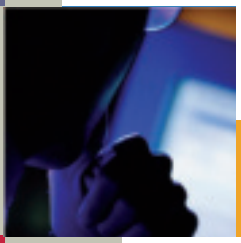
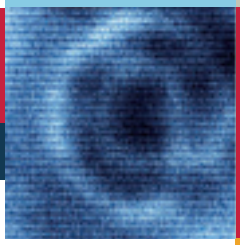
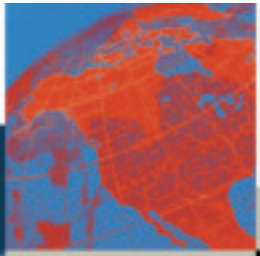




# Le guide pratique du chef d'entreprise face au risque numérique

Version du 24 mars 2009

CLUSIF



24 MARS
2009
LILLE
GRAND PALAIS

# 3e FORUM INTERNATIONAL SUR LA CYBERCRIMINALITE

*Ensemble pour un espace numérique plus sûr !*

1 200 PARTICIPANTS
30 PAYS INVITÉS
15 CONFÉRENCES SCIENTIFIQUES

# Pourquoi un guide de bonnes pratiques à destination des PMI-PME?

*Dans un contexte de mondialisation et de développement des technologies numériques, la dépendance des sociétés à l'égard des technologies de l'information et de la communication (TIC) présente des risques potentiels que savent exploiter des délinquants et des criminels avertis et de plus en plus souvent organisés.*

Le 22 mars 2007, le Forum International sur la Cybercriminalité a permis de mesurer l'intérêt de près de 600 participants pour les technologies numériques qui transforment notre vie quotidienne en offrant un espace de liberté et d'échanges sans précédent. Le 20 mars 2008, la deuxième édition du FIC a accueilli plus de 800 participants.

Résolument inscrite dans une démarche d'intelligence économique, la troisième édition mettra l'accent sur les axes de travail qu'il appartient aux autorités de suivre pour mener au mieux la protection des personnes et des biens dans le cyberespace et permettre ainsi tant le développement de l'économie numérique, le secteur le plus dynamique de l'économie mondiale, que le développement et la protection des PME-PMI.

Il s'agira ainsi tout particulièrement de :

- Permettre une lutte efficace contre la criminalité liée aux technologies numériques (pédophilie, terrorisme, blanchiment d'argent, contrefaçon...) en utilisant la détection, l'investigation et la poursuite, tant au niveau national qu'international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable.

- Intensifier la coopération entre les Etats liés à la Convention du Conseil de l'Europe d'avril 2001, les pays membres de l'UE et les candidats à l'accession.

- Structurer un partenariat sur une base transnationale, avec les entreprises et plus généralement avec les acteurs socio-économiques impliqués au quotidien dans le développement de l'économie de la connaissance et les acteurs concrets de la mutation de l'économie européenne.

La remise d'un guide pratique à destination des chefs de PMI-PME issu d'une coopération publique-privée fructueuse, trouve-t-elle ainsi toute sa pertinence et sa place dans le cadre de ce troisième FIC.

**Régis Fohrer**
Commissaire général
Forum International sur la Cybercriminalité

# Remerciements aux participants des comités scientifiques et de rédaction.

*Au nom du Forum International sur la Cybercriminalité, j'adresse mes meilleurs remerciements à l'ensemble des membres et partenaires pour la qualité des réflexions qui ont permis de donner toute la pertinence à ce guide, ainsi qu'au comité de rédaction et de relecture pour l'important travail de synthèse et d'écriture fourni.*

*Nous remercions tout particulièrement la CNIL pour le soutien apporté dans la mise en place des réunions de notre comité d'experts.*

**Régis Fohrer**
Commissaire général
Forum International sur la Cybercriminalité

## Liste des participants au comité scientifique

### • INSTITUTIONS

M. Alain JUILLET,
Haut responsable chargé de l'intelligence économique,
SGDN

M. Cyril BOUYEURE,
Coordonnateur ministériel à l'Intelligence Economique, MEIE

M. Philippe CLERC,
Directeur de l'Intelligence Economique
et des TIC, Assemblée des chambres françaises
de commerce et d'industrie

M. Gwendal LE GRAND,
Chef du service de l'expertise
à la direction des Affaires juridiques, internationales
et de l'expertise, CNIL

M. Pascal LOINTIER,
Président
du Club de la Sécurité de l'Information Français, CLUSIF,
conseiller sécurité de l'information, AIG Europe

M. Gérard PARDINI,
Chef du département Sécurité économique et gestion
de crise, Institut National des Hautes Etudes de Sécurité.

M. Jean-Philippe VACHERON,
Ingénieur d'études, CRCI-ARIST Nord-Pas de Calais,
animateur de l'action «sécurité des systèmes d'information»

M. Philippe VANDENBERGHE,
Chargé de mission défense et protection civile,
Direction Générale des Services de la Ville de LILLE

## • UNIVERSITAIRES ET PROFESSION DU DROIT

M. Eric CAPRIOLI,
Avocat à la cour de Paris,
Associé du Cabinet Caprioli & Associés, Docteur en droit

M. Jean Jacques LAVENUE,
Laboratoire IREENAT, Université de Lille 2

M. Jean-Paul PINTE,
Docteur en information scientifique et technique, maître de conférences, expert en veille et intelligence compétitive au sein du laboratoire d'ingénierie pédagogique, Université Catholique de Lille

Mme Blandine POIDEVIN,
Avocate, Barreau de Lille et de Paris

Mme Myriam QUÉMÉNER,
Magistrat, Parquet général de la Cour d'appel de Versailles, auteur de « Cybermenaces, entreprises, internautes » et co-auteur de « Cybercriminalité, défi mondial »

M. Christophe ROQUILLY,
Professeur de droit, directeur du centre de recherche LegalEdhec - performance juridique, EDHEC Business School

## • FORCES DE SÉCURITÉ FRANÇAISES ET ÉTRANGÈRES

M. Luc BEIRENS,
Commissaire divisionnaire, Chef de la Federal Computer Criminal Unit (FCCU), Belgique

M. David CASSEL,
Enquêteur en technologie numérique,
chef de la cellule d'investigations criminelles d'Arras

Colonel Joël FERRY,
Commandant de la Section de Recherche de Versailles

M. Eric LESTRINGUEZ,
Lieutenant-colonel de réserve, Gendarmerie Nationale

M. Alain PERMINGEAT,
Chef de la division lutte contre la cybercriminalité au Service Technique de Recherche Judiciaire et de Documentation de la Gendarmerie Nationale

## • ENTREPRISES

M. Patrick DESCHAMPS,
GEN'ETIQ

M. Daniel GUINIER,
OSIA

M. Olivier VARLET,
Directeur de Pôle MAUD

## REMERCIEMENTS AUX RÉDACTEURS

Lieutenant-colonel Régis FOHRER,
Forum International sur la Cybercriminalité

M. Pascal LOINTIER,
Président du Club de la Sécurité de l'Information Français, CLUSIF, conseiller sécurité de l'information, AIG Europe

• Groupe *« Le chef d'entreprises face au risque numérique - Risques identifiés et solutions proposées en 10 études de cas »*

Rédigé par M. Eric LESTRINGUEZ,
Lieutenant-colonel de réserve, Gendarmerie Nationale
avec la participation de

- M. Eric CAPRIOLI,
  Avocat à la cour de Paris,
  Associé du Cabinet Caprioli & Associés, Docteur en droit

- M. David CASSEL,
  Enquêteur en technologie numérique, chef de la cellule d'investigations criminelles d'Arras

- M. Daniel GUINIER,
  OSIA

- Mme Noëlle JEAN-PIERRE,
  Cabinet CAPRIOLI & Associés, Juriste TIC

- Mme Blandine POIDEVIN,
  Avocate, Barreau de Lille et de Paris

- M. Christophe ROQUILLY,
  Professeur de droit, directeur du centre de recherche LegalEdhec - performance juridique, EDHEC Business School

- M. Dominique DAGUE
  Illustrations humoristiques

• Groupe Etat des lieux *« Le chef d'entreprise face au risque numérique » - recommandations « approche institutionnelle »*

Rédigé par M. Jean-Paul PINTE,
Docteur en information scientifique et technique, maître de conférences, expert en veille et intelligence compétitive au sein du laboratoire d'ingénierie pédagogique, Université Catholique de Lille
avec la participation de

- Mme Nathalie FAVIER
  SGDN / DCSS I / CERTA

- MM. Gabriel GOLDSTEIN et Pierre CROS,
  Service de coordination à l'Intelligence économique, Bureau Dépendances Stratégiques, Ministère de l'Economie, de l'Industrie et de l'Emploi, Ministère du Budget, des Comptes Publics et de la Fonction Publique.

- M. Gwendal LE GRAND,
  Chef du service de l'expertise à la direction des Affaires juridiques, internationales et de l'expertise, CNIL

- M. Gérard PARDINI,
  Chef du département Sécurité économique et gestion de crise, Institut National des Hautes Etudes de Sécurité.

Les « avis d'expert » ont été rédigés par SPIE Communications et notamment :

M. Arnaud FEIST
Consultant Direction Régionale Nord Est

M. Yohan CAPLIER
Consultant Direction Régionale Nord Est

M. David DELANNOY
Consultant Direction Régionale Nord Est

M. Christian MEGARD
Marketing, Offre IRM (Informatique / Réseaux / Mobilité )

M. Julien HOPPENOT
Marketing, responsable offre sécurité

Cet ouvrage
a pu être réalisé
grâce à la collaboration
active et engagée de

- Les enseignants chercheurs :

EDHEC BUSINESS SCHOOL

Université Catholique de Lille

IREENAT

- Les acteurs de la sécurité :

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

CLUSIF

sécurité sécurité sécurité

- Les institutions :

GENDARMERIE

CNIL.

INHES
INSTITUT NATIONAL DES HAUTES ÉTUDES DE SÉCURITÉ

arist

CRCI

- Les acteurs juridiques :

Caprioli & Associés

Jurisexpert .net

- Partenaires privés :

SPIE

THALES

Microsoft

PROFIL TECHNOLOGY

OSIA

SOMMAIRE

PREFACE
de Mme Michèle Alliot-Marie, Ministre de l'intérieur, de l'Outre-mer et des Collectivités territoriales P 3

AVANT-PROPOS
Introduction du Lieutenant-colonel Régis Fohrer, FIC/IFC project manager P 4

REMERCIEMENTS participants aux comités scientifiques P 6

PRÉSENTATION des partenaires P 9

DÉFINITIONS de la cybercriminalité en entreprise et introduction P 11

CHAPITRE 1
Le chef d'entreprises face au risque numérique
Risques identifiés et solutions proposées en 10 études de cas P 13

- Le comportement à risques du salarié P 14
- La fraude financière via la comptabilité P 16
- La divulgation de savoir-faire P 18
- Les téléchargements illicites et intrusion via le réseau sans fil P 20
- La défaillance de sauvegarde des données P 22
- Le vol d'ordinateur portable ou de PDA P 24
- Le sabotage interne d'une base de données P 26
- Le dysfonctionnement ou l'altération par programmes malveillants P 28
- La diffamation par courrier électronique P 30
- La défiguration de site web P 32

CHAPITRE 2
Etat des lieux « Le chef d'entreprise face au risque numérique »
Recommandations des institutions P 38

Les entreprises et la cybercriminalité P 39
P 40
P 40

La loi protège votre entreprise P 43
P 43
P 44

Des services spécialisés pour aider les entreprises P 45
P 45
P 48

Perspectives pour l'entreprise P 54
P 54
P 54
P 57

POSTFACE P 62

WEBOGRAPHIE P 64

LES SOUTIENS DE NOS PARTENAIRES P 67

# Définition de la Cybercriminalité

Définition du Lieutenant-colonel
Régis FOHRER
La criminalité du XXIème siècle.

Faute d'une définition communément admise, la définition pertinente du terme « cybercriminalité » donnée par la communication n° 267 du 22 mai 2007 de la Commission européenne « Vers une politique générale en matière de lutte contre la cybercriminalité » a été retenue pour préparer les éditions successives du FIC. Aux fins de ce texte, « cybercriminalité » s'entend des « infractions pénales commises à l'aide des réseaux de communication électroniques et de systèmes d'information ou contre ces réseaux et systèmes ».

Ce terme englobe trois catégories d'activités criminelles.

- La première concerne les formes traditionnelles de criminalité, comme les fraudes ou les falsifications;
- La seconde concerne les infractions liées aux contenus illicites par voie électronique (violence sexuelle contre les enfants, incitation à la haine raciale...);
- La dernière connait des infractions propres aux réseaux électroniques (attaques visant les systèmes d'information, déni de service, piratage...).

Ainsi la cybercriminalité constitue dans un monde globalisé l'une des nouvelles formes de criminalité et de délinquance transnationales dont les conséquences peuvent être particulièrement graves pour les citoyens, les personnes vulnérables et le secteur de l'économie de toutes les nations de la planète.

Quatre grands types de menaces concernent particulièrement les entreprises :

- Les vols de supports et de données;
- Les intrusions dans les réseaux;
- Les interceptions de communications ou de flux de données;
- La manipulation des employés et des partenaires, cette dernière menace étant plus connue sous le terme de « social engineering ».

**Glossaire :**

MAC: media access control
NAC: network access control
PDA: personnel digital assistant
SSID: service set identifier
RFID: radio frequency identification
SSL: secure sockets layer
USB: universal serial bus
WEP: wired equivalent privacy
WI-FI: wireless fidelity
WLAN: wireless local area network
WMAN: wireless metropolitan network
WPA: wifi protected access
WPAN: wireless personal area network

# Introduction

par Pascal LOINTIER,
Président du Club de la Sécurité
de l'Information Français, CLUSIF
conseiller sécurité de l'information,
AIG Europe

Début des années 80, un grand constructeur américain lance un nouveau modèle d'ordinateur : le PC, pour Personal Computer. Ordinateur individuel… ce qui signifiait qu'on envisageait peu un emploi professionnel dans une PME ! Manifestement les choses ont évolué autrement et aujourd'hui non seulement la micro-informatique est complètement intégrée dans les systèmes d'information des entreprises de toutes tailles mais encore, l'individu est devenu à la fois un internaute et un citoyen muni d'une informatique embarquée : cartes de crédit, téléphones GSM avec fonctions d'assistant (PDA), navigateurs GPS…

Cette dépendance est une bonne chose car d'une part, elle accroît la productivité, fluidifie les échanges et d'autre part, facilite la sécurité des données au format électronique en terme de disponibilité et d'intégrité dans le temps. En effet, le rapport « France numérique 2012 », présenté par le gouvernement en octobre 2008 détaille nombre des avantages pour une entreprise quant à l'utilisation des technologies de l'information et de la communication (TIC) : « l'économie numérique est le principal facteur de gain de compétitivité des économies développées ».

Côté sécurité, les outils de sauvegarde, la délocalisation du lieu de conservation des dites sauvegardes permettent aujourd'hui, à moindre coût, d'organiser la disponibilité des données, c'est-à-dire, la pérennité de leur accès et de leur usage quelle que soit, ou presque…, la nature du dommage informatique.

Le bon fonctionnement au quotidien du système informatique et le gain de productivité généré par un traitement numérique ne doivent pas faire oublier que la menace est « polymorphe » : les causes d'un arrêt ou d'une dégradation du fonctionnement du système sont potentiellement très variées. Classiquement, on peut classer les causes en deux grandes catégories : les événements accidentels et les actes de malveillance.
Les accidents peuvent être divisés en deux origines, naturelles ou humaines (sans digression philosophique…) où dans le premier cas on considère des événements tels que les incendies, dégâts des eaux, perturbations électromagnétiques du fait de la nature ou d'une activité industrielle. Et dans le second cas, les erreurs de programmation, les erreurs de manipulation ou d'exploitation informatique.

Les malveillances où on pourrait distinguer le fait de programmes automatiques, virus, botnets, etc. où l'entreprise devient victime sans pour autant avoir été spécifiquement ciblée ; et la malveillance par l'agissement direct d'un individu. Pour cette dernière, et même si on médiatise beaucoup (trop) l'Internet et les hackers, les auteurs ou leurs actions les plus dommageables restent des employés de l'entreprise car leurs motivations sont les plus fortes et leur connaissance des faiblesses de sécurité souvent meilleure.

On pourrait encore élargir avec d'autres expositions telles que le non respect de textes réglementaires qui peuvent perturber l'activité de l'entreprise du fait de condamnations ou de l'atteinte à l'image et la notoriété.

Cette variété des origines d'un arrêt du système et l'évolution des architectures informatiques, opportunités de nouvelles expositions aux malveillances, notamment, ne doivent certainement pas être interprétées comme un frein à l'emploi des TIC. Il faut garder à l'esprit que toute technologie (et pas seulement informatique) comporte intrinsèquement un risque et un emploi malveillant spécifiques. L'automobile « coûte » cher en terme de dommages corporels et matériels et la bande à Bonnot a pour la première fois utilisé le véhicule lors d'attaques de banques…

Il faut donc accueillir les nouvelles technologies mais toujours dans une posture de vigilance : savoir comment accroitre son activité tout en limitant les nouveaux risques par des moyens raisonnables

C'est bien souvent l'insouciance et/ou la méconnaissance du risque qui permettent ou aggravent les conséquences d'un accident ou d'une malveillance informatique.

# Le chef d'entreprise face au risque numérique :

risques identifiés
et solutions proposées
en 10 études de cas.

# Le comportement à risqu

- *Une entreprise met en place un dispositif technique de gestion des accès basé sur un identifiant/mot de passe sans avoir sensibilisé les salariés aux règles de bon usage.*

- *Un salarié laisse un post-it sur son écran d'ordinateur avec ses identifiant et mot de passe.*

- *Un autre salarié utilise l'identifiant et le mot de passe pour accéder à l'ordinateur et en profite pour commettre des actes illicites : envoi de messages diffamatoires ou racistes, téléchargement de fichiers protégés par le droit d'auteur, etc...*

- *La personne physique ou morale subissant un préjudice dépose plainte contre l'entreprise et/ou contre l'expéditeur du message.*

## Impacts judiciaires

L'identifiant et le mot de passe servent à créer une présomption sur l'usager des outils. Ainsi, si le salarié ne respecte pas la procédure mise en place dans l'entreprise ou s'il ne peut apporter la preuve que ce ne peut matériellement être lui, sa responsabilité pourra être retenue.

Gestion des accès et responsabilité de l'employeur - L'employeur sera tenu pour responsable des actes illicites commis sur le fondement de la responsabilité des commettants du fait de leurs préposés vis à vis des tiers (art. 1384 du Code civil).

Usurpation d'identité

En matière pénale : L'usurpation d'identité n'est pas un délit pénal en soi, mais seulement au sens de l'art. 434-23 du Code pénal. Une proposition de loi envisage toutefois d'ajouter un art. 323-8 au Code pénal concernant l'usurpation d'identité numérique avec une peine d'un an d'emprisonnement et de 15 000 € d'amende.

En matière civile : La responsabilité civile édictée par l'art. 1382 du Code civil, est applicable dès qu'il y a une faute, un préjudice subi par la victime et un lien de causalité entre cette faute et ce préjudice.

**Définition :**
L'usurpation d'identité correspond à l'emprunt temporaire ou définitif de l'identité d'une personne existante, par appropriation des identifiants de cette dernière, pouvant constituer un délit.

# es du salarié

### Impacts managériaux et humains

Ambiance délétère au sein de l'entreprise.
Saisine des prud'hommes pour faute du salarié négligeant peu envisageable dans ces circonstances.
Le salarié victime des agissements ainsi que son employeur sont amenés à porter plainte contre X.

### Impacts financiers

Frais de procédure et condamnation possible de l'entreprise au civil en cas de dommage causé à un tiers.

### Impacts sur l'image

Répercussion possible sur l'image de l'entreprise en cas de contenu illicite ou diffamant.

### Préconisations

Mettre en place et faire appliquer une politique efficiente d'authentification et de gestion des accès, avec la participation des instances représentatives du personnel.
Ces dispositions feront partie de la charte d'utilisation des moyens informatiques, et en tout cas devront être adossées au règlement intérieur de l'entreprise.
Tous les employés devront être sensibilisés à cette nécessité et avertis des sanctions encourus.

### LES POINTS CLES A RETENIR

L'authentification est une fonctionnalité de sécurité essentielle au contrôle d'accès.
Les accès autorisés à l'information et aux ressources sont fonction du ou des rôles de chacun. Il est également nécessaire d'alerter les salariés sur les conséquences créées par la présomption d'identité et de les informer sur la procédure qu'ils doivent mettre en place en cas de perte de leur mot de passe ou identifiant.

### AVIS D'EXPERT :

*Les entreprises prennent généralement toutes les protections nécessaires à la sécurisation des accès extérieurs mais oublient bien souvent la menace interne. En effet, la confiance faite à l'employé représente une faille de sécurité considérable : transmission volontaire ou non de mot de passe, non verrouillage d'une session, introduction de virus via l'utilsation de ressources externes à l'entreprise (clé USB, connexion privée, disque dur externe…) Toutes ces menaces nécessitent une politique de sécurité interne qui passe par la sensibilisation (charte…) et l'accompagnement des utilisateurs ainsi qu'un contrôle performant des accès et des activités.*

# La fraude financière via la comp

- *Le chef-comptable, en poste depuis de nombreuses années, vient d'être mis en arrêt longue durée suite à un accident automobile.*

- *Un intérimaire est embauché d'autant plus rapidement que le bilan doit être clôturé prochainement.*

- *A l'occasion de rapprochements bancaires et stocks, ce remplaçant détecte une différence entre les factures payées à un fournisseur et les livraisons effectives de matériaux.*

- *En collusion avec un employé du fournisseur, le chef-comptable a détourné plusieurs centaines de milliers d'euros en moins de deux ans. Il apparaissait comme consciencieux, extrêmement zélé et d'ailleurs, ne prenait quasiment pas de congés.*

- *Une procédure judiciaire a été lancée mais la récupération des actifs détournés s'avère délicate. Ces derniers ayant été consommés ou investis dans des biens immobiliers dont la liquidation va prendre des mois.*

## Impacts judiciaires

Le licenciement du salarié ne peut se faire tant que son contrat se trouve suspendu sauf faute grave ou lourde qui ne pourra être démontrée que par une expertise comptable ou une enquête pénale.
Elles devront déterminer s'il a bénéficié de complicité.
Une procédure d'expertise devra être lancée afin de déterminer le préjudice exact subi par l'entreprise. Des conséquences fiscales sont également envisageables du fait de l'absence de fiabilité des documents comptables.

**Définition :**
La fraude financière est un acte illicite délibéré, réalisé par des moyens plus ou moins subtils, avec la volonté de tromper dans le but de s'approprier un avantage. Elle peut prendre diverses formes qui nécessitent ou non des complicités, et conduit à un préjudice pour la victime.

# tabilité

## Impacts managériaux et humains

Détection délicate a priori car tout le monde se connaissait dans l'entreprise et la suspicion d'une malversation semblait inimaginable. Dès la présomption fondée, le chef d'entreprise doit agir rapidement et discrètement en supposant l'existence de collusions internes.

## Impacts financiers

Effets multiples : perte des actifs détournés et difficultés à venir pour récupérer les fonds détournés d'autant plus que la PME ne s'était pas assurée contre les fraudes financières.

## Impacts sur l'image

Impact sur le sérieux de l'entreprise (rigueur dans les contrôles) et crainte de difficultés financières futures qui pourraient remettre en cause des contrats clients, voire d'autres fournisseurs...

## Préconisations

Mettre en place des contrôles informatiques et des procédures : double ordonnancement, séparation des circuits paiements et achats, limitation de seuils, audit et inventaires apériodiques.

## LES POINTS CLES A RETENIR

Les mécanismes de détournements sont le plus souvent très simples à comprendre et parfois stupides de la part du commettant car la détection n'est qu'une affaire de temps (cf fraude dite « en cavalerie*»). Etudier des scénarios techniquement possibles (c'est à dire sans présumer de la bonne foi des salariés) et mettre en place des indicateurs qui permettront la détection des situations atypiques.

(*) : La fraude financière dite «en cavalerie» peut prendre diverses formes. L'une consiste à créditer artificiellement un compte par des chèques croisés de montants croissants pour maintenir la confiance, ce qui nécessite des complicités successives, sinon de complaisances.

## AVIS D'EXPERT :

*La traçabilité des activités et des interventions du personnel joue un rôle primordial pour la prévention des fraudes. En effet, les fraudes d'ordre comptable par exemple peuvent entraîner des conséquences désastreuses pour une entreprise tant au niveau financier que pour son image. Pour se prémunir d'éventuelles tentatives de détournement de fonds au travers de manipulations comptables, un traitement électronique de l'ensemble des transactions ainsi que leur archivage est indispensable.*

# La divulgation de savoir-

- *Un stagiaire, s'appuyant sur une technique « d'ingénierie sociale », l'appel à la compassion, a récupéré les droits d'accès de son tuteur de stage pour « faciliter son travail dans l'entreprise ».*

- *Ces droits lui permettent de détourner des informations confidentielles d'un autre service de l'entreprise, à savoir du laboratoire de recherche qui était sur le point de déposer un brevet.*

- *Une fois le stage terminé, il va même obtenir un prix d'une prestigieuse école européenne.*

- *Il sera engagé par une société concurrente étrangère qui développera le produit et déposera plusieurs brevets voisins.*

## Impacts judiciaires

En matière pénale : Les faits peuvent être qualifiés d'abus de confiance au sens de l'art. 314-1 du Code pénal. Cette incrimination peut s'appliquer au collaborateur qui utilise frauduleusement les outils ou informations mis à sa disposition pour extraire des informations confidentielles, mais aussi d'atteinte au système de traitement automatisé de données (STAD) (Art. 323-1). Si ces informations présentent un caractère de secret de la défense nationale, le cas est traité à l'art. 413-9 du Code pénal, tandis que leur livraison à une puissance étrangère est du ressort de l'art. 411-6.
En matière civile : La responsabilité civile de celui qui commet un tel acte se réfère à l'art. 1382 du Code civil en cas de violation de la convention de stage. Enfin, au cas où des éléments relatifs à la vie privée interviennent, l'art. 9 du Code civil, dispose que chacun a droit au respect de sa vie privée. On relèvera peut-être par ailleurs des atteintes au droit de la propriété intellectuelle ou à la politique de confidentialité de l'entreprise.

**Définition :**
L'ingénierie sociale (en anglais «social engineering»), est une méthode d'exploitation de la crédulité humaine, par pression psychologique ou faisant appel à la compassion, pour disposer d'un bien ou d'informations.

# faire

## Impacts managériaux et humains

Remise en cause de l'organisation tardive en regard des conséquences.
Dévalorisation, voire licenciement, du tuteur de stage.
Perte de chiffres d'affaires et de contrats à venir.

## Impacts sur l'image

Influence sur l'image de la société causée par la fuite d'information.

## Préconisations

Vérifier le contenu de la convention de stage et la rendre tripartite (étudiant, école, entreprise). Vérifier dans l'entreprise l'existence de charte éthique et en expliquer le contenu à chacun.
Informer les salariés des risques consécutifs à la diffusion non contrôlée de droits d'accès.

Règles de classification, de marquage des données sensibles et contrôle des accès physiques et logiques (« besoin d'en connaître »). Procédure d'authentification forte pour les informations sensibles (contrôle biométrique ou par carte à puce ou mot de passe dynamique).
Récupération et analyse rapides des traces d'accès horodatées, comme moyen de preuve.

## LES POINTS CLES A RETENIR

La sensibilisation des personnels est primordiale : préserver les informations sensibles pour l'entreprise, réagir à tout phénomène atypique.
L'ingénierie sociale est difficile à prévenir et à détecter car elle s'appuie sur des comportements humains normaux et quotidiens : solliciter une aide, faire état de la gêne occasionnée en l'absence de collaboration, nécessité de réagir dans l'urgence sans avoir le temps d'appliquer les procédures standards, etc...

## AVIS D'EXPERT :

*La protection des données sensibles et leur non divulgation nécessitent la mise en place d'une politique de sécurité globale dans laquelle devront apparaître 3 types de mesures. L'authentification forte ou la biométrie, une stratégie globale de contrôle de données qui permettra d'installer les outils nécessaires pour que l'information reste dans l'entreprise, ainsi qu'une solution de gestion de logs pour tracer les contrevenants et établir les preuves en cas de fuites.*

# Les téléchargements illicites et

- *L'entreprise Z s'est toujours positionnée originalement : historiquement installée dans ses vieux mais prestigieux locaux parisiens conservés comme à l'origine, elle est toujours à la pointe de la technologie.*

- *Ainsi, pour ne pas dénaturer ses bureaux et s'économiser le coût du câblage, elle a doté ses commerciaux d'ordinateurs portables avec une connexion Wi-Fi, les membres de l'équipe de direction ne peuvent plus travailler sans leur nouveau PDA avec une connexion BlueTooth.*

- *La plupart des accès au système d'information local se font via des technologies sans fil.*

- *Un beau matin, le PDG reçoit la visite de représentants de la force publique lui demandant de s'expliquer sur le téléchargement dans son entreprise de plusieurs giga octets de films et de musique piratés.*

## Impacts judiciaires

La protection du droit d'auteur et des droits voisins dans la société de l'information relève de la loi n°2006-961 du 1er août 2006 (DADVSI). Il y a obligation pour l'entreprise de veiller à ce que son système d'information ne soit pas utilisé à des fins illicites (Arts. L226-17 du Code pénal, et 1384 al 5 du Code civil), voire à des fins de recel (Art. 321-1 du Code pénal).
L'entreprise est responsable du comportement de ses salariés. Elle a l'obligation lors de la mise en place de ces outils d'informer ses salariés des limites d'utilisation et des contrôles possibles (rôle des chartes informatiques ou annexes au règlement intérieur).


**Définition :**
Les technologies sans fil correspondent aux réseaux sans fil de type :
- personnels (WPAN), tels : Bluetooth, RFID, etc.,
- locaux (WLAN) : Wi-Fi,
- métropolitains (WMAN),
  en fonction de la portée.

# intrusion via le réseau sans fil

## Impacts managériaux et humains

Il règne dans l'entreprise un climat de suspicion et chaque collaborateur se sent atteint personnellement après avoir été auditionné par les enquêteurs.

## Impacts financiers

Les enquêteurs conduisent les constatations de manière à ne pas engendrer un ralentissement dans le fonctionnement de l'entreprise. Pour ce faire, il leur arrive de cloner le(s) disque(s) dur(s) susceptible(s) de détenir la preuve numérique. Ils travaillent alors sur le(s) clone(s) et remettent le(s) disque(s) réel(s) au chef d'entreprise. C'est pourquoi l'entreprise peut être paralysée pendant plusieurs jours, voire plus.

## Impacts sur l'image

Un des majors de l'industrie du film et de la musique porte le dossier en justice et l'affaire se trouve relayée par la presse spécialisée.

## Préconisations

Masquer le nom du réseau (SSID : service set identifier). Mettre en place un chiffrement de type WEP ou mieux WPA avec une authentification complémentaire par la carte réseau Wi-Fi (adresse physique MAC).
Mettre en place une charte informatique, effectuer des contrôles concernant l'intégrité du réseau, vérifier les déclarations CNIL.
Dans un autre ordre d'idée, l'usage d'une connexion Wi-Fi libre d'accès dans un hôtel ou sur un lieu public peut présenter un risque d'interception de vos données (messagerie, fichiers téléchargés) si la communication n'est pas sécurisée. Il faut que les échanges entre votre ordinateur et l'entreprise soient effectués en mode chiffré (WEP puis SSL pour la partie Internet par exemple).

## LES POINTS CLES A RETENIR

Un réseau sans fil doit être encore plus surveillé que les autres modes de connexion filaires au SI car le point d'entrée est difficile à identifier : la propagation des ondes hertziennes est très difficilement contrôlable.

## AVIS D'EXPERT :

*Pour sécuriser un réseau Wi-Fi, il existe différents mécanismes. WPA2, le mécanisme correspondant à la norme 802.11i, est à ce jour le plus abouti de ces mécanismes, il est basé sur l'authentification 802.1x (authentification forte par carte à puce, certificat, …) et le chiffrement AES pour assurer la confidentialité des informations transmises.*
*Des solutions permettent de déployer et d'exploiter très rapidement un réseau Wi-Fi en conformité avec les impératifs de sécurité de l'entreprise, tout en garantissant le confort des utilisateurs.*

# La défaillance de la sauvegarde

- *Le responsable informatique de la société X a élaboré une procédure de sauvegarde incrémentielle de ses données : sauvegarde totale le dimanche et enregistrement tous les soirs des modifications faites dans la journée.*

- *La secrétaire est chargée de changer les supports magnétiques et une semaine sur 2 un jeu différent est utilisé.*

- *Le 25 novembre, une panne survient, endommageant le serveur sur lequel sont centralisées toutes les données sensibles et notamment comptables.*

- *Lors de l'opération de restauration desdites données, le support de mercredi de la première semaine ainsi que celle du jeudi du second jeu s'avèrent illisibles.*

- *La restauration est impossible. Il faut repartir d'une ancienne sauvegarde totale, vérifier l'intégrité des données enregistrées (conformité à la réalité) et rejouer toutes les opérations de mise à jour. L'activité économique est fortement dégradée et certains clients n'hésitent pas à porter l'affaire en justice.*

## Impacts judiciaires

Outre les aspects contractuels et la responsabilité civile en cas de préjudice pour les clients, la loi sur la sécurité financière (LSF) n° 2003-706 du 1er août 2003 oblige à disposer des données qui découlent d'un contrôle interne de qualité, à ceci s'ajoute notamment le respect du livre des procédures fiscales au vu des arts. L169, L176 et L102 B.
Il faudra veiller aux clauses de responsabilités contenues dans les contrats clients. Etait-il imposé aux clients de sauvegarder eux-mêmes leurs données ? Une clause limitative de responsabilité existe-t-elle ? L'entreprise est-elle assurée ?

**Définition :**
On peut distinguer la sauvegarde de configuration qui concerne les programmes et leur paramétrage et la sauvegarde des données proprement dites. En fonction des emplois, on peut aussi distinguer une sauvegarde de production qui sera conservée sur site pour un accès et une remise en état plus rapide et la sauvegarde de recours, conservée hors site, pour gérer des événements majeurs (incendie, dégâts des eaux, etc...)

# des données

## Impacts managériaux et humains

Le service commercial, le service client ainsi que la comptabilité sont paralysés.
Il est nécessaire d'avoir recours à des mesures palliatives et de ressaisir les écritures.

## Impacts financiers

La ressaisie entraîne un trouble de trésorerie et de production,
et des frais supplémentaires.
Certains clients décident de changer de fournisseur et refusent de payer leurs factures en cours.

## Impacts sur l'image

Mauvaise image vis-à-vis des clients en attente de leur commande, qui sera retardée ou n'arrivera jamais. Impact sur la gestion de trésorerie avec des pénalités de retard, des intérêts non perçus et une communication de crise à financer.

## Préconisations

Développer un plan de sauvegarde avec, par exemple, un cycle de sauvegarde quotidienne sur un mois, une sauvegarde mensuelle avec une rotation annuelle. Externaliser le support de fin de semaine ainsi que la sauvegarde mensuelle.

## LES POINTS CLES A RETENIR

La sauvegarde des données est fondamentale. Elle ne concerne pas seulement les données de gestion/comptabilité mais aussi la configuration du système téléphonique et les données pilotant l'informatique industrielle (les machines-outils, la régulation et la logistique, etc).
Une fois la politique de sauvegarde élaborée, il est tout aussi fondamental de tester l'efficacité des enregistrements, c'est-à-dire, vérifier qu'on peut effectivement réinstaller les ressources et les données à partir des supports conservés hors site.
L'assurance est un bon moyen d'être remboursé des coûts de remise en état et des préjudices économiques subits.

## AVIS D'EXPERT :

*Le Plan de Reprise d'Activité, PRA (ou encore appelé Plan de Continuité d'Activité ou des Services), constitue l'ensemble des procédures et moyens techniques et humains à mettre en œuvre pour faire face à une situation de crise.*

*Au sein de l'entreprise, c'est ce plan qui va permettre d'assurer le maintien des activités critiques. La sauvegarde - et ses processus ad-hoc - en est une composante obligatoire et essentielle.*

# Le vol d'ordinateur porta

- *Le directeur commercial de la société Y se rend en TGV à Francfort pour négocier un important contrat portant sur 500 pièces de sa dernière innovation.*

- *Il emporte dans ses bagages son PC portable dans lequel il a pris soin de stocker le contrat qu'il doit signer, le tableau des marges et le dernier tarif à donner aux commerciaux locaux, le fichier client et le dernier projet innovant de l'entreprise qui doit sortir l'année prochaine.*

- *En montant dans le taxi, il se rend compte que son ordinateur a disparu.*

**Impacts judiciaires**

L'employeur licencie son salarié pour faute lourde, à laquelle sera plus probablement retenue la négligence. Le salarié peut saisir les instances prudhommales et obtenir la requalification de son licenciement. L'entreprise ne pourra pas réclamer réparation de son préjudice à son salarié. L'assurance ne prendra en compte que le prix du matériel volé.

**Impacts managériaux et humains**

La société et son directeur commercial sont décrédibilisés auprès du client allemand. L'entreprise supporte la responsabilité encourue.


**Définition :**
Le vol matériel est la soustraction de la chose d'autrui, ici matérialisé par un matériel ou des supports de données, par opposition au vol immatériel de données.

# ble ou de PDA

## Impacts financiers

Le marché qui aurait dû être signé est perdu.
Un fabricant étranger sort peu après un produit de caractéristiques voisines mais à prix cassé.

## Impacts sur l'image

La société allemande a des doutes sur la capacité de la PME française à protéger efficacement les informations confidentielles.

## Préconisations

Mettre en place une protection par mot de passe ou biométrique pour l'accès physique à l'équipement portable.
Chiffrer les données. Il existe maintenant des solutions simples et suffisamment robustes à la crypto-analyse, s'appuyant sur une offre commerciale ou « open source » (emploi libre).

Penser à faire une sauvegarde des données traitées pendant le déplacement. Le support (CD, clef USB) sera également chiffré.
Déposer dans la mesure du possible immédiatement les éléments volés si des titres de propriété intellectuelle peuvent être obtenus afin de préserver l'antériorité de l'entreprise et vérifier que l'entreprise a bien fait signer des clauses de non-débauchage à ses co-contractants pour éviter que les informations récupérées par un tiers soient utilisées pour concurrencer sans peine l'entreprise.

## LES POINTS CLES A RETENIR

Pour certains pays (Chine, Etats-Unis, Israël…), se renseigner avant déplacement sur les réglementations en vigueur (nature des moyens de chiffrement autorisés, autorisation légale d'accès pour des contrôles de sécurité intérieur, etc.).
Pour les téléphones-PDA, penser à conserver par ailleurs, l'IMEI, le numéro de téléphone, le numéro de carte SIM.

## AVIS D'EXPERT :

*En cas de vol, l'identification nécessaire pour ouvrir une session sur le portable sert uniquement à empêcher l'accès au PC. Cependant il n'est pas compliqué de récupérer le disque dur, et les données qui y sont stockées, en le connectant sur un autre ordinateur.*

*De ce fait il est essentiel de crypter les données sensibles sur l'ordinateur portable mais également sur les périphériques de stockage (CD, clés USB, disque dur externe, carte mémoire, …).*

# Le sabotage interne d'une

- *L'administration organise annuellement sur le territoire national un concours. Celui-ci se déroule en deux phases : une première pour l'admissibilité, une seconde pour les oraux, en vue de l'admission.*

- *L'ensemble des résultats concernant l'admissibilité est communiqué à partir du site Internet de l'administration.*

- *Les candidats admissibles reçoivent alors chez eux une convocation à des examens oraux.*

- *Or, suite à un appel téléphonique d'un candidat qui n'avait pas reçu cette convocation, il est apparu que différentes informations du site Internet avaient été falsifiées par leur webmaster en cours de licenciement.*

- *En effet, une page mentionnant les résultats d'un étudiant non admissible a été modifiée, de telle sorte que ledit candidat apparaissait comme admissible.*

## Impacts judiciaires

Ces faits sont clairement constitutifs des infractions visées aux arts. 323-1 et 323-3 du Code Pénal, du fait d'accéder et de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données (STAD), et de modifier les données qu'il contient. De plus, si des données personnelles circulent sur Internet, le non-respect de l'obligation de sécurité et la divulgation des données personnelles par négligence constituent des infractions au vu des art. 226-17 226-22 du Code pénal.

**Définition :**
L'intrusion se fonde sur le caractère frauduleux de l'introduction et du maintien en vue d'une récupération ou d'une modification, sinon d'une altération ou d'une destruction.

# base de données

### Impacts managériaux et humains

Des données personnelles circulent sur l'Internet.

### Impacts financiers

Coût de réorganisation de l'épreuve dans sa totalité.
Possibilité de paiement de dommages et intérêts aux candidats.
Frais d'expertise et de procédures.
Frais de gestion des poursuites légales.

### Impacts sur l'image

Le discrédit est jeté sur l'organisme victime de cette manipulation.

### Préconisations

Nécessité de conserver l'ensemble des données de connexion au serveur et de les remettre aux autorités compétentes. Eviter toute remise en service ou réinstallation qui serait susceptible de supprimer ces traces. Prévoir lors de l'inscription que ce type d'évènements peut amener l'organisateur à annuler l'épreuve.

### LES POINTS CLES A RETENIR

Le préjudice en termes d'image peut être considérable.
Le contrôle d'intégrité et l'authentification relèvent de la prévention, et la sauvegarde des données de la protection.
Le dispositif et la procédure d'alerte et la conservation des traces sont essentiels pour la suite.

### AVIS D'EXPERT :

*L'utilisateur reste le risque majeur pour la perte des informations. A fortiori lorsque celui-ci décide de venger un manquement à son égard (licenciement, refus d'une augmentation de salaire) par la destruction de la base de données de l'entreprise. Dans ce cadre, l'entreprise doit être en mesure :*
*- d'assurer la protection de ces données,*
*- de tracer les actions de l'inconvenant pour preuve,*
*- de reconstituer sans dégradation ces données.*

*Les solutions adéquates consistent en l'authentification forte, la corrélation de logs et bien sûr les systèmes de sauvegarde de données ainsi qu'une gestion des identités efficace.*

# Le dysfonctionnement ou l'altérati

- *Les virus font désormais partie de l'environnement informatique. Plusieurs dizaines de malwares (malevolent software, programme malveillant) sont créés chaque jour.*

- *L'entreprise pensait être en sécurité, mais sa protection antivirale était inadaptée, certains postes n'étant pas protégés, d'autres n'avaient pas la mise-à-jour automatique activée.*

- *Lors de la consultation par un salarié d'un site d'e-commerce accidentellement contaminé, le réseau de l'entreprise est alors très rapidement infecté, notamment le serveur de messagerie, celui des fichiers et les postes utilisateurs ayant été connectés aux deux serveurs...*

## Impacts judiciaires

L'introduction d'un code malveillant constitue un délit.
En matière pénale :
une atteinte au système de traitement automatisé de données (STAD) (Art. 323-1, 323-2, 323-3-1 du Code pénal), résultant d'une modification, voire d'une atteinte au fonctionnement même du système à l'aide d'un programme.
En matière civile : celui qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer, aux termes de l'Art.1382 du Code civil, s'il existe des dommages liés à la contamination étendue à des systèmes appartenant à des tiers, à partir de ceux de l'entreprise.

**Glossaire :**
NAC : network access control

**Définition :**
Les codes malveillants (en anglais «malware») : virus, vers, chevaux de Troie, bombe logique, espiogiciels etc., sont caractérisés par la présence de mécanismes de propagation, de déclenchement, et d'action, en général développés dans l'intention de nuire.

# on par programmes malveillants

## Impacts managériaux et humains

Le système d'information est totalement inutilisable : il faut arrêter le réseau pour éviter la propagation virale et nettoyer chacun des équipements. En premières conséquences, c'est une semaine d'inactivité avec chômage partiel de certains personnels, mais aussi l'usage de palliatifs pour les activités essentielles.

## Impacts financiers

Perte de chiffre d'affaires et d'opportunités commerciales.
Coûts de décontamination, de réinstallation de l'ensemble des systèmes.
Dommages et intérêts et frais de procédure éventuels, en cas de contamination d'installations tierces.

## Impacts sur l'image

Trouble chez les fournisseurs, les clients, et la banque, avec une nécessité de réduire l'incident.

## Préconisations

Un dispositif pare-feu et anti-virus de qualité doit être installé et maintenu constamment à jour, il doit être vérifié dans son bon fonctionnement et dans l'étendue du parc d'équipements protégés, une fois les outils de sécurité et les procédures mis en place. Les journaux d'événements seront régulièrement examinés et conservés, et les alertes prises en compte.

## LES POINTS CLES A RETENIR

Aucun dispositif technique n'est en mesure de bloquer les codes malveillants à 100 %.
L'accès à Internet est concerné, en même temps que les serveurs, les postes de travail, mais aussi les différents supports : disques externes, clés USB, cartes mémoire, CD-ROM, DVD, PDA en synchronisation etc...

## AVIS D'EXPERT :

*Les programmes malveillants peuvent causer d'importants dégâts au sein d'une société. Ces programmes peuvent être introduits de différentes manières au sein d'un système d'information : consultation de sites Internet, messagerie, utilisation de données personnelles, ….*
*Pour faire face à ces programmes il faut sécuriser au maximum tout accès vers et depuis l'Internet. Outre la mise en place de Firewall et d'antivirus, il existe également des solutions permettant de centraliser les accès Internet des utilisateurs et d'effectuer un contrôle d'accès au réseau (NAC) qui vérifie l'état d'un ordinateur avant de le connecter au système d'information.*

# La diffamation par courrier é

- *Un cadre d'entreprise a reçu un courrier électronique à son adresse professionnelle présentant l'identité d'un de ses collègues, qui n'est pourtant pas à l'origine de cet envoi.*
- *L'adresse de courrier électronique de ce collègue a été créée par un service de messagerie gratuite*
- *Ce courrier a été adressé à d'autres personnes sans que chacun des destinataires n'ait connaissance des autres envois*
- *Le contenu du message porte atteinte à l'honneur et à la considération d'un autre collègue de l'entreprise*

## Impacts judiciaires

Le contenu du message peut constituer une diffamation au sens de la loi du 29 juillet 1881 (art. 29), sinon une injure. Il y a aussi dans ce cas usurpation d'identité, du fait de l'usage de l'identité d'un tiers étranger à l'envoi du message. L'usurpation d'identité devrait prochainement être qualifiée de délit pénal.

En matière pénale : la diffamation qualifiée envers un particulier est punie, selon le contenu, jusqu'à un an d'emprisonnement et d'une amende de 12000 € à 45000 € (art.32).

En matière civile : une action en responsabilité civile pourrait être intentée sur les dispositions des arts. 1382 et 1383 du Code civil, en cas de préjudice subi.

En préalable, l'employeur alerté devra vérifier s'il dispose des moyens de contrôler les boîtes aux lettres internes sur ce motif selon sa charte informatique et le rôle dévolu à l'administrateur réseau.

**Définition :**
La diffamation est l'allégation ou l'imputation de mauvaise foi d'un fait déterminé qui porte atteinte à l'honneur ou à la considération de la personne physique ou morale à laquelle ce fait est imputé.

# lectronique

### Impacts managériaux et humains

La tension est montée entre les deux hommes avec un impact dans leur travail quotidien.

### Impacts financiers

Perte de productivité et d'opportunité difficiles à chiffrer.

### Impacts sur l'image

Répercussion possible sur l'image de l'entreprise en cas de contenu à caractère raciste ou sectaire.

### Préconisations

Vérifier si des contrôles peuvent être menés sur les messageries de l'entreprise.
Sur démarche de la victime et par injonction judiciaire à l'hébergeur de la boîte aux lettres de l'expéditeur, l'identité de la personne mise en cause sera établie et la pluralité des destinataires pourra être démontrée.
Il appartiendra à l'auteur apparent d'apporter la preuve de sa bonne foi, et à l'employeur de réagir dans le respect des règles puisque certains faits se déroulent sur le poste de travail de salariés.
Si le nom de l'entreprise a été utilisé, cette dernière sera aussi compétente pour agir en justice.

### LES POINTS CLES A RETENIR

L'action en diffamation se prescrit après 3 mois, à compter de la première émission de l'écrit qualifié de diffamatoire ou publication.

### AVIS D'EXPERT :

*Outil de communication, commun et répandu, la messagerie électronique peut être utilisée comme tous les médias de communication pour transmettre des informations erronées et agresser autrui. Ces messages diffamatoires doivent pouvoir être tracés afin de fournir la preuve de la diffamation et identifier l'émetteur. Il s'agit donc de placer sur les réseaux internes des sondes de tracking et être capable de stocker sur les serveurs de messagerie les messages diffamatoires reçus et émis.*

# La défiguration de site web

- *L'entreprise X est bien connue pour son catalogue en ligne d'articles de décoration.*
- *Son site Internet est le moteur de son activité commerciale et la société X ne se prive pas d'en vanter l'ergonomie et le nombre croissant de visiteurs.*
- *Le vendredi 13 décembre, la société X est obligée de mettre hors ligne son site. Sa page d'accueil a été modifiée, indiquant que la société a été rachetée par un groupe concurrent, et les liens menant aux sites de ce dernier. Les bases de données clients et les commandes sont altérées. L'attaque est menée par un groupe de jeunes hackers qui souhaitaient faire un coup.*

## Impacts judiciaires

Ces faits peuvent être qualifiés d'atteinte au système de traitement automatisé de données (STAD) (arts. 323-1 et 323-2 du Code pénal), résultant d'une altération des données contenues par suppression ou modification, voire d'une atteinte au fonctionnement même du système, suite à l'accès et au maintien frauduleux, à l'aide d'un programme (art. 46 de la LCEN, art. 323-3-1 du Code Pénal).

## Impacts managériaux et humains

Une partie du personnel administratif, de la préparation de commande et de la logistique, est mise au chômage technique pendant 11 jours.

**Glossaire :**
IP : internet protocole

**Définition :**
La défiguration (de l'Anglais «defacement») est une action délibérée dirigée contre un site Web pour sa dégradation, sa modification ou sa destruction de pages web, le plus souvent la page d'accueil.

### Impacts financiers

Le site n'a plus été en ligne durant 11 jours ce qui a entrainé une perte sèche d'exploitation immédiate, différé la livraison des commandes en cours et généré un important SAV pour certains clients qui avaient payé mais n'ont pas reçu leur colis.
Les événements ayant eu lieu en pleine période de fêtes, l'entreprise a vu son plus gros mois d'activité amputé de 50 %.

### Impacts sur l'image

L'image de marque de l'entreprise est mise à mal par la revendication et la médiatisation.
Les clients expriment leur mécontentement sur un blog connu.
Le chiffre d'affaires de l'entreprise a baissé et n'a pas encore repris le même essor qu'auparavant.
Les internautes qui se connectaient sur ce site pour la première fois n'y retourneront plus.

### Préconisations

S'assurer auprès du responsable ou du prestataire, de la mise à jour des correctifs du serveur Web.
Mettre en place un contrôle régulier de l'intégrité des pages et des bases de données associées.
Mettre en place et suivre l'efficience des dispositifs visant à prévenir la modification d'intégrité.
Conserver toutes les adresses IP et logs de connexion d'une façon fiable et avant dépôt de plainte pour la restauration.

### LES POINTS CLES A RETENIR

Les entreprises sont de plus en plus victimes de ce type d'attaque initialement tournée vers les sites institutionnels.
L'entreprise doit supprimer les failles présentes sur le dispositif web et son système d'exploitation par une mise à jour au fur et à mesure via les correctifs appropriés.

### AVIS D'EXPERT :

*Outil de communication et de marketing incontournable, le site web est devenu une cible de choix des hackers, des mécontents, d'une concurrence malhonnête. De par son utilisation, il doit être accessible depuis tout utilisateur d'Internet, donc potentiellement de personnes mal intentionnées. Ainsi l'accès et l'intégrité du site web doivent être surveillés et sécurisés, soit un mettant en place une infrastructure dédiée à cette sécurisation, soit en vérifiant les conditions effectives de sécurité lors d'un hébergement chez un prestataire.*

# Mais encore . . .

*Les 10 scénarios de malveillance que vous venez peut-être de découvrir sont des cas très fréquemment rencontrés dans l'environnement PME-PMI.*

Comme vous pouvez le constater, les risques sont variés de par leur nature et quant à leur impact. Une démarche de sécurité est donc une action dynamique, cyclique, qui doit mettre en œuvre une mise-à-jour périodique des moyens et procédures en place. Pour cela, une évaluation des risques et des enjeux par un consultant en sécurité des systèmes d'information permettra une meilleure harmonisation des plans de sécurité (sauvegarde, secours informatique, gestion des droits, antivirus et correctifs de sécurité, etc.) tout en ordonnant la mise en place de nouvelles solutions de sécurité.

**Il y aurait également …**

• *Le cybersquatting*
C'est le parasitisme des noms de domaines qui consiste à déposer un nom de domaine en usurpant le nom de l'entreprise ou celui de ses marques. Une variante est le typo-squatting qui repose sur une orthographe incorrecte en espérant que l'internaute saisisse le nom en commettant la faute d'écriture ou en se trompant de nom de domaine (ex : nasa.com qui était un site pornographique, le site officiel étant en .org…).

• *Le déni de service*
Il s'agit d'une indisponibilité de la ressource ciblée sans, toutefois, altérer ou détruire les données sur le site. On distingue ainsi le déni de service distribué qui s'appuie sur un réseau de zombies (botnets) pour viser par exemple le site web. Mais il peut également s'agir de bombing par saturation d'une ressource telle que la messagerie électronique (envoi de milliers de messages avec pièce jointe) ou encore du standard téléphonique maintenant de plus en plus en VOIP (voix sur IP).

• *La carence de fournisseur*
Le fait initial peut-être identique à un des scénarios présentés : sabotage de données, infection virale, etc. Mais comme il se produit chez un prestataire, l'entreprise à moins de facilités pour gérer la crise. D'autant plus qu'elle pensait être en confiance considérant la bonne renommée du prestataire ou qu'elle s'imaginait que les dispositions contractuelles (pénalités de retard et niveau de service qualité) ou un recours en responsabilité civile lui permettrait d'absorber le préjudice économique subi.

Pour ce qui est infogérance, hébergement, accès Internet, application service provider… il est fondamental que non seulement les informaticiens et les juristes valident le contrat de prestation mais aussi les réponses des « métiers et services » pour vérifier que les dispositions de reprises (délais) et compensations sont cohérentes avec les exigences de l'activité.

• *Les erreurs et les omissions*

Le comportement humain est très riche en matière de comportement à risques. Ainsi les erreurs de saisie, les mauvaises configurations des équipements, les cahiers des charges inadaptés, les conduites de projets non formalisées… sont autant de possibilités d'atteinte au bon fonctionnement du système d'information. L'omission et la négligence peuvent aussi générer des situations à risques !

• *Les risques environnementaux*

De plus, même des données et des ressources dites immatérielles peuvent subir une destruction ou une altération consécutive à un dommage physique. Comme indiqué dans l'introduction, l'incendie, les dégâts des eaux, qu'ils soient d'origine naturelle ou industrielle, peuvent provoquer l'indisponibilité d'une ressource. Un risque d'environnement de type pollution ou un conflit syndical peuvent empêcher l'accès physique à la salle informatique et rendre impossible l'exploitation des ressources informatiques. C'est pourquoi, en complément du plan de sauvegarde des données, il est fondamental de mettre en place non seulement un « plan de secours informatique » pour assurer la redondance des serveurs mais encore un « plan de continuité d'activité » qui permettra aux utilisateurs d'accéder aux serveurs relocalisés pendant la durée de gestion de crise.

• *La non-conformité réglementaire*

Enfin, l'impact et/ou le traitement judiciaire des actes malveillants présentés ne doit pas faire oublier une autre forme de risque pour l'entreprise : l'engagement de responsabilité pour non-conformité réglementaire. Que ce soit pour un défaut de déclaration, une conservation inadaptée, une divulgation accidentelle ou malveillante…

# Impact et occurrence des ris

Il vous est proposé une grille pour mesurer l'évaluation de la probabilité et l'impact des menaces évoquées dans les fiches. L'évaluation dépend toutefois de la situation de chaque entreprise, mais aussi de la sensibilisation et de la connaissance de celui qui l'exprime, en fonction de deux facteurs indépendants qui sont la possibilité d'occurrence et l'impact.

## Niveaux d'exposition

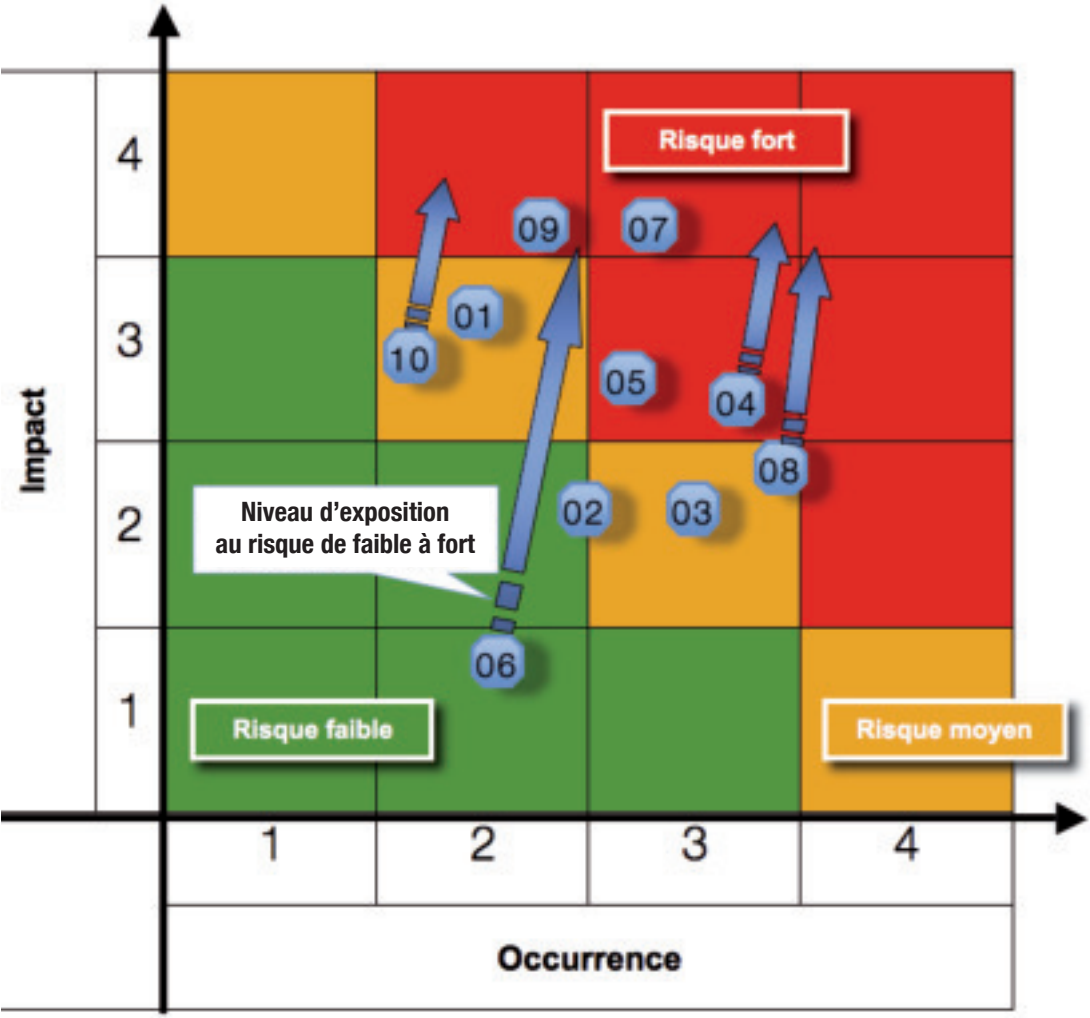
Pour faciliter l'estimation, il est également proposé les échelles suivantes :

**Impact du risque : 1** léger, **2** moyen, **3** sérieux, **4** catastrophique,
**Occurrence du risque : 1** légère, **2** modérée, **3** forte, **4** très forte,
et trois couleurs pour qualifier arbitrairement le niveau d'exposition au risque de faible, moyen et fort.

## Risques étudiés

- Le comportement à risques du salarié **01**
- La fraude financière via la comptabilité **02**
- La divulgation de savoir-faire **03**
- Les téléchargements illicites et intrusion via le réseau sans fil **04**
- La défaillance de la sauvegarde des données. **05**
- Le vol d'ordinateur portable ou de PDA **06**
- Le sabotage interne d'une base de données **07**
- Le dysfonctionnement ou l'altération par programmes malveillants **08**
- La diffamation par courrier électronique **09**
- La défiguration de site web **10**

# sques en entreprise



# Etat des lieux "le chef d'entreprise face au risque numérique"

## Recommandations des institutions.

# Les entreprises et la cybercriminalité

Bien que la sécurité informatique soit de plus en plus une réalité, un élément incontournable et une condition à la survie des entreprises, il apparait que le cheminement vers une prise de conscience du risque numérique ne soit pas encore totalement parcouru aujourd'hui.

En effet, la cybercriminalité gagne du terrain dans une économie mondialisée. L'enjeu de souveraineté nationale pour l'Etat est de garantir la sécurité de ses propres infrastructures, essentielles pour le développement des activités socioéconomiques de la nation et la protection des entreprises et des citoyens. Par ailleurs les entreprises doivent prendre des dispositions pour se préserver de la concurrence et de la malveillance.

Le terme de cybercriminalité a été inventé à la fin des années quatre-vingt-dix, alors qu'Internet se répandait en Amérique du Nord. Lors du Sommet de Lyon (27-29 juin 1996), les pays du G8 ont constitué un groupe de travail chargé d'étudier les nouveaux types de criminalité encouragés par, ou migrant vers Internet.

Dans un même temps, et à l'initiative des membres du groupe de Lyon, le Conseil de l'Europe a rédigé un projet de « Convention sur la Cybercriminalité » (1). Il s'agissait d'harmoniser les législations des Parties contractantes en la matière. A cet effet, cette convention, rendue publique pour la première fois en 2000, prévoyait de compléter l'arsenal juridique des Etats en matière procédurale, afin d'améliorer la capacité des services de police à mener en temps réel leurs investigations et à collecter des preuves sur le territoire national avant qu'elles ne disparaissent. Cependant, elle n'a pas fourni de définition claire de cette nouvelle forme de criminalité : le terme englobait tout un ensemble de nouveaux problèmes auxquels se trouvaient confrontées la police et les agences de renseignement, et découlant des performances toujours meilleures des ordinateurs, de la baisse du coût des communications, et du phénomène Internet.

La majeure partie a traité du droit et des conventions internationales : il s'agissait de définir les outils (coopérations internationales renforcées, nouveaux modes de preuve,…) susceptibles de fonder des poursuites efficaces à l'encontre des cybercriminels. C'est ainsi que l'on envisagea pour la première fois la mise en place de procédures de contrôles sur le réseau des réseaux : injonctions de conservation rapide de données stockées, mandats électroniques, recueil de données en temps réel, archivage des données relatives au trafic.

Un peu plus tard, le 25 février 2005, un rapport présenté par Thierry Breton, Ministre de l'Economie, des Finances et de l'Industrie au Ministre de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales évoque un chantier de lutte contre la cybercriminalité (2).

1/ Cf : http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=FRE
2/ www.telecom.gouv.fr/fonds_documentaire/rapports/cybercriminalite.pdf

Le rapport définit la cybercriminalité comme un nouveau domaine pour le droit pénal et la procédure pénale tout en mesurant l'émergence d'un corpus législatif et réglementaire et en intégrant sa dimension au niveau international.

Il est aussi question d'une prise en compte de la cybercriminalité par la police et la gendarmerie comme un champ d'action renouvelé et ouvert.

Ce même rapport a permis de mettre en avant un certain nombre de mesures à savoir :

- une meilleure connaissance statistique de la cybercriminalité ;
- un doublement des capacités d'investigation spécialisées des services de police et des unités de gendarmerie avec le renforcement de l'OCLCTIC, le doublement du nombre des enquêteurs spécialisés, la mise en place de référents ;
- le développement d'actions de formation communes ;
- un renforcement des capacités juridiques d'investigation ;
- un renforcement de la veille technologique et de la recherche et développement (R&D) ;
- un meilleur contrôle des contenus illicites véhiculés par Internet ;
- une meilleure protection des mineurs ;
- une politique de prévention ;
- la définition d'un certificat «citoyen» des fournisseurs de services de l'Internet.

## Un enjeu de coopération internationale

La recommandation 1507 de 2001 (3) du Parlement européen souligne la nécessité pour les Etats de convenir de règles et de sanctions légales communes, et d'entamer une coopération en matière de partage des informations et d'autres formes d'entraide, dans le respect des droits individuels, en particulier de celui de la vie privée.

L'impératif de lutte contre la cybercriminalité s'est, en outre, manifesté au niveau européen par la création, le 27 octobre 2008, d'une plate-forme européenne de lutte contre la cybercriminalité. Celle-ci résulte d'une décision du Conseil regroupant spécialement les ministres de l'Intérieur et les ministres de la Justice des Etats membres. Les informations recueillies par chacune des plates-formes nationales seront dorénavant transmises à la plate-forme d'alertes européennes. «Ce regroupement des signalements permettra de déterminer le pays le plus à même d'effectuer des poursuites », a précisé, à cette époque, la ministre Mme Michèle Alliot-Marie.

## Analyse de la menace. Bilan

Ces deux dernières années (2006 et 2007) ont été particulièrement riches en évènements et ont notamment permis d'identifier de nouveaux risques majeurs, mais aussi de constater que les attaquants développaient

3/ Cf : http://assembly.coe.int/default.asp

continuellement de nombreux outils ou techniques d'attaque afin de déborder les outils de sécurité mis en place et la vigilance des utilisateurs.

L'année 2007 notamment a été marquée par une augmentation particulièrement significative du nombre d'attaques traitées, augmentation qui peut être imputée d'une part aux échanges internationaux plus riches, et donc des renseignements sur les attaques ou tentatives plus fournis, mais aussi à l'augmentation des attaques informatiques dans le monde.

## Les codes malveillants, méthode d'attaque visant la récupération de données sensibles

L'utilisation de codes malveillants, de type Chevaux de Troie, destinés à réaliser des attaques dans le but de dérober des informations sensibles ne se limite pas au champ des activités secrètes ou sensibles des Etats. Elles touchent l'ensemble des activités dans lesquelles la concurrence existe. Les entreprises sont ainsi une cible de choix pour les attaquants.

Le glissement observé d'attaques massives, au moyen de virus informatiques médiatisés, vers des attaques ciblées et discrètes est le résultat de la criminalisation massive des pirates informatiques, désormais plus motivés par le gain que par la reconnaissance de leurs capacités techniques. Lorsqu'ils n'agissent pas directement, ils mettent à disposition leurs moyens techniques ou leur savoir-faire, moyennant rétribution, au plus grand nombre : particuliers, officines, entreprises, services spéciaux…

## La multiplication des attaques ciblées au plan mondial

Depuis 2005, le nombre d'attaques ayant délibérément ciblé des systèmes sensibles et utilisant des codes malveillants spécifiquement conçus à cet effet est en très forte augmentation. La France n'a pas été épargnée. Le modus operandi de ces attaques consiste en l'envoi d'un message électronique visant des autorités et semblant provenir d'un interlocuteur habituel ; ce message est accompagné d'une pièce jointe infectée qui installe un code malveillant ayant pour but de récupérer des informations sensibles lorsque le destinataire tente de l'ouvrir. Du fait de la difficulté à les détecter et du ciblage préférentiel des autorités, ces attaques ciblées constituent une menace particulièrement insidieuse.

## Les attaques informatiques dites politiques, utilisées comme moyen de protestation

Ce nouveau phénomène s'est particulièrement illustré lors des émeutes des banlieues en 2006 avec l'attaque du site internet de la Mairie de Clichy-sous-Bois. Il en a été de même avec la publication des caricatures du prophète Mahomet, élément déclencheur en France de défigurations de sites français.

## Les vulnérabilités qui favorisent les attaques

Il s'avère que ces différentes menaces s'expliquent par des vulnérabilités diverses dont les plus importantes sont exposées ci-dessous :

Les premières sont les vulnérabilités liées aux applications, à savoir une qualité laissant à désirer d'un logiciel qui permet alors d'exploiter des failles pour conduire des attaques. Il s'agit d'erreurs de conception ou d'implémentation. La réponse apportée par l'Etat pour les organismes gouvernementaux vient du CERTA sur la base de ses publications. On ne rappellera jamais assez que la mise à jour des applications et de leurs correctifs constitue la première ligne de défense des systèmes d'information.

Les autres vulnérabilités mises en cause concernent les conditions d'emploi. Il peut s'agir de l'environnement du travail et du paramétrage d'installation. On constate que ces incidents sont souvent liés à une mauvaise mise en œuvre de la PSSI. Les exemples sont diversifiés et nombreux et vont de l'hébergement mutualisé de sites sur un serveur propice à la propagation des codes malveillants, à la suppression de la protection apportée par les pare-feux, en passant par des erreurs de configuration des droits ou à la fuite d'informations circulant par des technologies rayonnantes, de type Wi-Fi ou Bluetooth.

Enfin, un élément qu'on ne peut ignorer puisqu'il participe à sa façon au système d'information, les vulnérabilités introduites par les utilisateurs. Elles résultent d'une mauvaise manipulation par les utilisateurs finaux du système d'information, et s'expliquent par la faible qualité des mots de passe, l'ingénierie sociale, le phénomène de filoutage…

Au printemps 2007, des émeutes ont lieu à Tallin (Estonie). Elles font suite au déboulonnement par les autorités estoniennes d'une statue de bronze érigée à la gloire des soldats de l'Union Soviétique à la fin de la Seconde guerre mondiale. De façon fulgurante, des attaques informatiques sont organisées, visant des sites Internet gouvernementaux et privés estoniens (médias, banques, assurances, bourse, …).
Ces attaques ont duré plusieurs semaines et ont pris plusieurs formes : défacements, déni de service …
Ce phénomène a fait l'objet d'une analyse par la DCSSI et par ses homologues étrangers, analyse permettant d'affirmer que les attaques ont été réalisées par des réseaux de machines compromises réparties sur l'ensemble de la planète, sans qu'on puisse identifier qui contrôlait ce réseau de machines zombies ; si le nombre de machines compromises est très nettement inférieur au million annoncé par la presse, il n'en demeure pas moins qu'il a suffit à paralyser l'internet d'un pays entier ; enfin, les codes malveillants employés lors de ces attaques se sont avérés plutôt classiques et relativement peu sophistiqués. La coopération internationale a permis d'identifier environ une centaine de machines situées en France ayant participé à ces attaques.

Il n'existe pas de solution simple car aujourd'hui, les logiciels malveillants peuvent s'attaquer à tous les utilisateurs d'Internet, des entreprises aux particuliers, en passant par les gouvernements. **La sécurité est donc bien l'affaire de tous, qu'il s'agisse des Etats, des entreprises ou des particuliers. Neuf grands principes permettent de structurer une démarche globale :** sensibilisation, responsabilité, réaction, éthique, protection des libertés, évaluation des risques, conception et mise en œuvre de la sécurité, gestion de la sécurité, réévaluation. La prise en compte de cette chaine permet de s'engager dans une démarche cohérente face à un problème universel. La réponse à ce défi passe également par l'approfondissement des connaissances par les différents groupes (gouvernements, entreprises, utilisateurs ou acteurs techniques). Coopération et partage doivent également fédérer ces acteurs. Toute solution appliquée par un sans être partagée par les autres sera inefficace. L'encouragement de bonnes pratiques doit associer dans une démarche convergente approche réglementaire, répression, solutions techniques, actions d'éducation et de sensibilisation et enfin coopération internationale.

# La loi protège votre entreprise

## Première réponse de l'Etat aux incidences concrètes sur la vie quotidienne : la loi

Dans la mesure où la protection des citoyens et des entreprises dans le cyberespace entre dans le champ des compétences régaliennes de l'Etat, il apparaît clairement que ce dernier a pu identifier des risques et des menaces. La première réponse, assez précoce finalement, de l'Etat français a donc été de légiférer en la matière. Les domaines concernés sont parfois abordés par les mêmes textes de loi, ce qui explique les redites ci-après.

### Informatique et libertés

Le premier principe a consisté à dire que « l'informatique doit être au service de chaque citoyen (…) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Ce principe correspond en fait au tout premier article de la loi Informatique et Libertés, du 6 janvier 1978, modifiée par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données personnelles, l'une à caractère général, l'autre relative à la protection de ces données dans les réseaux. La commission européenne a contribué au principe de protection de la vie privée et des libertés individuelles au travers des deux textes suivants :

- directive européenne 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

- directive européenne 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

### Cybercriminalité

Nouveau domaine pour le droit pénal, la cybercriminalité recouvre deux grandes catégories d'infractions :

- les infractions directement liées aux technologies de l'information et de la communication, à savoir les atteintes aux systèmes de traitement automatisés de données, la diffusion de programmes malveillants, les infractions à la loi Informatique et Libertés sanctionnées au pénal, les infractions aux moyens de paiement et les infractions à la législation sur la cryptologie ;

- les infractions dont la commission a été facilitée ou liée à l'utilisation de ces tech-

nologies, à savoir la diffusion de contenus illicites (pédopornographie, racisme, …), les escroqueries par faux moyens de paiement pour une transaction en ligne, et certaines autres formes d'escroqueries, mais aussi les contrefaçons de logiciels et autres atteintes à la propriété intellectuelle.

Pour couvrir l'ensemble de ces domaines, les principales lois qui ont été adoptées sont :

- la loi du 5 janvier 1988, dite loi Godfrain (accès frauduleux aux systèmes d'information) ;

- la loi sur la sécurité quotidienne du 15 novembre 2001 (conservation des données de connexion par les opérateurs, cryptologie, cartes de paiement) ;

- la loi pour la sécurité intérieure du 18 mars 2003 (perquisition dans un système d'information, préservation des données par les opérateurs) ;

- la loi pour la confiance dans l'économie numérique du 21 juin 2004 (conservation des données par les hébergeurs de contenus, saisie des données informatiques, renforcement de la loi Godfrain, cryptologie) ;

- la loi relative au droit d'auteur et aux droits voisins dans la société de l'information, du 1er août 2006.

D'autres textes sont venus compléter cet arsenal :

- l'article 163-4 du Code Monétaire et Financier (CMF) sanctionne la fabrication, la détention, et la cession de moyens informatiques permettant d'attaquer les cartes bancaires ;

- l'article 39 de la loi 2001-1062 modifiant le CMF crée un Observatoire de la sécurité des cartes de paiement.

Au niveau européen, il convient de signaler :

- la décision cadre 2005/222/JAI du 24 février 2005 relative aux attaques visant les systèmes d'information ;

- la directive 2006/24/CE du 15 mars 2006 sur la conservation de données dans le cadre de la fourniture de services de communications électroniques.

Par définition, le cyberespace ne connaît pas de frontières physiques. Il a donc fallu prendre en compte des dimensions internationales au-delà de l'Union Européenne : cela a été fait au travers du traité de Budapest (Convention du Conseil de l'Europe) sur la cybercriminalité en date du 23 novembre 2001 et de son protocole additionnel du 7 novembre 2002. Des travaux dans le domaine de la cybercriminalité sont également conduits par le G8.

## Réponses françaises à la cybercriminalité

### La France a ratifié la Convention du Conseil de l'Europe.

La loi n° 2005-493 du 19 mai 2005 a approuvé la Convention du Conseil de l'Europe sur la cybercriminalité et le protocole additionnel à cette Convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (J.O., n° 116, 20 mai 2005, p. 8729). Les décrets permettant la publication de la Convention et du protocole ont été adoptés le 23 mai 2006. Il s'agit du décret n° 2006-580, J.O., n° 120, 24 mai 2006, p. 7568 et du décret n° 2006-597, J.O., n° 122, 27 mai 2006, p. 7937.

**La prise en compte croissante de la menace représentée par la cybercriminalité s'est traduite par la mise en place d'un dispositif dédié au sein du ministère de l'Intérieur.**

Ainsi, le plan d'action du ministère de l'Intérieur, présenté le 14 février 2008, définit quatre cibles principales : l'usurpation d'identité, l'escroquerie en ligne, les contenus pédopornographiques, racistes ou antisémites, les incitations aux terrorismes.

Pour accomplir ces nouvelles missions, de nouveaux moyens sont consacrés à la lutte contre la cybercriminalité :

- Mise en place d'une plate-forme de signalement automatique de toutes les formes de malversation, escroquerie, incitation à la haine raciale ou pédopornographie constatées sur Internet (4) ;
- Doublement du nombre d'enquêteurs spécialisés en criminalité informatique, au sein de la direction centrale de la police judiciaire, et d'enquêteurs en technologie numérique de la gendarmerie ;
- Création de cursus à vocation technologiques au sein de la police nationale, comme il en existe dans la gendarmerie.

# Des services spécialisés pour aider les entreprises

Disposer d'outils, aussi performants soient-ils, ne suffit pas pour autant, encore faut-il pouvoir les mettre en œuvre. Pour cela, la France s'est dotée de services spécifiques. La réponse, sur le plan pénal et judiciaire, s'est concrétisée par la création de services spécialisés au sein de l'Etat.

## La création de services spécialisés au sein de l'Etat

L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) a été créé en 2000 (la première entité constituée remonte toutefois à 1996). Il est intégré au sein de la Direction Centrale de la Police Judiciaire (Ministère de l'Intérieur) et a pour vocation de lutter contre la cybercriminalité sur l'ensemble du territoire national. Il compte dans ses rangs à la fois des gendarmes et des policiers qui mettent en commun leurs compétences. Il est épaulé pour ce faire par la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) constituée en septembre 1994, placée quant à elle sous la direction de la Préfecture de Police

4/ www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action

de Paris. Cette brigade, composée de policiers uniquement, a les mêmes compétences techniques, mais est limitée de plein droit quant à sa compétence territoriale à Paris et sa petite couronne.

La Direction Centrale du Renseignement Intérieur (issue de la fusion entre la DST et la DCRG) dispose elle aussi d'enquêteurs spécialisés en criminalité informatique, dont le domaine de compétence concerne les services gouvernementaux, les établissements à régime restrictif ou encore tout ce qui concerne les données classifiées de défense, et plus généralement le domaine de la sécurité intérieure.

La gendarmerie pour sa part a créé dès 1998, au sein du service technique de recherches judiciaires et de documentation (STRJD), une division de lutte contre la cybercriminalité. Ses enquêteurs recherchent les infractions sur Internet (pédopornographie, vente de contrefaçons, recettes d'explosifs, haine raciale, etc.). Cette division conseille et aide aussi les unités territoriales confrontées à des affaires en relation avec Internet.

Il est utile de préciser que nombre d'autres services peuvent être amenés à participer à la lutte contre la cybercriminalité sans toutefois que ce soit leur objectif principal. Leur liste est trop importante pour être citée, et pourrait consister en l'annuaire complet des services de police et de gendarmerie, répartis sur le territoire national.

Il convient également de citer l'Institut de Recherches Criminelles de la Gendarmerie Nationale (IRCGN), reconnu pour son expertise grâce aux capacités mises en œuvre dans sa division « Ingénierie et numérique » ainsi que la Direction de la Police Technique et Scientifique de la police judiciaire, qui interviennent régulièrement en support technique de l'ensemble des autres services et dont les travaux permettent souvent de comprendre des technologies et techniques émergentes.

La formation des enquêteurs constitue une priorité du ministère de l'Intérieur qui abrite désormais les deux grandes directions que sont la DGPN et la DGGN. Les enquêteurs spécialisés en criminalité informatique (ESCI pour la police, NTECH pour la gendarmerie) sont aujourd'hui disséminés au sein de bon nombre de services sur l'ensemble du territoire national alors que pendant très longtemps les personnels des services parisiens ont été privilégiés pour bénéficier de telles formations.

Pour autant, l'Etat a compris également que de disposer de services chargés de la répression ne suffisait pas à assurer sa sécurité. Il s'est donc doté de services préventifs.

La Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), héritière du service central de sécurité des systèmes d'information lui-même créé en 1986, placée sous l'autorité du Secrétaire général de la Défense Nationale a été instituée par décret le 31 juillet 2001. Elle a pour missions de :

- contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information ;

- assurer la fonction d'autorité nationale de régulation pour la SSI en délivrant les agréments, cautions ou certificats pour les systèmes d'information de l'Etat, les procédés et les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les centres d'évaluation de la sécurité des technologies de l'information ;

- évaluer les menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir ;

- assister les services publics en matière de SSI ;

- développer l'expertise scientifique et technique dans le domaine de la SSI au bénéfice de l'administration et des services publics ;

- former et sensibiliser à la SSI, au travers de son centre de formation à la sécurité des systèmes d'information (CFSSI).

En 2003, la DCSSI a étoffé son dispositif de prévention et de réaction aux attaques en créant le Centre Opérationnel de la SSI (COSSI). Ce centre a été créé dans le cadre de l'élaboration des plans de vigilance (VIGIPIRATE) et d'intervention SSI (PIRANET). Le COSSI est globalement chargé d'assurer la coordination interministérielle des actions de prévention et de protection face aux attaques sur les systèmes d'information de l'Etat ou dont l'importance pour le fonctionnement du pays ou pour la vie de la population le justifie. En cas de crise, la cellule de crise interministérielle s'appuie sur le COSSI pour la conduite technique opérationnelle de la crise.

Le COSSI est ainsi composé d'une cellule de veille active 24 h / 24, 7 jours/7, chargée d'identifier les évènements et informations relatives aux vulnérabilités ou attaques susceptibles de toucher l'Etat ou les infrastructures vitales. Il englobe également le CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques), créé en 1999 et chargé d'assister les organismes de l'administration dans la mise en place des moyens de protection, notamment par la détection précoce des vulnérabilités, et dans la résolution des incidents ou des agressions informatiques dont ils sont victimes.
Pour ce faire, il est tenu :

- d'assurer une veille technologique ;

- d'organiser la mise en place d'un réseau de confiance, notamment dans ses contacts avec les HFDS, FSSI et RSSI des différents ministères qui participent au même mouvement et sans la coopération desquels cette mission pourrait être menée à bien ;

- de piloter la résolution d'un incident (si besoin avec l'appui du réseau mondial des CERTs) ;

- d'assurer le pilotage des réponses techniques pour le volet SSI du plan Vigipirate et en cas de déclenchement du plan gouvernemental d'intervention face à une agression « cyberterroriste ».

Le COSSI comporte également une composante exercice qui a donné lieu depuis 2003 à la réalisation d'une vingtaine d'exercices dont deux exercices majeurs.

Outre la DCSSI, en France, d'autres organismes officiels sont chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents :
il convient de citer le CERT IST dédié au secteur de l'Industrie, des Services et du Tertiaire, créé fin 1998, mais aussi le CERT RENATER, en activité depuis 1995, dédié à la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche). Il existe encore deux autres CERTs français, privés.

Enfin, le Livre blanc sur la défense et la sécurité nationale, publié le 17 juin 2008, place en deuxième position la menace informatique, après le terrorisme. Afin de se donner les moyens d'agir en la matière, il organise une réforme de la DCSSI, créant une nouvelle agence pour la sécurité des systèmes d'information, qui relèvera du Premier ministre et du secrétariat général de la défense et de la sécurité nationale (SGDSN). Elle disposera de moyens renforcés par rapport à la direction actuelle. Elle conservera les missions de la DCSSI auxquelles s'ajouteront :

- la mise en œuvre d'un centre de détec-

tion chargé de la surveillance permanente des réseaux sensibles et de la recherche de mécanismes de défense adaptés. Ce centre fonctionnera en coordination avec ceux des partenaires internationaux, notamment européens ;

- le soutien et le conseil aux administrations et au secteur privé, en particulier aux opérateurs d'importance vitale. L'agence constituera un réservoir de compétences afin de répondre aux besoins les plus essentiels.

Au niveau territorial, l'agence s'appuiera sur un réseau d'experts des observatoires de la sécurité des systèmes d'information, qui seront mis en place dans les zones de défense et de sécurité sous l'autorité des préfets de zone.

## De nombreuses actions de prévention et de sensibilisation des acteurs économiques

La politique de répression contre la cybercriminalité s'accompagne également de la mise en place d'un volet préventif, destiné à sensibiliser les acteurs économiques à cette menace.

### Une préoccupation affichée des instances européennes et atlantiques

Cette nécessité a été soulignée par la Commission européenne dans une Communication au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions : créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité (5). Le texte encourage les entreprises à mener directement des actions contre la criminalité informatique.
En mars 2004, un programme pluriannuel Safer Internet Plus (2005-2008), succédant au plan d'action Safer Internet (1999-2004), est doté d'un budget de 45 millions d'euros afin de lutter contre les contenus internet illicites et préjudiciables et de promouvoir une utilisation plus sûre d'internet et des nouvelles technologies en ligne, particulièrement pour les enfants. Les activités menées au titre du programme sont réparties selon plusieurs lignes d'action : lutte contre les contenus illicites, traitement des contenus non désirés et préjudiciables, promotion d'un environnement plus sûr, sensibilisation des consommateurs, protection des données et sécurité des informations et des réseaux (virus, spams, etc.).

L'Agence Européenne pour la Sécurité des Réseaux (ENISA), créée le 10 mars 2004 par un règlement du Parlement européen et du Conseil, est chargée de renforcer la capacité d'anticipation, d'examen et de résolution des problèmes rencontrés par les Etats-membres, les institutions communautaires et les entreprises en matière de sécurité des réseaux et des informations.

Lors de la réunion ministérielle de l'OCDE sur le futur de l'économie d'Internet, en juillet 2008, l'Organisation a affirmé sa volonté de travailler avec les pays développés et en développement ainsi que les organisations internationales pour améliorer les politiques à l'égard de l'économie Internet et accroître la coopération internationale sur des questions comme la cybercriminalité et la sécurité. Cette volonté se traduit, en particulier, par la rédaction de rapports, comme celui sur la menace des logiciels malveillants publié en juin 2008.

L'Organisation du Traité de l'Atlantique Nord (OTAN) s'est dotée, en avril 2008, d'une

5/ Cf.: COM(2000) 890 final - Non publié au Journal officiel

agence de recherche dédiée à la cyberdéfense « Cyber Defence Management Authority ». Basée à Bruxelles, la CDMA est chargée de coordonner les moyens de défense dans et entre les différents pays membres, qui veulent se protéger des attaques cybernétiques.

## Une préoccupation intégrée par les pouvoirs publics

La prise en compte par les pouvoirs publics de la nécessité de mettre en œuvre une politique de sensibilisation des entreprises contre la cybercriminalité apparaît avec l'analyse des bouleversements introduits par Internet dans le monde de l'entreprise.

Ainsi, en 2002, le rapport Yolin inclut dans les adaptations juridiques nécessaires à l'usage d'Internet comme facteur de compétitivité des petites et moyennes entreprises la mise en place de moyens juridiques aptes à lutter contre la cybercriminalité (6).

Le rapport du député Lasbordes (7), en date du 26 novembre 2005, et intitulé « La sécurité des systèmes d'information - Un enjeu majeur pour la France » traite des vulnérabilités qui affectent la sécurité de systèmes d'information des entreprises et des administrations, du fait de la malveillance d'acteurs économiques indélicats mais également celle induite par les NTIC.

Ce constat le conduit à écrire : « L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux et leur complexité croissante associant des acteurs aux multiples profils, ont renforcé la vulnérabilité des systèmes d'information. Détruire, altérer, accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement des réseaux, les motivations sont diverses et fonction de la nature des informations recherchées et de l'organisme visé. ». Soulignant que la sécurité des systèmes d'information est un véritable défi, à la fois technologique et économique, il formule 6 recommandations détaillées dans l'annexe n°2.

## Une préoccupation relayée par les associations professionnelles

Les associations professionnelles se sont, dans le même temps, fortement impliquées dans la sensibilisation des entreprises à la prévention de la cybercriminalité. Ainsi, le Club de la Sécurité de l'Information Français, le CLUSIF, qui a pour mission d'agir pour la sécurité de l'information en direction des entreprises et des collectivités publiques, publie chaque année, d'une part, un « Panorama sur la Cybercriminalité »(8) recensant les grandes tendances de ce phénomène ainsi que ses nouvelles formes, et, d'autre part, un rapport sur « les menaces informatiques et les pratiques de sécurité en France »(9), qui analyse les nouveaux risques informatiques, leur sinistralité, ainsi que les mesures permettant de les circonscrire. Toutefois et au-delà d'un simple constat, le Club met à la disposition des entreprises différents outils pour améliorer la sécurité de leur système d'informations :

- des fiches pratiques pour les TPE-PME ;
- des recommandations abordant des questions aussi diverses que le retour sur investissement en matière de sécurité de l'information ou la sécurisation d'un Intranet ;
- des méthodes d'analyses de risque mise à jour annuellement, comme MEHARI.

Le Club Informatique des Grandes Entreprises Françaises, le CIGREF, accorde, de son coté, une place importante à la sensibilisation des entreprises dans la lutte contre la

6/ Rapport Yolin 2002 p : 256 Lien Internet : http://www.ensmp.net/pdf/2001/&1028mirage2001.pdf
7/ Cf. lien : http://www.lasbordes.fr/IMG/pdf/26_novembre_doc_definitif.pdf
8/ Cf. le site Internet du CLUSIF : http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE
9/ Cf. le site Internet du CLUSIF : http://www.clusif.asso.fr/fr/production/sinistralite/index.asp

cybercriminalité : en 2008, ce Club a publié un rapport sur « Protection de l'information : Enjeux, gouvernance et bonnes pratiques ». Il propose une définition élargie de la protection de l'information comme « une démarche consciente visant à protéger, au sein de l'entreprise étendue, ce qui vaut la peine d'être protégé, tant au niveau des données que des supports d'information », impliquant « un système de gestion, une identification des informations sensibles, une analyse de risques, des acteurs, avec des rôles et responsabilités et un programme de réduction des risques » (10).
Dans ce document, les objectifs assignés à une politique de protection de l'information en entreprises sont les suivants :

- Protéger les actifs immatériels de l'entreprise ;
- Définir les orientations générales et les priorités ;
- Développer, mettre en œuvre et maintenir un référentiel de protection de l'information (politiques, rôles et responsabilités, processus, normes) ;
- Sensibiliser et éduquer le management/ les employés à tous les niveaux ;
- Identifier et traiter les faiblesses prioritaires ;
- Assurer la conformité et contrôler.

## Une préoccupation prise en compte par les instances de normalisation

Au niveau européen, la Commission européenne a présenté, le 6 juin 2001, une communication proposant, notamment, un soutien des projets de normalisation et de certification orientés vers les besoins du marché.
La mise en œuvre de cette politique s'est notamment traduite par la création de l'European Telecommunications Standards Institute (ETSI), c'est-à-dire de l'Institut européen des normes de télécommunications. Basé à Sophia-Antipolis, cet institut est l'organisme de normalisation européen du domaine des télécommunications qui travaille actuellement sur la sécurité des réseaux, en coopération avec le Comité européen de normalisation (CEN) et le Comité Européen de la Normalisation Electrotechnique (CENELEC).

Cette volonté a été relayée par la prise en compte de la prévention de la cybercriminalité dans la normalisation de l'AFNOR.
Le Référentiel des bonnes pratiques de l'AFNOR, d'août 2002, aborde la problématique de la sécurité des informations stratégiques – qualité de la confiance. Il propose 12 principes (11) destinés à préserver la confidentialité des informations, abordant la nécessité de délimiter un périmètre d'informations stratégiques à protéger, d'exploiter l'information librement disponible sur les marchés et la concurrence, de s'assurer un réseau de fournisseurs de confiance, de mettre en place des dispositifs de protection efficace reposant sur un personnel qualifié et sensibilisé, et d'analyser et d'exploiter tout incident éventuel (Cf. annexe n°1).

## Le Plan Numérique 2012 vient asseoir le développement de l'économie numérique.

Ce plan, porté par le Secrétariat d'Etat chargé de la prospective, de l'évaluation des politiques publiques et du développement de l'économie numérique a été adopté en octobre 2008 (12).

154 actions regroupées dans quatre chapitres et une annexe s'intéressent aux fléaux numériques, aux architectures et technologies de sécurité (pourriel (spam), phishing, archivage, carte nationale d'identité, authentification forte et signature électronique (Transparence et confidentialité, droits d'auteur, pertinence, etc...)). Ce document se veut être une démarche créatrice de confiance.

10/ Cf. site du CIGREF : http://cigref.typepad.fr/cigref_publications/2008/10/2008---protecti.html
11/ Ces principes figurent en annexe de ce chapitre.
12/ http://www.francenumerique2012.fr

## Quelques exemples d'actions prévues par le plan numérique 2012

- **Action 44 :** Améliorer la confiance dans les services de communication et de partage en ligne en luttant contre les usages délictueux ou abusifs de ces services.

- **Action 45 :** Missionner la CNIL pour qu'elle émette une recommandation au sujet de la protection des données liées aux plateformes, ainsi qu'à la suppression de vidéos atteignant à l'intégrité de la personne ou à caractère diffamatoire.

- **Action 76 :** Déployer à partir de 2009, la carte nationale d'identité électronique, sur la base d'un standard de signature électronique fortement sécurisé, pour atteindre, à terme, un objectif de 100 % de citoyens titulaires d'une carte nationale d'identité électronique.

- **Action 78 :** Développer l'usage de l'authentification pour le grand public.

- **Action 82 :** Promouvoir la protection des données personnelles au plan international.

- **Action 103 :** Créer un référentiel des métiers du numérique

- **Action 114 :** Développer le télétravail dans le secteur public

- **Action 124 :** Prévoir et assurer l'archivage électronique des données et documents numériques.

- **Action 125 :** Faciliter l'accès aux services de l'usager

- **Action 126 :** Assurer l'interopérabilité entre administrations

- **Action 127 :** Assurer l'accessibilité des sites de l'administration

- **Action 133 :** Développer les services de télésanté et de bien-être

- **Action 154 :** Fédérer nos partenaires européens autour d'une structure de gestion européenne de l'Internet des Objets (ou "racine ONS") et mettre en commun les programmes de R&D nécessaires à la création d'une architecture distribuée pour l'Internet des Objets en Europe.

## Les travaux de l'OCDE sur la sécurité de l'information et la vie privée

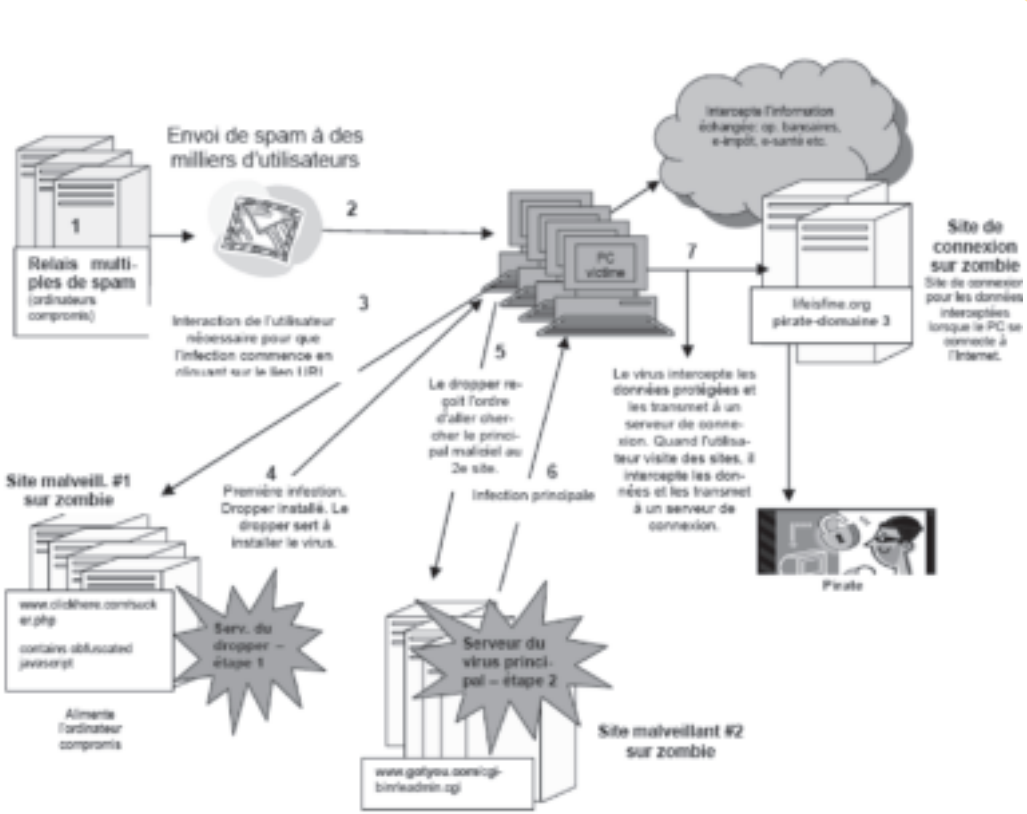
Un rapport a été rédigé au cours de l'année 2007 par le Groupe de travail sur la sécurité de l'information et la vie privée (WPISP, Working Party on Information Security and Privacy) de l'OCDE en partenariat avec le Groupe de pilotage sécurité et prospérité (SPSG, Security and Prosperity Steering Group) du Groupe de travail des télécommunications et de l'information (GTTEL) de la Coopération économique Asie-Pacifique (CEAP).

Ce document de 115 pages vise principalement « l' économie du maliciel » et recommande la mise en place d'une stratégie globale pour lutter contre les programmes informatiques malveillants («malware» en anglais), en passe de devenir une «menace sérieuse pour l'économie de l'internet». L'activité malveillante affecte selon le rapport tous les utilisateurs d'Internet, des entreprises au gouvernement ne passant par les simples internautes mais fait encore l'objet d'une «réponse locale fragmentée», estime l'Organisation de coopération et de développement économique (OCDE). Elle est aussi devenue « une industrie criminelle mondiale multi-millionnaire agissant dans l'ombre » souligne encore le rapport.

Selon l'OCDE, la «coopération internationale» est par conséquent «essentielle» pour lutter contre ce fléau, qui pourrait devenir «une menace sérieuse pour l'économie de l'internet et la sécurité nationale». Une large panoplie d'acteurs a un rôle à jouer dans le combat» contre la cybercriminalité, assure l'organisation, et les rôles et responsabilités de chacun doivent être mieux définis.
«Alors que les gouvernements se reposent toujours plus sur internet pour fournir des services aux citoyens, ils sont confrontés à des défis complexes» pour protéger leurs systèmes et réseaux informatiques d'une attaque ou d'une intrusion.
Les Etats-Unis ainsi que plusieurs pays européens ont ainsi signalé l'an dernier avoir été la cible d'attaques par internet, en provenance de Russie ou de Chine. Le grand public et les entreprises sont aussi visés par ces menaces en ligne, qui vont du simple blocage d'accès à des ressources jusqu'au vol d'information et d'identité en passant par l'espionnage, voire l'extorsion d'argent (rançons).
(Cf. Fig.1 ci-dessous). L'OCDE propose également plusieurs pistes d'action, parmi lesquelles une meilleure sensibilisation des internautes, l'attribution de ressources plus importantes pour poursuivre les cybercriminels ou encore l'établissement d'un code de bonnes pratiques.

**Figure 1 :**
**Système de vol d'identité en ligne utilisant des logiciels malveillants** (13)

13/ Source OCDE



## La Commission Nationale Informatiques et Libertés (CNIL) joue un rôle de conseil et de formation

La Commission Nationale de l'Informatique et des Libertés (14), autorité administrative indépendante est chargée d'assurer le respect des dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004.

Cette loi impose un certain nombre d'obligations aux responsables de fichier, et notamment aux chefs d'entreprises.

- Notifier la mise en œuvre du fichier et ses caractéristiques à la CNIL, sauf cas de dispense prévus par la loi ou par la CNIL.
- Mettre les personnes concernées en mesure d'exercer leurs droits en les en informant.
- Assurer la sécurité et la confidentialité des informations afin qu'elles ne soient pas déformées ou communiquées à des tiers non autorisés.
- Se soumettre aux contrôles et vérifications sur place de la CNIL et répondre à toute demande de renseignements qu'elle formule dans le cadre de ses missions.

En outre, les traitements les plus « sensibles » sont soumis à une autorisation de cette commission. Le non-respect de ces formalités par les responsables de fichiers est passible de sanctions administratives ou pénales.

Outre sa mission de contrôle, la CNIL conseille et renseigne les personnes et les organismes qui envisagent de mettre en œuvre des fichiers informatiques, que ce soit par téléphone, par courrier ou par ses publications. Elle s'est dotée d'un service d'orientation et de renseignement afin d'apporter une réponse rapide aux requêtes des particuliers comme des professionnels sur l'application de la loi.

Les entreprises et les administrations recourent de façon croissante aux moyens informatiques pour gérer leurs ressources humaines. L'ensemble du secteur des RH est concerné : recrutement, gestion des carrières et des compétences, le suivi du temps de travail, etc.…

Simultanément, les dispositifs de contrôle des salariés liés aux nouvelles technologies se multiplient : vidéosurveillance, cybersurveillance, applications biométriques, géolocalisation, etc.… Ces applications enregistrent de nombreuses informations à caractère personnel sur les salariés. La loi Informatique et Libertés fixe un cadre à la collecte et au traitement de ces données afin de les protéger, dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée. Le respect, par les entreprises et administrations des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard des salariés. C'est aussi un gage de sécurité juridique pour les employeurs qui sont responsables de ces traitements informatiques et de la sécurité des données personnelles qu'ils contiennent. Ils peuvent ainsi voir leur responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi.

C'est pourquoi la CNIL est chargée de veiller au respect de ces principes et souhaite informer les salariés des droits dont ils disposent, ainsi que les employeurs, en les conseillant sur les mesures à adopter pour se conformer à la loi. Un guide (15) a pour vocation de leur donner les clés pour bien utiliser ces outils et les fichiers mis en œuvre en matière de gestion des ressources humaines. C'est aussi le but du « correspondant informatique et libertés », interlocuteur privilégié de la CNIL dont la désignation permet, au-delà de l'exonération de déclaration, d'intégrer pleinement la problématique de la protection des données personnelles.

14/ www.cnil.fr

15/ http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf

# Perspectives pour l'entreprise

## Les Assises du numérique

Avec les Assises du numérique, qui se sont déroulées en juin 2008 (16), la France s'est dotée d'un cadre d'action de la politique publique en matière de lutte contre la cybercriminalité à l'horizon 2012. Son élaboration a associé les pouvoirs publics, les entreprises et plus généralement les différents acteurs du numérique, autorisant ainsi une approche globale de la criminalité sur Internet.

La lutte contre la cybercriminalité, avec neufs actions mêlant les approches répressive, pédagogique et de sensibilisation, est définie comme un domaine essentiel de l'action de l'Etat dans le secteur du numérique (Cf.Annexe n° 3). Les actions concernent la lutte contre la contrefaçon et les escroqueries sur Internet, l'accroissement des moyens affectés à la lutte contre la criminalité informatique, l'adaptation du droit à l'évolution de la fraude sur Internet, et des actions de prévention à l'égard des Internautes ainsi qu'une coopération renforcée entre les différentes administrations au niveau national et entre les différents Etats membres de l'Union européenne. **Les Assises du numérique font de la lutte contre la cybercriminalité une condition essentielle du succès de l'économie numérique française.**

16/ http://francenumerique2012.fr/

## Le DLM
### (Digital Legal Management) ou gestion du droit d'usage de l'information
## Une application pratique originale

Partant du constat français que 24 % des sinistres informatiques sont dus à un accident, 14 % à des erreurs humaines et 62 % à la malveillance et qu'Internet n'intègre que très faiblement encore une dimension de responsabilisation de ses utilisateurs, l'émergence de la nécessité de disposer d'une gestion du droit d'usage rétablissant les notions de responsabilités individuelles, entrepreunariales et institutionnelles s'est fait jour. La classification documentaire par usages individuels et par types de défiances permet d'élaborer une stratégie sécuritaire adaptée, rationnelle et optimisée.
L'approche « sécurité économique » apporte dans ce cadre de nombreux atouts et comporte une dimension complémentaire car elle a pour objectif de faire partager un état d'esprit et créer des espaces de confiance. La simplicité du DLM peut permettre d'adopter une nouvelle stratégie sécuritaire fondée sur la responsabilité individuelle qui permettra de protéger les systèmes d'information des erreurs humaines (inadvertance ou fraude) qui sont majoritairement à l'origine des pertes de valeurs.

## Le DLM repose ainsi sur un triptyque :

- Une stratégie de protection de l'information qui s'appuie sur la réputation des utilisateurs
- Un code de confiance
- Un modèle qui augmente la fluidité de l'information et réduit le coût de sécurité

Le grand apport de ce concept est d'opérer une distinction entre confiance et sécurité. La sécurité est un modèle économique tandis que la confiance est une relation interpersonnelle primordiale et donc, préalable à toute question pécuniaire.

**« Il ne peut pas y avoir de confiance entre deux individus sans qu'ils consentent au droit d'usage de l'information qu'ils prévoient de partager ; et au-delà avec leurs relations respectives »**

Le DLM est donc une stratégie basée sur le besoin d'appartenance à un groupe. Théoriquement, aucun individu n'est disposé à délivrer une information à un tiers au risque de perdre son emploi ou sa source de revenus. La sociologie des groupes montre que lorsque les individus sont responsabilisés pour leurs actes, ils agissent mieux, voir bien. La limite de ce mieux, c'est le risque qu'ils encourent à être exclus du (méta) groupe auquel ils appartiennent et, qui les nourrit !

La mise en œuvre du DLM permet de réaliser des échanges d'informations dont les limitations ont été préalablement consenties. Ainsi sur un portail informatique collaboratif chaque document disposera d'un droit d'usage (ne pas imprimer/transmettre/modifier, …) affecté à chaque d'utilisateur.

Dans un tel schéma, la pièce comptable peut être modifiée par le comptable, lequel n'a pas le droit de la publier ; le responsable financier peut la publier mais pas la modifier. Les échanges ont lieu sur la base d'un consentement. Comme nous l'avons exposé plus haut, le règlement intérieur d'une structure et les contrats de travail doivent prévoir le dispositif. Lorsqu'un utilisateur transgresse le droit d'usage consenti, la traçabilité de la transaction permet de l'exclure de l'espace de confiance dont il avait bien besoin pour travailler.

## Le DLM ne se contente pas de classifier les documents. Il anticipe les raisons pour lesquelles :

- des utilisateurs ne prendront pas le risque de se faire exclure de l'organisation qui est leur source d'activité,
- des utilisateurs pourraient renoncer à appartenir au groupe parce que leur bénéfice pourrait être supérieur dehors.

## Le DLM permet à l'organisation de rationaliser ses budgets d'investissements sécuritaires sur quatre axes de travail :

- l'invisibilité de l'information,
- la valeur marchande estimée de l'information,
- la période de criticité de l'information,
- le périmètre des utilisateurs et son turnover intra et hors organisation.

Ce dernier point est particulièrement sensible pour les données critiques archivées.

Sur le plan économique, le DLM accélère l'accès à l'information de qualité entre les acteurs de la valeur. Il réduit les contentieux et il rationalise, voire réduit les coûts de sécurité informatique. Sur le plan juridique, il protège les collaborateurs et la hiérarchie. L'information est fluide entre les individus ;

le besoin d'en connaître est satisfait. Les premiers tests ont montré que le DLM peut réduire les actions de malveillance d'un facteur par l'emploi de règles contextuelles, consenties et tracées entre les utilisateurs.

## Concrètement :

« L'information a besoin d'outils pour faire circuler l'information entre individus ». Une application pratique de DLM, dotée de fonctionnalités de sécurité appropriées concerne les machines multifonctions : photocopie + imprimante + scanner + télécopie (MFP) qui sont, par excellence, des outils d'acquisition-restitution de l'information entre utilisateurs. Ainsi, le DLM peut concourir au fait que « la bonne personne ait le droit d'usage du document à jour au moment où elle en a besoin pour créer de la valeur ».

# Annexe n°1 :

## Les 12 clés de la sécurité selon l'AFNOR

*(D'après le Référentiel de bonnes pratiques de l'AFNOR - Août 2002 Sécurité des Informations Stratégiques – Qualité de la confiance. Comment préserver la confidentialité des informations)*

**1)** Admettre que toute entreprise possède des informations à protéger (plans de recherche, prototypes, plans marketing, stratégie commerciale, fichiers clients, contrats d'assurance,…) ;

**2)** Faire appel à l'ensemble des capacités de l'entreprise (chercheurs, logisticiens, gestionnaires de personnel, informaticiens, juristes, financiers,…) pour réaliser l'inventaire des informations sensibles, des points faibles, des risques encourus et de leurs conséquences ;

**3)** Exploiter l'information ouverte sur l'environnement dans lequel évolue l'entreprise, observer le comportement des concurrents, partenaires, prestataires de service, fournisseurs, pour identifier les menaces potentielles ;

**4)** S'appuyer sur un réseau de fournisseurs de confiance pour ceux d'entre eux qui partagent ou accèdent à des informations sensibles ;

**5)** Ne pas chercher à tout protéger : classifier les informations et les locaux en fonction des préjudices potentiels et des risques acceptables ;

**6)** Mettre en place les moyens de protection adéquats correspondant au niveau de sensibilité des informations ainsi classifiées, s'assurer qu'ils sont adaptés et, si besoin, recourir à des compétences et expertises extérieures ;

**7)** Désigner et former des personnes responsables de l'application des mesures de sécurité ;

**8)** Impliquer le personnel et les partenaires en les sensibilisant à la valeur des informations, en leur apprenant à les protéger et en leur inculquant un réflexe d'alerte en cas d'incident ;

**9)** Déployer un système d'enregistrement des dysfonctionnements (même mineurs), et analyser tous les incidents ;

**10)** Ne pas hésiter à porter plainte en cas d'agression ;

**11)** Imaginer le pire et élaborer des plans de crise, des fiches « réflexe » afin d'avoir un début de réponse au cas où… ;

**12)** Evaluer et gérer le dispositif, anticiper les évolutions (techniques, concurrentielles,…) et adapter la protection en conséquence en se conformant aux textes législatifs et réglementaires en vigueur.

# Annexe n°2 :
## 6 recommandations du Rapport Lasbordes

Les six recommandations proposées correspondent à une double ambition : renforcer la posture stratégique de l'Etat en matière de TIC et de SSI et assurer la mise en œuvre opérationnelle des politiques et des décisions de l'Etat en matière de SSI. Certaines d'entre elles figuraient déjà dans le Plan de Renforcement de la Sécurité des Systèmes d'Information de l'Etat élaboré en 2004.

### Axe 1 : Sensibiliser et former à la sécurité des systèmes d'information

- Organiser une grande campagne de communication s'inscrivant dans la durée à destination de tous ;
- Mettre en place un portail Internet pour mettre à la disposition des utilisateurs – citoyens, administrations et entreprises - des informations d'actualité, des guides de bonnes pratiques, des contacts, des alertes sur les menaces,… ;
- Proposer au système éducatif - du primaire à l'enseignement supérieur – et au système de formation continue, des canevas modulaires de formation en SSI ;
- Informer l'utilisateur : à l'instar du port de la ceinture pour l'utilisation d'un véhicule automobile, imposer que la documentation utilisateur qui accompagne les produits personnels de communication mentionne les risques principaux encourus vis-à-vis de la protection des informations, les points de vigilance pour l'utilisateur et les recommandations types à mettre en œuvre (exemple : activer un pare-feu, protéger et changer régulièrement son mot de passe,…).

### Axe 2 : Responsabiliser les acteurs

- Etablir de manière obligatoire des chartes à l'usage des utilisateurs, annexées au contrat de travail – public et privé - ou aux règlements intérieurs des entreprises ;
- Labelliser les entreprises fournisseurs de produits ou services de SSI qui respectent un cahier des charges à établir.

### Axe 3 : Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence

- Identifier les maillons des systèmes d'information qui exigent des produits qualifiés ;
- Etablir et tenir à jour un catalogue des produits de sécurité nationaux qualifiés et des produits européens adaptés aux différents niveaux de sécurité à assurer ;
- Développer les financements publics de R&D ;
- Favoriser le développement des PME innovantes dans la SSI et renforcer les fonds d'investissement en capital développement ;
- Développer la politique de certification et de qualification par une augmentation des produits certifiés et qualifiés et une réduction des délais et des coûts de certification ;
- Accroître la présence et l'influence française dans les groupes de standardisation et les comités de normalisation ;
- Définir et mettre en œuvre une politique d'achat public, fondée sur le principe d'autonomie compétitive. Inciter les grandes entreprises à travers le pacte PME à faire confiance aux PME certifiées en SSI.

### Axe 4 : Rendre accessible la SSI à toutes les entreprises

- Inciter les entreprises à assurer leur SSI par la mise en place d'aides publiques ;
- Créer un centre d'aide et de conseil dans une logique de guichet unique ;
- Diffuser aux PME sous une forme adaptée les informations de veille, d'alerte et de réponse disponibles au niveau des CERT nationaux ;
- Initier et animer des forums thématiques publics – privés favorisant la circulation d'informations, les retours d'expériences, le partage des bonnes pratiques,…

### Axe 5 : Accroître la mobilisation des moyens judiciaires

- Reconnaître la spécificité des contentieux liés aux systèmes d'information ;
- Aggraver les peines prévues au Code pénal en matière d'atteinte à la SSI ;
- Introduire une exception au principe d'interdiction de la rétro-conception dans le Code de la Propriété intellectuelle pour des motifs de sécurité ;
- Assurer la sensibilisation des magistrats et des forces de sécurité par la formation initiale et continue ;
- Constituer un pôle judiciaire spécialisé et centralisé de compétence nationale ;
- Renforcer les coopérations internationales.

### Axe 6 : Assurer la sécurité de l'Etat et des infrastructures vitales

- Mettre à jour les politiques de SSI et les schémas directeurs de chaque ministère et les valider par une autorité centrale ;
- Conseiller en amont les maîtrises d'ouvrage de l'Etat pour des projets sensibles tels que par exemple la carte nationale d'identité ou le dossier médical ;
- Confier à une autorité centrale le rôle d'approuver formellement le lancement de ces projets sensibles ;
- Faire contrôler par une autorité centrale l'application de ces prescriptions par des inspections sur site et des tests d'intrusion sans préavis ;
- Mettre en place et animer une filière SSI transverse dans laquelle la mobilité sera organisée, tant à l'intérieur de la fonction publique qu'au travers de passerelles avec les entreprises et les centres de recherche ;
- Définir les profils de postes des responsables SSI. Renforcer leur autorité et leur responsabilité ; ils devront être indépendants des directions des systèmes d'information ;
- Pour les opérateurs d'infrastructures vitales : valider la politique de sécurité par l'autorité centrale et conduire des inspections et des tests d'intrusion ;
- Pour les entreprises sensibles, faire à la demande des audits et des tests d'intrusion.

## Annexe n°3 :

**Les Assises du numérique**

*Lutter contre toutes les formes de cybercriminalité*

La France doit se donner les moyens de lutter contre toutes les formes de cybercriminalité, que ce soit celle de l'atteinte aux réseaux (piratage, intrusions sur les sites…) ou celle de l'utilisation des réseaux (contrefaçon, escroquerie, pédopornographie, incitation à la haine raciale, propagande terroriste…).

Des efforts de coordination et de mutualisation, tant au niveau national qu'international, en matière de moyens mis à disposition et d'investigations effectuées dans ces domaines par la police et la gendarmerie nationales, ainsi que par les douanes ont déjà été initiés. Ces moyens doivent être renforcés et adaptés. La coordination internationale doit être accrue.

Ainsi, en termes d'organisation, les prérogatives de certains organismes pourront être revues et étendues pour prendre en compte de nouvelles formes de cybercriminalité, comme la multiplication des délits de contrefaçon sur Internet. Par ailleurs, la France doit jouer un rôle moteur dans la coordination internationale des moyens de lutte contre la contrefaçon, en particulier sur Internet et prendre une initiative forte dans ce domaine à l'occasion de la présidence française de l'Union européenne.

**Action n°83 : Accentuer la lutte contre la contrefaçon vendue sur Internet.** Adopter dans le cadre de la présidence française de l'Union européenne un plan intégré européen de lutte contre la contrefaçon, comprenant la lutte contre la contrefaçon vendue sur Internet, décliné au plan national à compter du 1er janvier.

**Action n°84 : Créer un groupe spécialisé sur les escroqueries sur Internet,** assurant la centralisation opérationnelle des enquêtes et moyens, au sein de l'Office central de lutte contre la criminalité liée aux technologies de l'information (OCLCTIC). De même, les outils statistiques de pilotage et de suivi, utilisés par la police et la gendarmerie nationale, doivent désormais prendre en compte les infractions constatées sur Internet.

**Action n°85 : Développer, dans le cadre du projet Ardoise** (Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes), un outil de connaissance des statistiques des infractions relevant de la "cybercriminalité". Enfin, parce que le volume des infractions constatées progresse d'année en année, il convient d'affecter plus d'effectifs à la lutte contre la cybercriminalité.

**Action n°86 : Doubler d'ici à 2012 le nombre d'enquêteurs spécialisés en criminalité informatique** dans la police nationale, la gendarmerie nationale et les services des douanes. Sur le plan juridique, la France doit également continuer à se doter d'outils adaptés, en matière de définition des délits et ou de sanctions.

**Action n°87 :** Introduire à l'occasion de la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) :

- Un délit d'usurpation d'identité sur les réseaux de communications électroniques ;
- Une disposition permettant, en accord avec les fournisseurs d'accès Internet, de bloquer sur signalement des sites pédo-pornographiques ;
- Des peines alternatives d'intérêt général pour les hackers condamnés sans intention de malveillance. Ces moyens juridiques et policiers renforcés doivent par ailleurs s'accompagner d'une meilleure information du cybernaute de la loi et des risques encourus et aussi informer le public sur les moyens d'éviter tous ces risques.

**Action n°88 : Créer d'ici à la fin de l'année, un site Internet de conseils pédagogiques dédié aux utilisateurs pour prévenir les infractions commises sur Internet.** Internet ne connaissant pas de frontières, la coopération internationale, notamment avec les partenaires européens de la France, doit être un pilier majeur de la lutte contre la cybercriminalité. Elle est déjà une réalité par l'har-

monisation progressive qui s'opère au niveau Européen, sur le plan législatif comme sur celui de la formation des forces de police des pays membres, en matière de lutte contre la cybercriminalité. Dans le cadre de la Présidence française de l'Union européenne, la France pourra proposer de mutualiser les efforts dans la lutte contre la cybercriminalité.

**Action n°89 : Créer d'ici à 2009, une plate-forme européenne d'échanges d'informations sur la cybercriminalité et les sites illicites** dans le cadre d'Europol, à l'image de la plate-forme française d'harmonisation, de recueil, d'orientation des signalements (PHAROS), qui sera opérationnelle fin 2008. L'action publique doit s'appliquer à rendre les plus jeunes conscients des risques associés aux outils de communication de l'Internet. C'est l'objectif des campagnes de sensibilisation et de pédagogie que le gouvernement a mis en œuvre, à l'instar de l'initiative de la Délégation aux Usages de l'Internet, qui a crée en 2003 un site Internet destiné à prévenir les mineurs contres les risques de l'Internet. Ces campagnes de sensibilisation menées souvent par différents ministères, bénéficieraient d'une meilleure coordination.

**Action n°90 : Coordonner des campagnes de sensibilisation portées par les différents ministères en lien avec la direction du développement des médias (DDM), le secrétariat général de la Défense nationale (SGDN) et la délégation aux usages de l'Internet (DUI).**
Au-delà des campagnes d'information, la protection la plus efficace consiste à former, très tôt, les plus jeunes aux nouvelles technologies, à les accompagner et à les aider à développer leur esprit critique dans l'utilisation du net. C'est d'ailleurs l'un des objectifs du brevet informatique et Internet (B2I), qui atteste de la capacité de l'élève à utiliser, avec esprit critique, les outils multimédias et Internet. Cette dynamique doit être consolidée par un effort de formation plus important à destination des plus jeunes, notamment des enfants de moins de 12 ans. Il s'agit notamment d'améliorer la formation des jeunes à la citoyenneté sur Internet à travers les modules du brevet informatique et Internet (B2I).

L'Internet doit demeurer libre pour continuer de s'enrichir. Ceci implique aujourd'hui la présence de nombreux contenus à caractère choquant pour les publics non avertis. L'accès de tous à Internet porte la promesse d'un accès inconditionnel à la connaissance et à l'information. Il est donc nécessaire que les plus jeunes puissent consulter l'Internet en toute quiétude.

Les moyens de communication se développent à une célérité qui met à mal l'efficacité du législateur. La concertation en amont entre les différents acteurs est indispensable à l'établissement d'une situation optimale et équilibrée. Pour poursuivre pleinement ses objectifs, l'État doit donc favoriser l'autorégulation des acteurs de l'Internet : par des chartes d'engagement, par une "softlaw" plus souple et plus apte à s'adapter aux incessantes évolutions technologiques, une ligne de conduite commune peut être dessinée, au profit d'un Internet respectueux de tous les internautes.

**Action n°91 : Améliorer la lutte contre contre les spams.**
Les opérateurs seront invités à travailler avec les pouvoirs publics pour améliorer les conditions dans lesquelles ils pourraient s'engager à limiter l'accès aux numéros et SMS surtaxés correspondant à des services frauduleux ainsi que la réception des messages ou appels provenant de ces numéros et les reversements financiers associés.

# POSTFACE

par Pascal LOINTIER,
Président du Club de la Sécurité de l'Information Français, CLUSIF
conseiller sécurité de l'information, AIG Europe

Après lecture de ce guide sur le risque numérique, vous n'êtes plus dans la méconnaissance des risques et des enjeux de continuité qu'ils constituent pour votre entreprise. Vous pouvez, toutefois, rester insouciant face au danger : un raisonnement probabiliste était d'usage avant 2001 ! Depuis, ces événements - New-York, Toulouse, les accidents aériens en série - ont provoqué une modification des comportements et la question posée est désormais la suivante : le scénario d'incident a-t-il un impact vital/critique pour mon entreprise ? Si la réponse est positive, il faut alors identifier une solution pour en réduire les conséquences : il s'agit bien de la survie de votre activité.

## Agir au plus tôt, ce qui ne signifie pas dans l'urgence

L'incident, accident ou acte de malveillance, peut survenir à tout moment. Il n'y a donc aucune justification à retarder une action de réflexion quant à sa politique de sécurité. Insistons sur ce point car la dernière étude diligentée par le Clusif « Menaces Informatiques et Politiques de Sécurité en France » fait d'abord état d'un paradoxe : 73 % des PME interrogées estiment avoir une dépendance forte par rapport au système d'information… mais 39 % d'entre elles n'ont pas réalisé une analyse globale des risques auxquelles on pourrait ajouter 30 % ayant effectuées une étude partielle, donc potentiellement incorrecte ou négligeant un facteur de risque critique !

## Faire un point de situation sur le niveau de sécurité

La première étape consiste bien à faire un point de situation sur l'état opérationnel des moyens déployés et l'application effective des procédures de sécurité et d'organisation. Quelle que soit la taille de l'entreprise et son allocation initiale de ressources, une analyse de risques est possible et doit être engagée. Pour cela, une PME peut se faire assister d'un consultant en sécurité des systèmes d'information (SSI). Il est important que cette « photographie » du système soit réalisée par un professionnel ayant une vision transversale des atteintes possibles et des scénarios d'incident. Un « intégrateur », fournisseur historique, un revendeur de produit de sécurité peut être très bon dans son domaine (serveurs performants, antivirus, pare-feu, moyen de sauvegarde) mais la sécurité du système d'information déborde largement la seule installation de produits. Il faut d'une part, prendre en considération tous les facteurs de sécurité ou toutes les déclinaisons de politiques de sécurité : sauvegarde, secours informatique, continuité des services, gestion des droits en interne et en télé-accès, départ du personnel stratégique, etc. et d'autre part, identifier les bonnes procédures de travail. En effet, la sécurité n'est pas systématiquement couteuse ou trop couteuse. Par une réorganisation du travail, on augmente considérablement son niveau de sécurité. Redisons-le car les mesures

sont insuffisamment appliquées par les PME, une politique de sauvegarde composées de cycle journaliers, hebdomadaires et mensuels garantit une meilleure intégrité des données. La conservation hors site des supports de sauvegarde, c'est-à-dire sur un autre site, garantit une meilleure disponibilité suite à un incendie ou un dégât des eaux. Le consultant SSI peut, en quelques jours et à la suite d'entretiens préparés avec les différents acteurs de l'entreprise, réaliser une telle analyse. On citera ainsi les actions de sensibilisation organisées par les Chambres de Commerce et d'Industrie en collaboration avec des prestataires régionaux. A l'issue de ce point de situation, un plan d'action, on parle de schéma directeur de la SSI, peut alors identifier les priorités d'action et la cohérence de déploiement des outils et surtout des procédures d'emploi.

## Le tableau de bord d'impact, aide à l'évaluation des besoins

Une fois cette analyse des facteurs de risques ou des scénarios de dysfonctionnement, l'étape suivante concerne l'appréciation des enjeux ou des conséquences. Là encore, l'étude CLUSIF fait état d'une situation qu'on pourrait presque qualifier d'affligeante : 72 % ne procèdent pas à l'évaluation de l'impact financier des incidents de sécurité et, corollaire, 75 % n'ont pas de tableau de bord de sécurité informatique. On pourrait avancer des éléments d'explication (et non de justification…) : réaction psychologique et volonté d'amnésie suite à un événement déstabilisant, absence de savoir-faire quant aux poste de remboursement à mesurer. Pourtant, le tableau de bord, qu'il soit d'impact (suite à une crise) ou de sécurité (dans l'exploitation courante) présentera plusieurs avantages. D'une part, c'est un début d'appréciation du RoSI, le retour sur investissement de sécurité, pour analyser comment la sécurité a contribué au maintien de la productivité de l'entreprise. D'autre part, il permet d'identifier le montant de capital garanti dans le cadre d'une assurance du système d'information. A ce titre, il est important de comprendre qu'une couverture d'assurance n'est pas une alternative à une politique de sécurité ou à la mise en place de moyens et procédures. Elle doit s'analyser comme un financement des frais de remise en état du système et un remboursement possible des préjudices économiques subits (pertes d'exploitations, frais supplémentaires, etc.)...

## Gérer le comportement humain et non le facteur humain

On l'a vu, une bonne politique insiste sur des procédures adaptées non seulement aux exigences du métier (nature des équipements, délai de disponibilité, traçabilité réglementaire, etc...) mais aussi à l'environnement humain. Cyniquement, on pourrait mettre en avant la paresse humaine, cette propension naturelle à ne pas systématiquement respecter des mesures perçues comme rébarbatives ou encore les erreurs ou omissions dans l'exécution des dites procédures. C'est pourquoi, la règle, même formalisée, ne se suffit à elle-même. Il est très important de prendre en considération les habitudes initiales de travail, la perception des enjeux et les avantages à gagner pour l'utilisateur quant il respectera ces nouvelles mesures. En clair, une note de service, une charte de bonne conduite informatique ne sauraient suffire : il faut motiver / intéresser les utilisateurs (y compris les directeurs…) au respect des usages édictés. La psychosociologie est là pour nous démontrer comment l'individu, et sa prise de décision, est susceptible d'interagir ou d'être orienté par des informations transmises par son environnement son groupe d'activité. On découvre alors que l'être individu n'est pas un être de raison, de rationalité et que des techniques permettent l'orientation du comportement…

### Mettre en place une dynamique

L'adaptation des moyens, la cohérence des pratiques et l'adhésion de l'usager aux bonnes pratiques ne peuvent malheureusement suffire… l'entreprise évolue et son système d'information aussi. Une dépendance ou un impact plus fort suite à l'accroissement d'activité, une évolution des architectures informatiques avec de nouvelles menaces à prendre en compte et enfin, les rotations de personnels font qu'une démarche cyclique doit être mise en place. Nouvel audit pour apprécier l'augmentation du niveau de sécurité, reconfiguration des équipements et installation de correctifs de sécurité et sensibilisation des nouveaux salariés… toutes ces actions sont nécessaires pour que « numérique » soit associé à gain de production et non à risques…

# Webographie

## E-Sources :

**Portail de la sécurité informatique :**
www.securite-informatique.gouv.fr
www.nouvellesmenaces.eu

**Portail du CLUSIF :**
www.clusif.fr

**Serveur thématique sur la sécurité des systèmes d'information (DCSSI) :**
www.ssi.gouv.fr

**CIGREF :**
www.cigref.fr

**CNIL :**
www.cnil.fr

**La mission du Haut Responsable en charge de la Haute Intelligence Economique :**
www.intelligence-economique.gouv.fr

**INHES :**
www.inhes.fr,
www.cahiersdelasecurite.fr

**Documentation**
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=FRE
www.telecom.gouv.fr/fonds_documentaire/rapports/cybercriminalite.pdf
http://assembly.coe.int/default.asp
www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action
http://cigref.typepad.fr/cigref_publications/2008/10/2008---protecti.html
www.clusif.asso.fr/fr/production/sinistralite/index.asp
www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE
www.clusif.fr/fr/production/ouvrages/pdf/PanoCrim2k8-fr.pdf

**Rapport Yolin 2002 p 256 :**
http://www.ensmp.net/pdf/2001/&1028mirage2001.pdf

**Rapport Lasbordes - La sécurité des systèmes d'information**
**Un enjeu majeur pour la France - novembre 2005**
www.lasbordes.fr/article.php3?id_article=166
www.lasbordes.fr/IMG/pdf/26_novembre_doc_definitif.pdf

**Plan de développement de l'économie numérique**
www.francenumerique2012.fr

**Guide pour les entreprises et les salariés - CNIL**
www.cnil.fr/fileadmin/docume...blications/CNIL_GuideTravail.pdf

# Autres sites pour en savoir plus :

**Guide de l'Intelligence économique en Suisse occidentale**
http://campus.hesge.ch/areso/files/guide.pdf

**DCRG - Intelligence économique défensive :**
**Physionomie nationale du risque financier - novembre 2006**
www.intelligence-economique.gouv.fr/IMG/pdf/Physionomie_nationale_du_risque_financier.pdf

**Les normes de sécurités :**
http://www.iso.org/iso/fr/home.htm
et notamment les normes suivantes :
ISO 13335 Gestion de la sécurité des TIC
ISO 15408 Evaluation de la sécurité des TIC
ISO 27001 Certification de la qualité des pratiques
ISO 27002 Code de bonne pratique pour la gestion de la sécurité de l'information, etc.

**Blog de Jean-Paul Pinte**
Jean-Paul Pinte vous invite à suivre l'actualité sur son blog :
http://cybercriminalite.wordpress.com/

# Les soutiens de nos partenaires

# Les services de Gendarmerie

*Plusieurs dispositifs cohabitent au sein de la Gendarmerie pour la lutte contre la cybercriminalité : IRCGN, STRJD, SR, N-Tech. Bien qu'ils semblent nombreux, ils ont chacun leur spécialité et travaillent en collaboration.*

## IRCGN (Institut de Recherches Criminelles de la Gendarmerie Nationale)

Implanté à Rosny-Sous-Bois depuis 1987, l'IRCGN est un laboratoire de police scientifique. Ses deux missions : l'expertise scientifique (toxicologie, incendie, biométrie...) et la mise à disposition de spécialistes dans le cadre d'enquête; puis surtout l'anticipation des futures évolutions de la criminalité et la façon de les contrecarrer. Depuis 1992, la structure accueille le département Informatique & électronique divisé en quatre unités : une de recherche et développement, et trois unités d'expertises (traitement de l'information, réseaux & télécommunications, et électronique).

## STRJD (Service Technique de Recherches Judiciaire et de Documentation)

Créée en 1976 et implanté à Rosny-Sous-Bois, le STRJD met en corrélation tout les évènements trouvés au cour de différentes enquêtes afin de les accélérer. Cinq divisions composent le STRJD, dont la DLCC (Division de Lutte Contre la Cybercriminalité) crée en 1994 qui regroupe deux départements principaux : la DSI (Département de Surveillance de l'Internet) et le DRAMI (Département de répression des atteintes aux mineurs sur Internet) dont le CNAIP (Centre National d'Analyse des Images Pédopornographiques) répertorie 24h/24 toutes les images pédopornographiques. Les autres divisions travaillant en relation avec la criminalité numérique coopèrent donc toujours avec la DLCC.

## SR (Section de Recherche)

Les sections de recherche (SR) apportent expertises techniques et scientifiques (recherche de preuves) dans le cadre d'enquêtes. Depuis l'avènement d'Internet le nombre de leurs missions s'est réellement accru et leurs expertises sont demandées surtout en matière de criminalité numérique (analyse de disques durs ...).

## N-Tech

Depuis 2001, des enquêteurs des sections et brigades de recherche sont formés aux nouvelles technologies au CNFPJ (Centre National de Formation de Police Judiciaire), à l'IRCGN et à l'université. Ils apprennent à décortiquer les disques durs, les données, la programmation, la cryptologie etc. Leur rôle est d'assurer l'expertise et l'analyse de la criminalité numérique au niveau régional. Leurs missions se recentrent autour des affaires de pédopornographie à l'échelle régionale (prérogatives initiales), comme à l'échelle nationale, voire dans des affaires internationales. Leurs enquêtes proviennent souvent de commission rogatoires, ou de demandes d'expertise. Néanmoins, les N-Tech effectuent un travail de veille avec des logiciels spécialisés comme l'IRCGN et le STRJD, ce qui leur permet parfois de lancer des enquêtes d'« initiative », après bien sûr avoir retransmis l'information auprès des services de l'IRCGN, du STRJD et de l'OCLCTIC. Une des priorités de Mme la Ministre Michèle Alliot-Marie, est le doublement des effectifs N-Tech d'ici quelques années.

MINISTERE DE L'INTERIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

GENDARMERIE Au service de l'Homme

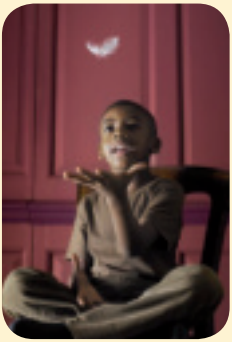
# SPIE Communications Les entreprises et la cybercriminalité

Acteur majeur en matière de services « informatique, réseaux & télécoms » en France, SPIE Communications se positionne au cœur de la convergence voix-données et comme l'une des premières Sociétés de Services en Informatique au travers de son activité d'infogérance autour des Postes de travail et des Serveurs. Le chiffre d'affaires 2007 de SPIE Communications est de 285 M€. SPIE Communications focalise sa croissance sur le « service de proximité », en privilégiant, sur le terrain, réactivité, fiabilité technique et satisfaction maximale de l'utilisateur final. Aujourd'hui, SPIE Communications compte 66 700 clients en France et emploie plus de 2000 personnes réparties sur 6 directions régionales.

SPIE Communications a développé une réelle expertise dans le domaine de la sécurité et exerce aujourd'hui ses compétences dans tous les domaines informatiques : contenu, communication, accès, sécurité des postes de travail, gestion des identités, Network Access Center (NAC), … et propose une offre de service étendue allant du conseil à l'infogérance en passant par l'intégration, l'hébergement et les services managés

Cette expertise se traduit par un programme rigoureux de formation et plus de 50 certifications réparties sur l'ensemble du territoire prévues en 2009.

Afin de répondre aux fortes contraintes juridiques auxquelles sont soumis nos clients, SPIE Communications a développé une spécialité dans les domaines de la gestion de logs et du NAC sur lesquelles nous avons effectué de très belles réalisations et investissons massivement. Notre service de veille permet également d'anticiper les changements technologiques et d'avoir une approche pragmatique sur des sujets comme le DLP ou les problèmes de sécurité liés à la voix sur IP.



Présent sur les principaux évènements autour de la sécurité, SPIE Communications, au travers de sa direction régionale Nord Est, a choisi le salon de la Cybercriminalité pour venir à la rencontre des utilisateurs et intervenir sur différents sujets dont le nomadisme.

Sur le stand, des démonstrations interactives seront organisées autour de :

- La gestion de logs,
- La sécurisation des réseaux Wi-Fi,
- La sécurisation du poste de travail,

La direction régionale Nord Est a en effet décidé de faire de la sécurité des systèmes d'information un de ses axes majeurs de développement en 2009 en créant un pôle sécurité et en consolidant son offre de conseil. Nous réalisons notamment des prestations de prédiagnostic de sécurité, d'aide à l'élaboration de politique de sécurité, d'audits de vulnérabilité, mais également de la conduite du changement, des études d'opportunité, de faisabilité ou d'homogénéisation du système d'information.

SPIE

# Thales

## Cybersécurité : Protection des systèmes d'information et résilience des organisations

En ouvrant leurs systèmes d'information au grand public, fournisseurs et partenaires dans un environnement de nomadisme et de mutualisation des données, les organisations ont franchi un point de rupture entre leurs dispositifs traditionnels de protection et les risques encourus.

Il est urgent d'appliquer toutes les règles déjà définies et de les appliquer sans faille. L'écart entre les pratiques d'une part et les standards et référentiels d'autre part constitue à lui seul un gisement de sécurisation qui est à la fois important et facile d'accès. Les actions d'audit, de sensibilisation et de formation sont, dans ce contexte, de nature à faire baisser rapidement le niveau de risque.

Cependant il serait faux de penser que les actions offensives sont toujours effectuées par des individus à l'extérieur des organisations. Bien au contraire, les études montrent que la majorité des dommages sont déclenchés au sein même des entreprises ou des administrations.

Et tandis que s'accroît l'exposition des réseaux aux menaces d'intrusion, les risques encourus s'étendent à l'ensemble des fonctions qui, de plus en plus, s'y concentrent. Très économique, la téléphonie sur IP mutualise les réseaux entre l'informatique et les télécommunications, exposant ces deux fonctions vitales au déni simultané des services vocaux et des services de données.

Les nouveaux concepts de sécurisation des systèmes d'informations devront donc s'élaborer à deux niveaux, celui de la réduction des risques et celui de la résilience face aux chocs extrêmes.

Il est clair que les nouveaux défis de la sécurité sont des défis de créativité. Ici comme ailleurs l'innovation viendra des rapprochements, entre le civil et le militaire d'une part, entre le public et le privé d'autre part. On ne saurait trop encourager le partage des

approches méthodologiques (EBIOS, Critères communs, …) ainsi que des outils et produits, mais aussi le renforcement mutuel des capacités d'analyse de flux.

A la transversalité institutionnelle doit correspondre une transversalité dans les organisations. La sécurité est aujourd'hui une contrainte dispersée dans de multiples fonctions. Très rares sont les organigrammes qui en individualisent la responsabilité globale. Celle-ci devrait être assumée par un directeur de la sécurité, rattaché à la direction générale comme toute fonction vitale ou stratégique et interlocuteur des pouvoirs publics.

Enfin, le moment est venu d'élargir le concept de résilience. Bien au-delà de la seule capacité des systèmes à fonctionner en cas de panne, il faut l'étendre à l'organisation elle-même pour la rendre capable de « manager la surprise ». Il conviendra donc de rapprocher deux fonctions trop souvent distantes, celle qui s'engage sur la continuité d'activité et celle qui anticipe la gestion des crises.

Reste à positionner sur le marché de la sécurité des systèmes critiques, des prestataires capables de mobiliser en leur sein des équipes pluridisciplinaires de consultants, d'architectes systèmes et d'ingénieurs pour proposer une approche à la fois technique et organisationnelle et fédérer le meilleur des quatre mondes, civil et militaire, public et privé.

Thales a pris l'initiative dans ce domaine en créant ISS, Information System Security qui réunit l'ensemble des compétences du Groupe en matière de sécurité.

Dans cette organisation, Thales concentre toute l'expertise sécurité, à la fois sur le conseil (Connaissance des normes et standards, audits, test de pénétration, ….), les technologies (cryptage, télécommunications sécurisées, signature électronique, …) et les services.

Le Groupe consolide une approche de bout en bout de la sécurité qui couvre l'ensemble d'une chaîne « Secured by Thales » :

- analyse du contexte : identification des menaces, contraintes et règles applicables
- analyse des risques : risques acceptables, niveau de sécurité à atteindre
- conception sécurité : design sécurité et recommandations
- développement ou acquisition des technologies de sécurité
- tests et audits de sécurité interne : test d'intrusion, résistance aux attaques
- évaluation du niveau de sécurité, en regards des normes du secteur : banque, défense...
- audit et certification : vérification des modifications demandées.

Bien qu'il soit souhaitable d'envisager la sécurité de manière globale dès le lancement d'un projet, la sécurisation peut être mise en œuvre sur des projets déjà existants et sur des points précis de la chaîne Secured by Thales.

**Gérard PESCH**
Directeur Security Consulting & Evaluation
THALES ISS

« Microsoft a pris depuis longtemps des engagements forts »

## Notre monde numérique avance à pas de géant :

interconnecté, foisonnant, mobile, coopératif, à l'image d'un internet qui évolue sans cesse. Chaque jour, les technologies ouvrent des horizons nouveaux et le champ des possibles. Dans leur sillage, les interrogations sont nombreuses. Comment préserver la vie privée et garantir la sécurité des données ? Comment s'assurer que des technologies différentes dialoguent simplement dans un univers technologique si divers ? Comment faire d'internet un espace de confiance pour les enfants et les adolescents ?

Sur nombre de ces sujets, nous sommes parmi ceux qui pensent qu'une régulation est nécessaire. Mais parce que notre société numérique évolue à très grande vitesse, il est du devoir des acteurs économiques de prendre leurs responsabilités.

Sur chacun de ces enjeux : protection de la vie privée, sécurité des données, ouverture et interopérabilité, protection de l'enfance en ligne, Microsoft a pris depuis longtemps des engagements forts. Certains ont créé la surprise par leur ampleur et nombre d'entre eux ont été salués par la presse.
D'autres sont encore méconnus. En tout état de cause, nous ne les considérons pas comme un aboutissement mais comme des étapes.

Car dans cet univers en constante évolution, tous les acteurs doivent, sans relâche et sans faux semblants, assumer leurs devoirs. Pour notre part, nous nous y engageons jour après jour avec tous ceux qui sont concernés : citoyens, pouvoirs publics, partenaires, associations professionnelles...

**Pour plus d'informations, consultez nos sites :**
http://www.microsoft.com/France/apropos
et http://www.microsoft.com/france/securite

Microsoft

# Profil Technology

## "Le risque numérique vient aussi de l'intérieur"

Les entreprises sont généralement bien sensibilisées aux risques venant de l'extérieur (virus, malwares etc.) et sont équipées en conséquence. Trop peu intègrent par contre la dimension interne du risque numérique et ses conséquences en termes de productivité, d'investissements superflus voire même légales.

Les risques pour les entreprises et les chefs d'entreprise sont pourtant nombreux et ont des **conséquences financières directes ;**
qu'il s'agisse de perte de productivité, de surcharge de bande passante, du stockage de contenus illégaux sur les ordinateurs de l'entreprise ou d'interventions illégales sur des forums via le réseau de l'entreprise. Ces risques peuvent s'avérer très pénalisants et nécessitent une protection adaptée généralement pas ou peu gérée par les logiciels de sécurité classiques (anti-virus, anti-malware, etc.).

Quatre risques principaux peuvent être ainsi identifiés : la diffusion d'informations confidentielles, la surcharge de la bande passante, la perte de productivité et les contenus ou interventions illégales.

**La diffusion d'informations confidentielles**
est souvent effectuée de bonne foi.
Elle peut notamment porter :

- sur l'envoi des coordonnées directes du dirigeant, provoquant ainsi de nombreux contacts téléphoniques à but commercial ;
- sur la diffusion par erreur de documents comptables (factures, bilans, etc.) ou commerciaux non-définitifs (tarifs, fiches produits, etc.) et pouvant se retrouver entre les mains de partenaires ou concurrents ;
- sur l'achat avec la carte bancaire de l'entreprise sans intention de nuire mais sans validation préalable, un problème devenu récurrent dans certaines entreprises ;
- etc.

**La surcharge de la bande passante** due à la consultation de vidéos en ligne (DailyMotion, YouTube, etc.), les téléchargements abusifs (P2P notamment), les jeux en réseau… impactent directement les ressources informatiques de l'entreprise et participent fortement à l'inflation des besoins d'investissements matériels dans ce domaine.

**La perte de productivité** liée à la consultation de sites extra-professionnels (voyages, bourse, réseaux sociaux, messageries instantanées, sites de recherche d'emploi, etc.) se voit peu en termes d'utilisation de la bande passante, mais un grand nombre d'heures de travail sont ainsi perdues chaque année. Ainsi, on estime que chaque employé peut perdre jusqu'à une journée de travail par semaine en activités extra-professionnelles sur Internet !

**La détention ou la diffusion de contenus illégaux** en passant par le réseau de l'entreprise peut également poser un problème de responsabilité légale au chef d'entreprise.

Afin d'établir un bon niveau de protection et améliorer les ratios coûts/rentabilité des ressources informatiques mises à la disposition de ses employés, le chef d'entreprise peut limiter ces 4 risques en mettant en place des solutions techniques adaptés.
Celles-ci doivent permettre de filtrer les sites Internet accédés par les employés selon leurs besoins professionnels, d'interdire l'envoi de certaines informations et documents par email par certains groupes ou personnes, voire de limiter les contacts emails autorisés, d'interdire certaines applications ou types (vidéos ou exécutables par exemple), de disposer de rapports sur l'utilisation faite des outils informatiques à disposition des employés (attention, la déclaration à la CNIL est obligatoire dans le cas d'un stockage de données nominatives ou pour pouvoir être utilisé comme preuve juridique, l'employé doit également être prévenu de la mise en place d'un tel système) afin de pouvoir les consulter en cas d'activités illégales et de pouvoir adapter la solution aux utilisations particulières au sein de chaque entreprise.

Si des solutions existent, elles sont souvent mal adaptées aux problématiques des PME : produits souvent lourds à administrer ou appliances nécessitant une installation. Une solution logicielle au déploiement simplifié semble être la mieux adaptée à ces problématiques, car elle a l'avantage de la souplesse pour sa mise en œuvre au cœur de réseaux déjà existants, et permet une gestion directe depuis le poste du chef d'entreprise par exemple, sans forcément devoir passer par un administrateur réseau.

www.ProfilTechnology.com

# Clusif

Véritable **observatoire des pratiques et des risques liés à la sécurité de l'information,** le CLUSIF, Club de la sécurité de l'information français, agit pour sensibiliser tous les acteurs économiques et dans l'intérêt général des utilisateurs des systèmes d'information.
Ce Club professionnel est un lieu d'échanges où secteurs public et privé, monde de l'Education (2ème et 3ème cycles universitaires, Grandes Ecoles) et des fédérations professionnelles se rencontrent et mettent en commun leurs réflexions.
Le CLUSIF intervient pour l'intérêt de tous dans des contextes très ouverts incluant la sécurité des réseaux, la lutte antivirus, les plans de continuité d'activité, la sécurité physique des centres informatiques, la malveillance téléphonique, le management des risques, le droit, la défense de l'information, la cybercriminalité...
Le mode de production repose d'une part sur l'organisation de conférences thématiques ouvertes au public et d'autre part, la constitution de Groupes de Travail dont l'objectif est la rédaction d'un document ou d'une prise de position publique.
De nombreux travaux sont issus réalisés, tous **gratuits et disponibles en téléchargement** et certains traduits en anglais : panoramas de la cybercriminalité, études sur les menaces informatiques et les pratiques de sécurité en France, synthèses, ouvrages de référence.

Le CLUSIF est aussi l'auteur de la méthode d'analyse de risques MEHARI™ qui permet de concilier les objectifs stratégiques des directions générales et les nouveaux modes de fonctionnement de l'entreprise avec un management des risques incluant l'analyse des vulnérabilités. C'est un excellent outil de contrôle et de gestion, à court, moyen ou long terme de la sécurité de l'Information de toute structure. La flexibilité de MEHARI™ permet de qualifier le respect de normes telles que ISO 2700x, ou de lois, telle que la Loi de Sécurité Financière. MEHARI™ constitue aussi un outil efficace pour traiter les risques opérationnels liés au traitement de l'information, tels que ceux décrits par la réglementation Bâle II pour les professions bancaires. MEHARI™ est totalement gratuit, à télécharger sur le site web de l'association.

En raison de la diversité de ses membres et de la variété des sujets traités en réunions ou en conférences, le CLUSIF est sollicité pour répondre à des consultations gouvernementales. Il participe ainsi à des travaux à caractère national ou international. L'association est également interviewée par des médias de la presse écrite, de la radio ou de la télévision pour fournir un décryptage des événements lorsque les journalistes veulent comprendre ou remettre en perspective un incident informatique qui défraie la chronique.

L'action d'intérêt général s'est aussi renforcée ces dernières années par la mise en place de portails : cybervictime, mastères SSI, CLUSIR et CLUSI notamment. Le portail cybervictime, réalisé en collaboration officielle avec les services d'Etat met à disposition un point de contact avec les services de Gendarmerie et de Police pour les Internautes ou les entreprises victimes d'une malveillance informatique. Le portail SSI, plus récent, a pour objet d'orienter les étudiants vers des mastères universitaires pour des études spécialisées en sécurité des systèmes d'information. Il sera prochainement complété par une rubrique d'offres et demandes de stages étudiants. Enfin, les portails CLUSIR (huit régions) et CLUSI (cinq pays) informent d'activités en région ou à l'étranger par des associations consœurs : prise de contact, documentations produites et l'annonce d'événements locaux.

**www.clusif.asso.fr**

# CNIL

Afin de comprendre et d'accompagner le développement technologique et pour qu'il respecte au mieux les principes de protection des données, la CNIL entretient de nombreux contacts avec les entreprises du secteur privé qui conçoivent des nouvelles technologies et les conseille. De nombreuses actions ont été menées en 2008 : auditions en séance plénière d'industriels comme Orange, Auchan, Carrefour, Leroy-Merlin, HP et Métrobus ; visites d'entreprises, de centres de recherche ou de « showrooms » comme au CEA-Minatec de Grenoble, aux laboratoires de recherche d'HP à Bristol ou à l'Echangeur à Paris, ont été organisées avec des membres de la Commission. Au quotidien, le lancement de nouvelles offres est l'occasion pour des sociétés comme Microsoft, Google, Hitachi ou des compagnies d'assurance de venir présenter leurs produits à la CNIL. Lors de ces réunions, la CNIL est amenée à recommander des mesures techniques permettant une meilleure protection des données personnelles, dès la conception du système. Ces échanges permettent ainsi à la CNIL d'anticiper au mieux l'avènement des nouvelles technologies et de jouer un rôle essentiel en accompagnant ces entreprises afin que leurs innovations intègrent la protection des données. L'intérêt des entreprises est évident car elles gagnent ainsi la confiance de leurs utilisateurs.

Les dispositifs de contrôle des salariés liés aux nouvelles technologies se multiplient : vidéosurveillance, cybersurveillance, applications biométriques, géolocalisation. Ces applications enregistrent de nombreuses informations à caractère personnel sur les salariés. La loi Informatique et Libertés fixe un cadre à la collecte et au traitement de ces données afin de les protéger, dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée. Le respect, par les entreprises et les administrations, des règles de protection des données est un facteur de transparence et de confiance à l'égard des salariés. C'est aussi un gage de sécurité juridique pour les employeurs qui sont responsables de ces traitements informatiques et de la sécurité des données qu'ils contiennent. Ils peuvent ainsi voir leur responsabilité, notamment pénale, engagée en cas de non-respect des dispositions de la loi. C'est pourquoi la CNIL est chargée de veiller au respect de ces principes et souhaite informer les salariés des droits dont ils disposent, ainsi que les employeurs, en les conseillant sur les mesures à adopter pour se conformer à la loi. Un guide a pour vocation de leur donner les clés pour bien utiliser ces outils et les fichiers mis en œuvre en matière de gestion des ressources humaines. C'est aussi le but du « correspondant informatique et libertés », interlocuteur privilégié de la CNIL dont la désignation permet, au-delà de l'exonération de déclaration, d'intégrer pleinement la problématique de la protection des données personnelles et de se prémunir contre de nombreux risques vis-à-vis de l'application de la loi.

## L'Institut National des Hautes Études de Sécurité - INHES

L'INHES est un établissement public sous tutelle du ministère de l'Intérieur. Il a pris en 2004 la succession de l'IHESI, créé en 1989, en restant fidèle à sa vocation : faire se rencontrer tous ceux qui oeuvrent pour la sécurité et, ensemble, développer une culture commune pour mieux faire face aux menaces et aux risques. Lieu de formation de haut niveau dans un cadre moderne et convivial, lieu de libres débats, l'INHES organise la réflexion au service de l'action, avec la conviction que la sécurité est la première des libertés..
Au cœur de son activité se trouve la session nationale qui forme chaque année une centaine d'auditeurs de l'Institut, hauts responsables du secteur public comme du secteur privé. Ils rejoignent ensuite le réseau d'auditeurs qui assure une veille permanente sur l'évolution des questions de sécurité.
L'INHES offre, par ses travaux et ses publications, une expertise aux pouvoirs publics et notamment au Ministère de l'Intérieur. Il a vocation à couvrir tout le champ de la sécurité : statistiques de la délinquance, enquêtes de victimation, lutte contre la délinquance, aide à la décision des services de la police et de la gendarmerie nationales, sécurité civile et suivi des questions économiques.

Au sein de l'Institut, le Département Sécurité et intelligence économiques et Gestion de crise assure notamment une veille au profit des pouvoirs publics dans le domaine de la Sécurité et de l'Intelligence économiques et participe activement à la stratégie nationale d'intelligence et de sécurité économique pour la partie de cette politique publique mise en œuvre par le ministère de l'Intérieur. C'est à ce titre que le département suit tout particulièrement les questions liées à la cybercriminalité. Il soutient également les actions interministérielles de sensibilisation et de formation, diffuse une lettre électronique mensuelle d'information, coordonne des activités de recherche à travers un groupe de travail spécialisé et produit une expertise dans le domaine de la sécurité économique.

**www.inhes.interieur.gouv.fr**

## SGDN

La sécurité de l'information est l'une des composantes de la démarche d'intelligence économique avec la gestion de l'information et des connaissances et l'influence et la contre-influence. Pour une entreprise comme une administration, cette approche est aujourd'hui essentielle car il faut relever le défi d'un nomadisme constant et d'une gestion d'une multitude de supports informatiques contenant des informations sensibles. A cela, il convient d'ajouter les prédations et les risques encourus à tous les échelons qu'ils soient techniques ou humains.
Ainsi, le haut responsable chargé de l'intelligence économique (HRIE) a-t-il toujours porté une attention particulière pour apporter des solutions au chef d'entreprise face aux risques numériques. Plusieurs travaux ont été, par exemple, réalisés sur les outils de veille, la récupération de données informatiques contenues sur des supports informatiques endommagés ou des sensibilisations sur l'infogérance sauvage ou le vol d'ordinateurs portables. C'est pourquoi, le HRIE salue ce travail réalisé qui participe, certes à la sensibilisation des chefs d'entreprise, mais surtout à leur donner les outils et méthodologies pour réduire leur exposition à ce risque.

**www.intelligence-economique.gouv.fr**

# LEGALEDHEC

LegalEdhec est le Centre de Recherche de l'EDHEC dédié à la performance juridique. L'objectif principal de LegalEdhec est de réfléchir sur les modes de recours au droit par l'entreprise en vue de soutenir ou de créer des avantages concurrentiels. En d'autres termes, cela revient à déterminer la place que le droit devrait occuper dans la stratégie d'entreprise. L'une des idées-clef est que les entreprises doivent raisonner en terme de gestion juridique des risques, tout autant qu'en terme de gestion des risques juridiques. A cet effet, divers travaux sont menés par les membres de LegalEdhec, certains en partenariat avec des institutions extérieures. Ainsi, un ambitieux projet est actuellement développé avec l'Association Française des Juristes d'Entreprise (AFJE), sur le thème de la culture juridique d'entreprise.

LegalEdhec s'applique également à observer la performance juridique dans des domaines particuliers qui sont le droit de la concurrence, le droit de la propriété intellectuelle, la compliance réglementaire, et l'économie numérique. Le choix de ces champs est certes lié aux expertises des membres du Pôle mais, de manière plus objective, ils correspondent également aux domaines de risque les plus fréquemment cités par les entreprises. Notre ambition est de réussir à faire reconnaître le caractère stratégique du recours au droit dans l'entreprise, à élaborer des critères de mesure de la performance juridique, et, le cas échéant, de proposer des évolutions législatives ou réglementaires lorsqu'il apparaît que la performance juridique passe actuellement par la transgression de la loi.

Les travaux de LegalEdhec donnent lieu à de nombreuses publications et participations à des conférences, tant au niveau national qu'international.

Pour plus d'informations :
**http://www.performancejuridique.com**

EDHEC BUSINESS SCHOOL
Lille - Nice

# L'I.R.E.E.N.A.T.

(Institut de Recherche sur l'Evolution de l'Environnement Normatif des Activités Transnationales), e.a. N° 3612 de l'Université de Lille 2, dirigé par le Professeur Jean-Jacques Lavenue, est spécialisé dans l'étude de la dimension publique de la mise en oeuvre de la réforme de l'Etat et des nouvelles technologies (e-administration, sécurité juridique et sécurité informatique, protection libertés). Cette équipe de recherche composée de juristes de droit public et de droit privé, d'informaticiens, et de politologues travaille actuellement dans le cadre de projets ANR à des recherches relative à la prise en compte de la dimension juridique de la mise en oeuvre des technologies de surveillance complexe (video, audio, interconnexion de fichiers), notamment pour la protection de libertés et des données personnelles :

- Projet CanADA (Comportements anormaux: Analyse, Détection, Alerte);
- Projet Scarface (Caractérisation Sémantique de Visages pour la Recherche dans des Archives Video);
- Projet Smartvision ( Système multi senseur de détection d'objets cachés pour une meilleure gesstion du flux passager) de controles par par systèmes mutisenseurs (scanners corporels dans les aeroports) et les problèmes de protection des libertés.

# Osia

**La société OSIA** est une société spécialisée en sécurité des SI, depuis sa création en 1991 à Strasbourg. Elle intervient dans l'analyse et l'audit de la sécurité, pour des expertises technologiques, et la conception de politiques de sécurité et de plans de continuité de divers secteurs stratégiques : télécommunications, finances, aéronautique, énergie, recherche, santé, etc., et enfin en matière d'intelligence économique.

Elle est dirigée depuis 1991 par Daniel Guinier, Dr. ès Sciences, consultant principal, certifié CISSP, ISSMP, ISSAP en sécurité des SI et MBCI en gestion de continuité, membre senior IEEE et ACM, et du New York Academy of Sciences. Il est expert OSEO/ANVAR depuis 1989, et expert judiciaire depuis 1991, avec de nombreuses expertises traitant pour la lutte contre la cybercriminalité. Il est lieutenent-colonel de réserve citoyenne de la Gendarmerie Nationale.
Il a contribué à plusieurs normes internationales en sécurité : IEEE, NIST, et de façon significative à la protection du patrimoine informationnel, la biométrie, la signature et l'identité électroniques, l'inforensique et l'archivage légal. Il a été ingénieur de recherche, au CNRS de 1967 à 1990, et entre temps, professeur à la US Naval Postgraduate School, puis PDG de la société OSIA dès 1991. Il est régulièrement conférencier en Europe et en Amérique du Nord, et enseigne en 3ème cycle aux universités de Compiègne (UTC-IMI) et de Strasbourg (IECS/IAE), et au CESSSI (SCSSI/DCSSI) de 1992 à 1994. Enfin, il est l'auteur de plus de 200 publications et de deux livres : «Sécurité et qualité des SI» (Masson, 1991), «Catastrophe et management» (Masson, 1995), «Le courrier électronique et l'archivage légal» (IBM). Il est aussi coauteur de deux autres livres : «Les SI - Art et pratiques» - Sécurité et cybercriminalité (Eyrolles, 2002) et «Les tableaux de bord pour diriger en contexte incertain» - La sécurité des tableaux de bord (Eyrolles, 2004), et de «l'encyclopédie de l'informatique et des systèmes d'information» - La politique de sécurité (Vuibert, 2006).

**Contact :**
**Mèl guinier@acm.org ;**
**Tél. 03 88 76 12 81.**

# L'Université Catholique de Lille

rassemble, dans une dimension de visibilité, de mutualisation, de transversalité, d'interdisciplinarité et de synergie, 6 Facultés, 20 Grandes Écoles, Écoles et Instituts, 33 équipes de recherche, un groupe hospitalier de 700 lits, un institut de rééducation psychothérapeutique.
Ces établissements partagent avec leurs 20.307 étudiants en 2008-2009 une même philosophie éducative conjuguant excellence et humanisme, performance et solidarité. Ils inscrivent leurs actions au service de l'homme, de la société et du monde pour contribuer aux évolutions économiques et sociales.

Dans cet ensemble universitaire se côtoient aussi des équipes de recherche autour d'un conseil de recherche couvrant aujourd'hui 8 thématiques de recherche :

- la théologie,
- les lettres et sciences humaines,
- la médecine,
- les sciences,
- l'éthique,
- le droit,
- l'économie,
- l'ingénierie pédagogique.

Le Laboratoire de recherche en Ingénierie Pédagogique intègre aussi la dimension « Sciences de l'Information et de la Communication » et des travaux y sont menés autour de la place de l'individu dans la Société de l'Information, de la cyber-citoyenneté, de l'Intelligence économique et des outils de veille compétitifs qu'il convient dés aujourd'hui d'intégrer dans nos enseignements pour former les futurs travailleurs du savoir.

C'est à ce titre que ce laboratoire est aujourd'hui présent sur le terrain par ses écrits, ses enseignements, ses recherches et ses nombreuses conférences et interventions en France et à l'étranger.

Le laboratoire assure également en tant que cellule de veille l'animation de bulletins hebdomadaires d'informations sur ces problématiques à destination de publics professionnels. Le blog
**http://cybercriminalite.wordpress.com/**
animé par Jean-Paul Pinte, Docteur en Information Scientifique et Technique, enseignant-chercheur au sein du laboratoire et expert en veille et intelligence compétitive en est un exemple.

**http://www.univ-catholille.fr/**

# L'Arist

L'ARIST Nord Pas de Calais, service de la Chambre Régionale de Commerce et d'Industrie (CRCI), accompagne les entreprises en matière d'intelligence économique, en leur proposant différents modes d'intervention selon leur besoin :

- Sécurité des systèmes d'information (pré-diagnostic SSI),
- Protection du savoir-faire (pré-diagnostic propriété industrielle et accompagnement à la mise en œuvre des outils de propriété industrielle),
- Suivi des évolutions et sécurisation des projets (prestations de veille)
- Prospective et développement de l'entreprise (méthode Casciopée)
- Recherche de partenaires (dans le cadre du Réseau Entreprise Europe notamment)

L'activité de l'ARIST s'inscrit dans le cadre du réseau des Chambres de Commerce et d'Industrie, certaines actions étant menées avec le soutien de l'Etat, de la Région et de l'Europe.

Contact : aristnpdc@aristnpdc.org
Tel. 03 20 63 68 00

# Le Service de coordination à l'intelligence économique

Le dispositif d'intelligence économique commun au ministère de l'Economie, de l'Industrie et de l'Emploi et au ministère du Budget, des Comptes Publics et de la Fonction Publique est placé sous l'autorité de Cyril Bouyeure, Coordonnateur ministériel à l'intelligence économique (CMIE). Rattaché au Secrétaire général des ministères, le CMIE anime l'action des différentes directions afin de mutualiser les compétences en matière d'intelligence économique.
Le CMIE dirige le Service de coordination à l'intelligence économique (SCIE) qui comprend un échelon central et un réseau de 23 Chargés de mission régionaux à l'intelligence économique (CRIE). Les missions du SCIE procèdent de 3 priorités :

**• Sensibiliser et former les chefs d'entreprises à la démarche d'intelligence économique**

Les actions de sensibilisation (réalisations et diffusions de supports d'information, formations, colloques...) couvrent les volets défensif (sécurité des systèmes d'information, protection de la propriété intellectuelle...) et offensif (démarches d'acquisition de l'information, utilisation d'outils numériques...).

Ces actions ciblent en priorité les PME, moins sensibilisées et disponibles à ces enjeux. Les pôles de compétitivité, sources de développement technologique, sont par ailleurs accompagnés pour mieux connaître leur environnement concurrentiel international et se protéger contre toute intrusion extérieure non sollicitée. Une action est en cours sur la sécurisation de leurs plateformes électroniques d'échanges.

**• Assurer la protection d'actifs stratégiques pour l'économie nationale**

Au titre de la défense de ses intérêts économiques essentiels, l'Etat se doit d'assurer la protection et la défense du patrimoine technologique industriel national. Le réseau des CRIE participe aux actions de défense des entreprises sensibles dont les activités sont considérées comme stratégiques.

De manière générale, le SCIE a une expertise sur les risques de dépendance dans le domaine des technologies de l'information et des nouveaux services numériques.

**• Constituer une capacité de veille stratégique**

Le SCIE mène une veille stratégique destinée à éclairer les menaces et opportunités, pour l'économie française, résultant des évolutions prévisibles de l'environnement concurrentiel.

Les domaines d'investigation sont diversifiés :
évolutions des politiques publiques et des stratégies des grands groupes internationaux, fonctionnement de certains marchés, veille technologique, suivi des pays émergents...

# Caprioli & Associés

Fondé en 1995 par **Eric A. Caprioli,** avocat à la Cour de Paris, spécialiste en droit de la propriété intellectuelle et des TIC, Docteur en droit, le **Cabinet Caprioli & Associés** dispose d'une expertise juridique confirmée ainsi que de connaissances techniques poussées en matière de technologies de l'information et de la communication (TIC).

**Basé à Paris et à Nice,** le Cabinet Caprioli & Associés regroupe une équipe composée d'une dizaine de personnes ayant une formation juridique intégrant le droit des nouvelles technologies. En outre, qu'il s'agisse des responsables du pôle Sécurité et dématérialisation, du Pôle Vie privée et Données personnelles, du Pôle Informatique et Propriété intellectuelle et du pôle Droit public, chacun de ses membres enseigne depuis plusieurs années, et ce, notamment sur les aspects juridiques des TIC. Enfin, exerçant depuis sa création dans la sécurité de l'information et des questions connexes, le Cabinet Caprioli & Associés jouit d'une expérience reconnue dans ces domaines.

Le Cabinet intervient à titre principal dans des domaines d'activités couverts par une équipe d'avocats et de juristes hautement qualifiés, créatifs et spécialisés, soucieux de fournir des prestations de qualité, en consulting et accompagnement de projets liés notamment à la dématérialisation des échanges et au développement des TIC, en conseil juridique (par exemple, contrats, politiques, chartes informatiques, …) et dans le domaine du contentieux et de l'arbitrage.

Les membres du Cabinet ont également développé une activité rédactionnelle florissante, auteurs appréciés d'articles et d'ouvrages techniques publiés et de documents en ligne sur le site du cabinet **(www.caprioli-avocats.com)**. Afin d'honorer les demandes des organismes publics et des entreprises, ils participent à des conférences nationales et internationales, des colloques universitaires et organisent des sessions de formation juridique particulièrement adaptées aux attentes des professionnels.

Caprioli & Associés


## Blandine POIDEVIN

Avocat au Barreau de Lille
3 rue Bayard 59000 LILLE
10 rue Weber 75116 Paris
Tel : 00.333.20.21.97.18
Fax : 00.333.20.63.22.25
Mail : bpoidevin@jurisexpert.net


Tiers-aviseur au CMAP
(arbitrage des «.fr»)

Le Cabinet de Maître Blandine POIDEVIN est inscrit au Registre des Représentants d'Intérêts de la Commission Européenne. Blandine Poidevin est partenaire du cabinet Arden du barreau de Californie, USA et du cabinet Langlais du barreau de Montréal.

A l'issue d'une formation en droit des affaires, elle s'est orientée vers un diplôme de propriété industrielle et de nouvelles technologies dès 1996.

A ce jour, elle a développé un domaine de compétences particulier en matière de droit des technologies. Elle accompagne des entreprises innovantes et des collectivités, au niveau Régional, National et International.

A ce titre, elle participe à des négociations, notamment en matière de contrats informatiques, et à la mise en place d'un cadre juridique respectant les normes les plus pointues en matière de sécurité informatique.

Elle enseigne des matières telles que la négociation des contrats informatiques, le droit du commerce électronique, auprès de l'Université de Droit de LILLE II, l'Ecole des Mines de DOUAI, l'ESC LILLE et l'IAE.

Elle dirige chaque année les travaux universitaires de plusieurs étudiants des masters professionnels 2e année. Elle est fréquemment consultée lors de la rédaction de décrets ou de projets de loi relatifs à son domaine d'activité.

Elle collabore régulièrement avec des organismes de formation internationaux, tels que REED BUSINESS INFORMATION, ainsi qu'avec des revues scientifiques autorisées, telles que EXPERTISES DES SYSTEMES D'INFORMATION.

Jurisexpert.net

s@ntinel

# Une synergie internationale, une ambition collective.

## NOS OBJECTIFS

Dans un contexte de mondialisation et de développement d'Internet, la dépendance des sociétés à l'égard des technologies de l'information et de la communication (TIC) présente des risques potentiels que savent exploiter des délinquants et des criminels avertis et de plus en plus souvent organisés.

Le 22 mars 2007, le Forum international sur la cybercriminalité a permis de me¬surer l'intérêt de près de 600 participants pour les technologies numériques qui transforment notre vie quotidienne en of¬frant un espace de liberté et d'échanges sans précédent. Le 20 mars 2008, la deuxième édition du FIC a accueilli plus de 800 participants.

Devant les attentes des chefs d'entreprises, il a été décidé de poursuivre leur accompagnement par la création d'un pôle professionnel de lutte contre la cybercriminalité: S@NTINEL.

- Un site web et un blog (en cours),
- Des visites d'entreprises,
- Des conférences et ateliers thématiques,
- Un forum international sur la cybercriminalité...

## LES PUBLICS CONCERNÉS

- Dirigeants d'entreprises,
- Pôles de compétitivité,
- Réseau consulaire,
- Directeurs des systèmes d'information,
- Responsables sécurité des systèmes d'information,
- Responsables de collectivité,
- Organisations professionnelles,
- Associations,
- Université, instituts de formation,
- Praticiens de la justice,
- Fonctionnaires des services compétents pour lutter contre la criminalité numérique de la région Nord-Pas-de-Calais, des pays voisins intéressés.

## ACTIONS

- Développer votre image et votre notoriété en vous associant à une action d'exception,
- Partager votre expérience avec les acteurs des TIC européens,
- Valoriser vos savoir-faire et produits lors de rencontres thématiques, ateliers et visites d'entreprises,
- Établir des contacts privilégiés avec les dirigeants ou responsables informatiques des entreprises,
- Offrir à vos cadres et à vos clients une formation et une information régulières,
- Promouvoir l'interopérabilité des équipements et des services sur le plan régional, transfrontalier et européen,
- Sensibiliser, former aux enjeux de la cybercriminalité,
- Accompagner les dirigeants d'entreprises dans les mutations de leurs systèmes d'information,
- Promouvoir des solutions techniques et comportementales,
- Promouvoir et renforcer la mise en réseau, l'échange et la diffusion de bonnes pratiques présentant un intérêt commun,
- Encourager la recherche scientifique et technique,
- Favoriser un échange entre les mondes des entreprises, les organismes publics, les professions de justice, le milieu associatif, le milieu universitaire,
- Faire évoluer les politiques nationales et européennes dans ce domaine

Le cyberpôle professionnel d'excellence
de lutte contre la criminalité numérique
128 ter, Grand Rue
59100 ROUBAIX

s@ntinel

Edition :

Agence AB Com'
Aude MARTY
2bis rue Jules Barni
80000 Amiens
03 22 72 08 80

Création :
Bruno LEPLAT
4 rue Masclef
80 000 Amiens
06 61 33 55 20





Retrouvez ce guide en version numérique
sur www.fic2009.fr