



GUIDE DE LA SECURITE ECONOMIQUE



CCI DE LA VENDEE
Centre d'Information Economique
16 rue Olivier de Clisson— BP 49
85002 LA ROCHE SUR YON CEDEX

Tél: 02 51 45 32 53
Fax : 02 51 62 72 17
Courriel : cie@vendee.cci.fr
www.vendee.cci.fr

Informations et préconisations
à destination des PME-PMI





Et si la sécurité économique devenait un enjeu dans la performance de nos entreprises ?

Quelle que soit la taille et l'activité de l'établissement, le chef d'entreprise doit intégrer la sécurité économique dans sa stratégie.

Dans cette compétition économique mondiale, l'entreprise se doit d'être dans les starting-blocks pour progresser et rester performante. Chaque décision, chaque orientation nouvelle, est déterminante pour décrocher de nouvelles victoires et ainsi assurer l'avenir de l'entreprise. Des choix tactiques qui s'échafaudent sur l'analyse et la perception de son environnement. Ne pas connaître ses atouts et ses faiblesses, c'est octroyer un avantage considérable à son adversaire et lui faire connaître c'est perdre d'avance.

Alors s'engage une réflexion sur l'information stratégique que l'entreprise possède et des méthodes mises en place pour la protéger. Pour toujours garder une longueur d'avance mieux vaut s'entraîner dans le secret !

Les menaces existent au niveau du système d'information de l'entreprise, des personnes, du patrimoine... Sans tomber dans la paranoïa et sans développer des technologies sophistiquées, quelques premières règles de bon sens peuvent s'appliquer au quotidien. A nous de les adopter le plus simplement possible.

Pour vous aider, la Chambre de Commerce et d'Industrie de la Vendée vous propose « Le guide de la sécurité économique ». Cet outil vous apporte des éléments de réflexion sur les éventuelles menaces extérieures et vous offre un inventaire de quelques principes de vigilance et de précaution.

Arnaud Ringeard
Président de la Commission Intelligence Economique
de la Chambre de Commerce et d'Industrie de la Vendée



Pourquoi un guide de la sécurité économique ?

Ce guide est un exposé des bonnes pratiques en matière de sécurité économique et un outil de sensibilisation et de réflexion sur les risques économiques, environnementaux, informatiques...

Votre entreprise peut un jour être exposée à une agression économique de par sa situation géographique, son secteur d'activité, son dynamisme, sa capacité d'innovation....

Soyez dès à présent réactifs face aux éventuelles menaces en instaurant quelques principes de vigilance et de précaution.

**Adoptez le programme Sécurité Economique
pour la bonne santé de votre entreprise**

SOMMAIRE

I - Mon entreprise est potentiellement concernée par la sécurité économique

- Mon entreprise n'est pas menacée... mais les risques existent et sont bien réelsp 4
- Autodiagnostic d'évaluation des risques en entreprisep 5

II - Mon entreprise souhaite en savoir plus sur la sécurité économique

- Identification des acteurs et détermination des risques éventuelsp 6
- Qui intervient dans mon entreprise ?p 6
- Comment cet "acteur" intervient-il dans l'entreprise ?p 6
- Quels sont les risques encourus par l'intervention de cet "acteur" ?p 6
- Comment protéger le patrimoine de mon entreprise ?p 7
- Comment protéger la diffusion des informations ?p 7
- Votre entreprise doit instaurer des règles de bonne conduite
ou adopter le principe de précaution.....p 7
- Comment travailler en toute confiance avec des prestataires,
des fournisseurs et autres contacts ?p 8
- S'informer sur la réglementationp 10
- Les principales sources d'informationp 11
- Les interlocuteurs Sécurité Economique en Vendéep 12



I - Mon entreprise est potentiellement concernée par la sécurité économique

Mon entreprise n'est pas menacée ...

En France, fin 2007, 3 530 faits d'insécurité économique, pour 1741 entreprises, soit une progression sur un an de + 102 %.

La Région des Pays de la Loire est la 2^{ème} région concernée, après la Région Ile de France (tissu économique très dense, forte capacité d'innovation des entreprises, pluri-activités...)

Les secteurs les plus visés sont : l'automobile, l'aéronautique, la métallurgie et assimilés, l'agroalimentaire, l'électronique et micro-électronique, la robotique et automatismes, les transmissions et le transport...

Les secteurs nouvellement menacés sont : la banque, l'assurance, la finance, l'emballage, la papeterie, le cartonnage, le ferroviaire/méto, le médical, le bâtiment, les travaux publics, l'énergie gaz...

... mais les risques existent et sont bien réels.

Une société sur trois est vulnérable sur le plan financier :

- Atteinte au savoir-faire
- Prise de contrôle par des étrangers ou par la concurrence
- Difficulté de trésorerie
- Atteinte du système d'information
- Atteinte à la réputation de son image...

Une indécatesse sur six est commise par une personne présente dans les locaux mais extérieure à l'entreprise (stagiaire, chercheur étranger, membre d'une délégation étrangère, visiteur...) :

- Malveillance fortuite ou non
- Pillage d'informations
- Déstabilisation volontaire de tout ou partie des services de l'entreprise
- Intrusion organisée...

Une entreprise sur trois aborde la question de la sécurité informatique à ses nouveaux venus, 1/3 des entreprises dispose de directives :

- Piratage de votre messagerie ou de l'ensemble de votre système d'information
- Perte de données stratégiques
- Vol de matériel...

Vous souhaitez en savoir plus sur les risques, réalisez votre auto-diagnostic sécurité économique

Autodiagnostic d'évaluation des risques en entreprise

PROTECTION DU PATRIMOINE DE L'ENTREPRISE

Pensez-vous identifier précisément les données sensibles de votre entreprise ?

- Qui les détient ?
- Avez-vous mis en place des procédures de protection ?

Comment sont protégées vos données ?

- Avez-vous déposé un brevet, une marque, des modèles ?
- Avez-vous mis en place des contrats de confidentialité ?

Testez-vous la sécurité de votre entreprise en vue de l'améliorer ?

- Avez-vous mis en œuvre des contrôles d'accès et de protection physique des bâtiments (code d'accès, gardien, alarme, badge visiteurs...)?

PROTECTION DE L'INFORMATION

Au cours de ces deux dernières années, avez-vous été victime de tentatives de détournements d'informations ?

- Est-ce une intrusion physique, un piratage informatique, un détournement de procédures, une divulgation de rumeurs, un débauchage de personnel, une sollicitation de vos partenaires... ?

Comment gérez-vous vos déchets papiers, vos vieux ordinateurs ?

- Détruisez-vous automatiquement vos documents papier ?
- Procédez-vous au nettoyage « complet » de vos vieux ordinateurs avant recyclage ?

Disposez-vous de dispositifs et/ou de procédures de sécurité de l'information économique ?

- Avez-vous créé des contrôles anti-intrusion ?
- Disposez-vous d'archives verrouillées, d'armoires ignifugées... ?

PROTECTION DE L'ENTREPRISE EN RELATION AVEC SON ENVIRONNEMENT

Faites-vous appel à des cabinets de formation, d'audits, de conseils ?

- Connaissez-vous bien ces sociétés à savoir la composition de l'actionnariat, les dirigeants, la nationalité ?

Avez-vous recours à des prestataires extérieurs pour le nettoyage de vos locaux, pour le gardiennage ?

- Connaissez-vous bien ces sociétés et le personnel chargé de réaliser ces prestations ?

Connaissez-vous vos visiteurs, les avez-vous identifiés formellement ?

- Possédez-vous le nom et l'activité de leur entreprise ?
- Accompagnez-vous systématiquement toutes ces personnes ?

Lors de l'arrivée d'un nouveau salarié ou d'un stagiaire, l'informez-vous suffisamment des règles de sécurité mises en place dans l'entreprise ?

- Assurez-vous un encadrement des nouvelles personnes ?
- Avez-vous déployé une charte informatique et un règlement intérieur ?



II - Mon entreprise souhaite en savoir plus sur la sécurité économique

Identification des acteurs et détermination des risques éventuels

Au préalable, l'entreprise doit, avant toute intervention d'un nouvel acteur (recours à un prestataire ou d'une personne extérieure), identifier ses données sensibles et évaluer les procédures de protection qu'elle a mises en œuvre.

Ce premier questionnement (qui détient quoi, qui accède à telle ou telle information, comment celle-ci est exploitée, restituée, conservée...) fait entrer l'entreprise dans une démarche de sécurité économique.

Qui intervient dans mon entreprise ?

Les prestataires en contrat avec l'entreprise :

Sécurité des locaux, nettoyage externalisé, conseil (en gestion, comptabilité, juridique, informatique...), maintenance (informatique, photocopieurs...), assurance, formation, surveillance des locaux, gestion des distributeurs de friandises et boissons, restaurateur-traiteur, installateur ou réparateur divers...

Les contacts permanents, occasionnels et non permanents :

Salariés intervenant dans le cadre d'un contrat avec l'entreprise : commerciaux, stagiaires, visiteurs, employés temporaires (recrutement par agence de travail temporaire)...

Comment cet « acteur » intervient-il dans l'entreprise ?

Niveau d'action :

Après d'une personne, d'un groupe de personnes, d'un service, toute l'entreprise est concernée.

Degré d'intervention :

Spontané, occasionnel, rare, régulier, facultatif, obligatoire.

Objet d'intervention :

Technique, économique, financier, commercial, autre.

Quels sont les risques encourus par l'intervention de cet « acteur » ?

Des risques économiques (dépendance, indépendance), techniques, environnementaux, commerciaux, juridiques.

Comment protéger le patrimoine de mon entreprise ?

L'entreprise doit identifier l'information stratégique, et plus exactement, qui la détient dans l'entreprise, comment elle est protégée...

L'entreprise peut se protéger en déposant des noms de société, des brevets, des marques, des dessins et des modèles (pour de plus amples informations : www.inpi.fr).

Comment protéger la diffusion des informations ?

L'entreprise se doit de contrôler la diffusion de ses informations par une sensibilisation de ses salariés en adoptant le principe de vigilance.

L'entreprise doit admettre qu'elle possède des données sensibles qu'elle doit protéger.

Citons quelques exemples d'imprudence :

- lors des déplacements (train, hôtel, restaurant), les conversations engagées à table au restaurant (oralement ou par téléphone) peuvent être entendues par le concurrent qui se trouve par malchance proche de votre table. Le travail réalisé dans le train (écran d'ordinateur ou documents papiers) peut être lu par une tierce personne.
- l'envoi d'informations importantes par e-mail ou encore par télécopie peut être détourné.
- l'information divulguée sur le site internet, sur les supports de communication ou exposée lors d'un salon peut-être trop abondante.

Votre entreprise doit instaurer des règles de bonne conduite ou adopter le principe de précaution :

Sécurité de l'information :

- centraliser et sécuriser vos documents confidentiels,
- communiquer que ce qui est communicable sur sa société,
- ne pas abandonner des documents au photocopieur,
- ne pas laisser à la vue de tout le monde un projet,
- ne pas laisser la réflexion de la dernière réunion sur le paper-board de la salle de réunion,
- ne pas oublier de broyer les documents confidentiels.

Sécurité des locaux :

- déterminer quelles sont les zones sensibles,
- instaurer des codes d'accès dans tout ou une partie de vos locaux (à modifier régulièrement).

Sécurité informatique :

- instaurer des droits d'accès personnalisés en fonction du profil de la personne : salarié, stagiaire...
- sauvegarder régulièrement vos données,
- ne pas laisser « ouverte » toute session informatique : verrouiller le plus possible votre ordinateur en votre absence en générant un mot de passe complexe mélangeant de préférence des lettres, des chiffres et autres caractères,
- ne pas envoyer d'informations confidentielles par voie électronique.



Comment travailler en toute confiance avec des prestataires, des fournisseurs et autres contacts ?

L'entreprise doit assurer une meilleure gestion de ses contacts par la mise en oeuvre des solutions suivantes :

Un contrôle des personnes entrantes, quelle que soit la nature du contact avec l'entreprise (sous réserve des dispositions de la CNIL) :

- . les identifier, les localiser (possibilité de créer un badge « visiteur »),
- . la mise en place d'un registre des contacts à remplir par toutes les personnes étrangères à l'entreprise (civilité, objet de la venue, horaires de la visite et/ou de l'intervention, interlocuteur dans l'entreprise).

Une limitation des espaces « visites » : ne plus recevoir spontanément dans votre bureau, votre atelier... mais dans un espace « réunions/rendez-vous » proche de votre accueil.

Un accompagnement des personnes « visiteurs » dans l'entreprise, loin des ateliers et plus particulièrement des derniers prototypes, c'est-à-dire ne pas laisser seule toute personne étrangère à l'entreprise, y compris avec le personnel de la société de nettoyage, de maintenance, de dépannage...

Un engagement de confidentialité peut être demandé (simple attestation), par exemple : un règlement intérieur, une charte informatique.

Avec les professionnels, prestataires, sociétés intervenantes, quelques précautions supplémentaires :

Avant de s'engager, il apparaît nécessaire de s'assurer de la solidité structurelle de ce professionnel (forme juridique, moralité des dirigeants, CV, moyens techniques et humains), son professionnalisme (références, résultats opérationnels, teneur de ses engagements, véracité de son réseau...), sa déontologie (discrétion, légalité des méthodes d'action, gestion de la confidentialité..).

Lors du premier contact, l'entreprise peut à un moment donné communiquer des données économiques sensibles, via un cahier des charges, pour obtenir des propositions commerciales. Pour se préserver, elle se doit d'annexer lors de ce premier contact un « acte d'engagement de confidentialité » (cette clause est également insérée dans le contrat de réalisation de la prestation).

Au début de la réalisation de la prestation, une fiche « prestataire » peut être élaborée. Elle synthétise différentes informations telles que la nature des travaux, le lieu d'intervention, la liste nominative des personnes intervenantes sur le chantier, la date de début et de fin des travaux... Cette fiche offre la possibilité pour l'entreprise de suivre la réalisation du contrat en toute transparence. Tout changement (un nouvel interlocuteur) implique la réactualisation de la fiche.

En fin de contrat, selon les activités, une clause de confidentialité portant sur plusieurs années peut-être jointe au contrat pour que le prestataire n'utilise pas les données confidentielles de l'entreprise une fois la prestation réalisée.

Remarque : de nombreuses professions possèdent un code de déontologie (notaires, avocats, experts-comptables, sociétés de surveillance, agences de travail temporaire ...).



S'informer sur la réglementation

Une règle générale : ne pas être excessif dans le contrôle et la surveillance des salariés et des personnes entrantes, ne pas tomber dans la paranoïa.

« La cybersurveillance au cœur du processus de travail » est réglementée (cf rapport présenté par M. Hubert Bouchet, vice-président délégué de la CNIL).

Assurez-vous que vous avez bien déclaré vos bases de données clients/contacts à la CNIL

Le non respect de la déclaration de votre collecte d'informations est sanctionné pénalement. Pour connaître vos droits et procédures, consulter le site internet www.cnil.fr et vous « adopterez les bonnes pratiques Informatiques et Libertés ».

Introduction de clauses dans le contrat de travail et/ou élaboration de documents organisationnels

Il s'agit de :

- clause de confidentialité dans un contrat de travail, contrat d'engagement professionnel,
- clause de restitution des documents,
- clause de non concurrence,
- charte informatique ,
- circulaire sur le traitement et la sauvegarde de l'information,
- document interne d'accord de confidentialité à destination d'une ou plusieurs personnes (engagement par écrit du respect de confidentialité).

Action au plan pénal et civil de l'entreprise en cas de :

- vol, extorsion, chantage, atteinte aux systèmes d'informations, secret professionnel, secret des correspondances, atteinte aux droits de la personne.

Les principales sources d'information

AFNOR : Association Française de Normalisation

www.afnor.fr

Consulter le référentiel des bonnes pratiques « Sécurité des informations stratégiques : comment préserver la confidentialité des informations » - août 2002.

CNIL : Commission Nationale de l'Informatique et des Libertés

www.cnil.fr

Protection informatique et libertés. Déclarations des collectes de données : informations, documents. Rapports et études : Cybersurveillance sur les lieux du travail.

INPI : Institut National de la Propriété Industrielle

www.inpi.fr

Protection du patrimoine de l'entreprise.

Ministère de l'Economie, de l'Industrie et de l'Emploi

www.industrie.gouv.fr

Consulter « Le guide de la sécurité économique : protéger l'information stratégique de votre entreprise » et www.entreprises.gouv.fr

Prestataires Internet

www.quelnet.fr

Portail créé par la CCI de Paris.

Possibilité de découvrir en ligne un exemple de contrat d'un client.

Mission du Haut Responsable en charge de l'Intelligence Economique

www.intelligence-economique.gouv.fr

Club de la Sécurité de l'Information Français

www.clusif.asso.fr

Pour aller plus loin sur la sécurité économique

Chambre de Commerce et d'Industrie de la Vendée

- Pour obtenir de plus amples informations sur la sécurité économique
- Pour vous aider à identifier et appréhender les risques et les menaces qui pèsent sur votre entreprise
- Pour vous orienter vers les principaux interlocuteurs
- Pour connaître les prochains événements et les réunions développés par la CCI

Contact : Michelle Garandeau ou Ghislaine Filippozzi - 02 51 45 32 32

Pour vous apporter une réponse personnalisée, en fonction de votre préoccupation et de votre activité : les services de l'Etat sont en mesure de vous répondre.

Gendarmerie Nationale

- Vous êtes victime d'un vol, d'une extorsion
- Vous vous sentez exposé, vulnérable

Contact : Capitaine Rochereau Gérard—Chargé de mission - 02 51 58 06 60

Direction Départementale du Renseignement Intérieur (ex RG/DST)

- Vous souhaitez être sensibilisé sur la protection de vos informations et de votre savoir-faire
- Vous pensez être la cible d'ingérences étrangères
- Vous détenez un renseignement de sécurité
- Vous exercez une activité à caractère stratégique, sensible, innovant

Contact : 02 51 45 15 75

Direction de la Protection et de la Sécurité de la Défense (DPSD)

- Vous devez élaborer des mesures de protection de vos installations
- Vous désirez une sensibilisation ou un soutien en matière de protection du patrimoine industriel
- Vous êtes un industriel travaillant pour la défense nationale

Contact : 02 28 24 27 53