

LA SÉCURITÉ ÉCONOMIQUE

« Parole d'entreprises »

Toul, le 27 mars 2019

Jean-Pierre Di Federico

La sécurité économique

Le risque

Les risques en entreprise

- Intrusion, accès et déplacement sur site

- Stagiaires

- Visites de site

- Rejets de l'entreprise

Les risques hors entreprise

- Déplacements en voiture

- Transports en commun

- Voyages à l'étranger

- Hébergement

- Salons professionnels

Les risques spécifiques

- Création et Propriété industrielle

- Perte de compétence-clé

- Nouveau partenariat et levée de fonds

- Achats et Approvisionnement

- Numérique

- Réputation

- Interruption d'activité

LA SÉCURITÉ ÉCONOMIQUE

La Sécurité Economique est un des trois volets de l'**Intelligence Economique** avec :

- **la veille**
- **l'influence**

*La Sécurité Economique, c'est **protéger les biens***

- **matériels** (bâtiments, outils, etc.)
- **immatériels** (données, savoir-faire, réputation, etc.)

Pour cela, il s'agit de

- **avoir conscience** des risques
- **diminuer le préjudice** éventuel

avec un juste comportement entre « **naïveté** » et « **paranoïa** »

LE RISQUE

Le risque de préjudice d'un événement porte sur

- l'**occurrence** de l'événement
- la **gravité** des effets de l'événement

Le risque peut être

- **réduit** (occurrence et/ou gravité de l'incident)
- **transféré** (assurance)
- **assumé**

mais doit être **identifié** par une démarche d'**analyse de risques**

Une prévention par des gestes

- simples
- automatisables

LES RISQUES EN ENTREPRISE

Intrusion, accès et déplacement sur site

Stagiaires

Visites de site

Rejets de l'entreprise

INTRUSION, ACCES, DEPLACEMENT sur SITE

L'effraction n'est pas nécessaire pour porter atteinte à la sécurité économique

Pour **retarder** et **dissuader** :

- **Clôturer** le site
- **Protéger** les accès (serrures, grilles, etc.)
- **Contrôler** les accès (personnel d'accueil, registre, badge, etc.)
- **Limiter** les accès (visiteurs, fournisseurs, etc.)
- **Détecter** l'intrusion
- **Eclairer** les accès
- **Sensibiliser** le personnel à la vigilance

www.referentsurete.com

STAGIAIRES

Un stage est une opportunité pour accéder à l'information sensible

- **Porter attention** aux stagiaires **étrangers** et demander conseil aux Services de l'Etat en cas de doute
- **Intégrer** une clause de **confidentialité** au contrat de stage
- **Accompagner** le stagiaire par un **tuteur**
- **Limiter** les accès du stagiaire aux **réseaux informatiques**
- **Relire le mémoire** de stage avant diffusion

VISITES DE SITE

Une visite d'entreprise peut accueillir des gens aux intentions malveillantes

- Prévoir une **procédure de visite**
- **Vérifier le profil et la motivation** des visiteurs et adapter la visite
- **Accueillir** les visiteurs dans une **salle neutre**
- **Accompagner** le visiteur en permanence
- **Faire porter un badge** visible
- **Déterminer les locaux à visiter** et ceux à ne pas faire visiter
- **Ne pas permettre** aux visiteurs d'accéder au **réseau informatique**

REJETS DE L'ENTREPRISE

Les secrets sont parfois dans la poubelle...

- **Broyer** ou faire broyer les papiers sensibles jetés
- **Porter attention** aux informations mises en **archives**
- **Porter attention** aux matériaux et maquettes mis au **rebut**
- **Mettre hors d'usage** les disques durs, clés USB, cartes mémoires, imprimantes en fin de vie
- **Porter attention** aux contrats de maintenance des photocopieurs et autres matériels informatiques comportant des **mémoires**

LES RISQUES HORS ENTREPRISE

Déplacements en voiture

Transports en commun

Voyages à l'étranger

Hébergement

Salons professionnels

DEPLACEMENTS EN VOITURE

Les *accidents de la route* sont la première cause de mortalité au travail et le v

- **Conduire est exclusif** de toute autre activité et téléphoner au volant multiplie par 5 le risque d'accident
- **La responsabilité de l'employeur** en cas d'accident peut être engagée en raison du lien de subordination
- **Ne laisser en vue** aucun matériel dans une voiture stationnée sur la voie publique
- **Ne laisser dans le coffre** aucun matériel informatique ou données sensibles

TRANSPORTS EN COMMUN

Vous n'êtes pas tout seul dans les transports en communs et on peut vous y dérober matériel et information

- N'emporter que ce qui est **nécessaire**
- **Garder** constamment vos **outils informatiques** auprès de vous (700 micros sont perdus ou volés par semaine à Roissy)
- **Soyez discrets** dans vos conversations et vos communications téléphoniques
- Ne travaillez pas sur des documents sensibles dans le **train** ou **l'avion**
- N'oubliez pas que toute **liaison hertzienne** peut être interceptée (Bluetooth, Wifi, clé 3/4G, etc.)

VOYAGES A L'ETRANGER

Autres lieux, autres moeurs et autres lois : un voyage à l'étranger se prépare et réclame la vigilance à tout instant

- Se renseigner sur le **niveau de risque** du pays (www.diplomatie.gouv.fr)
- Ayez une **copie de votre passeport** dans les bagages
- N'amener que l'**indispensable**
- **Eviter les habitudes** de lieux et d'horaires
- **Rester discret** dans le comportement et les conversations
- **Respecter** les lois et coutumes
- **Rester vigilant** avec les personnes qui vous abordent (élicitation)

HEBERGEMENT

Vous n'êtes pas chez vous à l'hôtel... la chambre est accessible à d'autres

- **Ne rien laisser** de sensible dans la chambre d'hôtel
- Ne pas penser que vous êtes le seul à avoir la combinaison du **coffre-fort**
- Ne rien jeter de sensible dans la **poubelle**
- Utiliser avec prudence **informatique**, **fax** ou **photocopieur** de l'hôtel
- Vérifier le contenu de vos **bagages** avant de partir et les fermer à clé

SALONS PROFESSIONNELS

Les salons sont un lieu où tout le monde cherche de l'information

- **Préparer le salon** en définissant ce que vous voulez y montrer et dire et ce que vous devez **ni dire ni montrer**
- **Ne compter que sur vous** pour sécuriser le stand et le matériel
- Faites attention à l'usage des nouvelles technologies destinées à **capter l'information** : appareil photo, clé USB sous toutes les formes, etc.
- Garder strictement personnel l'usage de vos **outils informatiques**
- Identifier les **visiteurs** du stand
- Etre en permanence **discret et vigilant**
- Faire un **retour d'expérience** du salon

LES RISQUES SPECIFIQUES

Création et Propriété industrielle

Perte de compétence-clé

Nouveau partenariat et levée de fonds

Achats et Approvisionnement

Numérique

Réputation

Interruption d'activité

CREATION et PROPRIETE INDUSTRIELLE

L'innovation technique se protège par le secret ou le brevet

- Intégrer aux contrats des clauses de **confidentialité** et des clauses de **non-concurrence**
- **Poursuivre en justice** la violation des clauses prévues, la concurrence déloyale, le vol, la contrefaçon ou la divulgation de secret de fabrique
- **Constituer la preuve** de l'innovation par une enveloppe Soleau ou un cahier de laboratoire permettant de dater la création.
- **Déposer un brevet** et le faire vivre
- Prendre conseil auprès de l'**INPI** (www.inpi.fr)

PERTE DE COMPETENCE-CLE

Le départ de certaines personnes peut présenter le risque de perte de comp

- **Identifier** les personnes ayant une compétence-clé
- **Gérer les RH** en fonction des compétences-clés
- Intégrer dans les **contrats de travail** des clauses de confidentialité et de non-concurrence et agir en justice le cas échéant
- Organiser au sein des équipes **la transmission** des compétences-clés
- S'interroger en cas de débauchage sur une éventuelle **action hostile**

NOUVEAU PARTENARIAT et LEVEE DE FONDS

L'entrée en relation avec un nouveau partenaire financier ouvre l'avenir et pro

- **Vérifier** l'historique, les bilans, les actionnaires, les dirigeants, etc.
- **Vérifier** la notoriété, les compétences techniques, l'état financier, etc.
- **Etre** vigilant si le schéma d'actionnariat est confus, les dirigeants n'ont pas de secrétariat, des liens sont établis avec les paradis fiscaux, etc.
- Dans la phase initiale de négociation et avant la signature d'une première lettre d'intention, ne communiquer aucune **information stratégique ou confidentielle**
- **Prendre conseil** auprès des banques, avocats, experts-comptables ainsi que des services de l'Etat compétents en Sécurité Economique (Gendarmerie, DIRECCTE, etc.)

ACHATS et APPROVISIONNEMENT

Les risques liés aux achats et approvisionnements peut affecter l'image de l'entreprise

- Evaluer la capacité des fournisseurs à **honorer** leurs contrats
- Tenir compte des critères liés à l'**environnement** et aux **exigences sociales**
- **Diversifier** les sources d'approvisionnement
- Veiller a ne pas être **le seul client** du fournisseur
- Sécuriser le **tranfert de savoir-faire** au fournisseur par des clauses de confidentialité ou d'exclusivité

NUMERIQUE (1/2)

Le **risque numérique** porte sur les **systèmes informatiques connectés à un réseau**. Administrations, entreprises et particuliers sont concernés

*Le risque numérique est très lié au **comportement de l'utilisateur**. La méconnaissance de l'outil informatique et des procédures en sont parfois la cause mais il relève surtout d'une **banalisation du risque** et d'un certain **fatalisme** contre lequel l'utilisateur doit lutter*

Trois préjudices possibles vis à vis des données :

- la destruction : perte de données
- la capture : exploitation frauduleuse, usurpation d'identité (phishing), vente, ingénierie sociale pour l'« arnaque au président »
- la modification : cryptage (ransomware), prise de contrôle, défacement

Trois intrusions possibles dans le système informatique :

- la liaison à distance (WIFI, Bluetooth, etc.)
- l'introduction de connecteurs (clé USB, etc.)
- le message (pièce jointe, lien internet, etc.)

NUMERIQUE (2/2)

LES BONS USAGES :

- Ne pas **abandonner**, **perdre** ou se faire **voler** son micro ou portable
- Utiliser des **mots de passe** forts et les remplacer régulièrement
- **Mettre à jour** son système de navigation et ses logiciels
- Effectuer des **sauvegardes** régulières
- Analyser les **liens** et **pièces jointes** avant de cliquer
- Rester prudent sur les **réseaux sociaux**
- Ne pas utiliser des **clés USB** suspectes
- Couper les liaisons **WIFI** et **Bluetooth** en fin d'usage
- Prendre conseil auprès de l'ANSSI (www.securite-informatique.gouv.fr)

Le Nouveau Règlement Général européen sur la protection des Données Personnelles

REPUTATION

L'image de l'entreprise fait partie de son patrimoine immatériel et les risques d'altération sont grands dans un monde de communication

- S'assurer de l'intégrité du **site internet** de l'entreprise (défacement)
- **Faire une veille** sur l'image de l'entreprise ainsi que de ses sous-traitants et partenaires principaux
- **Corriger** les atteintes d'image
- Gérer la **communication**

INTERRUPTION D'ACTIVITE

L'interruption d'activité par un événement perturbateur peut affecter la survie de l'entreprise (incendie, inondation, panne informatique, etc.)

- Concevoir un **Plan de Continuité d'Activité** (PCA) à partir des scénarios
- Prioriser les **fonctions** à maintenir ou adapter
- Préparer des **modes** de fonctionnement alternatifs
- Inventorier les **fournisseurs** de moyens adaptés aux circonstances

MERCI POUR VOTRE ATTENTION

DES QUESTIONS ?