est nasa.org, par exemple). Il existe une variante : le « typosquat » qui repose sur une orthographe incorrecte (elyseee.fr pour elysee.fr, par exemple).

F2. Utiliser en toute sécurité les réseaux sociaux

Aussi banalisé qu'il soit, l'usage des réseaux sociaux par les salariés n'est pas toujours anodin. En effet, un salarié peut, volontairement ou non, porter préjudice à son établissement par ses publications. C'est pourquoi chaque établissement doit adopter une politiqur en la matière et chaque salarié un comportement adéquat.

ORGANISATIONNEL

➤ Mettre en place une charte sur le bon usage des réseaux sociaux à l'attention des salariés.

➤ Instaurer des séances de sensibilisation régulière du personnel et rappeler les enjeux liés à l'usage des réseaux sociaux pour l'entreprise et le caractère juridique de la charte.

➤ Expliquer les principales vulnérabilités associées à l'usage des réseaux sociaux telles que :

- la publication de contenus révélant son activité professionnelle ou la politique de l'entreprise ;
- les interactions sociales entre les utilisateurs connus ou inconnus ;
- la possibilité d'être utilisés comme vecteurs de transmission de logiciels malveillants, d'attaque par **hameçonnage** ou par **ingénierie sociale**.

COMPORTEMENTAL

➤ Appliquer les bonnes pratiques indiquées dans la charte de l'entreprise.

➤ Avant toute diffusion, s'assurer que l'information publiée n'est pas susceptible de compromettre les intérêts de l'entreprise.

➤ Ne jamais utiliser le même mot de passe pour accéder à un réseau social et aux ressources informatiques de l'entreprise.

➤ Éviter de communiquer des informations professionnelles et personnelles trop détaillées (organigramme, positionnement hiérarchique, responsabilités professionnelles, missions à l'étranger, projets en cours, situation matrimoniale, date et lieu de naissance, numéro de téléphone, etc.) sur les réseaux sociaux.

➤ Utiliser prudemment les données de géolocalisation ouvertes sur les réseaux sociaux. Elles peuvent apporter des renseignements sur l'emploi du temps professionnel : absence, vacances, missions, etc. Vérifier régulièrement les paramètres de confidentialité et de sécurité des comptes. Privilégier une authentification forte pour protéger les mots de passe.

➤ Être vigilant quant aux multiples sollicitations via les réseaux sociaux (contacts par messagerie, commentaires – *posts* –, liens hypertexte, photos de célébrités, etc.). Ces approches peuvent mener vers des pages malveillantes et permettre de pirater des comptes, dérober des informations personnelles ou professionnelles ou infecter les systèmes d'informations d'un établissement.

Mots clés

Hameçonnage (*phishing*) : méthode d'attaque qui consiste à imiter les couleurs d'une entreprise ou d'une institution pour inciter le destinataire à fournir des informations personnelles.

Ingénierie sociale : recueil d'informations basée sur l'étude de l'environnement personnel et/ou professionnel, à partir notamment des informations publiées sur les réseaux sociaux par la personne ciblée.

Pour aller plus loin

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)
- Guide d'hygiène informatique
- Recommandations de sécurité relatives aux mots de passe

G1. Se déplacer au quotidien

Parce qu'ils sont routiniers et prévisibles, les petits déplacements au quotidien exposent les acteurs économiques à d'importantes vulnérabilités facilitant la perte ou la fuite d'informations sensibles dont les conséquences peuvent s'avérer très préjudiciables à l'entreprise.

TECHNIQUE

➤ Installer un **filtre de confidentialité** sur les écrans des ordinateurs portables, des tablettes et des smartphones à usage professionnel.

COMPORTEMENTAL

➤ Éviter de transporter les données sensibles lors des déplacements quotidiens, notamment entre le domicile et le travail. Prévoir une **solution de chiffrement** (conteneur chiffré ou clé USB sécurisée).

➤ En cas d'utilisation des fonctions Wifi/Bluetooth des appareils nomades dans les transports en commun, garder à l'esprit que toute liaison peut être interceptée (dans ce cas, il est recommandé d'utilisé un **VPN**). Il est vivement conseillé de désactiver les fonctions Wifi/Bluetooth de vos appareils nomades utilisés à des fins professionnelles (smartphones, tablettes, ordinateurs portables) dans les transports en commun et espaces publics (gares, aéroports, salons professionnels, etc.)

➤ Éviter au maximum de parler de sujets professionnels dans les transports (métro, bus, taxis, trains, avions) et les espaces publics partagés (restaurants, cafés, salles d'attente, etc.)

➤ Dans un lieu public, rester discret dans ses lectures professionnelles (rapports, notes en cours, courriels, etc.).

➤ Taper discrètement ses identifiants et mots de passe d'accès à l'ordinateur, ou à sa messagerie.

➤ Privilégier les prises secteurs pour recharger vos appareils nomades plutôt que les prises USB afin d'éviter le risque d'aspiration de vos données (*juice-jacking*)

➤ Ne jamais laisser ses outils de travail (mallette, ordinateurs portables, téléphones, etc.) sans surveillance.

➤ Lors des déplacements en voiture, déposer discrètement ses affaires dans le coffre verrouillé et non sur la banquette arrière ou le siège passager. Lors des stationnements, ne pas laisser d'ordinateurs portables ou de documents contenant des données sensibles dans la voiture, même dans le coffre.

➤ Dans le cas d'une location, éviter les interfaces entre le smartphone et le véhicule afin d'éviter la récupération et le transfert de vos données (sms, contact, photos etc.). En cas d'utilisation du Bluetooth, penser à effacer les données présentes dans le système d'information du véhicule.

Mots clés

Filtre de confidentialité : film de protection qui se place sur un écran et qui restreint la vision des données affichées de part et d'autre de l'axe de vision.

Solution de chiffrement : outil permettant la transformation de données dans le but d'en cacher le contenu.

VPN : le réseau privé virtuel (en anglais *Virtual Private Network*), est un système permettant de créer un lien direct et généralement sécurisé par du chiffrement entre des ordinateurs distants.

Pour aller plus loin

➤ L'Anssi propose des solutions techniques de chiffrement sur son site Internet.

G2. Se déplacer à l'étranger

Pour de nombreuses entreprises ou organismes de recherche, voyager est indispensable. Présence, visibilité et démonstration de qualités sur la scène internationale conditionnent, en effet l'accès à de nouvelles opportunités. Pour autant ces déplacements accentuent le risque de perte, de vol et de fuite d'informations. Il est donc nécessaire de les préparer afin d'adopter les comportements qui permettront de limiter ces risques.

Préparation du déplacement

ORGANISATIONNEL

➤ Prendre en compte la situation politico-sécuritaire du pays de destination : consulter le site internet du ministère de l'Europe et des Affaires étrangères (MEAE) et se rapprocher de son assurance.

➤ Se renseigner sur les us et coutumes et les législations locales, notamment en matière de chiffrement de données.

➤ Lors d'un voyage dans un pays à risque :
- s'inscrire préalablement sur le site dédié Ariane du MEAE ;
- signaler son déplacement à l'ambassade ou au consulat ;
- convenir d'un contact à intervalle régulier en France.

➤ Garder à l'esprit que la menace d'ingérence économique n'est pas limitée aux seuls pays dits « à risque ».

➤ Préparer les numéros de téléphone d'urgence : assistance et services diplomatiques.

➤ Disposer d'une copie de ses papiers d'identité, rangés dans un endroit distinct des originaux. Ils peuvent être déposés sur le site service-public.fr, portail internet gratuit et confidentiel permettant de créer facilement un espace de stockage accessible 24h/24.

➤ En cas de traitement médical, se munir des copies des ordonnances afin de justifier la possession de produits, parfois interdits dans certains pays.

➤ N'emporter que les documents indispensables à la mission. Dans le cas de transport de données sensibles, penser à les chiffrer, si possible.

➤ Se renseigner (douanes, ambassades, conseillers du commerce extérieur) sur les législations et les pratiques locales, notamment douanières, afin de connaître les modalités d'entrée de marchandises et de matériels sur le territoire tiers : déclaration préalable, normes, sécurité sanitaire, etc.

➤ Déclarer la marchandise dès l'arrivée dans le pays tiers (hors UE) auprès des autorités douanières compétentes (visa du **carnet ATA**, par exemple).

TECHNIQUE

➤ En cas de sensibilité particulière du déplacement, prévoir un ordinateur portable et un téléphone dédiés.

➤ Désactiver les ports USB, les connexions WIFI et Bluetooth des ordinateurs portables depuis le panneau de configuration.

Pendant le séjour

COMPORTEMENTAL

➤ Ne pas considérer le coffre-fort de l'hôtel comme un lieu sûr pour stocker des informations sensibles.

➤ Surveiller en permanence ses documents et ses moyens nomades de communication. Les conserver avec soi.

➤ Être prudent dans les communications : garder à l'esprit que les conversations au téléphone ou par internet peuvent être interceptées (Wifi des hôtels, des entreprises locales visitées, des lieux publics, etc.).

➤ En cas d'utilisation du Wifi, éviter les mises à jour des systèmes d'exploitation/ applications.

➤ Rester vigilant dans ses relations et son comportement :
- éviter les sollicitations impromptues, demandées à titre amical ;
- veiller à ne pas s'exposer à tout ce qui pourrait relever de la provocation, y compris de ses partenaires, dans le cas d'une demande sortant du cadre officiel ;
- éviter les excès de toute nature susceptibles d'être utilisés à son encontre.

➤ Éviter les signes d'appartenance ou d'identification à une entreprise ou à une organisation.

➤ Rester discret dans les lieux publics : ne pas s'engager dans des conversations sensibles ou confidentielles dans les chambres d'hôtel, chez un particulier, au restaurant ou encore sur les réseaux sociaux.

➤ Dans les salons et réunions internationaux, maîtriser l'information à diffuser, se méfier des faux clients et des sollicitations multiples.

➤ Dans le cas d'une location de voiture, ne pas connecter le smartphone avec le véhicule afin d'empêcher la récupération et le transfert de vos données (sms, contact, photos…). En cas d'utilisation du Bluetooth, penser à effacer les données présentes dans le système d'information du véhicule.

Après le séjour

ORGANISATIONNEL

➤ Organiser des échanges de bonnes pratiques avec des collègues ou des confrères sur le déplacement dans le pays.

➤ Conserver les documents prouvant que la marchandise transportée n'a pas été acquise dans un pays tiers (carnet ATA, ou déclaration d'exportation temporaire sous conditions), afin de ne pas se voir réclamer le paiement de droits de douane éventuels ou de la TVA.

TECHNIQUE

➤ Ne pas utiliser les supports informatiques remis lors de votre voyage (clés USB, goodies, etc.) avant de les avoir minutieusement fait analyser.

COMPORTEMENTAL

➤ Rendre compte au responsable sûreté de l'entreprise, de tout fait qui aura suscité l'étonnement lors du déplacement (cf. Rapport d'étonnement en annexe 1).

G2. Se déplacer à l'étranger

Mots clés

Carnet ATA : du nom de la convention ATA (Admission temporaire) de Bruxelles de 1961, il est délivré par les chambres de commerce et d'industrie, il se substitue aux différents documents douaniers normalement requis pour une opération d'importation ou d'exportation temporaires et permet ainsi de réaliser ces opérations en suspension de droits et taxes.

Rapport d'étonnement : compte rendu à adresser au responsable sûreté de l'entreprise relatant toute situation anormale ou inhabituelle (lors d'un déplacement ou au sein/aux abords de l'entreprise). L'ensemble de ces rapports permettra au responsable sûreté de disposer d'une vision générale des vulnérabilités de son entreprise et des activités qui s'y exercent afin d'adapter la politique de sécurité en lien avec les autorités.

Pour aller plus loin

- **Ministère de l'Europe et des Affaires étrangères (MEAE)**
  - Conseils aux voyageurs
  - Fil Ariane (déclarer ses voyages à l'étranger)
- **Agence nationale de la sécurité des systèmes d'information (Anssi)**
  - Passeport de conseils aux voyageurs
- **Club des directeurs de sécurité des entreprises (CDSE)**
  - Passeport pour la sécurité des voyageurs salariés à l'étranger
- **Douanes**
  - Les régimes suspensifs douaniers et fiscaux

G3. Participer à un salon professionnel

Si les salons professionnels sont souvent porteurs de nouvelles opportunités commerciales, ils sont également un point d'attention particulier pour les acteurs économiques les moins loyaux. Pour « exposer sans trop s'exposer » il est donc indispensable de préparer rigoureusement ces événements en intégrant de solides paramètres de sécurité.

Avant le salon

ORGANISATIONNEL

➤ Définir les informations qui pourront être ou non diffusées sur le salon. Eviter les dossiers de presse trop complets. Préparer par écrit, avec les collaborateurs et/ou une agence de communication, les éléments de langage sur les sujets délicats ou indiscrets (innovation, savoir-faire, etc.).

➤ Désigner un responsable en charge du matériel sensible lors du montage et du démontage du stand, périodes particulièrement exposées.

➤ Identifier par badge les animateurs du stand.

➤ Si possible, choisir l'emplacement de son stand en fonction de la concurrence (ni trop près ni trop loin) et s'assurer que le stand initialement proposé n'est pas déplacé sur un autre emplacement au dernier moment.

➤ Ne pas placer les matériels sensibles en bordure du stand, ou prévoir, le cas échéant, des vitrines fermant à clé.

➤ Envisager une zone permettant des échanges en toute discrétion.

➤ Sensibiliser les collaborateurs sur les risques de manipulation (flatterie, partage d'un intérêt commun, fausse vérité, information gratuite, etc.) et convenir à l'avance avec eux de réponses adaptées, notamment en cas d'interview par la presse.

➤ Vérifier la couverture assurantielle de l'entreprise par rapport aux salons.

➤ Prévoir des plaquettes de plusieurs niveaux d'information successifs, destinées à être communiquées en fonction des garanties de sérieux et d'engagement du client potentiel.

TECHNIQUE

➤ Limiter autant que possible le nombre de documents ou de matériels sensibles.

➤ Préparer un ordinateur uniquement dédié aux présentations pour le salon et dénué de toutes données sensibles. Verrouiller les ports USB de tous les autres ordinateurs, une clé USB pouvant contenir un logiciel malveillant.

➤ Mettre en place une déchiqueteuse pour détruire de façon sécurisée les documents de travail (devis, schémas, etc.).

➤ Lister les produits qui seront présentés durant le salon.

➤ Si possible, développer, des prototypes ou des répliques anodines pouvant être exposés sans risque de dévoiler une caractéristique majeure du produit (non à l'échelle de préférence) ou de permettre un prélèvement, notamment quand l'innovation réside dans les matériaux.

Pendant le salon

TECHNIQUE

➤ Désactiver les fonctions Bluetooth et Wifi des appareils nomades de communication.

➤ Sécuriser le matériel informatique et de démonstration du stand : antivols, vitrines fermées à clé, etc.

➤ Utiliser un mot de passe personnel dédié au salon composé au minimum de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien personnel et ne figurant pas dans le dictionnaire.

➤ En cas d'échange de documents lors d'une présentation commerciale, utiliser une clef USB destinée uniquement à cet usage, et effacer ensuite les données avec un logiciel d'effacement sécurisé.

➤ Ne pas utiliser les « *flash code* » proposés par les clients, concurrents, ces derniers peuvent en effet contenir des logiciels malveillants.

COMPORTEMENTAL

➤ Éviter d'utiliser les moyens de communication mis à disposition (comme les bornes Wifi gratuites).

➤ Appréhender avec discernement les rencontres fortuites ou trop amicales et bienveillantes.

➤ Savoir éconduire des visiteurs « parasites » (mise en place de contre-mesures dans le cas d'actions d'entraves commerciales de style « saturation » de stand par des concurrents ou des complices de ceux-ci).

➤ Demander systématiquement une carte de visite à ceux qui témoignent un intérêt aux produits, saisir les informations enregistrées sur leur badge et vérifier l'identité de ses interlocuteurs.

➤ Éviter de répondre aux sondages, questionnaires et enquêtes multiples. Identifier clairement les demandeurs et s'assurer de la destination des informations transmises.

➤ Être vigilant en permanence : la fatigue gagne souvent en fin de journée et vers la fin du salon, et avec elle la vulnérabilité augmente.

➤ Éviter les entretiens et les conversations sensibles dans les lieux publics (transports, restaurants, hôtels, etc.)

➤ Ne pas aborder de sujets confidentiels au téléphone.

➤ Être vigilant lors des échanges dans les événements connexes au salon (dîners, cocktails, conférences, pause déjeuner, machine à café, etc.).

➤ Ne jamais laisser de documents sensibles sans surveillance, les conserver avec soi. Aucune réserve n'est sûre (coffre de la voiture, coffre-fort de la chambre d'hôtel, réserve du stand, etc.).

➤ Ne jamais laisser sans surveillance les matériels à risque (prototypes, maquettes, ordinateurs personnels, etc.), notamment hors des heures d'exposition.

➤ Surveiller constamment ses outils de travail (mallettes, ordinateurs, téléphones portables, etc.).

G3. Participer à un salon professionnel

Après le salon

ORGANISATIONNEL

➤ Lors de la clôture, faire place nette sur le stand et vérifier l'ensemble des matériels et documents.

➤ Faire un retour d'expérience et rédiger un **rapport d'étonnement** relatant tout problème ou événement inattendu survenu lors du salon.

➤ Exploiter les cartes de visites des « démarcheurs » (se demander s'ils sont des clients ou des concurrents potentiels).

➤ Établir un bilan de l'activité et suivre les commentaires au sein de la profession et des médias (forums internet, presse spécialisée, etc.).

➤ Aviser les services de l'État de toute tentative d'ingérence et de tout événement ayant suscité l'étonnement durant le salon.

ANNEXE 1
Le rapport d'étonnement dans le cadre de la sécurité économique

Le rapport d'étonnement se présente comme un document formalisé, relativement concis, qui rapporte l'observation d'un fait ou d'un comportement inhabituel, a priori illogique au regard du contexte, ou intrusif quant aux activités de l'entreprise[1]. Il relate les faits de façon brute, dans la plupart des cas sans analyse (mais peut parfois comporter des commentaires qui présentent un potentiel risque pour l'entreprise).

Il a pour objet d'attirer l'attention des décideurs ou des responsables sûreté/sécurité afin que, sur la base de leur analyse du document, ils puissent définir et mettre en œuvre les mesures pertinentes, en réponse au risque découvert, ou accompagner le personnel afin de lui permettre d'adapter son comportement et ainsi prévenir les périls.

L'accumulation de rapports d'étonnement sur plusieurs faits similaires permettra de transformer des signaux faibles en véritables analyses de risques.

Le rapport porte sur des faits internes ou externes à l'entreprise :

- internes > comportement particulier ou atypique, processus à risque, demande suspecte, courriels/communications internes suspects ;
- externes > à l'occasion d'une réunion à l'extérieur, d'un salon, d'un déplacement à l'étranger, changements dans le cadre d'une relation fournisseurs/prestataires/sous-traitants, réception de courriels/communications externes suspects, etc.

Aspects méthodologiques

➤ Communiquer et sensibiliser les personnels à l'utilité de faire remonter tout type d'étonnement, positif ou négatif, par exemple par le biais d'un *memento*.

➤ Déterminer en amont les personnes qui seront destinataires de ces rapports d'étonnement : supérieur hiérarchique, responsable sûreté, référent « intelligence économique », RSSI, etc.

➤ Élaborer un masque/trame du rapport à mettre à disposition des salariés de l'entreprise.

➤ Garder une certaine confidentialité sur le rapport durant la phase de vérification des faits rapportés.

➤ Agir en conséquence si le rapport met en évidence des faits induisant un risque pour l'entreprise.

Concernant la forme, il est possible de mettre au point deux types de rapports d'étonnement :

- généraliste > un format unique pouvant convenir à toutes les problématiques de l'entreprise (organisation, relation commerciale, sécurité, sûreté, etc.) ;
- thématique > un format spécifique à chaque problématique.

[1] Le rapport d'étonnement a souvent pour objet de signaler un risque ou un fait négatif mais il peut également faire état d'une opportunité ou d'un fait positif, potentiellement bénéfique à l'entreprise (identification de nouvelles technologies, de nouveaux marchés, etc.).

Exemple de rapport d'étonnement

DATE : 13/09/2020

ÉMETTEUR : MARTIN MICHEL

DIRECTION/SERVICE : DIRECTION DE LA STRATÉGIE

DESTINATAIRE : DIRECTEUR SURETÉ/SÉCURITÉ-DIRECTEUR GÉNÉRAL-SECRÉTAIRE GÉNÉRAL

SUJET : comportement suspect d'un individu dans le TGV Paris-Londres

FAITS : le 13 septembre 2020, lors d'un déplacement professionnel à destination de Londres, j'ai été amené à entrer en contact avec un individu au comportement suspect. L'individu occupait ma place à mon arrivée à bord du train. En tenue *sportswear*, il n'avait aucun bagage avec lui, ni valise ni porte-document ou ordinateur. Au cours de la discussion, l'individu a tenté d'obtenir des informations sur ma vie personnelle, des détails sur ma vie professionnelle et a tenté d'amener à plusieurs reprises la discussion sur des sujets auxquels je m'intéresse (juridiques, géopolitiques). Parlant de lui, il a mentionné résider a Barcelone, ville dont est originaire ma femme et dans laquelle je passe souvent des vacances.

COMMENTAIRE : la curiosité de l'individu me paraissant suspecte, je suis resté très évasif dans mes réponses. Souhaitant à aucun moment alimenter/relancer la discussion, je n'ai pu obtenir aucun élément sur son identité ou ses fonctions.

ANNEXE 2

Loi Sapin II du 9 septembre 2016

La loi n° 2016-1691 du 9 décembre 2016 relative à « la transparence, à la lutte contre la corruption et à la modernisation de la vie économique », dite « loi Sapin II », a notamment introduit de nouvelles dispositions pour lutter plus efficacement contre la corruption. Cette loi a pour ambition de porter la législation française aux meilleurs standards européens et internationaux en matière de lutte contre la corruption, et de contribuer ainsi à une image positive de la France à l'international.

LES PRINCIPALES NOUVEAUTÉS

➤ Imposition aux entreprises d'une **obligation de prévention et de détection** des risques de corruption.

Cette obligation, qui ne concerne que les « grands groupes », est développée ci-dessous.

➤ Instauration de l'**Agence française anticorruption (Afa)**.

Il s'agit d'un service à compétence nationale chargé de la détection et de la prévention des atteintes à la probité, placé auprès du ministre de la Justice et du ministre des Finances.

➤ Création d'une **peine complémentaire de mise en conformité**.

Cette peine pourra être prononcée à l'encontre des personnes morales condamnées pour atteinte aux dispositions anti-corruption, et son respect sera placé sous le contrôle de l'Afa.

➤ Introduction d'une **procédure transactionnelle**, alternative aux procédures judiciaires.

Appelée « Convention judiciaire d'intérêt public », cette procédure consiste en un accord entre le procureur de la République et les entreprises soupçonnées de corruption, permettant à ces dernières d'échapper à la reconnaissance de leur culpabilité moyennant le paiement d'une amende pénale d'intérêt public et l'application d'un programme de conformité.

L'OBLIGATION DE PRÉVENTION ET DE DÉTECTION DES RISQUES DE CORRUPTION

- **Qui est concerné ?**

➤ Pour les dispositions anticorruption : les sociétés exerçant tout ou partie de leur activité en France.

➤ Pour les obligations de prévention et de détection : les « grands groupes », c'est-à-dire :
- les sociétés employant au moins 500 salariés et dont le CA > 100 millions d'euros ;
- les groupes de sociétés d'au moins 500 salariés, dont la société mère a son siège social en France, et ayant un CA consolidé > 100 millions d'euros.

- **Quelles obligations ?**

Pour se mettre en conformité face aux nouvelles obligations, les entreprises concernées doivent mettre en place :

1. Un « Code de conduite » des comportements prohibés

Ce « Code de conduite » devra prévoir des sanctions disciplinaires et être intégré au règlement intérieur : (il faudra donc consulter les représentants du personnel, informer l'inspecteur du travail et prévoir le dépôt du règlement au greffe du Conseil de prud'hommes et son affichage dans les locaux de l'entreprise).

2. Une procédure interne de lancement d'alerte

Cette procédure devra permettre aux employés d'alerter d'un comportement ou d'une situation contraire au « Code de conduite » (la mise en place de la procédure d'alerte est détaillée dans la fiche D 6).

3. Une cartographie des risques

Cette cartographie, qui devra être régulièrement actualisée, est destinée à identifier, analyser et hiérarchiser les risques de corruption. Elle devra être adaptée aux problématiques propres à la société, notamment en fonction des secteurs d'activités et des zones géographiques dans lesquels elle exerce son activité.

4. Procédures de vérification de l'intégrité des clients, fournisseurs, partenaires et intermédiaires

Ces procédures de vigilance visent à éviter d'entrer en relation d'affaires avec des tiers susceptibles de recourir, ou d'être sujet, à des méthodes corruptives. Des clauses anticorruption efficaces, garantissant de pouvoir se dégager de la relation d'affaires corrompue, devront être prévues.

5. Procédures de contrôle comptables

Ces procédures internes ou externes ont pour objectif de vérifier la possible dissimulation de sommes allouées à la corruption et au trafic d'influence. Le Service central de prévention de la corruption (SCPC), en mars 2015, a recommandé de prévoir une vérification périodique et de transmettre le compte-rendu de ces vérifications aux instances dirigeantes. Il est remplacé aujourd'hui par l'Agence française anticorruption (Afa, voir *supra*).

6. Dispositif de formations

L'effort de formation devra tout particulièrement être porté sur les équipes dirigeantes et sur les fonctions à risque. Ces formations devront être adaptées selon les zones et fonctions du personnel concerné et être renouvelées régulièrement.

7 Sanctions disciplinaires en cas de violation du « Code de conduite »

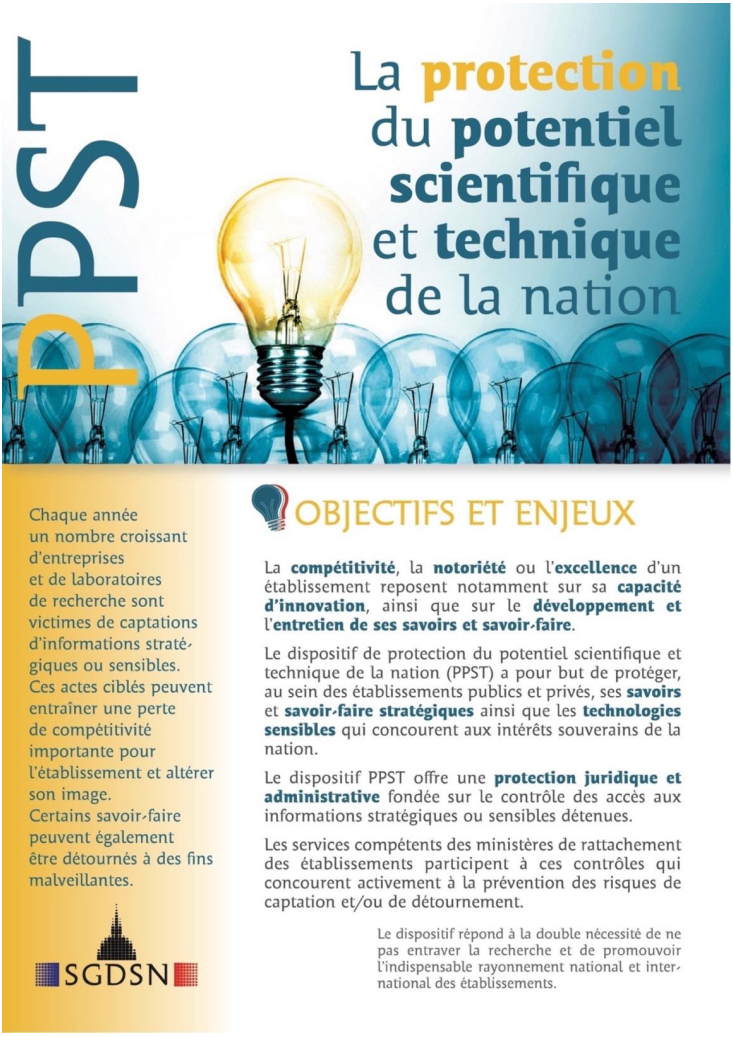
Les salariés devront connaître les sanctions disciplinaires éventuellement applicables en cas de violation des prescriptions du « Code de conduite ».

8. Dispositif de contrôle interne et d'évaluation des mesures adoptées

Il s'agit de vérifier si le programme de conformité est adapté aux besoins, aux risques et aux problématiques de l'entreprise, et si sa mise en œuvre est effective. Un audit de conformité peut compléter ce contrôle interne afin de détecter d'éventuelles failles dans la procédure mise en place.

ANNEXES 3

La protection du potentiel scientifique et technique de la nation



FONCTIONNEMENT

La réglementation prévoit **l'identification des zones à régime restrictif (ZRR) abritant les activités de recherche ou de production stratégiques de l'établissement**. Il peut s'agir de bureaux, de laboratoires, de plates-formes expérimentales, etc.

Lorsqu'une personne souhaite accéder à une ZRR pour y **travailler** (travail contractuel ou relevant d'une convention de coopération, sous-traitance, etc.) une **demande d'accès** doit être formulée auprès du ministère de rattachement de l'établissement. Le ministère instruira le dossier de demande d'accès et émettra un avis fondé sur une analyse technique et de sécurité dans un délai maximum de deux mois.

Le dispositif offre un espace de **dialogue privilégié entre l'établissement et son ministère de rattachement.**

AVANTAGES

- ✓ **Contraintes limitées** pour l'établissement. Aucune mesure de protection physique n'est exigée en dehors d'un espace clos. L'établissement protège sa/ses zone(s) selon ses moyens et son besoin de protection
- ✓ **Flexibilité** du dispositif pour l'entité qui identifie et cible son besoin de protection en lien avec le ministère concerné
- ✓ **Protection juridique** renforcée contre les actes malveillants ayant des conséquences sur la compétitivité de l'établissement
- ✓ Appartenance à **une communauté de confiance** favorable aux partenariats industriels ou de recherche
- ✓ **Accompagnement étatique personnalisé** dans la démarche d'élévation du niveau de sécurité de l'établissement

MISE EN ŒUVRE

Le dispositif PPST offre une **protection juridique et administrative** qui découle de la constitution d'une zone abritant les activités identifiées comme sensibles ou stratégiques. Les contours physiques de cet espace clos doivent être matérialisés par une signalétique informant du statut de la zone.

Chaque entité décide selon ses moyens et ses besoins de déployer ou non des moyens de protection supplémentaires (lecteur de badge, caméra de surveillance).

CYBERSÉCURITÉ

Les établissements adhérant au dispositif PPST doivent se doter d'**une politique de sécurité des systèmes d'information (PSSI)**. La PSSI est un document interne à l'établissement qui contribue à ce que chaque utilisateur adopte les bons réflexes d'hygiène informatique, tels que préconisés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le but de cette politique est de réduire les incidents de sécurité et les coûts associés.

Plus d'informations sur :
www.ssi.gouv.fr

Je suis concerné par le dispositif si, la captation indue ou le détournement des savoirs, savoir-faire et technologies développés ou mis en œuvre dans mon établissement peuvent :

- Porter préjudice de manière significative à ma **compétitivité**, à celle de mes partenaires industriels ou à celle du pays ;
- Générer une menace du fait d'un usage possible à des fins **terroristes** sur le territoire national ou à l'étranger ;
- Permettre le développement d'une **arme conventionnelle** ;
- Favoriser le développement d'une **arme de destruction massive**.

ACTEURS ET RESPONSABILITÉS PPST

PREMIER MINISTRE / SGDSN

Le secrétariat général de la défense et de la sécurité nationale (SGDSN) assure, par délégation du Premier ministre, le pilotage et la coordination interministérielle du dispositif. Il veille au déploiement du dispositif et est garant du respect des procédures.

CHEF D'ÉTABLISSEMENT

Il est responsable de la PPST dans son établissement et en délègue la mise en œuvre au personnel compétent (fonctionnaire de sécurité et de défense, officier de sécurité, responsable de la ZRR, responsable désigné).

MINISTRES / HFDS

Le ministre compétent, par le biais de son haut fonctionnaire de défense et de sécurité (HFDS) détermine le besoin de protection en relation avec les établissements. Il crée et supprime les ZRR. Il émet des avis sur les demandes d'accès.

CONTACTS

Pour toute question, merci de contacter le service du Haut fonctionnaire de défense et de sécurité de votre ministère de rattachement:

- Ministère chargé de l'agriculture
  intelligence.economique@agriculture.gouv.fr
- Ministère chargé de la défense
  dga-ssdi.visit.fct@intradef.gouv.fr
- Ministère chargé du développement durable
  ppst.diepi.sdsie.sg@developpement-durable.gouv.fr
- Ministère chargé de l'économie et des finances
  ppst.hfds@finances.gouv.fr
- Ministère chargé de la recherche
  hfds-zrr-creation@recherche.gouv.fr
- Ministère chargé de la santé
  hfds-ppst@sante.gouv.fr

- SGDSN :
  ppst@sgdsn.gouv.fr
- Plus d'informations sur :
  www.sgdsn.gouv.fr

A propos du SGDSN

Service du Premier ministre travaillant en liaison étroite avec le Président de la République, le secrétariat général de la défense et de la sécurité nationale (SGDSN) assiste le chef du Gouvernement dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Il est chargé de l'animation et de la coordination interministérielles du dispositif PPST.

Textes de référence

- Code pénal - article 410-1
- Décret N°2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
- Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation.
  N°3415/SGDSN/AIST/PST
  du 7 novembre 2012

ANNEXE 4

Le *Clarifying Lawful Overseas Use of Data Act* ou *Cloud Act*

La loi américaine du 23 mars 2018 appelée *Cloud Act*, visant à clarifier l'usage des données hébergées en dehors des États-Unis en matière judiciaire, a des conséquences majeures sur la souveraineté des données des entreprises françaises recourant à des prestataires américains. Elle a pour objectif de préciser d'avantage les règles relatives aux réquisitions des autorités américaines sur les données stockées en dehors de leur territoire et pose des difficultés en termes de respect de la vie privée, des Européens en particulier.

Elle offre la possibilité aux autorités de poursuite américaine, en s'appuyant sur leurs entreprises nationales du numérique, de saisir des données partout dans le monde, en dehors de toute procédure d'entraide judiciaire, et sans offrir de réelle réciprocité aux États hébergeant les entreprises ou les données visées par ces saisies. Dans le cadre des procédures de justice américaine, cette loi facilite ainsi l'accès par les autorités qui en font la demande aux données des entreprises étrangères, sans que les autorités compétentes du pays, ni que les hébergeurs de données, ni même que leurs clients finaux ne soient informés de cette demande.

Dans ce contexte le recours par des entreprises à des prestataires de service français ou européens doit être favorisé.

CONTACTS UTILES

Cet annuaire présente une liste non exhaustive de partenaires institutionnels pouvant vous accompagner dans votre démarche de sécurité économique ou vous offrir leur expertise sur leur domaine de compétence.
Y figurent notamment certains services d'enquête judiciaire à même de mener des investigations sur des délits visant les entreprises, des attaques et intrusions informatiques perpétrées dans un but crapuleux aux captations d'actifs industriels.
Une démarche de plainte, si elle est souhaitée par les dirigeants, doit s'anticiper, tant au niveau des éléments de traçabilité qu'en terme d'engagement juridique que celle-ci implique.

MINISTÈRE DES ARMÉES

➤ Direction du renseignement et de la sécurité de la défense (DRSD)

La DRSD est le service de renseignement « dont dispose le ministre des Armées pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles ».

La DRSD assure une mission de contre-ingérence au profit des entités du ministère des armées et des entreprises en lien avec la défense afin de protéger leurs intérêts économiques et financiers et apporter une contribution renforcée en matière de cyber-défense. Sa devise est « renseigner pour protéger ».

http://www.defense.gouv.fr/dpsd

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

➤ Direction générale des douanes et droits indirects (DGDDI)

Administration de régulation des échanges, la DGDDI est chargée de faciliter et sécuriser les flux de marchandises (notamment lors de la demande d'intervention en matière de lutte contre la contrefaçon, ou pour la réglementation en matière de biens à double usage). En prise directe avec la chaîne logistique des opérateurs, au cœur des flux de marchandises, elle oriente et accompagne les opérateurs vers les solutions douanières les plus adaptées à leurs opérations de commerce international. Le statut d'opérateur économique agréé est l'un des instruments clés de cette démarche.

Demande d'intervention contrefaçon : contrefac@douane.finances.gouv.fr

Prohibitions : dg-e2@douane.finances.gouv.fr

Opérateur économique agréé : dg-e3-oea@douane.finances.gouv.fr

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

➤ **Service du haut fonctionnaire de défense et de sécurité (SHFDS)**

HFDS Bercy

Le HFDS conseille et assiste le ministre de l'Économie, des Finances et de la Relance et le ministre chargé de l'Action et des Comptes publics pour toutes les questions relatives aux mesures de défense et de sécurité, et aux situations d'urgence affectant la défense, la sécurité et la vie de la nation, tout particulièrement dans le domaine économique.

Pour les acteurs économiques relevant des ministères précités, il assure notamment des missions de conseil, de coordination et de contrôle s'appliquant :

- à la protection et à la sécurité des infrastructures et des secteurs d'activités d'importance vitale (SAIV) dont le dysfonctionnement provoquerait rapidement un arrêt de l'économie du pays. Cela concerne les secteurs : finances, industrie, communications électroniques, audiovisuel et information ;

- à la protection du potentiel scientifique et technique (PPST).
https://www.economie.gouv.fr/hfds/service-secretaire-general-haut-fonctionnaire-de-fense-et-securiteservice-hfds.bercy@finances.gouv.fr

ppst.hfds@finances.gouv.fr

➤ Service de l'information stratégique et de la sécurité économiques (Sisse)

Placé auprès de la Direction générale des Entreprises (DGE) du ministère de l'Économie des Finances et de la Relance, le Sisse a notamment pour missions :

- d'identifier les secteurs, les technologies et les entreprises relevant des intérêts économiques, industriels et scientifiques de la nation et centraliser les informations stratégiques les concernant ;

- de concourir à l'élaboration de la position du gouvernement en matière d'investissements étrangers ;

- d'informer les autorités de l'État sur les personnes, entreprises et organismes présentant un intérêt ou représentant une menace pour les intérêts stratégiques ;

- de contribuer à veiller à la bonne application de la loi du 26 juillet 1968 (protection d'informations sensibles).

www.entreprises.gouv.fr/information-strategique-Sisse

sec.cSisse@finances.gouv.fr

Le Sisse pilote et anime un réseau de Délégués à l'information stratégique et à la sécurité économiques (Disse) qui sont en poste dans les Directions régionales de l'économie, de l'emploi, du travail et des solidarités (Dreets). pour la mise en œuvre de la politique d'intelligence économique territoriale. Les Disse viennent ainsi en appui de l'autorité préfectorale dans les régions.

Auvergne-Rhône-Alpes	ara.disse@dreets.gouv.fr
Bourgogne-Franche-Comté	bfc.disse@dreets.gouv.fr
Bretagne	bret.disse@dreets.gouv.fr
Centre Val de Loire	cvl.disse@dreets.gouv.fr
Corse	corse.corressisse@dreets.gouv.fr
Grand Est	ge.disse@dreets.gouv.fr
Hauts-de-France	hdf.disse@dreets.gouv.fr
Île-de-France	idf.disse@drieets.gouv.fr
Normandie	norm.disse@dreets.gouv.fr
Nouvelle-Aquitaine	na.disse@dreets.gouv.fr
Occitanie	oc.disse@dreets.gouv.fr
Pays de la Loire	pdl.disse@dreets.gouv.fr
Provence-Alpes-Côte d'Azur	paca.disse@dreets.gouv.fr
Antilles Guyane	971.disse@deets.gouv.fr
La Réunion	973.disse@deets.gouv.fr

➤ Institut national de la propriété industrielle (Inpi)

Au-delà de son action d'enregistrement et de délivrance de titres de propriété industrielle (brevets, marques, dessins et modèles, Indications géographiques), l'Inpi agit en faveur du développement économique par ses actions de sensibilisation et de valorisation de l'innovation et de ses enjeux. L'Inpi accompagne tous les innovateurs pour qu'ils transforment leurs projets en objets de marché, leurs innovations en valeur.

Établissement public autofinancé et placé sous la tutelle du ministère en charge de la propriété industrielle, l'Inpi participe également activement à l'élaboration et la mise en œuvre des politiques publiques dans le domaine de la propriété intellectuelle, du soutien à l'innovation et à la compétitivité des entreprises, tout comme de la lutte anti-contrefaçon.

www.inpi.fr - contact@inpi.fr

MINISTÈRE DE L'INTÉRIEUR

➤ Brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti)

La préfecture de Police dispose d'un service de lutte contre la cybercriminalité, la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti, service de la Direction régionale de la Police judiciaire (DRPJ).

Chargée de mener des enquêtes judiciaires sur des attaques ciblant plus particulièrement les systèmes et réseaux informatiques de personnes morales, la Befti est saisie par des magistrats des Tribunaux de grande instance de Paris, Nanterre, Saint Denis et Créteil.

La Befti assure également des assistances techniques au profit des services de la préfecture de Police ainsi que des actions de sensibilisation auprès de divers acteurs économiques.

Les victimes sont invitées à déposer plainte auprès des commissariats.

➤ Direction de la coopération internationale (DCI)

La Direction de la coopération internationale, direction commune de la police et de la gendarmerie nationales, est en mesure de vous conseiller, aussi bien dans la phase préparatoire de vos déplacements que lors de vos séjours professionnels à l'étranger.

Contact DCI : dci-partenariats@interieur.gouv.fr

➤ Direction générale de la sécurité intérieure (DGSI)

La DGSI est le service de référence concernant les menaces économiques étrangères pouvant porter atteinte aux entreprises françaises et plus généralement aux intérêts fondamentaux de la nation.

Dans le cadre de ses missions, la DGSI réalise des actions de sensibilisations individuelles et collectives auprès des entreprises publiques et privées, elle participe de manière active à la politique publique de l'intelligence économique et apporte aussi son soutien pour répondre aux enjeux d'une économie mondialisée dans un esprit de partenariat avec les entreprises.

securite-economique@interieur.gouv.fr

➤ Gendarmerie nationale

La Gendarmerie nationale dispose d'un réseau de référents Sécurité économique et protection des entreprises (SEcoPE) disséminés sur toute l'étendue du territoire.

Présents jusqu'au niveau départemental, ces référents agissent pour prévenir les atteintes à la sécurité économique et sensibiliser les acteurs territoriaux dans une dynamique de réseau et de partenariat.

Les référents sécurité économique et protection des entreprises de la gendarmerie sont à votre écoute.

securite-economique@gendarmerie.interieur.gouv.fr

➤ **Service central du Renseignement territorial (SCRT)**

Le SCRT qui a une compétence nationale étendue aux zones de police et de gendarmerie, rencontre au quotidien les chefs d'entreprises, les responsables syndicaux, les salariés, les responsables associatifs et institutionnels afin de capter les alertes sociales qui, en fragilisant le tissu économique d'un bassin d'emploi, peuvent déboucher sur des risques de trouble à l'ordre public.

Grâce à son implantation territoriale et à ce réseau de correspondants en milieu ouvert, le SCRT est en capacité de coordonner ses efforts avec ceux de la DGSI dans le cadre de la mise en œuvre d'une politique publique d'intelligence économique. Le SCRT, au travers de ses référents départementaux, assure une mission de veille sur l'économique territoriale, en lien avec les référents sûreté implantés dans les directions départementales de la sécurité publique ; il est également le partenaire naturel de la DGGN.

SDLC / OCLCTIC

➤ **Sous-direction de la lutte contre la cybercriminalité (SDLC)**

Au sein de la direction centrale de la police judiciaire (police nationale), la SDLC constitue, depuis 2014, le pôle national de compétences dans son domaine. Elle s'adapte en permanence à la généralisation de l'utilisation des nouvelles technologies dans la commission des infractions et s'inscrit dans un contexte international de mobilisation des institutions pour apporter des réponses à ces menaces. La SDLC développe une politique globale de lutte contre la cybercriminalité intégrant les missions de prévention et de répression. Elle définit les stratégies opérationnelles et de formation. Depuis mars 2018, le réseau des référents cybermenaces zonaux mis en place par la SDLC permet à des équipes innovantes, policiers, réservistes et partenaires privés, de mener des actions de sensibilisation et de prévention auprès des entreprises du tissu économique local et d'améliorer la collaboration entre la police nationale et le secteur privé.

https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

➤ Agence nationale de la sécurité des systèmes d'information (Anssi)

Rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), sous l'autorité du Premier ministre, l'Anssi assure la sécurité et la défense des systèmes d'information de l'État et des opérateurs critiques en créant les conditions d'un environnement de confiance.

www.anssi.gouv.fr

LA SÉCURITÉ ÉCONOMIQUE AU QUOTIDIEN

Entrepreneurs, chercheurs, ingénieurs, financiers, représentants du personnel, fonctionnaires, salariés du secteur public et du secteur privé, votre activité économique, votre compétitivité, et même parfois votre emploi reposent – pour partie – sur votre capacité à protéger, au quotidien, votre production, votre savoir-faire, vos informations et votre entreprise. Vous en êtes ainsi les meilleurs garants.

Bien entendu, il est indispensable de rester ouvert et de transmettre de l'information à ses partenaires. Bien entendu, il faut soigner sa communication envers ses clients et ses financeurs. Notre économie n'offre aucune perspective à ceux qui se renferment sur eux-mêmes.

Mais pour autant, il est désormais tout aussi indispensable de considérer l'information comme un bien précieux qu'il faut gérer avec rigueur, professionnalisme et surtout bon sens.

En 2014, vous découvriez les 22 fiches pratiques de sécurité économique. Devant le succès remporté, le Service de l'intelligence stratégique et de la sécurité économiques a donc jugé utile de les mettre à jour et de les compléter par des entrées abordant de nouveaux risques.

Ensemble nous contribuons ainsi à améliorer la sécurité de notre économie et sa compétitivité globale.