Protection du patrimoine informationnel
2007 - FedISA - CIGREF

Protection du patrimoine informationnel

Eric Caprioli
Paul De Kervasdoué
Jean-François Pépin
Jean-Marc Rietsch

Les Auteurs

Jean-Marc Rietsch

Jean-Marc Rietsch

Pilote de l'ouvrage, JM Rietsch est expert des métiers de la confiance et plus particulièrement de l'archivage électronique. Ingénieur Civil des Mines, JM Rietsch a débuté sa carrière professionnelle par le développement logiciel et l'offre de services pour les PME-PMI. En 1993, il oriente sa carrière vers la sécurité et plus particulièrement la sauvegarde des données informatiques et dépose un brevet sur le sujet. En 2001, JM Rietsch participe au lancement du premier tiers archiveur en France. JM Rietsch est Président de FedISA (Fédération de l'ILM du Stockage et l'Archivage), créée en 2005 afin de pouvoir répondre aux attentes des utilisateurs dans le domaine. Il est également le fondateur de EIFISA (European Institute for ILM storage & Archiving), société spécialisée dans la formation sur le domaine et à l'origine d'un premier mastère sur l'archivage électronique « légal ».

Eric Caprioli

Eric Caprioli

Avocat à la Cour de Paris, Docteur en droit, spécialiste en droit de la propriété intellectuelle et des NTIC, Expert aux Nations Unies sur les questions de droit du commerce électronique depuis plus de 12 ans, Membre du Comité directeur de la certification près le SGDN depuis 2003 (arrêté du 28 janvier 2003, publié au JO), Président de l'association nationale des professionnels de la propriété incorporelle (ANPPI). Auteur de nombreux articles sur la dématérialisation, la signature, la preuve et l'archivage électronique, conférences et ouvrages sur le droit de l'économie numérique, dont celui sur la Loi pour la Confiance dans l'économie numérique (LCEN), éditions LGDJ publié en janvier 2005. Voir le site du cabinet: www.caprioli-avocats.com. Fondateur du cabinet d'avocats Caprioli &Associés, Paris et Nice.

Paul De Kervasdoué

Paul De Kervasdoué

Titulaire d'un master en sciences économiques et d'une formation CPA de HEC, Paul de Kervasdoué a effectué sa carrière comme responsable informatique puis comme DSI dans le domaine de la finance avant de se lancer dans le consulting. Il dispose de 30 ans d'expérience en sécurité des technologies de l'information. Il fut également vice président du Clusif pendant 12 ans et responsable de la commission d'évaluation de la sécurité des systèmes. Il dirige actuellement et depuis 11 ans le cabinet AQUIS (Actions pour la Qualité Informatique et la Sécurité) dont les domaines d'intervention concernent l'audit, la mise en place de plan de continuité d'activité et l'évaluation des risques. Il intervient également comme conférencier dans plusieurs universités et grandes écoles d'ingénieurs.

Jean-François Pépin

Jean-François Pépin

Délégué Général du CIGREF (www.cigref.fr) depuis juillet 2001, Jean-François PEPIN est diplômé du Centre de Perfectionnement aux Affaires (CPA) et Président fondateur du « Cercle Intelligence Economique d'Entreprise » des Anciens HEC. Membre permanent de l'Académie d'Intelligence Economique, il est le co-rédacteur du Manifeste d'Intelligence Economique d'Entreprise publié en 2006. Il est par ailleurs Diplômé de l'Institut des Hautes Etudes de Sécurité Intérieure (IHESI - 10ème session nationale), Auditeur au Centre d'Etudes Diplomatiques et Stratégiques (session 2000) et à l'Institut des Hautes Etudes pour la Science et la Technologie (IHEST - 1ère Promotion - 2007). Jean-François PEPIN est chargé de cours à l'IAE (Institut d'Administration des Entreprises) Université de Paris I (Master Management des Associations).

Sommaire

Editorial

Alain Juillet

Dans le cadre de la globalisation, le développement des technologies de l'information et de la communication est en train de bouleverser nos habitudes, nos techniques et nos méthodes. Des opportunités de marché existent partout pour ceux qui savent chercher et osent prendre des risques calculés tandis que les menaces sont réelles pour les chantres de l'immobilisme et du repli sur leur pré-carré national.

Le chef d'entreprise de demain devra intégrer la flexibilité, la réactivité et la capacité de remise en cause permanente dans son mode de gouvernance pour être en mesure de se battre à armes égales avec des concurrents venus de tous les horizons. Il devra prioritairement développer sa recherche et s'orienter résolument vers l'innovation, tout en développant sa connaissance des marchés et de ses concurrents pour faire la course dans le peloton de tête.

Tout ceci est rendu possible par la maîtrise de l'information stratégique utile permettant d'avoir tous les éléments d'appréciation nécessaire pour prendre à temps la bonne décision en attaque comme en défense. Ce constat montre combien la détention, le stockage et l'utilisation de l'information sont devenus un véritable actif de l'entreprise qu'il convient de valoriser et de protéger face à des prédateurs en tout genre.

Depuis longtemps les opérateurs des pays occidentaux avaient pris l'habitude d'évaluer les entreprises sur des bases strictement financières reposant sur des valorisations du patrimoine matériel et des flux. Depuis quelques années on a découvert qu'il fallait également prendre en compte le patrimoine immatériel pour avoir une juste évaluation de l'entreprise.

Chacun comprend les conséquences financières pour l'entreprise, d'un détournement de brevet, d'un piratage de documents, ou du vol d'un portable avec le fichier d'une négociation. Chacun comprend que la valeur d'une bibliothèque ne s'évalue pas exclusivement au poids du papier ou au nombre de mètres de livres qui y sont stockés.

Il est toujours frappant de constater combien nos concitoyens ont tendance à percevoir le capital immatériel comme la compilation des brevets et des savoir-faire en oubliant que l'information en constitue une valeur essentielle. Le capital informationnel avec ses données stockées, ses renseignements disponibles et ses analyses fournies aux décideurs, est un élément décisionnel indispensable qui doit être mieux valorisé pour être reconnu.

Si l'on admet cette réalité on comprend l'absolue nécessité d'en assurer la protection tant en interne qu'en externe. Le capital informationnel contient les clés pour la mise à niveau, le sursaut de croissance où l'ouverture de marchés pour un concurrent indélicat, ou pour faire fortune en vendant les secrets de l'entreprise dans le cas d'un employé mécontent ou vénal. C'est une richesse de l'entreprise qu'il convient de protéger au même titre qu'une usine ou un procédé de fabrication.

C'est tout le mérite des auteurs de ce livre blanc d'avoir travaillé sur le thème de la sécurité du patrimoine informationnel pour ouvrir les yeux de nos concitoyens sur la valeur de ce capital et la nécessité de sa protection. Souhaitons, dans l'intérêt de tous, que les futurs nombreux lecteurs en deviennent également convaincus.

Alain Juillet
Haut Responsable à l'Intelligence Economique (HRIE)
Paris, Octobre 2007

Préface

Didier Lambert - Jean-Marc Rietsch

Le patrimoine informationnel de l'entreprise a une forte valeur financière au titre de l'actif immatériel de l'entreprise et à ce titre doit être protégé. Ce peut être des données clients (données, voix et images), des logiciels maisons portables et documentés, du savoir faire, etc. Au même titre que le capital humain, il n'entre pas, en général, dans les valeurs d'actifs financiers d'une entreprise. Par contre la valeur comptable de remplacement du capital humain est maintenant chiffrée et provisionnée dans le cadre du risque opérationnel (Accords de Bâle II) pour la banque, la bourse et les sociétés d'assurances. Pourquoi dès lors ne pas prendre en compte de la même façon la valeur financière du patrimoine informationnel de l'entreprise ? D'où l'enjeu à bien définir ce patrimoine, le protéger, le développer et l'enrichir.

Il est ainsi du devoir du chef d'entreprise entre autres par l'action du DSI, de manager ce patrimoine informationnel. Comme évoqué précédemment, il ne s'agit pas seulement de le sécuriser mais aussi de pouvoir le développer harmonieusement et de le cultiver. Le sens en est ici d'en faire usage et de recueillir les fruits du patrimoine informationnel propre à l'entreprise (l'usufruit). Le DSI dispose également dans ses fonctions du droit mais aussi de l'obligation de supprimer certaines données, comment faire alors pour ne pas détruire l'information ?

L'archivage électronique doit entre autres contribuer à protéger ce patrimoine sachant que le thème de l'archivage électronique devient de plus en plus un sujet d'actualité pour bon nombre d'organisations tant publiques que privées. Ceci s'explique certes par une augmentation extrêmement forte du volume de données électroniques gérées au quotidien mais aussi par une évolution des technologies et surtout des processus d'entreprise voire des obligations nées à la suite de différents événements. Pour preuve les plus récentes évolutions en la matière relatives aux réglementations financières qui imposent désormais la conservation d'informations jusque là négligées.

Ainsi que nous avons pu le traiter dans un précédent livre blanc « L'archivage électronique à l'usage du dirigeant», la problématique de l'archivage électronique ne se limite pas à une simple dématérialisation des techniques d'archivage traditionnelles. Il est indispensable de prendre en compte l'ensemble du cycle de vie des données et dès lors, pourquoi ne pas profiter de ces évolutions pour donner une nouvelle valeur à la donnée archivée. Ainsi, même archivée, l'information peut rester facilement accessible et renforcer d'autant le système d'information de l'entreprise et par là même sa compétitivité en permettant de disposer de la bonne information au bon moment.

Au regard de l'évolution des usages, des contraintes associées et des techniques, il existe aujourd'hui une véritable nécessité d'informer l'ensemble des parties prenantes intéressées aux questions de gestion et de conservation sécurisée de l'information électronique.

FedISA, Fédération de l'ILM, du Stockage et de l'Archivage a pour objectif de véritablement répondre aux besoins identifiés et s'est fixée pour principales missions de :

- sensibiliser les responsables concernés aux nouvelles technologies et aux obligations afférentes (obligation d'archivage, de continuité d'activité, de traçabilité...) ;
- informer les utilisateurs sur les nouvelles technologies en effectuant une véritable veille tant technologique que juridique, normative ou encore organisationnelle et ce à un niveau national et international ;

- donner au responsable de tels projets les éléments permettant de pleinement les justifier par rapports aux risques encourus (légaux et financiers) et autres avantages compétitifs comme une meilleure réactivité ;

- participer à la formation à ces nouveaux métiers de l'entreprise comme le « records manager ».

Pourquoi un partenariat CIGREF - FedISA ?

Compte tenu de sa mission « promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise », le CIGREF, association regroupant 127 Grandes Entreprises françaises, est partenaire de cette publication.

Le présent ouvrage s'adresse essentiellement aux dirigeants et responsables dans les entreprises afin de les aider à y voir plus clair et leur fournir les notions importantes à avoir pour aborder ce genre de problématique.

Ce document est ainsi rédigés pour le chef d'entreprise et adressées au DSI, pour action en majorité à destination du Responsable Sécurité des Systèmes d'Information.

Au-delà de la sensibilisation il s'agit également de souligner le rôle essentiel que peut et doit tenir le DSI compte tenu de sa position et de ses responsabilités vis-à-vis de l'information en général et de l'archivage en particulier en tant que constituants essentiels du capital immatériel de l'entreprise. Comme évoqué précédemment la pluralité des métiers concernés est indispensable et qui, mieux que le DSI, peut permettre d'établir un dialogue entre les différentes fonctions concernées au sein de l'entreprise sans oublier les autres parties prenantes intéressées.

Didier Lambert
Président du CIGREF

Jean-Marc Rietsch
Président de FedISA

Introduction

le principal objectif de l'ouvrage est de montrer la cohérence et surtout la continuité des préoccupations que doit avoir tout chef d'entreprise en matière de sécurité, d'archivage électronique, d'intelligence économique et de patrimoine informationnel.

Contrairement à ce qui peut apparaître au premier abord, ces différentes notions sont intimement liées et plutôt que de les traiter séparément nous voulons montrer comment, au contraire, il est préférable de les aborder comme un ensemble indissociable.

Tout comme pour le premier livre blanc nous avons opté pour une organisation sous forme de fiches qui se découpent en quatre parties.

Au fur et à mesure des progrès incessants de notre société naissent parallèlement de nouveaux concepts qui contribuent largement à semer le trouble voir la complexité là où il n'y a pas lieu d'être. Plus nous avançons et plus ce phénomène s'intensifie de telle sorte que le chef d'entreprise se voit confronté à un ensemble d'informations apparemment différentes mais qui au fond traitent du même sujet et répondent à une même préoccupation.

Au travers du cas particulier de l'archivage électronique, de la sécurité informatique et de l'intelligence économique nous allons nous efforcer de démontrer dans cet ouvrage que finalement le but poursuivi est quasiment le même, à savoir protéger et enrichir le patrimoine informationnel de l'entreprise.

Dans la mesure où cet ouvrage constitue une des richesses de l'entreprise au sens de son actif immatériel, la sécurité consiste à protéger ce dernier de façon générale tandis que l'archivage constitue un des éléments sécuritaires particulier en matière de pérennité et de la non altération des données. L'intelligence économique peut être vue sous deux angles, l'un également de défense de ce patrimoine et un autre plutôt actif d'enrichissement de ce dernier.

La première partie concerne la protection proprement dite du patrimoine traitant de l'ensemble des aspects sécuritaires traditionnels abordés également dans le sens de l'archivage électronique. La deuxième partie aborde les aspects plus juridiques de cette protection et la responsabilité du chef d'entreprise face à son patrimoine. La troisième partie traite la façon de se protéger en matière d'assurance. Enfin la quatrième et dernière partie est plutôt destinée à traiter la façon d'enrichir et de développer le patrimoine de l'entreprise au travers de l'intelligence économique.

Première partie : Sécurité technique

Au niveau des éléments sécuritaires à prendre en considération nous nous appuyons sur la pratique en matière d'audit de sécurité DICP (disponibilité, intégrité, confidentialité, preuve / traçabilité). Nous ajouterons à ces éléments l'identification - l'authentification et la pérennité, base de l'archivage électronique.

Deuxième partie : Juridique

Il s'agit ici d'aborder la questions des outils juridiques liés à la protection du patrimoine informationnel, à savoir : politique de sécurité des systèmes d'information, politique d'archivage, charte d'utilisation, contrats de travail, contrats avec les prestataires de services, les obligations de confidentialité et les conditions destinées à l'usage du chiffrement.

Nous proposons également un développement spécifique destiné à aborder de manière générale la protection de l'information par le droit des propriétés intellectuelles (brevets, marques, dessins, bases de données, logiciels, droits d'auteur). De façon particulière est également traitée la notion de dépôt chez un tiers comme le notariat, l'INPI (Institut Nationale pour le Protection Intellectuelle), l'APP (Agence pour la Protection des Programmes) ou encore Logitas (équivalent à l'APP).

Sont également traitées les obligations et la responsabilité de l'entreprise et plus particulièrement du chef d'entreprise sous l'angle contractuel lié à une perte d'exploitation informatique suite à un sinistre, un accident ou de la malveillance mais aussi sous l'angle délictuel suite par exemple au non respect des recommandations et obligations de la loi informatique et liberté.

Troisième partie : Assurance

Malgré toutes les protections dont le chef d'entreprise peut s'entourer il est néanmoins nécessaire pour lui de s'assurer contre l'impondérable. D'où cette troisième partie destinée à lui permettre de connaître quels sont les moyens mis à sa disposition pour faire face aux conséquences liées directement à la perte d'une partie de ce patrimoine.

Quatrième partie : Enrichissement

L'Intelligence Economique d'Entreprise

Protéger le patrimoine informationnel de l'entreprise c'est aussi, assurer la maîtrise de l'information stratégique dans un contexte d'entreprise étendue et dans un environnement géopolitique incertain : une affaire de culture managériale pour tout dirigeant !

Les fiches

Chacune des fiches qui suivent a été conçue de façon à pouvoir être lue indépendamment des autres. Ce choix a été dicté par un souci d'efficacité destiné à permettre de trouver rapidement les premiers éléments de réponse aux problèmes que l'on se pose. A contrario, ceci provoque immanquablement certaines répétitions ou renvois le cas échéant à d'autres fiches complémentaires.

Chacune des fiches est organisée de la même manière en trois parties. La première, le contexte, est plus particulièrement destinée à bien positionner le problème posé, la deuxième partie précise les enjeux concernés tandis que la troisième énonce les recommandations qui nous semblent fondamentales.

Nous avons préféré mettre directement à l'intérieur du texte les références utiles afin de faire gagner du temps au lecteur qui désirerait approfondir tel ou tel aspect.

Pour la première série de fiches sur la sécurité technique nous avons également ajouté une partie spécifique dédiée aux méthodes d'audit à appliquer tandis que pour les fiches juridiques cette organisation n'a pas pu être respectée compte tenu des informations abordées.

Remarques liminaires sur les fiches techniques :

Méthodes d'audit recommandées

Produire un audit de sécurité informatique et télécoms vise à quantifier les facteurs de sécurité. Cela consiste à leur donner des notes de 1 à 5 avec une position neutre (ou non applicative). Il semble en effet souhaitable d'élargir l'éventail des notes plutôt que de se limiter à une simple réponse : oui ou non.

Selon l'usage visé, les méthodes d'audit sont distinctes et sans vouloir passer ici en revue l'ensemble des méthodes disons que : EBIOS et FEROS sont particulièrement adaptées pour bâtir une cible de sécurité pour un produit sensible du type cible de sécurité d'un FIREWALL ou du masque de la carte bancaire par exemple.

MEHARI est une méthode intéressante (mise au point par le CLUSIF il y a une dizaine d'années) mais inductive. Comme un mécano, cela dépend de la construction du questionnaire qui en est faite. Autrement dit deux questionnaires d'audit MEHARI pour une même cible sont normalement différents. Cela rend pratiquement impossible la constitution d'un référentiel des réponses d'audit pour un groupe d'entreprises ou a fortiori pour un secteur économique déterminé : les banques, le secteur industriel, les laboratoires pharmaceutiques, les hôpitaux etc.

MARION est une méthode d'audit de sécurité qui a plus de 20 ans maintenant. Malheureusement sa mise à jour est ancienne (10 ans). Mais elle présente toujours un grand intérêt didactique car les questions sont regroupées dans 27 facteurs qui traitent l'ensemble des questions de sécurité informatique et télécoms sur un axe déterminé. Le caractère invariant des questions permet de bâtir aisément un référentiel des notes d'audit par nature d'activité professionnelle. A l'intérieur d'une grande entreprise, cela est aussi utile et permet de disposer d'une grille d'audit homogène pour l'ensemble des départements et ou des filiales.

ISO 27001 (anciennement BS7799) est une méthode d'audit d'origine anglaise. Il s'agit de la plus pratiquée au monde aujourd'hui C'est essentiellement la raison qui nous amène à la recommander.

Critères premiers de sécurité

Le terme sécurité est un ensemble fourre-tout qui se décompose en 24 critères différents. Les critères premiers sont au nombre de quatre :

- Disponibilité ;
- Intégrité des (flux et traitements) ;
- Confidentialité ;
- Traçabilité (preuve et contrôle).

Dans les fiches techniques ci-après, nous découpons les méthodes d'audit ISO 27001 et MARION pour chacun de ces quatre critères premiers et seulement pour ceux-ci. De ce fait la partie audit ne sera pas abordée pour les notions de pérennité et d'identification -authentification qui ne constituent pas les critères premiers.

Nous avons trouvé utile de faire apparaître cette notion d'audit dans la mesure où elle nous paraît indispensable afin de pouvoir établir un état des lieux suffisamment précis de la sécurité informatique, comme nous le verrons au cours du développement des différentes fiches.

Le détail des fiches est le suivant :

Protection du patrimoine informationnel

Phase	N° fiche	Thèmes
		Définition du patrimoine informationnel
Sécurité technique	1	Disponibilité/Accessibilité
	2	Intégrité
	3	Identification/Authentification
	4	Confidentialité
	5	Traçabilité/Preuve
	6	Pérennité/Archivage électronique
Juridique	7	Outils juridiques liés à la protection du patrimoine informationnel
	8	Protection de l'information par le droit de la propriété intellectuelle
	9	Obligations et responsabilités de l'entreprise et du chef d'entreprise
Assurance	10	Assurance perte d'exploitation informationnelle - Comment évaluer et garantir le risque
Enrichissement		IE et Capital immatériel de l'entreprise
		IE et Gestion des risques informationnels

Définition du patrimoine informationnel

Le patrimoine informationnel peut être considéré comme l'ensemble des données et des connaissances, protégées ou non, valorisables ou historiques d'une personne physique ou morale. Il s'agit donc d'assurer la protection et la valorisation de l'information. A ce titre, l'information doit être sécurisée depuis sa création ou sa collecte, tant pendant la phase de transmission que pendant la phase de conservation.

Les informations doivent ainsi être conservées de façon intègre dans le temps. Par ailleurs la confiance en une information découle également de son imputabilité. Il faut en effet pouvoir être sûr que c'est bien la personne authentifiée qui est à l'origine de l'envoi des données et de ce fait assurer une traçabilité des dites données. L'information doit également être disponible, avec une garantie d'accès sans interruption ni dégradation et aux seules personnes autorisées. Enfin la valeur d'une information ne dépend pas uniquement de sa conservation intègre dans le temps mais également de son exactitude, de sa pertinence et de sa validité.

Pour remplir l'ensemble des fonctions précédemment évoquées, le patrimoine informationnel doit ainsi être sécurisé au sein du système d'information. Sans sécurité, il pourrait évidemment être soumis au pillage en règle effectué par des concurrents, des prestataires ou d'autres hackers.

Nous retrouvons bien ici l'ensemble des aspects de la sécurité technique tel que nous allons la traiter avec dans l'ordre la disponibilité, l'intégrité, l'identification /authentification, la confidentialité, la traçabilité et la pérennité.

Contexte

La disponibilité est le premier critère de sécurité du patrimoine informationnel. En effet, à quoi peut bien servir un ensemble de données stratégiques s'il n'est plus accessible, suite à un arrêt soudain du système d'information ? Cependant il est clair que toutes les données n'ont pas le même degré d'importance. Ainsi une donnée médicale (même archivée) concernant un patient en train d'être opéré nécessite une disponibilité immédiate alors qu'une information comptable pourra souffrir quelques heures d'attente avant d'être récupérée.

Remarque : De façon plus générale, il est très important de pouvoir classifier les données qui constituent la base du patrimoine informationnel. En effet les solutions techniques mise en place ont chacune un coût différent suivant leur degré de sophistication. Afin de pouvoir effectuer un choix optimum du point de vue économique, il est ainsi fondamental de pouvoir disposer de plusieurs solutions. Chacune de ces dernières sera ensuite associée aux données classées par ordre d'importance suivant le critère concerné, à savoir : disponibilité, confidentialité ou encore valeur. Ce raisonnement rejoint ici l'idée fondamentale de l'ILM (Information Lifecycle Management) qui est de différencier les règles de stockage selon la valeur de l'information et d'ajuster au mieux les coûts de stockage aux exigences de sécurité, de conservation et de disponibilité des données.

Accessibilité

Au-delà de la disponibilité, la notion d'accessibilité est bien évidemment un élément crucial de tout système d'information puisque déterminante pour retrouver les données sachant qu'il ne s'agit pas d'un élément sécuritaire au sens strict du terme. Cette notion revêt en fait deux composantes, l'une relevant essentiellement de l'organisation des données, l'autre des performances techniques. S'ajoute à cela la notion des droits d'accès que nous aborderons dans la fiche 3 traitant de l'identification et de l'authentification.

L'organisation des données du patrimoine informationnel constitue un élément fondamental de la qualité de ce dernier. Il convient donc d'utiliser une structure cohérente et efficace, permettant de retrouver facilement et rapidement l'information, notamment au travers d'un plan de classement. Par ailleurs, la constitution d'un index selon les règles de l'art s'avère indispensable. Le recours à des moteurs de recherche est également possible, mais il faudra néanmoins faire attention au phénomène de « bruit » (beaucoup de réponses), rendant l'information inexploitable.

En ce qui concerne les performances d'accès, elles sont directement liées aux techniques utilisées tant en matière de support qu'en matière de réseau. Du point de vue des supports il est évident que les temps d'accès ne seront pas les mêmes suivant la technologie utilisée (disques magnétiques, bandes, etc.). En matière de réseau au niveau interne, les choix pourront être opérés entre des architectures de type NAS, SAN ou équivalentes, tandis qu'au niveau externe l'accessibilité sera directement liée d'une part à la bande passante du réseau et, d'autre part, au nombre de connexions simultanées que le système d'information sera capable de traiter.

Une analyse du risque financier permet de quantifier les pertes directes et indirectes dues à l'indisponibilité du système d'information.

En matière d'archivage électronique la disponibilité intervient essentiellement comme un complément à la notion d'accessibilité, destiné à définir les espaces temps pendant lesquels il est acceptable que le système d'archivage ne soit plus accessible. En effet en fonction d'un certain nombre d'éléments comme simplement la maintenance ou encore les pannes et les dysfonctionnements de tout ordre, il peut s'avérer que le système d'archivage ne soit plus accessible pendant un temps donné.

Ainsi la disponibilité se définit comme **la capacité d'un système d'information à pouvoir être utilisé à tout moment en fonction des performances prévues**.

Cela ne va pas de soi et l'arrêt du système pour une durée indéterminée constitue probablement la plus grande crainte des Directeurs de Systèmes d'Information. La disponibilité est un des premiers facteurs qualifiant la sécurité et aussi la qualité du système d'information. Il convient alors de garantir la disponibilité pour obtenir la pérennité dans le temps du système d'information (voir Fiche 6 : Pérennité) c'est-à-dire la continuité des traitements et des flux d'information : voix, données images.

En général l'unité de compte est le million d'euros pour un arrêt d'une journée et moins de 100 postes de travail. La solution pour garantir la disponibilité est de nature technique informatique et télécoms et revient à **bâtir un plan de continuité**. Sous l'angle financier il est également possible de s'assurer et de mobiliser des capitaux en frais supplémentaires et reconstitution des médias sinistrés (voir Fiche 10 : Assurance Perte d'Exploitation Informationnelle).

La disponibilité se qualifie aussi par la **durée de retour à la normale** du système d'information, après arrêt de celui-ci, on distingue ainsi :

- Haute disponibilité : de quelques minutes d'arrêt à 12 heures
- Moyenne disponibilité : de 12 heures à 48 heures
- Basse disponibilité au delà de 48 heures.

La haute disponibilité impacte des métiers nombreux et variés : la continuité de soins médicaux et hospitaliers, le contrôle aérien, les salles de marchés boursières, certains processus industriels etc. Autrement dit, l'absence de continuité d'un système d'information peut entraîner la mort ou des pertes financières de plusieurs dizaines de millions d'euros (salle des marchés par exemple). La haute disponibilité est synonyme de site de replis immédiat en cas de sinistre important (incendie, dégât des eaux) pour héberger des équipes de salariés de l'entreprise ainsi qu'un nouveau système d'information (informatique et télécoms) chargé avec les sauvegardes (copies de secours) pour redémarrer très rapidement la production de l'entreprise sinistrée.

Enjeux

Bâtir le plan de continuité pour la cible étudiée, tel est l'enjeu principal et technique d'une bonne disponibilité. Les sinistres n'arrivent pas qu'aux autres et il faut donc prévoir une solution technique de secours voire d'hébergement, à compléter par une assurance destinée à couvrir les conséquences financières du sinistre dont les montants sont issus de l'analyse de risque menée préalablement.

L'enjeu est également financier dans la mesure où en plus des exemples donnés précédemment certaines réglementations imposent de pouvoir fournir des informations dans un laps de temps donné sous peine de sanctions importantes. Sur ce dernier point nous pouvons citer la règle 17a-4 publiée par la SEC (Security Exchange Commission) qui impose une production des données en moins de 48h.

Il existe en fait deux types de plan de continuité en cas de sinistre partiel ou total :

- Continuité de Service :
  La continuité de service implique l'hébergement de la seule équipe informatique chez un tiers pour redémarrer provisoirement le système d'information chez ce dernier avec le matériel et le logiciel ad hoc.
- Continuité d'activité :
  La continuité d'activité prend en compte la continuité de service informatique et télécoms et implique aussi l'hébergement des utilisateurs pour continuer leur activité. Il s'agit par exemple d'une salle de marché bis lorsque la salle de marché de l'entreprise est sinistrée. Dans ce cas, il s'agit le plus souvent de « haute disponibilité » dans la mesure où une salle de marché bis doit être disponible dans les 4 heures suivant le sinistre.

En fait dans les deux cas, le plan de continuité de service ou d'activité consiste en un ensemble de procédures, de planning et d'annuaires (du personnel et des fournisseurs) pour le redémarrage de l'activité (sur site ou hors site), après sinistre du centre de traitement de l'information ou de l'immeuble hébergeant celui-ci.

Si bâtir un plan de continuité de service représente l'enjeu technique du maintien de la disponibilité informatique, cela doit se faire sur des bases solides avec :

- de bonnes sauvegardes (copies de recours),
- un réseau télécoms bis opérationnel,
- un système informatique de substitution compatible (testé en grandeur réelle au préalable) avec le système sinistré.

Audit technique

Un état des lieux s'impose en matière de disponibilité informatique et télécoms avant de bâtir un quelconque plan de continuité afin de pouvoir tenir compte et corriger les éventuelles faiblesses détectées. Cet état des lieux revient à mettre en œuvre un audit de sécurité informatique et télécoms. A titre indicatif, le questionnaire d'audit MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) du CLUSIF (Club de la Sécurité des Systèmes d'Information Français) classe de manière claire et indépendante les cinq premiers facteurs de disponibilité d'un système d'information, à savoir :

- Les systèmes et procédures de continuité ;
- La sauvegarde ;
- La sécurité des télécoms ;
- L'environnement de base ;
- La sécurité incendie.

Ces cinq premiers critères représentent à eux seuls plus de la moitié du poids des 27 facteurs de la méthode MARION en matière de disponibilité. En l'absence de procédures de continuité, les deux premiers facteurs de base de la disponibilité sont la sauvegarde et les moyens télécoms.

La méthode d'audit d'origine anglaise BS7799 devenue ISO 27001 permet aussi d'établir un diagnostic précis de la disponibilité du système d'information. Cela est cependant plus délicat car les facteurs y sont moins bien cloisonnés que dans la méthode MARION. Il existe en effet un seul facteur « Business Continuity Management » avec un seul thème associé « Aspects of Business Continuity Management ».

L'audit de la disponibilité du SI correspond à un simple instrument de mesures quantifiées et ne représente pas une fin en soi mais un préalable indispensable. Par exemple si la sécurité des sauvegardes obtient la note 1 sur une échelle allant de 1 à 4, il est fondamental de revoir le mode et la périodicité des sauvegardes avant toute chose.

En effet la construction d'un plan de continuité opérationnel destiné à garantir dans le temps la disponibilité du SI s'appuie forcément sur les sauvegardes qui se doivent d'être efficientes.

Recommandations

Effectuer un audit de la disponibilité informatique et télécoms	Utiliser de préférence les méthodes ISO 27001 (ex BS7799) ou MARION afin de bien connaître avant toute chose les faiblesses à corriger au préalable.
Classifier l'information	Effectuer une classification en terme de disponibilité, des informations gérées et transportées par les réseaux informatiques et télécoms de l'entreprise.
Utiliser un progiciel pour bâtir un plan de continuité	Par exemple le progiciel CONTINUITY PLAN doit permettre la mise en place d'un plan de continuité opérationnel et exhaustif.
Choix d'un site d'hébergement interne ou externe	Le matériel mis à disposition de l'entreprise sinistrée peut être mutualisé entre plusieurs entreprises utilisatrices ou non. Néanmoins louer un matériel commun auprès d'une entreprise d'hébergement informatique et télécoms peut coûter jusqu'à dix fois moins cher qu'une solution individuelle de dotation de matériel informatique et télécoms propre à l'entreprise. En effet dans la mesure où, heureusement un sinistre n'arrive pas tous les jours, la prise en compte des probabilités de sinistre permet au loueur de proposer des tarifs attractifs à ses clients du fait même de la mutualisation effective des moyens mis à disposition.
Effectuer des tests réguliers	Le plan de continuité demande à être testé deux fois par an en grandeur réelle.

Contexte

La disponibilité de l'accès aux données du patrimoine informationnel constitue un point clé de sa sécurité (voir Fiche 1 : Disponibilité). Ne pas recueillir d'information est en effet un problème d'indisponibilité, tandis qu'obtenir des informations fausses ou mutantes est un souci d'intégrité. Ce dernier point est également très important et à traiter avec d'autant plus d'attention que la durée de conservation des données sera longue et donc les risques plus nombreux.

L'intégrité est ainsi définie comme **la propriété qui assure qu'une information n'est modifiée que par les utilisateurs habilités dans les conditions d'accès normalement prévues.** On recherche donc par l'intégrité, l'absence de modification volontaire ou involontaire des flux et des traitements.

L'article 4.f du Règlement CE n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information définit l'intégrité des données comme : « la confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas été modifiées ».

Si l'intégrité représente un critère de sécurité de base, il en est néanmoins le plus diffus et donc le plus difficile à mettre en œuvre sur la totalité de la cible du traitement de l'information.

L'intégrité se subdivise normalement en deux sous-ensembles distincts pour s'approcher davantage de la mécanique du traitement de l'information :

- L'intégrité des flux de données,
- L'intégrité des traitements.

En général, les atteintes à l'intégrité sont d'origine malveillantes. Les cas d'accidents ou d'erreurs sont beaucoup plus rares. Selon le CLUSIF (Club de la Sécurité des Systèmes d'Information Français), sur une période de plus de 10 ans, la malveillance s'accroît de près de 15 % par an, principalement au détriment de l'intégrité des données et des traitements. Le monde de l'Internet est en effet un champ d'expérimentation mondial pour l'atteinte à l'intégrité des données, des messages et des traitements.

Nous attirons l'attention sur le fait qu'en matière d'archivage électronique, l'intégrité en constitue la véritable clé de voûte. Ainsi, suivant les dispositions de l'article 1316-1 du Code civil, l'écrit doit être « conservé dans des conditions de nature à en garantir l'intégrité ». L'auteur, signataire de l'acte, doit être sûr que le document qu'il a signé (établissement), transmis et conservé est le même (contenu identique) que celui reçu et conservé, le cas échéant, par le ou les destinataire(s).

Cependant il existe plusieurs interprétations possibles de l'intégrité suivant que l'on se place du côté purement technique ou plutôt du côté organisationnel et juridique. Par principe l'intégrité technique d'un document électronique est mise en cause dès l'instant où un seul des bits constituant le document est modifié. A l'inverse l'intégrité au sens juridique d'un document consiste à conserver le sens de l'information qu'il contient sans s'attacher nécessairement à la forme. Ainsi le fait de modifier un accent dans un texte ne va pas en changer fondamentalement le sens alors que cela suffira à lui faire perdre son intégrité technique.

Afin d'apporter une solution à cette difficulté d'interprétation, le Forum des droits sur l'internet et la Mission Économie Numérique ont recommandé dans leur rapport 2006 que la notion d'intégrité du document telle que prévue par l'article 1316-1 du Code civil soit assurée par le respect cumulé des trois critères suivants :

- Lisibilité du document,
- Stabilité du contenu informationnel,
- Traçabilité des opérations sur le document (voir Fiche 5 : Traçabilité / Preuve).

Enjeux

Les enjeux de l'intégrité des flux et des traitements sont fondamentaux, spécialement à l'heure d'Internet dans la mesure où il est indispensable de pouvoir faire « confiance » aux données constituant l'élément essentiel du patrimoine informationnel. En effet la perte d'intégrité peut présenter des dangers vitaux comme par exemple des mutations de données du groupe sanguin d'un dossier médical partagé (stocké dans un centre d'hébergement des dossiers médicaux) ou bien d'un identifiant patient, etc. Les cas pratiques donnant lieu ou non à des recours juridiques sont très nombreux et inquiétants, du fait de leur croissance exponentielle depuis plus de quinze ans.

Par ailleurs l'enjeu est également juridique dans la mesure où l'entreprise se doit de garantir l'intégrité de ses traitements et des flux d'informations qu'elle émet, au risque d'être condamnée comme indiqué ci-après.

Aspects juridiques

Le législateur par l'article 323-2 du code pénal cherche à punir les auteurs de virus : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données (STAD) est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende ».

La loi de juin 2004 relative à la confiance dans l'économie numérique : article 323-3-1 du code pénal stipule que « le fait sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

Pour la retransmission de virus, la responsabilité de l'entreprise pourrait être retenue lorsque le virus qui s 'est propagé dans l'espace TCP/IP (Internet Protocol) est apparu depuis plusieurs mois et que l'entreprise n'a pas mis en place des systèmes de sécurité suffisamment efficaces. En effet cela entre dans le champ de l'article 1383 du code Civil où « chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence ».

La responsabilité délictuelle de l'employeur est aussi engagée par le fait de ses salariés (article 1384 du CC) « dans l'exercice de ses fonctions (du salarié) ».

Audit technique

Il est indispensable de faire un audit de l'intégrité des flux et des traitements pour garantir la pérennité du patrimoine informationnel. Nous présentons ici deux méthodes d'audit sécurité et pour chacune d'entre elles nous précisons les facteurs clés relatifs à l'intégrité des flux et des traitements.

MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux)
Développée par le CLUSIF cette méthode permet d'auditer **les atteintes potentielles à l'intégrité** en prenant en compte les facteurs suivants de sécurité par ordre de poids décroissant :

- Contrôles programmés poids 15/100
- La gestion des projets et des développements poids 8/100
- Les procédures de recette poids 8/100
- Le suivi de l'exploitation poids 8/100
- La sécurité des télécommunications poids 8/100
- La sécurité logique de base poids 8/100
- La sauvegarde poids 7/100
- Les contrôles permanents poids 7/100
- La réglementation et l'audit poids 6/100

Avec seulement neuf facteurs sur 27, nous réunissons 75% de la pondération des facteurs d'intégrité.

BS7799 (ISO 27001)
Aujourd'hui ce type de questionnaire d'audit est le plus utilisé au monde. Les neufs premiers facteurs caractéristiques de l'intégrité sont :

- Security in development and support process ;
- Media handling and security ;
- Information Security Infrastructure;
- Security of system files;
- Security requirements of system;
- Equipment security ;
- Operational procedures and responsibilities ;
- Network management ;
- Review of security policy and technical compliance.

Avec ces facteurs nous dépassons les deux tiers des critères d'intégrité à auditer.

Recommandations

Effectuer un audit de l'intégrité des flux et des traitements	Utiliser de préférence les méthodes ISO 27001 (ex BS7799) ou MARION afin de bien connaître avant toute chose les faiblesses à corriger au préalable
Architecture réseau, lutter contre les codes malicieux	**Agir de façon préventive :** - Prévoir des firewall ; - Mettre en place une zone démilitarisée (DMZ) pour contrôler l'entrée et la sortie des messages TCP/IP ; - Disposer de bons antivirus, anti spams, anti chevaux de Troie aux titres de la prévention et du contrôle des flux de données et des traitements ; - Supprimer les cookies afin d'éviter une traçabilité facile de vos accès ; - Tester les progiciels du commerce, notamment obtenus gratuitement par téléchargement, sous l'angle de leur intégrité pour détecter et détruire d'éventuels sous-programmes pirates. **Agir de façon curative :** - Auditer régulièrement le système d'information pour supprimer les programmes (SPAM), chevaux de Troie, et autres types de codes malicieux.
Transfert d'informations sensibles	- Utiliser un VPN (Virtual Private Network) et/ou le chiffrement des données sensibles par les algorithmes autorisés : RSA, triple DES, AES, etc ; - Sceller/signer électroniquement les messages ; - Veiller à l'identification et à l'authentification (voir Fiche 3) des personnes ayant accès à votre site informatique.
Contrôles d'intégrité des données	- Mettre en place des dispositifs permettant des contrôles d'intégrité efficaces essentiellement basés sur l'utilisation des empreintes ; - Effectuer des contrôles réguliers sur les données de façon ponctuelle, par sondage ou sur la totalité des données en fonction de l'importance de l'information gérée.
Contrôler les journaux d'audit	La surveillance des journaux d'audit permet d'analyser les éventuelles attaques internes et externes à l'encontre de l'entreprise et de prendre les mesures correctives en conséquence.

Contexte

L'identification des personnes en Europe n'est pas encore chose acquise lorsque l'on sait qu'il existe des millions de personnes (pourtant vivantes) qui n'ont pas de nom. Authentifier une personne procède d'une démarche encore plus élaborée consistant à certifier le lien entre la personne et son identification. Au niveau du patrimoine informationnel l'importance est évidente de pouvoir le protéger en identifiant aussi parfaitement que possible les personnes y ayant accès afin entre autres de respecter la confidentialité des données (voir Fiche 4).

Identifier quelqu'un consiste à **établir l'identité de la personne** c'est-à-dire son caractère permanent et fondamental tandis qu'authentifier revient à **certifier l'exactitude de son identité**.

L'article 4.e du Règlement CE n° 460/2004 du Parlement européen et du conseil du 10 mars 2004 définit l'authentification comme « *la confirmation de l'identité prétendue d'entités ou d'utilisateurs* ».

La dualité de ces deux notions d'identification et d'authentification est chose importante en matière de contrôle d'accès afin d'authentifier la personne après l'avoir identifié. Cela touche le système d'information mais aussi le contrôle d'accès physique à tel ou tel bâtiment.

Au sujet du terme authentification

En réalité, le terme authentification ne s'applique qu'aux objets et l'on parle régulièrement, par exemple, d'authentifier une œuvre d'art. Ainsi, l'usage de ce terme en informatique est souvent employé à tort pour signifier « identification ». L'origine de cette erreur provient d'un anglicisme lié au terme anglais authentication, faux ami qui veut dire à la fois « identification » et « authentification ». Mais en français, seul le terme « identification » convient pour déterminer si un objet ou une entité est bien untel ; il s'agit d'une certaine façon d'un véritable contrôle d'identité. À l'inverse, « l'authentification » sert à déterminer si un objet, et non plus une personne, a les caractéristiques prétendues.

Le principe est en général d'identifier la personne grâce à un système d'identifiant (login) assorti d'un mot de passe. Malheureusement rien n'indique de façon certaine qu'il s'agit bien de la bonne personne. En effet même si l'identifiant et le mot de passe sont corrects, il se peut très bien que l'utilisateur qui se connecte les ait dérobés à leur propriétaire. Afin de pallier cet inconvénient majeur en terme de sécurité, on aura en général recours à ce que l'on a coutume d'appeler un système « d'authentification forte » consistant à vérifier avec quasi certitude que la personne qui s'identifie est bien celle qu'elle prétend être.

Nous reprenons ci-après les sept systèmes d'identification/authentification les plus utilisés, à savoir :

1. Identifiant (login) et mot de passe (password) : dispositif le plus courant mais très peu sûr.

2. Identifiant et OTP (One-Time Password) : L'utilisateur dispose d'un token ou « calculateur » qui lui fournit un mot de passe (à usage unique et à durée limitée)

au moment où il se connecte. Pour pouvoir utiliser son calculateur, il doit tout d'abord y introduire un mot de passe.

3. Le certificat électronique sur carte à puce ou clé USB : L'utilisateur dispose d'un certificat électronique stocké sur son support et activé grâce à un code PIN. Cette solution nécessite l'existence d'une infrastructure PKI afin de pouvoir délivrer et suivre la vie des certificats.

4. La clé « Confidentiel Défense » : Il s'agit en fait d'une déclinaison particulière du cas précédent. En général le support est multi-fonctions et permet ainsi le stockage de certificat X509, de données, de ressource cryptographique (pour le chiffrement à la volée du disque dur et des flux applicatifs). Afin de contrer les risques des « key loggers » (enregistrement des touches frappées à l'insu de l'utilisateur), le code PIN doit être composé directement sur la clé sans passer par le clavier (exemple du dispositif utilisé par la Gendarmerie Nationale où la souris fait office de lecteur de carte et dispose d'un clavier numérique pour frapper le code PIN).

5. La carte à puce avec identifiant et mot de passe : Ce système correspond à une version allégée de la troisième solution dans la mesure où elle ne nécessite pas d'infrastructure PKI.

L'authentification de l'utilisateur est faite directement à partir de l'annuaire d'entreprise (par exemple en s'appuyant sur le protocole LDAP (Lightweight Directory Access Protocol).

6. Les solutions biométriques qui utilisent des lecteurs biométriques (iris de l'œil, index, configuration de la face, contour de la main, etc.) pour contrôler les accès. Cependant le critère choisi est plus ou moins facile à mettre en œuvre et présente une force variable. De fait la configuration de l'index avec ses points de contrôle reste encore aujourd'hui le mécanisme biométrique le plus abouti. La police scientifique de la fin du XIXème siècle avait fait le bon choix avant que des lecteurs électroniques du doigt ne soient mis au point, cent ans plus tard ! Trois possibilités sont offertes afin de conserver les données à comparer au moment de la lecture biométrique, à savoir : au niveau du poste de travail, au niveau d'une carte cryptographique ou au niveau d'un serveur (se pose alors le problème légal du stockage de données biométriques centralisées en un seul endroit).

7. Le RFID (Radio Frequency Identification) actif : Cette technologie permet d'identifier l'utilisateur sans contact physique, à quelques mètres de distance. Le badge de l'utilisateur possède une alimentation propre qui lui permet de dialoguer avec une antenne connectée au poste de travail. Ce dernier détecte alors l'arrivé ou le départ d'un utilisateur sans aucune autre action particulière de sa part si ce n'est d'indiquer son mot de passe, au moins une fois.

En résumé, l'authentification d'une personne est basée sur l'un au moins des trois critères suivants :

- Ce que sait la personne, par exemple un mot de passe ;
- Ce que possède la personne, un token ou un certificat électronique ;
- Ce qu'est la personne, aspect biométrique.

Enjeux

Afin de protéger le patrimoine informationnel sous l'angle de l'identification et de l'authentification, il est donc nécessaire de réaliser un bon contrôle d'accès tant aux informations qu'aux programmes de traitement. L'enjeu consiste à faire en sorte que les informations ne soient accessibles qu'aux personnes connues d'une part (notion de confidentialité) et autorisées d'autre part (notion d'habilitation avec sa consonance légale).

Pour des données particulièrement sensibles il est parfois nécessaire de limiter l'accès à l'aide d'indices de sécurité et de niveaux d'habilitations. Ces habilitations priment alors sur tout droit d'accès « standard ». Le principe consiste à attribuer un ou plusieurs « indices de sécurité » aux documents concernés tandis que les utilisateurs se voient attribuer un ou plusieurs niveaux d'habilitations qui les empêchent d'accéder aux documents dotés d'indices plus élevés.

Pour réaliser un bon contrôle d'accès il faut ainsi mettre en œuvre un double processus destiné à vérifier tout d'abord l'existant et ensuite à anticiper et préparer toute modification du système d'information.

Contrôle d'accès sur le système d'information existant :

- Réaliser un état des lieux en la matière en auditant les profils (individuels ou de groupe) et le mot de passe correspondant ou la caractéristique biométrique utilisée. Il s'agit ici d'analyser la portée et les limites du système actuel en matière de sécurité physique et ou logique ;

- Bâtir et gérer un système de contrôle d'accès aux données, à choisir parmi ceux évoqués précédemment ;

- Filtrer l'accès aux données existantes en définissant par exemple des profils dont l'accès est protégé par des mots de passe ou des caractéristiques biométriques.

Contrôle d'accès sur le système d'information nouveau ou réaménagé :

- Mettre en place un mot de passe unique pour faciliter la tâche des utilisateurs en matière d'accès au système d'information, du type SSO (Single Sign On) ;

- Définir le périmètre et la cible du nouveau projet de contrôle d'accès ;

- Analyser puis mettre en place et tester le triptyque : identification - autorisation d'accès - authentification ;

- Formaliser le processus d'accès ;

- Associer l'ensemble des acteurs concernés à la démarche ;

- Contrôler le système d'accès sur la base de son support réel (protocole LDAP ou autre), des flux d'informations émis et reçus, des outils d'accès, des moyens d'audit et de reporting associés mis à la disposition de l'officier de sécurité.

Recommandations

Contrôle d'accès	Bien définir les accès et les contrôles à instaurer. Définir au besoin des indices de sécurité pour les informations sensibles et des niveaux d'habilitation pour les utilisateurs correspondants.
Classifier l'information	Effectuer une classification en terme de confidentialité et sensibilité, des informations gérées et transportées par les réseaux informatiques et télécoms de l'entreprise.
Considérer l'identification/authentification comme un projet informatique	Avant de rechercher les solutions techniques et les produits de sécurité sur le marché, il convient d'analyser l'identification et l'authentification des personnes et des objets comme un projet informatique à part entière et de le traiter comme tel en suivant les processus énoncés précédemment. Entre autres il faudra : - prendre en compte l'existant, - savoir gérer l'évolution de la solution retenue dans le temps et dans le mode de contrôle.
Bien analyser les solutions techniques existantes afin de choisir les mieux adaptées	Les solutions techniques d'identification et d'authentification sont techniquement au point y compris les plus performantes de type carte à microprocesseur ou clés USB. Signalons également l'existence de cartes vocales et de cartes à piste magnétique. Attention au fait que pour chaque type est associée une grande variété de lecteurs.
Contrôler les journaux d'audit	La surveillance des journaux d'audit permet d'analyser les éventuelles attaques internes et externes à l'encontre de l'entreprise et de prendre les mesures correctives en conséquence.

Contexte

Au niveau du patrimoine informationnel, la confidentialité est une caractéristique très importante abordée également au niveau du contrôle d'accès (voir fiche 3 : Identification/Authentification). En fait la confidentialité revêt à la fois la notion de secret et de diffusion restreinte à un petit nombre de personnes.

La confidentialité représente **une propriété qui assure que** dans les conditions normalement prévues, **seuls les utilisateurs autorisés (ou habilités) ont accès aux informations concernées**.

La principale limite de la confidentialité tient au fait qu'une personne ne peut être tenue pour responsable d'aucune divulgation si les éléments révélés étaient déjà dans le domaine public ou si elle en avait déjà connaissance ou pouvait les obtenir de tiers par des moyens légitimes.

Dans le cadre du patrimoine informationnel, les informations confidentielles sont évidemment importantes et en général assez peu nombreuses : confidentialité médicale (personne atteinte du VIH etc.), confidentialité de votre code de carte bancaire, mot de passe personnel pour le contrôle d'accès physique et (ou) logique dans l'entreprise, secrets liés à la tactique militaire, etc.

Comme vu précédemment la confidentialité intervient au niveau du contrôle d'accès. Néanmoins dans certains cas il peut être judicieux d'anticiper la situation où des personnes non autorisées parviendraient néanmoins à accéder au système d'information. Dans ce dernier cas la confidentialité des données peut cependant être préservée grâce à la mise en oeuvre d'un système de chiffrement. La caractéristique principale d'un tel système est de rendre les données illisibles par toute personne ne possédant pas la clé pour les déchiffrer. Cependant la connaissance et l'accès à cette clé peuvent poser beaucoup de difficultés, surtout au bout de nombreuses années.

Suivant la situation, la confidentialité des informations doit être plus ou moins bien maîtrisée. Ainsi dans le cas de l'outsourcing ou de l'info gérance par exemple, on devra porter une attention toute particulière à la confidentialité. De même selon la sensibilité des données traitées tant à l'intérieur qu'à l'extérieur de l'entreprise il y aura lieu d'être particulièrement vigilant quant au respect de la confidentialité desdites données. En fait il existe trois principaux moyens pour assurer la confidentialité :

- La mise en place d'un système de contrôle d'accès ;
- Le chiffrement des données ;
- L'externalisation des données. De part les engagements et les responsabilités prises par l'hébergeur, une solution externe doit permettre d'éviter tout problème de confidentialité en interne dans l'entreprise.

Rappelons à ce sujet que près des 2/3 des délits informatiques ont des origines internes. Pour un maximum de sécurité on pourra avoir recours à une externalisation de données chiffrées.

Enjeux

Comme nous allons le voir, les enjeux sont essentiellement de deux ordres, légal et commercial avec les conséquences financières correspondantes.

Informations à caractère personnel : L'un des premiers enjeux d'atteinte à la confidentialité touche à l'accès aux bases de données regroupant en particulier des informations à caractère personnel. Dans ce contexte, l'article 34 de la Loi Informatique, Fichiers et Libertés modifiée par la loi du 6 août 2004 (loi n°2004-801) dispose que « le responsable du traitement est tenu de prendre toutes préoccupations utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

A défaut d'avoir pris « toutes préoccupations utiles », l'employeur s'expose aux peines prévues à l'article 226-22 du code pénal qui punit de cinq ans d'emprisonnement et de 300.000 euros d'amende le fait « par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ».

Même si ce délit est non intentionnel, l'employeur pourrait être tenu pour responsable (même à son insu) de l'imprudence ou de la négligence de ses salariés, ayant permis la divulgation d'une donnée à caractère personnel. D'où l'importance d'auditer les facteurs de sécurité pouvant générer les atteintes à la confidentialité des informations. Cela pose aussi la question de la destruction des informations à caractère personnel et plus généralement du cycle de vie de celles ci. Le respect de la confidentialité passe effectivement par la non conservation, au-delà d'un certain temps (en général la durée de prescription applicables), de données à caractère personnel. Il s'agit en fait du respect du « droit à l'oubli » tel que développé par la CNIL, consacré par la loi du 6 janvier 1978 modifiée en août 2004. (voir fiche 9 : Obligations et responsabilités de l'entreprise et du chef d'entreprise).

Autres informations :

Le patrimoine informationnel touche évidemment beaucoup plus de données que seulement celles ayant un caractère personnel, nous pouvons encore citer : base de données clients, base de données des processus métier de l'entreprise, annuaire fournisseurs, base de données des archives sensibles, contentieux, situation de trésorerie, aspect fiscal, audit comptable, etc.

La confidentialité des données constitue également un enjeu commercial. En effet, dans le cadre de marchés importants, la connaissance des conditions offertes par la concurrence peut permettre de gagner un marché ou au contraire de le perdre.

Audit technique

Tout comme pour l'intégrité, il est indispensable de faire un audit de la confidentialité pour garantir la pérennité du patrimoine informationnel. Nous présentons ici deux méthodes d'audit sécurité et pour chacune d'entre elles nous précisons les facteurs clés relatifs à la confidentialité.

MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux)
Développée par le CLUSIF cette méthode permet d'auditer les atteintes potentielles à la confidentialité en prenant en compte les facteurs suivants de sécurité par ordre de poids décroissant :

- Contrôles programmés poids 15/100
- La sécurité logique de base poids 14/100
- La sécurité des télécommunications poids 13/100
- Les contrôles d'accès physiques poids 11/100
- La réglementation et l'audit poids 7/100

L'audit de ces cinq facteurs (sur 27) représente 60% du poids total. Autrement dit, moins de 20% des facteurs représente à lui seul 60% des poids. Il convient donc, pour repérer le niveau de confidentialité du patrimoine informationnel, de prendre en compte en priorité ces cinq facteurs.

BS7799 (ISO 27001)
Aujourd'hui ce type de questionnaire d'audit est le plus utilisé au monde. Les cinq premiers facteurs d'audit caractéristiques de la confidentialité sont :

- Business requirement for access control ;
- Outsourcing ;
- Secure area ;
- Mobile computing & teleworking ;
- User access management

Ces cinq facteurs représentent aussi à eux seuls au moins 60% des poids de la confidentialité dans le cadre de l'audit sécurité BS 7799. Il y a naturellement une forte convergence entre les méthodes MARION et BS7799 (ISO 27001) pour analyser le degré de confidentialité du patrimoine informationnel de l'entreprise. Mais cette tâche est indispensable surtout à l'heure d'Internet et du protocole TCP/IP qui rend possible l'attaque à partir de l'extérieur, d'informations confidentielles à l'intérieur de l'entreprise.

La pénétration des attaquants dépend des mesures techniques et organisationnelles prises par l'entreprise pour contrer ces attaques malveillantes.

Recommandations

Effectuer un audit de confidentialité	Utiliser de préférence les méthodes ISO 27001 (ex BS7799) ou MARION afin de bien connaître avant toute chose les faiblesses à corriger au préalable.
Classifier l'information	Effectuer une classification en terme de confidentialité, des informations gérées et transportées par les réseaux informatiques et télécoms de l'entreprise.
Contrôle d'accès	L'on reprend ici la notion d'identification et l'authentification des personnes et des biens. Il convient également de protéger les codes d'accès à telle ou telle application sensible.
Recours au chiffrement	Pour les données particulièrement sensibles il peut être utile d'avoir recours au chiffrement qui constitue une garantie importante pour la confidentialité des informations. Le chiffrement peut également être largement employé pour sécuriser la confidentialité des flux.
Externaliser	Le fait d'avoir recours à un hébergeur tiers peut être gage de confidentialité de certaines données dans la mesure où elles ne se trouvent plus à l'intérieur de l'entreprise.
Contrôler les journaux d'audit	La surveillance des journaux d'audit permet d'analyser les éventuelles attaques internes et externes à l'encontre de l'entreprise et de prendre les mesures correctives en conséquence.

Contexte

La traçabilité est un des moyens de garantir l'intégrité des données (voir fiche 2 : Intégrité) et à ce titre revêt un intérêt tout particulier dans la sécurisation du patrimoine informationnel. La preuve, telle que nous l'abordons ici, constitue également un élément fort dans la mesure où l'on doit pouvoir faire « confiance » aux données gérées, caractéristique également abordée au niveau de l'intégrité.

La trace se définit simplement comme une empreinte ou une suite d'empreinte sur le sol marquant le passage d'un homme, d'un animal ou d'un véhicule (définition du Petit Larousse). La traçabilité est une procédure visant à suivre automatiquement un objet (garder la trace des évènements vécus par cet objet) depuis sa naissance jusqu'à sa conservation finale ou sa destruction. Ainsi le petit Poucet en mettant des cailloux blancs sur son chemin pour retrouver sa route en sens inverse dans la forêt, faisait déjà une action de traçabilité en gardant la trace du chemin parcouru.

Le simple fait de constituer un journal séquentiel et donc de tracer les différentes opérations effectuées par exemple sur un système d'archivage électronique offre une véritable garantie. Il deviendra en effet extrêmement difficile voire impossible pour un tiers de mettre en doute le système en insinuant par exemple qu'il a été possible de modifier les journaux d'événements ainsi générés. Sur ce point la traçabilité vient donc en parfait complément de l'intégrité comme vu au sujet des recommandations du Forum des Droits sur Internet au sujet de l'intégrité du contenu de l'information.

La traçabilité revêt ainsi deux aspects fondamentaux que sont le contrôle (réalité des actions effectuées sur un objet) et la preuve (la trace des actions opérées).

Au cours de l'épidémie de la vache folle, il se posait un problème de traçabilité sur l'origine de la bête et la continuité des étapes liées à la découpe de l'animal jusqu'à ce que la pièce de bœuf arrive sur l'étal du boucher. A chaque instant il faut pouvoir prouver l'origine et contrôler les phases de découpe de l'animal, pour qu'il n'y ait pas d'effet de substitution, par exemple.

La traçabilité, comme critère premier de la sécurité s'applique de manière plus large à l'ensemble des échanges de données (voix, données images).

Aspects juridiques *Délits liés à l'absence de traçabilité*

L'usurpation d'identité *est un délit grave qui doit être combattu par la traçabilité du système d'information. Cela devient un délit pénal dès l'instant ou « le fait de prendre le nom d'un tiers (a été réalisé) dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales »(article 434-23 du Code Pénal). A l'heure actuelle, il est impossible d'affirmer que « prendre » une adresse IP, un nom de domaine ou une adresse email soit assimilable au « nom d'une personne » au sens de l'article 434-23 du code pénal. Le droit pénal étant d'interprétation stricte, les juges refuseraient probablement une telle assimilation avec des attributs de la personne prise dans sa dimension numérique.*

Si le nom patronymique d'un individu est reproduit sans son autorisation dans un nom de domaine, (cybersquatting), l'usurpation d'identité pourrait être éventuellement sanctionnée civilement (1382 du code civil).

La détention d'images pédophiles *sur les serveurs de l'entreprise est sanctionnée avec ou sans usurpation d'identité au titre de l'article 227-23 du Code Pénal « le fait de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique ». Il en va de même du « fait d'offrir, de rendre disponible, ou de diffuser une telle image ou représentation par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter ». Les peines sont portées à sept ans de prison et 100.000 euros d'amende en cas d'utilisation d'un réseau de communications électroniques à destination d'un public non déterminé.*

Enjeux

Par rapport à ce qui précède, les enjeux pour l'entreprise sont particulièrement importants tant du point de vue juridique que financier ou encore commercial (image). Notamment vis-à-vis de l'accès à Internet il est indispensable de mette en place un robuste système de traçabilité. De même il faut absolument réaliser un audit de traçabilité régulier afin de pouvoir détecter entre autres la présence d'images illicites sur les serveurs de l'entreprise (y compris le poste du salarié concerné).

La traçabilité participe également à la garantie d'intégrité et par la même fera que tel document pourra être retenu comme élément de preuve par un juge alors qu'en l'absence d'une telle traçabilité le même document n'aurait pas pour autant été retenu du fait par exemple de soupçons importants concernant son intégrité.

Audit technique

BS7799 (ISO 27001)

Aujourd'hui ce type de questionnaire d'audit est le plus utilisé au monde. Les cinq premiers facteurs d'audit caractéristiques de la traçabilité sont :

- System audit considerations ;
- Review of security policy and technical compliance ;
- Accountability for assets ;
- Protections against malicious software ;
- Monitoring system access and use.

Ces cinq facteurs représentent à eux seuls au moins 70% des poids de la traçabilité dans le cadre de l'audit sécurité BS 7799 (ISO 27001). La traçabilité pour la cible d'un système d'information est plus délicate à mesurer que celle de la traçabilité d'un produit. Mais aujourd'hui il est pratiquement impossible de mesure la traçabilité d'un produit sensible (exemple les poches de sang) sans avoir recours à l'usage d'un système d'information.

Recommandations

Effectuer un audit de traçabilité	Utiliser de préférence la méthode ISO 27001 (ex BS7799) afin de bien connaître avant toute chose les faiblesses à corriger au préalable.
Classifier l'information	Effectuer une classification en terme de sensibilité, des informations gérées et transportées par les réseaux informatiques et télécoms de l'entreprise.
Le contrôle a priori	Etablir un journal d'audit sécurisé à ne pas diffuser de manière ouverte.
Le contrôle a posteriori	Auditer les menaces subies et les caractéristiques de l'attaquant potentiel en appliquant par exemple la classification PISE (Grand Public - Initié - Spécialiste - Expert)
La preuve	- Utiliser une Tierce Partie de Confiance (« Notaire électronique ») pour certifier un transfert d'information à l'extérieur de l'entreprise ; - Mettre en œuvre les mesures d'enregistrements vocaux et de télésurveillance nécessaires et permises par l'activité de l'entreprise et son environnement ; - Le cas échéant avoir recours au scellement / signature des informations (voir Fiche 6 : Pérennité et Archivage Electronique).

Contexte

La pérennité du patrimoine informationnel consiste outre sa conservation dans le temps, à assurer la continuité des traitements et des flux d'information quels qu'ils soient (voix, données images). Ce dernier point rejoint ainsi la notion de disponibilité (voir fiche 1 : Disponibilité / Accessibilité). Le terme de « patrimoine » prend également ici tout son sens en mettant en avant sa notion historique.

Une des caractéristiques de la pérennité consiste certes à être capable d'accéder à l'information dans le temps mais surtout de façon intelligible c'est-à-dire permettant de l'interpréter. Compte tenu de l'évolution particulièrement rapide des technologies, la conservation sur le long terme représente un véritable défi dont la réponse est autant technologique qu'organisationnelle. Ceci nécessite d'une part un codage des données indépendant des systèmes : soit par des formats de codage très simples, ouverts et de ce fait relativement pérennes ; soit par des formats normalisés adaptés à la conservation, comme le PDF/A ; soit par une structuration des données de type XML qui permet de s'affranchir d'un format propriétaire tout en facilitant la navigation au sein du document et son exploitation. D'autre part s'ajoute à cela la nécessité d'effectuer des migrations périodiques vers de nouveaux supports

La conservation dans le temps ne touche pas que les supports, les contenus risquent également de perdre de leur exploitabilité s'ils ne sont pas entretenus car plus le temps passe et plus l'information peut devenir difficile d'accès. Par ailleurs la conservation de la signature numérique pose un véritable problème dans la mesure où elle interdit toute migration de format de codage (au risque de perdre son intégrité) pourtant indispensable afin d'assurer la lisibilité sur le long terme. Cependant ceci est vrai si l'on veut conserver la possibilité de vérifier la signature dans le temps. En revanche, il est tout à fait possible de vérifier la signature une fois pour toute avant l'archivage des documents et de conserver la trace de ces contrôles en ayant par exemple recours à un tiers du type autorité de gestion de preuve qui par ailleurs permettra également de régler le problème de la faiblesse de tout procédé cryptographique qui ne peut résister indéfiniment aux avancées et évolutions techniques qui font qu'un jour ou l'autre il sera percé.

L'archivage électronique se doit par définition de garantir la pérennité mais plus encore, dans la mesure où il correspond à l'organisation raisonnée d'une conservation sécurisée de l'information créée aujourd'hui afin de pouvoir la réutiliser demain ou après-demain. De plus en plus ce besoin d'archivage est ressenti comme une nécessité pour les entreprises et devient une obligation. L'archivage répond en fait à trois besoins distincts :

1. l'entreprise se doit de prouver ce qu'elle a fait ou ce qu'elle n'a pas fait et doit également pouvoir produire, en cas de contentieux, les pièces nécessaires à la défense de ses droits et de ses intérêts ;
2. l'on doit pouvoir réutiliser des données dans la conduite des affaires comme des études déjà réalisées et réutilisables dans le cadre d'un nouveau projet, au lieu de recréer l'information, opération qui peut coûter cher et faire perdre un temps précieux ;
3. l'intérêt pour l'entreprise de préserver sa mémoire, tant pour constituer une culture d'entreprise, que pour communiquer envers ses clients, ses partenaires et ses salariés.

Enjeux

Pour le patrimoine informationnel, la notion historique est évidemment fondamentale et l'enjeu peut se résumer aux conséquences pour l'entreprise de ne pouvoir retrouver des informations alors qu'elle a besoin de les communiquer ou de les utiliser. Il en va de même pour l'archivage électronique pour lequel nous avons néanmoins détaillé cinq enjeux qui s'appliquent également parfaitement au patrimoine informationnel :

1. juridique : le principal risque est de ne pas pouvoir produire les données requises par un audit ou un juge dans la forme requise ; non seulement les données doivent avoir été archivées mais elles doivent présenter des caractéristiques d'authenticité, d'intégrité et de non répudiation ;
2. logistique : les données ont été bien archivées techniquement mais il est pratiquement impossible d'y accéder car elles n'ont pas été caractérisées pour pouvoir effectuer des recherches et les moteurs de recherche ne produisent que du « bruit » inexploitable ; ou encore, les données existent mais ne sont pas intelligibles (on a perdu le moyen de les décoder et de les interpréter) ;
3. sécuritaire : des données confidentielles (données stratégiques, personnelles) risquent d'être divulguées parce qu'elles ne sont pas ou insuffisamment protégées, ou encore parce qu'elles auraient du être détruites ;
4. technique : l'enjeu technique est double : dans l'espace avec les problèmes d'interopérabilité entre systèmes, et dans le temps avec le défi de pérennité des données sur le long terme, face à l'obsolescence récurrente des formats, supports et outils de restitution ;
5. financier : l'enjeu financier est double également : coût d'une amende ou d'une condamnation judiciaire et dans une moindre mesure, mais à ne pas négliger tout de même, temps perdu à la recherche d'information ou investissement perdu dans des outils non maintenus dans le temps.

Recommandations

Classifier l'information	Effectuer une classification en terme de durée de conservation des informations gérées par l'entreprise et constituant le patrimoine informationnel, mais également en terme de sensibilité (confidentialité - valeur) et d'accessibilité.
Choix du format	Utiliser un codage des données indépendant des systèmes : - formats très simples et ouverts ; - formats normalisés adaptés à la conservation ; - structuration des données de type XML.
Evaluation des volumes	La maîtrise des volumes est utile afin de : - définir les priorités de gestion (les types de données et de documents les plus volumineux seront prioritaires) ; - estimer les besoins en stockage (critère à combiner à la durée de conservation) et donc une partie des coûts.
Choix du support	Prévoir d'utiliser plusieurs types de support à adapter en fonction des durées de conservation mais aussi d'accessibilité et de sensibilité de l'information.
Prévoir les migrations	Plutôt que de chercher le support idéal qui n'existe pas encore, prévoir dès l'origine les migrations indispensables permettant de garantir la conservation des données dans le temps.
Vérification des scellements / signatures électroniques	Avoir recours à un tiers du type autorité de gestion de preuve. Dans le cas contraire garder l'ensemble des éléments nécessaires à la vérification dans le temps et surtout prévoir a minima d'horodater régulièrement les documents concernés afin de contourner l'obsolescence des procédés cryptographiques.

Contexte

Le patrimoine informationnel constitue une réalité économique, susceptible d'une valorisation à plus ou moins long terme pour les grandes entreprises comme pour les PME innovantes (à titre d'exemple, les droits attachés au brevet, les bases de données, les secrets de fabrique, les droits sur un logiciel, etc., font partie de ce patrimoine immatériel susceptible d'être valorisé ; voir notamment concernant l'innovation le dossier du Journal Spécial des Sociétés de juillet 2007 « Le Management de l'innovation », sous la direction d'Eric Caprioli, p.24 et s). Le Droit doit donc s'employer à en définir les contours puis à en assurer efficacement la protection.

Contours juridiques de la notion de patrimoine informationnel

Le droit n'a pas encore appréhendé le concept de patrimoine informationnel dans toute sa nouveauté et sa plénitude. Il sera donc étudié à partir des définitions juridiques préexistantes et établies tant par le législateur que par la pratique.

La notion de patrimoine

Le patrimoine est une notion juridique classique. Il se définit juridiquement comme « *l'ensemble des biens et des obligations d'une même personne (c'est-à-dire de ses droits et charges appréciables en argent), de l'actif et du passif envisagés comme formant une universalité de droit, un tout comprenant non seulement ses biens présents mais aussi ses biens à venir* » (Gérard Cornu, Vocabulaire juridique, P.U.F., V° Patrimoine). Il s'agit de l'ensemble des rapports de droits qui sont appréciables en valeur monétaire, dans lesquels une personne est engagée soit positivement soit négativement. Les titulaires d'un patrimoine peuvent être des personnes physiques ou des personnes morales (sociétés notamment). Les biens composants ce patrimoine peuvent être matériels ou immatériels, corporels ou incorporels (par exemple, des créances, un fonds de commerce, des droits de propriétés intellectuelles). La richesse s'affranchit désormais de toute matérialité et la notion de patrimoine évolue donc en fonction de l'orientation prise par la Société.

L'information

En s'affranchissant de toute matérialité, le patrimoine intègre un bien qui jusqu'à présent n'était susceptible d'appropriation qu'avec difficulté : l'information. Elle se définit, selon l'arrêté du 3 octobre 1984 du Ministre de l'éducation nationale et du Ministre chargé des P.T.T., portant enrichissement du vocabulaire de télécommunications, comme « *un élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement* » (Arrêté du 3 octobre 1984 du Ministre de l'éducation nationale et du Ministre délégué auprès du Ministre du redéploiement industriel et du commerce extérieur, chargé des PTT, portant enrichissement du vocabulaire de télécommunications, J.O. du 10 novembre 1984).

Le patrimoine informationnel

En fonction des définitions mentionnées ci-dessus, le patrimoine informationnel pourrait être considéré comme **l'ensemble des données, protégées ou non, valorisables ou historiques d'une personne physique ou morale**. Il s'agit donc d'assurer la protection et la valorisation de l'information. A ce titre, elle doit être sécurisée depuis sa création ou sa collecte, tant pendant la phase de transmission que pendant la phase de conservation (Eric A. Caprioli, Jean-Marc Rietsch, Marie-Anne Chabin, Dématérialisation et archivage

électronique, éd. Dunod, 2006 ; des mêmes auteurs, L'archivage électronique à l'usage du dirigeant, Livre blanc FEDISA CIGREF, 2005, disponible sur le site www.cigref.fr.).

Les informations doivent être conservées de façon **intègre** dans le temps (voir fiche 2 : Intégrité), c'est-à-dire qu'elles doivent demeurer intactes depuis le moment de leur création jusqu'à leur destruction. L'article 4.f du Règlement CE n° 460/2004 du Parlement européen et du conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information définit l'intégrité des données comme : « la confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas été modifiées ». Aucune modification des données, aussi infime soit-elle ne doit être permise, et ce pendant toute la durée de vie. Cette certitude permet d'acquérir une certaine confiance dans les données transmises.

La confiance en une information découle également de son **imputabilité**. Il faut pouvoir être sûr que c'est bien la personne authentifiée qui est à l'origine de l'envoi des données et de ce fait assurer une traçabilité des dites données. L'article 4.e du Règlement CE n° 460/2004 du Parlement européen et du conseil du 10 mars 2004 définit l'authentification comme « la confirmation de l'identité prétendue d'entités ou d'utilisateurs ». L'anonymat constitue un risque évident pour la valorisation d'une donnée. Lorsqu'une donnée est imputable, il est plus difficile de la dénier. Cela implique qu'aucune contestation ne doit pouvoir être élevée (ou alors très difficilement) concernant l'existence, l'origine ou la destination d'une action ou d'une transaction.

L'information doit également être **disponible** (voir fiche 1 : Disponibilité / Accessibilité), c'est-à-dire que son accès doit être garanti sans interruption ni dégradation et aux seules personnes autorisées.
La valeur d'une information ne dépend pas uniquement de sa conservation intègre dans le temps mais également de **son exactitude**, de sa pertinence et de sa validité. Pour cela, la sécurité commence au moment de la collecte et de l'enregistrement des données. Les informations doivent être contrôlées par l'entreprise et si elles ne le sont pas, leur degré de vraisemblance doit être reconnu comme moindre. Leur contenu ne doit pas être entaché d'erreur ou de négligence directement imputable à l'intervention humaine. Les informations collectées et destinées à figurer dans une base de données ou un système d'information peuvent être, au départ, exactes, mais faire l'objet de traitements défectueux imputables à des négligences ou à des erreurs humaines, voire à des manipulations. D'autres fois, elles proviennent d'erreurs dues au traitement de l'information. Dans certains cas, les défauts entachant le corpus documentaire ne procèdent pas d'erreurs de nature intellectuelle mais trouvent plutôt leur origine dans une défaillance d'ordre technique liée à la saisie des données.

L'exactitude - au sens strict - vise la conformité avec la réalité de l'information fournie. La jurisprudence fourmille d'exemples où la responsabilité d'un fournisseur de renseignements est retenue pour avoir communiqué une information inexacte, c'est-à-dire contraire à la « vérité objective » (Cass. civ., 14 mars 1978, D. 1979, p.549). De plus, l'exactitude de ces données s'envisage dans la durée et postule, dès lors, une exigence de mise à jour de l'information. Plusieurs décisions de justice témoignent de cette obligation de diffuser des informations actuelles, à jour, non périmées. Ainsi, l'arrêt rendu le 30 janvier 1974 par la Cour de cassation confirme qu'à

bon droit, les juges du fond ont pu décider qu'une agence de renseignements commerciaux avait commis une faute engageant sa responsabilité contractuelle en fournissant une information sans émettre aucune réserve alors qu'elle n'avait en sa possession sur la personne concernée que « des renseignements périmés et sommaires remontant à plus de six mois » (Cass. com., 30 janvier 1974, D.S. 1974, p. 428).

Pour remplir les fonctions mentionnées ci-dessus, **le patrimoine informationnel doit être sécurisé au sein du système d'information**. Sans sécurité, il pourrait être soumis au pillage en règle effectué par des concurrents, des prestataires ou d'autres hackers.

C'est pourquoi la sécurité des systèmes d'information est devenue un enjeu essentiel au sein de l'Union européenne comme le prouve le Règlement communautaire instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information. Cette Agence a pour mission principale de réaliser des analyses à long terme sur les risques émergents et qui affectent les systèmes d'information en Europe. Ce Règlement communautaire donne une définition de sa sécurité des systèmes d'information en son article 4. c. : « sécurité des réseaux et de l'information » : la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles » (J.O.U.E. 13.3.2004, p 1 et s.).

Les instruments juridiques et organisationnels de protection

La protection du patrimoine informationnel repose certes sur des moyens techniques (pares-feux, antivirus, routeurs, cryptologie, etc.) (voir fiches sur la sécurité technique), mais nécessite aussi la mise en place d'instruments juridiques dont nous allons présenter les principales caractéristiques. Ces instruments s'inscrivent dans une véritable stratégie où le droit joue un rôle essentiel : celui d'intelligence juridique et stratégique. **Il s'agit de la maîtrise, la valorisation et la protection du patrimoine informationnel appartenant à une entité publique ou privée, par la mise en place de procédés légaux, réglementaires, contractuels ou organisationnels** (V. Eric A. Caprioli, *Introduction au droit de la sécurité des systèmes d'information,* in *Mélanges en l'honneur de Xavier Linant de Bellefonds*, éd. LexisNexis, à paraître en 2007).

La politique de sécurité des systèmes d'information

L'entreprise et les administrations doivent prévoir le rôle et les responsabilités de tous les acteurs concernés par la sécurité informatique (utilisateurs, DSI, RSSI, prestataires externes, stagiaires etc.). Cette première mesure est imposée par la nécessité de protéger le patrimoine informationnel de ses acteurs car le facteur humain constitue le premier risque, ce dernier étant souvent à l'origine de vols, de pannes, d'erreurs d'utilisation, de délits divers ou de malveillances. La première démarche de l'entreprise doit donc consister à élaborer une Politique de

Sécurité des Systèmes d'Information (PSSI) fondée sur l'édiction de règles clairement définies, notamment concernant les actions opérées sur le patrimoine informationnel (règles concernant la modification d'un fichier, l'enrichissement d'une base de données, etc.).

La **confidentialité** des informations de l'entreprise est un autre facteur fondamental à prendre en compte et des règles de mise en œuvre devraient figurer au sein de la PSSI (ou dans un autre document qui pourrait s'intituler " politique de confidentialité "). Il s'agira notamment de procéder à la classification des informations générées, traitées et archivées sur le patrimoine informationnel et de déterminer les niveaux de confidentialité que les salariés et tiers doivent respecter en fonction de leur rôle au sein de l'entreprise et des droits d'accès qui leur ont été conférés.

L'entreprise doit également prévoir une politique de délégation de pouvoir en ce qui concerne la sécurité et l'administration des technologies de l'information (voir fiche 9 : Obligations et responsabilités de l'entreprise et du chef d'entreprise).

Charte d'utilisation des communications électroniques

La charte d'utilisation des communications électroniques constitue un recueil fonctionnel des règles applicables aux salariés et aux prestataires externes lorsqu'ils utilisent les moyens informatiques et les réseaux (matériels et logiciels) mis à leur disposition dans et/ou par l'entreprise. En fonction de l'environnement technique de l'entreprise, cette charte devra intégrer notamment une clause prévoyant l'interdiction du téléchargement ou de l'introduction d'œuvres protégées par le droit d'auteur sur les postes informatiques mis à disposition des salariés, mais aussi l'interdiction de communiquer des données confidentielles faisant partie du patrimoine informationnel de la société à d'autres personnes (C. Prud. Nanterre, 15 septembre 2005, R.D.B.F., Mars-avril 2006, p. 31 et s, note Eric A. Caprioli).

Cette charte devrait inclure des éléments permettant l'administration des preuves et des traces informatiques qui conditionnent, en grande partie, la pertinence et l'efficacité des recours judiciaires de l'entreprise voire à des fins de preuve pour dégager sa responsabilité. La charte peut aussi parfaitement intégrer les questions relatives à la conservation des données de connexion et de la gestion des accès aux postes de travail et aux réseaux. Il s'agit de légitimer la cybersurveillance au sein d'une entreprise (et notamment celle des personnes pouvant accéder au patrimoine informationnel de l'entreprise). Les mesures de sécurité devront être proportionnées eu égard à la finalité poursuivie par l'entreprise. Mais la simple adoption d'une charte peut s'avérer insuffisante. L'entreprise doit assurer ce changement par des actions de sensibilisation et de formation. La sécurité du patrimoine informationnel doit faire partie intégrante de la culture de l'entreprise.

Contrats de travail et règlements intérieurs

L'élaboration d'une charte d'utilisation des communications électroniques ne se suffit pas à elle-même. Elle doit pouvoir être opposable à l'ensemble des salariés et pour cela il est indispensable de l'intégrer comme annexe du contrat de travail des salariés ou du règlement intérieur de l'entreprise. De la sorte, tout non respect de la charte peut être sanctionné.

Il est cependant nécessaire de s'assurer du respect d'un certain formalisme entourant cette opposabilité. Les instances représentatives du personnel doivent être consultées et informées de tout ce qui

concerne les décisions de mise en œuvre dans l'entreprise de moyens techniques permettant un contrôle de l'activité des salariés (cybersurveillance) conformément à l'article L. 432-2 al. 1 du Code du travail. De plus, les salariés doivent être informés de la mise en place de cette charte (art. L. 121-8 du Code du travail). Tous les dispositifs techniques qui collectent et traitent des données à caractère personnel doivent être déclarés ou autorisés (biométrie) à la CNIL.

Contrats avec des tiers

Il arrive souvent que des prestataires externes, des sous-traitants ou des stagiaires utilisent les systèmes d'information de l'entreprise. Cette utilisation qui présente des risques importants doit être encadrée et contrôlée. En 2005, une stagiaire chinoise travaillant chez un équipementier automobile a été accusée d'avoir copié des données sur son disque dur avant de les emporter chez elle. Ce téléchargement anormal de fichiers a alerté l'administrateur informatique. En conséquence de quoi, l'entreprise a porté plainte en se fondant sur un accès frauduleux dans un système automatisé de données (STAD). La stagiaire a quant à elle justifié la copie de ces données par la rédaction de son rapport de stage ainsi que par le fait que ces données étaient parfaitement accessibles sur l'intranet de l'entreprise.

Il semble donc indispensable de prévoir des clauses de confidentialité et de propriété intellectuelle et de rendre opposable la Charte d'utilisation par le biais des différents contrats ayant trait à la sécurité des systèmes d'information de l'entreprise et qui sont souscrits avec des tiers.

Le guide juridique du DSI ou du RSSI

Le RSSI (Responsable Sécurité des Systèmes d'Information) ou le RSI (Responsable Sécurité de l'Information) est en charge de la sécurité de l'information au sein de l'entreprise (ou dans un groupe d'entreprises). Mais le plus souvent, les fonctions de RSSI sont directement effectuées par le Directeur des Systèmes d'Information (DSI) Le périmètre de son intervention est essentiel, mais la position hiérarchique nécessairement transversale du RSSI est également très importante dans la mesure où elle a une incidence directe sur les pouvoirs et responsabilités de celui-ci. L'efficacité de la sécurité des systèmes d'information est ainsi conditionnée par son positionnement interne et par les délégations de pouvoirs qui lui sont confiées.

Dans la détermination de ces pouvoirs, il sera important d'étudier l'organisation interne de l'entreprise (organigramme et périmètre des fonctions attribuées). Cette démarche est nécessaire puisqu'elle permet d'analyser les contraintes propres à l'entité et de prévoir les règles de sécurité qui lui seront applicables. Pour cela il faudra mettre en place une politique de sécurité de l'information mais aussi une formalisation des obligations et responsabilités du RSSI que l'on trouve dans le Guide juridique du DSI ou du RSSI. Cela permettra de mieux évaluer les risques juridiques qui relèvent de la fonction ainsi que le périmètre de ses attributions (E. A. Caprioli, Régime juridique du Responsable Sécurité des Systèmes d'Information, Livre bleu Tome III, Octobre 2006, disponible sur le site www.caprioli-avocats.com. Bernard Foray, La fonction RSSI, éd. Dunod, 2007).

Contexte

Certaines informations constituent des créations ou des œuvres de l'esprit et sont donc susceptibles d'être protégées par des droits de propriété intellectuelle. La violation de ces droits est passible des sanctions civiles et/ou pénales prévues pour le délit de contrefaçon. D'autres informations ne peuvent pas être protégées par ces droits, mais uniquement par le secret. La protection de l'information peut être abordée de deux façons complémentaires :

- l'une purement juridique en fonction des droits de propriété intellectuelle visés ;
- l'autre plus technique : la mesure technique de protection et d'information.

Protection juridique par les droits de propriété intellectuelle

Les différents droits intellectuels seront envisagés tour à tour, étant précisé que chacun possède un régime juridique spécifique.

Les différents droits de propriété intellectuelle susceptibles de protéger l'information

1. Le droit d'auteur

Les œuvres de l'esprit sont protégées par le droit d'auteur. Il convient de rappeler qu'un monopole est reconnu au titulaire des droits sur l'œuvre (pour une durée de soixante-dix ans après la mort de l'auteur) assorti de certaines exceptions. L'atteinte portée à ce monopole est constitutive du délit de contrefaçon (Art. L. 335-2 CPI pour les compositions musicales, écrits, dessins, peintures et toute autre production imprimée ou gravée en entier ou en partie, Art. L. 335-3 pour les œuvres de l'esprit et pour les logiciels. V également les art. L. 335-4 et s CPI).

Pour bénéficier de cette protection, il convient de rappeler que l'oeuvre doit présenter une forme perceptible qui est originale, c'est-à-dire marquée de l'empreinte de la personnalité de l'auteur. Le titulaire des droits pourra alors faire interdire tout acte de reproduction ou de représentation de l'information. Les prérogatives relevant du droit moral n'appartiennent qu'à la personne de l'auteur et ne sont pas cessibles (paternité, respect, divulgation, retrait et repentir).

Dans le domaine particulier des logiciels, en France comme chez tous les signataires de la Convention de Münich sur le brevet européen, le logiciel est protégé par le seul droit d'auteur et non par le droit des brevets (Article 52-2 c de la CBE du 5 octobre 1973, entrée en vigueur le 7 octobre 1977) même si de nombreux brevets européens de logiciels visant la France font l'objet de dépôts à l'Office européen des brevets et que l'exclusion des programmes d'ordinateur des matières brevetables fait l'objet de remises en cause régulières (V. sur le sujet, Ch. Caron, L'Europe timide des logiciels, Comm. com. électr. 2002, chron. 20). C'est la loi du 3 juillet 1985 qui a levé toute ambiguïté à ce sujet en ajoutant le logiciel aux œuvres de l'esprit susceptibles d'être protégées. Le logiciel doit pour cela remplir la condition d'originalité qui s'entend ici d'un « apport intellectuel » de l'auteur (Cass. ass. Plén., 7 mars 1986, D. 1986, jurisp. p. 405, concl. Cabannes).

Ce qui est protégé c'est à la fois le logiciel et le matériel de conception préparatoire (L. 112-2, 13° du Code de la propriété intellectuelle). C'est l'expression du logiciel qui est protégeable, donc une série d'instructions rédigées par le programmeur en code source ou code objet. Quant au matériel de conception préparatoire, on peut citer l'exemple du manuel d'utilisation, qui peut constituer

une œuvre littéraire. En revanche, sont exclus de la protection, les fonctionnalités du logiciel qui procurent le résultat recherché (TGI Paris, 4 oct. 1995 : JCP G 1996, II, 22673, note H. Croze).

Le droit d'auteur sur un logiciel confère un monopole, détaillé à l'article L. 122-6 du Code de la propriété intellectuelle, qui permet à son bénéficiaire de faire interdire la reproduction de son logiciel, la traduction, l'adaptation, l'arrangement ou toute modification du logiciel et la mise sur le marché, y compris la location d'exemplaires du logiciel. On pourra souligner ici l'absence de droit de représentation. Toutefois, la protection de l'information contenue dans un logiciel a des limites. Ces exceptions, qui ne bénéficient qu'à l'utilisateur licite du logiciel, sont détaillées à l'article L. 122-6-1 du Code de la propriété intellectuelle. Il s'agit du droit d'utilisation et de correction du logiciel, de la possibilité d'étudier le logiciel, du droit de réaliser une copie de sauvegarde, et enfin du droit à décompilation. Ce dernier a une importance toute particulière et peut être un facteur de risque pour l'entreprise car il peut permettre de récupérer des informations afin de réaliser des actes de contrefaçon. Mais la décompilation n'autorise pas toute utilisation des informations recueillies, l'article L. 122-6, IV CPI, imposant notamment qu'elles ne soient pas, sauf nécessité, communiquées à des tiers, ni utilisées pour mettre au point un autre logiciel.

Si la protection d'une œuvre originale par le droit d'auteur naît du seul fait de la création et n'est donc subordonnée à l'accomplissement d'aucune formalité particulière, il peut être judicieux d'effectuer un dépôt privé de l'œuvre (chez un huissier, un notaire grâce au service de dépôt électronique notarial ou auprès d'organismes d'auteurs). Le dépôt offre en effet l'avantage d'apporter une date certaine à la création. Il permet ainsi de faire échec à une revendication effectuée par un tiers de mauvaise foi. Dans le domaine des logiciels et des bases de données, des organismes tels que l'APP (agence pour la protection des programmes), ou Logitas, permettent d'effectuer des dépôts (aux Etats-Unis, le copyright office). A l'APP, le dépôt se déroule de la façon suivante : Lors d'un dépôt de diffusion, deux exemplaires de l'œuvre, telle qu'elle est diffusée au public, sont placés dans deux logibox dont une est conservée par l'APP et l'autre remise au titulaire des droits. Ce type de dépôt concerne notamment les bases de données, les manuels d'utilisation ou les programmes informatiques sous formes exécutables. Lors d'un dépôt des sources d'un logiciel, deux exemplaires de l'œuvre, dans sa version non destinée à être diffusée au public, sont placés dans deux logibox dont l'une est conservée par l'APP et l'autre remise à l'adhérent. Ce type de dépôt permet de prévoir contractuellement l'accès aux sources du logiciel. Contrairement à l'APP et pour un service équivalent, Logitas effectue un contrôle systématique des procédures décrites en accompagnement des sources.

2. Les droits sur les bases de données

La base de données que le Code de la propriété intellectuelle définit dans son article L. 112-3, alinéa 2 comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessible par des moyens électroniques ou par tout autre moyen », fait également l'objet d'une protection par le droit d'auteur, quelque soit son support (électronique ou papier). Pour démontrer son originalité, il conviendra de prendre en compte le choix ou la disposition des matières. Un recueil dans lequel les informations sont classées par ordre alphabétique ne sera pas protégé (CA Paris, 29 oct. 2003 : Comm. com. électr. 2004, comm.

37, note Ch. Caron). Un apport intellectuel de l'auteur doit nécessairement être caractérisé. L'information contenue dans la base de données n'est ici pas protégée mais elle fait l'objet d'une protection spécifique.

L'entreprise peut, en effet, bénéficier d'une protection sur le contenu d'une base de données qu'elle a développée (droit sui generis du producteur de la base de données de l'article L. 341-1 du Code de la propriété intellectuelle). Pour être considéré comme producteur de la base, et donc bénéficier de cette protection, l'entreprise doit prendre l'initiative et le risque des investissements correspondants. Un investissement substantiel est donc exigé, et doit être prouvé par celui qui s'en prévaut. L'investissement porte sur la constitution de la base (recherche, rassemblement des informations et vérification de leur fiabilité (CJCE, 9 nov. 2004 : Comm. com. électr. 2005, comm. 2, note Ch. Caron.). Cet investissement pourra être financier, matériel ou humain.

Le monopole dont bénéficiera l'entreprise est d'une grande utilité et d'une grande efficacité car il protège tout le contenu de la base de données, quand bien même les informations appartiendraient au domaine public. L'article L. 342-1 du Code de la propriété intellectuelle confère un premier droit au producteur de la base de données, c'est celui d'interdire certaines extractions du contenu de sa base. Lorsque l'extraction est partielle, elle devra être quantitativement ou qualitativement substantielle. L'article L. 342-1, 2° du Code de la propriété intellectuelle, permet quant à lui au producteur de la base d'interdire la « réutilisation, par la mise à disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme ». Enfin, une caractéristique forte de ce droit sui generis provient également du fait que la protection peut, dans la pratique, être perpétuelle puisque la durée de protection initiale de 15 ans recommence à courir à chaque fois qu'un investissement substantiel est réalisé.

3. Le droit des brevets d'invention

Les créations de caractère technique peuvent faire l'objet d'une protection par le brevet. Ce titre délivré par l'INPI ou par l'Office européen des brevets (OEB) confère à son titulaire un monopole temporaire d'exploitation sur l'invention déposée (20 ans non renouvelable). C'est ce droit exclusif conféré au titulaire du brevet qui en fait une arme industrielle et commerciale redoutable. Pour bénéficier de la protection, l'invention doit respecter plusieurs conditions énumérées par l'article L. 611-10 du Code de la propriété intellectuelle : elle doit être nouvelle et impliquer une activité inventive (ces deux conditions s'appréciant par rapport à l'état de la technique), et elle doit être susceptible d'application industrielle. L'article exclut par la même occasion un certain nombre de créations qui ne remplissent pas ces conditions, à savoir : les théories scientifiques et méthodes mathématiques, les créations esthétiques, les plans, principes et méthodes, les programmes d'ordinateurs et enfin les présentations d'informations. Une invention brevetable peut être un produit, un procédé, une application ou une combinaison nouvelle de moyens connus.

Des informations peuvent donc présenter des caractéristiques qui en font un procédé brevetable. En effet, un procédé (ou moyen) peut revêtir une forme immatérielle (une façon de faire, une manière d'opérer). Il sera alors indispensable à l'entreprise propriétaire du procédé, d'effectuer un dépôt auprès de l'INPI en prenant soin de ne pas divulguer l'invention au risque de la faire tomber dans l'état de la technique.

Il est à noter que ce dépôt peut s'effectuer par voie électronique. Développé en collaboration avec l'Office européen des brevets, le dépôt électronique de brevets est un service offert par l'INPI qui permet de déposer par voie électronique et en toute sécurité les demandes de brevets français, européens et PCT (patent cooperation treaty) ainsi que les pièces complémentaires pour la procédure française, sans avoir recours au papier. Soulignons que le brevet européen n'est pas un titre de propriété intellectuelle unique comme la marque communautaire. La procédure d'examen de la demande est unique et se déroule devant l'OEB. La demande doit viser les Etats pour lesquels on souhaite une protection (parmi les signataires de la Convention sur le brevet européen du 5 octobre 1973). Après sa délivrance par l'OEB, le brevet européen éclate en brevets nationaux dans chacun des Etats où il est demandé.

4. Le droit des marques

La marque est un signe distinctif. Elle peut être apposée sur un produit, ou bien accompagner un service. Sa fonction est de permettre au consommateur de distinguer les produits ou services d'une personne physique ou morale de ceux de ses concurrents (article L. 711-1 du Code de la propriété intellectuelle). Elle constitue un moyen pour les commerçants d'attirer et retenir une clientèle, et dans l'esprit du consommateur, elle est souvent la garantie d'une certaine qualité. Le dépôt d'une marque confère à son titulaire un droit exclusif d'une période de 10 ans renouvelable indéfiniment, mais qui produit des effets uniquement sur le territoire où elle a été enregistrée. Le signe doit présenter certaines caractéristiques pour faire l'objet d'un dépôt. En premier lieu, il doit pouvoir être représenté graphiquement. L'article L. 711-1 du CPI nous donne une liste non limitative de signes susceptibles de constituer des marques. On peut les regrouper en trois groupes : les marques nominales, les marques figuratives (logos, graphismes, couleurs, formes, etc.) et les marques sonores. Les marques nominales et figuratives peuvent d'ailleurs se combiner, on dit alors qu'elles sont « semi-figuratives ».

Le signe doit aussi respecter des conditions de validité. Il doit être licite et distinctif (article L. 711-2 du CPI). Le signe licite s'entend de celui qui n'est pas contraire à la loi, l'ordre public et les bonnes mœurs, et qui n'est pas frauduleux ou déceptif, c'est-à-dire qu'il n'induit pas le public en erreur. Le signe est distinctif lorsqu'il permet d'identifier un produit ou un service parmi les produits ou services de même nature, proposés par les concurrents. La marque ne doit donc pas être générique ou nécessaire, ni être descriptive du produit ou service (notamment de l'espèce, la qualité, la quantité, la destination, la valeur ou la provenance du produit ou service). Le signe choisi doit également être disponible, c'est-à-dire ne pas porter atteinte à des droits antérieurs (L. 711-4 du CPI). Ces droits antérieurs peuvent être constitués par des marques, dénominations sociales, noms commerciaux, enseignes ou noms de domaine. Ces droits ne sont opposables que dans la limite du principe de spécialité, c'est à dire qu'ils existent dans le même secteur commercial que celui dans lequel on veut déposer la marque. En revanche, certains droits antérieurs sont opposables même dans le cadre d'un secteur d'activité totalement différent : le droit d'auteur, le dessin ou modèle protégé, une appellation d'origine, un droit de la personnalité.

La marque est un droit de propriété industrielle particulier en ce sens qu'il oblige son titulaire à exploiter commercialement son signe. Le titulaire d'une marque qui ne fait pas l'objet d'un usage sérieux pendant une période ininterrompue

de cinq ans encourt la déchéance de sa marque (L. 714-5 du CPI).

Le droit sur la marque permet de faire sanctionner les actes de contrefaçon qui s'entendent de la reproduction à l'identique du signe (L. 713-2) ou de son imitation. Dans le cas d'une imitation du signe, la démonstration d'un risque de confusion entre les marques est nécessaire (L. 713-3 du CPI). D'autres actes sont susceptibles s'être sanctionnés par l'action en contrefaçon : c'est notamment le cas de l'usage non autorisé d'une marque, son apposition, ou encore l'importation et l'exportation de marchandises présentées sous une marque contrefaite.

La marque communautaire a été créée par le règlement CE n° 40/94 du 20 décembre 1993. Elle ne se substitue pas aux marques nationales. C'est un titre unique qui produit ses effets sur tout le territoire de la Communauté. Son dépôt et son examen s'effectuent auprès de l'Organisation de l'harmonisation du marché intérieur (OHMI). Le dépôt au niveau international existe également grâce à l'Arrangement de Madrid qui permet à celui qui a déposé sa marque dans le pays d'origine, de déposer sa marque auprès de l'OMPI (organisation mondiale de la protection industrielle) à Genève. Une fois enregistrée, l'OMPI notifie la marque aux diverses administrations nationales qui peuvent l'admettre ou la refuser.

5. Le droit des dessins et modèles

Ce droit a pour objet de protéger l'apparence d'un produit ou d'une partie de produit. L'objet déposé doit présenter certaines caractéristiques à savoir : être visible (objet concret et apparent), nouveau (au regard de l'art antérieur), et avoir un caractère propre c'est-à-dire que l'impression d'ensemble qu'il suscite chez l'observateur averti doit différer de celle produite par tout dessin ou modèle divulgué avant le dépôt de la demande d'enregistrement. Ce caractère propre est une condition qui a été ajoutée par le nouveau droit des dessins et modèles issu de l'ordonnance n°2001-670 du 25 juillet 2001 portant adaptation du code de la propriété intellectuelle au droit communautaire. Un arrêt de la chambre commerciale de la Cour de cassation en date du 6 février 2007 (N° pourvoi : 04-17274, disponible sur le site www.legifrance.gouv.fr) est venu confirmer que l'appréciation de la validité d'un dépôt d'un modèle relève du droit en vigueur au moment de ce dépôt. L'exigence de caractère propre ne s'applique donc pas aux modèles déposés antérieurement à l'ordonnance. Certaines créations sont, en revanche, écartées de toute protection par les dessins et modèles : les formes exclusivement imposées par la fonction technique du produit, les formes des pièces d'assemblage et les créations contraires à l'ordre public et aux bonnes mœurs.

Comme la marque, le modèle doit être déposé à l'INPI (ou l'OHMI pour le modèle communautaire), et confère un droit exclusif à son titulaire sur le territorial où le dépôt a été effectué. La durée initiale du droit protégé est de 5 ans et peut être prorogée plusieurs fois pour atteindre une durée maximale de 25 ans. La protection conférée par ce droit permet de s'opposer à toute contrefaçon. Il peut s'agir de la reproduction à l'identique ou de l'imitation du dessin ou modèle. Les actes de commercialisation d'objets contrefaisants sont des contrefaçons, tout comme leur importation.

Le modèle peut parfaitement bénéficier d'un cumul de protection avec le droit d'auteur s'il constitue une création de forme originale marquée de l'empreinte de la personnalité de son auteur.

Il existe également deux types de modèles communautaires : le modèle communautaire enregistré (auprès de l'OHMI), qui bénéficie d'une période de protection maximale de 25 ans, et le modèle communautaire non enregistré qui confère à son titulaire un monopole d'exploitation de trois ans à compter de la date à laquelle il a été divulgué pour la première fois au public au sein de l'Union européenne.

6. Le savoir-faire et le secret de fabrique

Certaines informations, qui ne sont pas susceptibles d'être protégées par un droit de propriété intellectuelle ou que l'entreprise ne souhaite simplement pas voir divulguées au public, peuvent faire l'objet d'une réservation par le secret. Bien entendu, le secret ne constitue pas un droit privatif. Il revêt deux formes juridiques : le savoir-faire (ou know-how) et le secret de fabrique.

Le savoir-faire est défini par le règlement d'exemption n° 772/2004 du 27 avril 2004 (article 1 (i)) comme : « un ensemble d'informations pratiques non brevetées, résultant de l'expérience et testées, qui est : (i) secret, c'est-à-dire qu'il n'est pas généralement connu ou facilement accessible ; (ii) substantiel, c'est-à-dire important et utile pour la production des produits contractuels ; (iii) identifié, c'est-à-dire décrit d'une façon suffisamment complète pour permettre de vérifier qu'il remplit les conditions de secret et de substantialité ». La définition communément retenue est celle de Monsieur le Professeur Jean-Marc Mousseron : le savoir-faire est une « connaissance technique transmissible, mais non immédiatement accessible au public et non brevetée ». La réservation du savoir-faire n'est en principe pas possible par voie d'appropriation car seul un droit de propriété intellectuelle tel que le brevet, peut conférer un droit de propriété sur de simples informations. Toutefois, la protection du savoir-faire peut être assurée de différentes manières. En premier lieu, la jurisprudence a eu l'occasion de reconnaître l'incrimination de vol d'informations, par exemple lorsqu'un employé recopie des formules de fabrications confidentielles (Lyon, 24 février 1988, PIBD 1988, III p. 225). Deuxièmement, le titulaire du savoir-faire bénéficie des règles de la responsabilité civile, avec l'action en concurrence déloyale contre ses concurrents, et l'action en responsabilité de droit commun contre les non concurrents. Enfin, l'utilisation de mécanismes contractuels peut s'avérer indispensable par exemple lorsque dans le contexte d'une négociation avec un tiers, l'accès doit être accordé à une partie du savoir-faire. Le titulaire devra imposer au tiers la signature d'un accord de confidentialité. Ce type d'accord se divise le plus souvent en deux obligations : une obligation de non divulgation à des tiers du savoir-faire, et une obligation de non exploitation de ce savoir-faire.

Le secret de fabrique s'entend quant à lui de « tout procédé de fabrication, offrant un intérêt pratique ou commercial, mis en œuvre par un industriel et gardé secret à l'égard de ses concurrents » (Cass. crim., 29 mars 1935 :Bull. crim., p.350). Les peines sanctionnant la divulgation du secret de fabrique, par tout directeur ou salarié d'une entreprise, sont prévues aux articles L. 621-1 du Code le la propriété intellectuelle et l'article L.152-7 du Code du travail. Ce délit est puni de deux ans d'emprisonnement et de 30.000 euros d'amende. La tentative de révélation est punie de la même manière.

7. Autres signes distinctifs : nom commercial, enseigne, dénomination sociale et nom de domaine

A côté de la marque, le patrimoine informationnel de l'entreprise est constitué d'autres signes distinctifs

utilisés dans la vie des affaires, produisant des effets quand ils sont exploités dans les relations avec la clientèle. Ainsi, la dénomination sociale identifie la personne morale, le nom commercial un fonds de commerce, l'enseigne le lieu d'une exploitation commerciale et le nom de domaine un site Internet.

Le choix de ces signes diffère de celui d'une marque car il n'existe pas à proprement parler de conditions de validité ou d'acquisition de tels signes. Même totalement dépourvu de caractère distinctif, un signe peut parfaitement être exploité dans le commerce. Cependant sa défense, fondée sur la responsabilité civile, contre l'usage d'un signe similaire, suppose qu'il soit distinctif. Par conséquent la distinctivité n'est pas une condition légale mais permet d'assurer la protection du signe.

Le signe doit par ailleurs être **disponible**. La dénomination sociale, le nom commercial, l'enseigne ou le nom de domaine peuvent se heurter à des droits antérieurs. Il peut d'agir d'une marque, et dans ce cas le titulaire du signe visant des produits ou services similaires à ceux de la marque antérieure, sera éventuellement condamné pour contrefaçon. Le signe **ne doit pas non plus porter atteinte à une marque de renommée** (bénéficiant d'une protection spéciale à l'article L. 713-5 du CPI), **ni à une dénomination géographique antérieure telle qu'une appellation d'origine**. Enfin, la dénomination sociale, le nom commercial, l'enseigne ou le nom de domaine **ne doivent pas porter atteinte au nom d'un tiers.** Concernant le cas dans lequel le signe correspond au nom de famille de l'exploitant, le nom peut déjà être exploité dans le même secteur d'activité et une telle situation est de nature à créer un risque de confusion dans l'esprit du public. Mais par analogie au droit des marques, l'exploitant pourra utiliser son nom sauf dans le cas où il chercherait à profiter de la réputation du signe antérieur.

La protection de ces signes distinctifs, est assurée par la voie non privative du droit commun de la responsabilité civile. Cette protection est subordonnée à son usage dans les rapports avec la clientèle. Cet usage est une condition nécessaire et suffisante de la protection. *L'inscription au RCS ne constitue pas une condition de protection de la dénomination sociale, du nom commercial et de l'enseigne*. La date à prendre en compte pour se défendre contre un signe postérieur est celle du commencement de l'exploitation du signe et non celle de l'inscription au RCS.

Pour le **nom de domaine**, la formalité d'enregistrement n'est pas non plus comparable avec l'enregistrement d'une marque. Si l'enregistrement du nom de domaine est nécessaire à son utilisation sur l'Internet, il constitue une réservation technique du signe qui n'est pas de nature à conférer de droit privatif. L'exploitant du site identifié sous le signe a en revanche qualité pour agir en concurrence déloyale même s'il n'est pas personnellement le bénéficiaire de l'enregistrement, car il est la victime d'un risque de confusion avec un signe postérieur

La protection de ces signes se trouve limitée, au même titre que les marques, par **le principe de spécialité**. Le nom commercial et l'enseigne ne sont protégés qu'à l'égard des produits ou services qui constituent l'objet de l'activité du fonds ou du lieu d'exploitation qu'ils identifient. Pour la dénomination sociale, la question est plus délicate car une jurisprudence longtemps dominante estimait que la dénomination sociale était protégée en dehors du domaine d'activité de la personne morale. La Cour de cassation soumet désormais clairement la protection de la dénomination sociale au

principe de spécialité (Cass.com., 30 novembre 2004, PIBD 2005, n° 802, III, 117). Le nom de domaine est lui aussi soumis au principe de spécialité. La protection de tous ces signes soumise au régime de spécialité s'étend en revanche aux spécialités similaires.
Mais si le signe bénéficie d'une protection, celle-ci est nécessairement limitée géographiquement. En cas de conflit avec une marque postérieure, la dénomination sociale, le nom commercial ou l'enseigne, doivent avoir un rayonnement national.

Les sûretés sur le patrimoine informationnel

Le patrimoine informationnel est composé de biens meubles incorporels. Cette catégorie éclatée regroupe des biens aussi disparate que le fonds de commerce, les créances, les propriétés industrielles, les instruments financiers, la monnaie, les parts sociales, ou encore les droits d'exploitation des logiciels, etc.

L'ordonnance n° 2006-346 du 23 mars 2006 relative aux sûretés (J.O n° 71 du 24 mars 2006 p. 4475) a bouleversé le régime applicable aux sûretés portant sur des biens incorporels. Désormais le nantissement ne porte que sur des meubles incorporels. L'article 2355 du code civil le définit comme « l'affectation en garantie d'une obligation, d'un bien meuble incorporel ou d'un ensemble de biens meubles incorporels, présents ou futurs ». Le débiteur (la personne qui entend effectuer un nantissement d'un bien meuble incorporel) n'a plus à se déposséder du bien au profit du créancier du bien faisant l'objet du gage pour le rendre opposable. Ce gage est publié sur un registre spécial dont les modalités seront fixées par un décret en Conseil d'Etat. La dépossession n'est donc plus qu'une simple modalité d'opposabilité du gage. Les gages portant sur des droits de propriété intellectuelle nécessitent l'établissement d'un contrat écrit (à titre d'exemple, l'article L.714-1 du CPI l'exige pour les marques). En revanche, à défaut de publicité sur un registre, la connaissance personnelle de l'acte par les tiers vaut publicité. L'entreprise qui donne en garantie des éléments de son patrimoine informationnel a une obligation de conservation de l'élément du patrimoine informationnel (obligation d'exploiter les droits et obligation d'agir en contrefaçon le cas échéant).

La gestion du patrimoine informationnel s'inscrit donc dans cette optique de valorisation des biens meubles incorporels.

Les mesures techniques de protection et d'information

Les informations détenues par une entreprise sont, nous l'avons vu, susceptibles de constituer des œuvres de l'esprit protégées par le droit d'auteur. Néanmoins, face aux insuffisances du seul droit d'auteur pour sauvegarder les intérêts des auteurs dans le contexte du tout numérique, sont utilisées des mesures techniques permettant d'empêcher les actes non autorisés par le titulaire de droits. La loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (J.O n° 178 du 3 août 2006 p. 11529), a posé le principe de validité du recours aux mesures techniques de protection (MTP) et d'information (MTI) des œuvres (E. A. Caprioli, *Mesures techniques de protection et d'information des droits d'auteur*, Com. com. électr. Nov. 2006, Etude n° 30, p. 25). La directive européenne du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information définit ces mesures en son article 6 § 3 comme : « *toute technologie, dispositif ou composant qui, dans le cadre normal de son fonctionnement, est*

destiné à empêcher ou à limiter, en ce qui concerne les œuvres ou autres objets protégés, les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur prévu par la loi, ou du droit sui generis prévu au chapitre III de la directive n° 96/9/CE ». Le nouvel article L. 331-5 du Code de la propriété intellectuelle introduit les mesures techniques de protection tandis que l'article L. 331-22 du même code introduit les mesures techniques d'information. Les premières (MTP) auront pour fonction soit de contrôler l'accès à l'œuvre soit limiter l'utilisation de celle-ci. Les secondes (MTI) regroupent « *toute information fournie par un titulaire de droits qui permet d'identifier une œuvre, une interprétation, un phonogramme, un vidéogramme, un programme ou un titulaire de droit, toute information sur les conditions et modalités d'utilisation d'une œuvre, d'une interprétation, d'un phonogramme, d'un vidéogramme, ou d'un programme, ainsi que tout numéro ou code représentant tout ou partie de ces informations* ».

La loi du 1er août 2006 introduit les articles L. 335-3-1 (pour le droit d'auteur) et L. 335-4-1 (pour les droits voisins) du Code de la propriété intellectuelle pour sanctionner l'atteinte contre ces mesures. Les sanctions sont les suivantes : tout d'abord, est punie de 3.750 euros d'amende toute atteinte délibérée, à des fins autres que la recherche et la sécurité informatique, aux mesures techniques réalisée par un internaute par ses propres moyens ; ensuite, est puni de six mois d'emprisonnement et de 30.000 euros d'amende le fait de procurer ou de proposer sciemment à autrui, directement ou indirectement, des moyens de contournement. Pour pouvoir bénéficier de cette protection, il faut souligner que deux conditions sont nécessaires : les mesures techniques doivent répondre aux critères d'efficacité et de fonctionnalité.

Le décret n° 2006-1763 du 23 décembre 2006 relatif à la répression pénale de certaines atteintes portées au droit d'auteur et aux droits voisins (J.O. du 30 décembre 2006) est venu fixer les sanctions pénales encourues à l'occasion de certaines atteintes portées au droit d'auteur et aux droits voisins. L'article premier du texte ajoute deux articles à la partie réglementaire du Code de la propriété intellectuelle : l'article R. 335-3 relatif à la détention en vue d'un usage personnel ou l'utilisation d'un dispositif anti-mesures techniques de protection mentionné à l'article L. 331-5 du CPI ou de recourir à un service pour y porter atteinte et l'article R. 335-4 relatif à la détention en vue d'un usage personnel ou l'utilisation d'un dispositif anti-mesures techniques d'information détaillé à l'article L. 331-22 du CPI ou de recourir à un service pour porter atteinte à un droit d'auteur, un droit voisin ou à un droit de producteur de base de données. Les actes visés sont désormais passibles de contraventions de quatrième classe, soit une amende de 750 euros. Ces sanctions n'ont pas vocation à s'appliquer à la détention d'un dispositif de contournement ou de neutralisation d'une MTP ou d'une MTI en vue de sa distribution, mais uniquement pour un usage personnel. Enfin, la recherche informatique et la sécurité des systèmes d'information constituent les exceptions à ces règles

Contexte

En tant que valeur d'une entreprise, le patrimoine informationnel doit être protégé. Cette protection repose sur les propriétés intellectuelles et industrielle (voir fiche 8 : La protection de l'information par le droit de la propriété intellectuelle) mais aussi sur la sécurité des systèmes d'information utilisés par l'entreprise (voir fiches sur la Sécurité technique). A ce titre, l'entreprise et ses représentants doivent respecter les obligations légales qui en découlent car la dimension juridique ne saurait être négligée.

La définition du régime juridique applicable au patrimoine informationnel permet de prévoir les risques auxquels l'entreprise et ses dirigeants sont soumis. Cette étape constitue un pré requis nécessaire afin de déterminer les solutions contractuelles et organisationnelles envisageables pour dégager - au maximum - l'entreprise et ses dirigeants de tout ou partie de leur responsabilité.

Obligations et responsabilités

Le patrimoine informationnel de par sa nature est soumis à des corps de règles différents : la loi Informatique, Fichiers et Libertés, le droit de la responsabilité civile ou le Code pénal.

Non-respect des obligations découlant de la loi Informatique, Fichiers et Libertés

Le patrimoine informationnel détenu par une entreprise est constitué de différents types d'informations, et notamment de données à caractère personnel contenues dans des bases de données, qu'il s'agisse de celles de prospects, de clients, partenaires commerciaux, etc. C'est à ce titre que la Loi Informatique, Fichiers et Libertés du 6 janvier 1978 modifiée par la loi du 4 août 2004, crée des obligations à la charge de ces entreprises. Cette loi précise les sanctions pénales applicables à toute entreprise qui ne respecterait pas les principes en matière de données à caractère personnel. La loi pose en principe que c'est le responsable du traitement qui engage sa responsabilité pénale en cas de non-respect des prescriptions qu'elle impose.

Les principales obligations sont les suivantes :

- L'obligation d'information qui signifie que toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée (article 32 de la loi Informatique, Fichiers et Libertés) ;
- Le respect du droit d'accès, impliquant que toute personne justifiant de son identité a le droit d'interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication (article 39, 41 et 42 de la loi) ;
- Le respect du droit de rectification, permettant à toute personne de faire rectifier, compléter, actualiser, verrouiller ou effacer des informations qui la concernent lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite (article 40 de la loi) ;
- Le respect du droit d'opposition, qui autorise toute personne à s'opposer, pour des motifs légitimes, à figurer dans un fichier (article 38 de la loi) ;
- Le respect de formalités préalables car certains traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte

aux droits et aux libertés doivent, avant leur mise en oeuvre, être déclarés ou soumis pour autorisation à la CNIL. Le non accomplissement des formalités déclaratives est sanctionné de 5 ans d'emprisonnement et 300.000 euros d'amende (art. 226-16 du code pénal).

Les personnes morales peuvent également être déclarées pénalement responsables (article 226-24 du code pénal) et sont passibles de peines plus lourdes (le taux maximum de l'amende est porté au quintuple de celui prévu pour les personnes physiques).

Les données à caractère personnel sont diverses et leur traitement n'entraîne pas les mêmes obligations. Par exemple, l'utilisation des données biométriques pour les accès physiques ou l'authentification sont soumises à autorisation (deux autorisations uniques ont été adoptées en 2006 : une pour la reconnaissance du contours de la main, une autre pour les empreintes digitales).

De plus, en vertu de l'article 34 de la loi Informatique et liberté, l'entreprise doit prendre toutes les mesures de sécurité utiles pour préserver les données saisies afin qu'elles ne soient pas « déformées, endommagées ou que des tiers non autorisés y ait accès ». Cette obligation est en principe une obligation de moyens (Cass. crim. Arrêt du 30 octobre 2001, Pourvoir 99-82136. Inédit). L'article 226-17 du code pénal prévoit des peines allant jusqu'à 5 ans d'emprisonnement et 300.000 euros d'amende (V. par exemple, Cass. crim. 19 décembre 1995, Bull. crim. n°387, Rev. Sc. Crim. 1996, 676, obs. J. Francillon). Cependant, ce manquement peut aussi avoir pour conséquence d'engager la responsabilité civile du responsable du traitement accompagnée de sanctions prononcées par la CNIL. La sécurité de ces données doit être proportionnelle à leur nature et au risque qu'implique le traitement concerné.

Le responsable du traitement engage également sa responsabilité et pourra se voir sanctionné par la CNIL. Il ne peut en conséquence qu'être conseillé aux entreprises de mettre en place une politique « Vie privée et données personnelles », passant notamment par la réalisation du recensement des fichiers et des formalités préalables aux traitements. Pour assurer cette politique, la désignation d'un « Responsable Vie privée et données personnelles » de l'entreprise apparaît nécessaire. Dans certains cas l'entreprise pourra nommer un Correspondant à la protection des données à caractère personnel (E. A. Caprioli et I. Cantéro, *Le choix d'un correspondant à la protection des données*, JCP éd. E, 2006, 1976).

Une bonne gestion des données à caractère personnel est donc nécessaire pour disposer d'un patrimoine informationnel « légal ». Cela implique que la personne responsable des traitements de l'entité définisse une politique, nomme des correspondants (dans un groupe avec de multiples filiales, succursales, etc.) et sensibilise le personnel à cette problématique.

Responsabilité civile découlant du fait d'un salarié

Les articles 1382 et 1383 du Code civil énoncent un principe de responsabilité à raison des dommages causés de son propre fait mais encore par sa négligence ou par son imprudence. Pour écarter cette responsabilité de droit commun, il est possible d'apporter la preuve que la cause du dommage relève d'un cas de force majeure. L'appréciation de ces cas d'exonération de responsabilité ne pourra se faire qu'au cas par cas.

Les systèmes d'informations peuvent être la cible d'attaques informatiques

engendrant un sinistre, une menace ou un risque portant atteinte au patrimoine informationnel des entreprises. On peut définir un « sinistre » comme l'incident dont la survenance entraîne des dommages pour le système touché. Un « risque » est un événement pouvant causer des dégâts. Une « menace » est un sinistre dont la probabilité d'occurrence est élevée pour une cible donnée. Une attaque est la concrétisation de cette menace par l'exploitation d'une vulnérabilité du système. On peut citer comme exemple d'attaques, les intrusions ou la diffusion de virus détruisant le patrimoine informationnel.

A défaut de mettre en place une politique de sécurité en interne pour protéger ce patrimoine, l'entreprise risque de voir sa responsabilité engagée. En l'absence d'un minimum de diligence (à travers des outils techniques comme les anti-virus (voir fiches Sécurité technique) et des outils juridiques tels que des chartes d'utilisation des communications électroniques (voir fiche 7 : Les outils juridiques liés à la protection du patrimoine informationnel), l'entreprise s'expose à des graves risques d'attaques informatiques susceptibles d'engendrer un sinistre.

Dans le cadre d'un contentieux, il appartiendra au juge de déterminer la responsabilité de l'entreprise au regard des mesures de sécurité préventives qui ont été prises. L'appréciation de cette responsabilité se fera au regard de l'état de l'art. On peut par exemple imaginer qu'un sinistre causé par un virus non connu au jour du dommage par les anti-virus n'engagera pas la responsabilité de l'entreprise. Un sinistre causé par un virus connu depuis plusieurs mois pourra, en revanche, engager sa responsabilité.

Le chef d'entreprise peut lui aussi voir sa responsabilité civile engagée du fait d'un dommage causé par l'absence de sécurité entourant le patrimoine informationnel de l'entreprise ou l'agissement d'un salarié dans les fonctions pour lesquelles ils sont employés. Les cas d'exonération de l'employeur sont interprétés très strictement pas les tribunaux (article 1384, al. 5 du code civil, relatif à la responsabilité du commettant du fait de ses préposés).

Les atteintes aux Systèmes d'information (STAD, système de traitement automatisé des données)

En dehors du risque de sinistre informatique, le patrimoine informationnel peut se voir piller par des intrusions non autorisées dans le système informatique de l'entreprise. Ces actes, quelque soit le moyen utilisé, sont sanctionnés par les articles 323-1 à 323-7 du Code pénal. La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (JO du 22 juin 2004, p. 11175 et s. Eric A. Caprioli, Pascal Agosti, La confiance dans l'économie numérique, Petites Affiches du 3 juin 2005, p. 4 et s) a créé une nouvelle incrimination en matière d'atteinte aux STAD (système de traitement automatisé de données) par virus informatique. Un STAD s'entend de l'ensemble des éléments physiques et des programmes employés pour le traitement des données, ainsi que des réseaux assurant la communication entre les différents éléments du système informatique. Pour ces raisons, le patrimoine informationnel est considéré comme inclus au sein du système d'information d'une entreprise (que ce dernier soit ou non externalisé).

Plusieurs actes sont ici susceptibles d'être sanctionnés. C'est le cas en premier lieu de l'accès frauduleux à tout ou partie du patrimoine informationnel. Il s'agit de toute action de pénétration ou d'intrusion (connexion pirate, interrogation d'un fichier sans autorisation). Le deuxième acte susceptible d'être réprimé est le maintien frauduleux dans le patrimoine informationnel

de l'entreprise qui correspond aux situations anormales telles que connexion, visualisation, ou opérations multiples alors que la personne qui y accède a pris conscience que ce maintien est anormal. L'atteinte volontaire au fonctionnement du système d'information contenant le patrimoine informationnel est pénalement sanctionnée dans les cas où un individu a intentionnellement entravé le fonctionnement du système en ne respectant pas le droit d'autrui. Enfin, les atteintes volontaires aux données, c'est-à-dire leur altération, sont également sanctionnées pénalement, ce délit supposant une altération intentionnelle et au mépris des droits d'autrui. Le responsable est l'auteur de l'infraction, c'est-à-dire celui qui a commis l'élément matériel (accès, maintien, atteinte volontaire au système ou aux données). Il peut s'agir d'un dirigeant ou d'un salarié, mais d'une manière générale, le chef d'entreprise même s'il n'a pas participé matériellement au délit, est condamné au motif qu'il a méconnu son obligation de contrôle de la pratique de ses préposés, sauf s'il a accompli des diligences normales compte tenu des moyens dont il dispose. La responsabilité de l'entreprise personne morale pourra également être retenue pour les diverses infractions existantes en matières d'atteinte aux STAD.

Tableau récapitulatif des sanctions

Infraction	Peines
Intrusion ou le maintien frauduleux dans un système de traitement automatisé de données (article 323-1 al. 1 du Code de pénal)	2 ans d'emprisonnement et 30.000 euros d'amende
Intrusion ou le maintien frauduleux dans un système de traitement automatisé de données (article 323-1 al. 1 du Code de pénal)	3 ans d'emprisonnement et 45.000 euros d'amende
Fait d'entraver ou de fausser un système de traitement automatisé de données (article 323-2 du Code pénal)	5 ans d'emprisonnement et 75.000 euros d'amende
Introduction frauduleuse de données dans un système de traitement automatisé (article 323-3 du Code pénal)	5 ans d'emprisonnement et 75.000 euros d'amende
Importation, détention, offre, cession ou mise à disposition d'un équipement, instrument, programme informatique ou de toutes données conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues aux articles précédents (article 323-3-1 du Code pénal), sans motif légitime	Peine prévue pour l'atteinte elle-même ou pour l'infraction la plus sévèrement réprimée
Tentative des délits prévus aux articles 323-1 à 323-3-1 (article 323-7 du Code pénal)	Mêmes peines

Un salarié de l'entreprise peut également porter atteinte au patrimoine informationnel sans intrusion dans un STAD. Il faudra alors recourir au droit commun pour appréhender ce type d'actes (abus de confiance, escroquerie, voire un accès non autorisé...). On rentre ici dans le cas délicat du vol d'informations. En principe l'information n'est pas appropriable en tant que telle, sauf certains cas comme le secret de fabrique (voir fiche 8 : La protection de l'information par le droit de la propriété intellectuelle). Mais la jurisprudence a reconnu à plusieurs reprises l'incrimination de vol d'informations (délit qui existe déjà aux Etats-Unis et dans de nombreux pays européens) par exemple dans le cas d'un employé ayant recopié des formules de fabrications confidentielles (Lyon, 24 février 1988, PIBD 1988, III p. 225). Plus célèbre, l'arrêt Bourquin (Cass. Crim. 12 janvier 1989, Bull. crim. 1989, n° 14), dans lequel la Cour de cassation sanctionnait le vol du contenu informationnel de disquettes informatiques. De même a été reconnu l'abus de confiance sur une information. En l'espèce, un entrepreneur avait obtenu le numéro de carte bancaire d'une cliente pour le transmettre à un sous-traitant (Cass. Crim. 14 novembre 2000, Bull. crim. n° 1003 ; Droit Pénal 2001. com.28).

Les solutions envisageables

Concernant les risques liés à l'externalisation

De plus en plus souvent, les entreprises externalisent certaines activités liées à leur système d'information - et par là une partie de leur patrimoine informationnel - auprès de professionnels informatiques afin d'accroître les performances et de rationaliser les frais et charges liés à leur administration et à leur gestion (exemples de services externalisés : les serveurs peuvent être hébergés chez un professionnel, le back-up, la production informatique (infogérance), la sécurité du SI, l'archivage électronique, etc.). Leur sécurité constitue donc un enjeu essentiel pour leur bonne marche.

Cette relation unissant l'entreprise et le prestataire externe sera définie dans la rédaction d'un contrat d'externalisation tel que l'infogérance. Il est important de préciser que dans ce genre de relations, le prestataire fournit un accès à des serveurs qu'il met à disposition de son client. Il faut cependant souligner que le fournisseur de service n'est en aucun cas propriétaire du contenant où sera stockée l'information.

Les serveurs devront être protégés avec l'élaboration d'une politique de sécurité des systèmes d'information.

Préalablement à toute négociation contractuelle, l'entreprise doit s'assurer que son prestataire est fiable et qu'il dispose d'outils conformes à l'état de l'art. Il faut prévoir également que celui-ci s'engage à faire évoluer son matériel afin d'être en conformité avec les standards techniques, l'état de l'art et les besoins spécifiques de l'entreprise (par exemple si c'est une banque, des clauses contractuelles relatives au contrôle interne devront figurer dans le contrat du fait du règlement CRBF n°97-02 ou autres).

Le contrat devra impérativement prévoir une clause de confidentialité relative aux données et informations de l'entreprise qui figurent dans les serveurs du prestataire. En effet, le prestataire n'intervient que pour stocker des informations mais en aucun cas, il ne doit les utiliser ou les transférer à des tiers non autorisés. Les informations externalisées restent la pleine propriété de l'entreprise. Rappelons que la sécurité s'inscrit dans le temps. Ainsi, ce qui importe pour

l'entreprise, c'est de s'assurer de la continuation des services électroniques dont il a délégué la gestion au prestataire, même après la résiliation du contrat. La phase de service régulier peut prendre fin lorsque l'entreprise a décidé de réinternaliser la fonction informatique ou lorsque l'entreprise n'est pas satisfaite des prestations fournies et souhaite les confier à un nouveau prestataire. Elle doit pouvoir à tout moment reprendre ou faire reprendre la gestion du ou des systèmes d'information.

La réversibilité du système d'information constitue donc une sécurité juridique mais aussi technique et organisationnelle pour l'entreprise (ex : en matière d'archivage électronique).

Les délégations de pouvoirs au DSI ou au RSSI

Une atteinte au patrimoine informationnel pouvant découler d'une faille dans la sécurité du système d'information, l'entreprise peut recourir au mécanisme de la délégation de pouvoirs. C'est un mécanisme qui a pour effet de transférer la responsabilité pénale du chef d'entreprise vers le préposé délégataire. Elle trouve souvent application dans le domaine de l'hygiène et de la sécurité mais se justifie pleinement dans le domaine des systèmes d'information.

L'entreprise pourra ainsi prévoir une politique de délégation de pouvoir en ce qui concerne la sécurité et l'administration des technologies de l'information. La conséquence essentielle sera donc que la responsabilité pénale correspondant aux fonctions déléguées ne sera plus supportée par le dirigeant mais par le délégataire. Ce dernier devra bien entendu avoir eu connaissance de la délégation, l'avoir accepté et l'entreprise délégante ne doit pas avoir participé à la commission de l'infraction (Cass. crim., 20 mai 2003, Bull. crim., p.404.) Bien évidemment les conditions de validité de la délégation devront être remplies (compétences du délégataire, appartenance de ce dernier au même groupe ou à la même société, délégation sans ambiguïté, certaine et opportune, moyens humains et financiers d'exercer la mission).

Contexte

La question de l'assurance Perte d'Exploitation Informationnelle fait partie intégrante du dispositif veillant à protéger le patrimoine informationnel de l'entreprise. En effet **l'assurance est essentielle pour garantir financièrement ce patrimoine** en cas d'indisponibilité prolongée du système d'information ou de perte de données numérisées (voix, données, images) du fait d'un accident ou d'une malveillance. La sécurité à 100% ne pouvant exister, l'assurance vient en quelque sorte couvrir la différence entre le niveau de sécurité atteint par l'entreprise pour le fonctionnement de son système d'information et le 100%.

Il y a déjà 40 ans, une compagnie d'assurance américaine, spécialisée dans le risque informatique, a amené en Europe Continentale, la notion nouvelle d'assurance « **Tout Risque Sauf** ». Cette notion est essentielle pour couvrir le risque informatique par nature très diversifié dans ses causes accidentelles ou malveillantes. Les conséquences d'un sinistre sont onéreuses et se chiffrent en millions d'euros voire rapidement en dizaine de millions d'euros quand l'outil de production de l'entreprise à savoir son système d'information, devient indisponible. Autrement dit, toutes les causes sont assurées **sauf** un nombre très limité de celles-ci, parmi lesquelles nous citons :

- Guerre civile ou étrangère,
- Risque atomique,
- Sabotage direct du mandataire social.

Les autres causes sont couvertes par ce type d'assurance, ce qui est très pratique pour l'entreprise cliente bénéficiaire de cette assurance PEI. Par exemple l'indisponibilité prolongée pendant plusieurs jours du système information d'une entreprise a pu être couverte financièrement sachant que l'origine du sinistre venait des inspecteurs de maintenance du système informatique. Cela n'était pas dans les causes exclues, et cette défaillance de l'équipe de maintenance a pu ainsi être indemnisée.

Cependant la cible couverte par l'assurance PEI demande à être précisément décrite : espace géographique, périmètre, contenu, etc. Par ailleurs l'assurance PEI étant une assurance de capitaux, il faut donc en calculer les montants plafonds pour garantir les risques potentiels de l'entreprise. Ces risques sont en général évalués par la méthode des scénarios. Par nature l'assurance PEI couvre deux risques principaux nés de l'indisponibilité du système d'information à savoir :

- Les frais supplémentaires : Il s'agit des frais de tout type pour obtenir le redémarrage du système d'information arrêté ;
- La reconstitution des médias : Les médias comprennent : voix, données et images. Sachant qu'ils peuvent évidemment être perdus ou endommagés en cas de sinistre, l'assurance PEI permet de financer leur reconstitution. Celle-ci est beaucoup moins onéreuse sur support magnétique ou optique qu'à partir d'un support papier. Au cours de la phase d'audit il est donc important de vérifier entre autres la qualité et la fraîcheur des sauvegardes informatiques de l'entreprise.

Montant du sinistre brut/net

Au plan méthodologique, il convient tout d'abord de déterminer le montant du sinistre total ou partiel en étudiant de manière inductive un bon scénario de sinistre, adapté au métier de l'entreprise concernée. Cela permet de chiffrer le montant des pertes directes et indirectes dues au sinistre. Le montant total des pertes directes et indirectes constitue le montant du sinistre brut pour le scénario considéré, d'où l'importance du choix d'un scénario objectif et de qualité pour pouvoir induire les résultats calculés au niveau opérationnel de l'entreprise.

Après avoir obtenu le montant du sinistre brut, il convient de soustraire de celui-ci le montant des cibles assurées (Assurance Bris de Machine pour les pertes directes) pour obtenir le montant du sinistre net.

Se pose alors une question complémentaire importante : Est-ce que le montant du sinistre net est compatible avec le risque financier que la Direction Générale de l'entreprise estime pouvoir supporter (stop loss) ? Autrement dit, quel est financièrement pour l'entreprise étudiée, le montant du risque maximum tolérable (RMT) ?

Au-delà de cette borne supérieure, le risque résiduel doit être transféré par l'entreprise auprès d'un Compagnie d'assurance (ou d'une « Captive » propre à l'entreprise).

Nous ne traitons pas ici de deux types d'assurances bien différentes par nature :

- L'assurance Bris de Machine qui assure valeur à neuf, le parc des machines informatiques et télécoms de l'entreprise ;
- L'assurance Responsabilité Civile qui couvre la responsabilité des sociétés d'info gérances et plus généralement les SSII et les sociétés de Facilities Management.

Il est à noter que la disponibilité et la traçabilité du système d'information est de la responsabilité du Maître d'Ouvrage et n'est que très rarement transférable à une entreprise tierce. Il est donc important d'une part de pouvoir auditer l'entreprise tierce en matière de sécurité informatique et d'autre part de prendre une assurance PEI au nom du Maître d'Ouvrage pour financer les frais supplémentaires et la reconstitution des médias, en cas de sinistre. Comme dans le bâtiment, le Maître d'Œuvre n'a pas vocation à se substituer aux responsabilités du Maître d'Ouvrage.

Enjeux

Pour couvrir les risques d'atteinte à la disponibilité et à la traçabilité du système d'information, il est nécessaire de bâtir un plan de continuité d'activité (PCA) du système d'information et surtout d'en tester le fonctionnement au moins deux fois par an (voir fiche 1 : Disponibilité / Accessibilité). L'assurance perte d'exploitation informationnelle (PEI) représente en principe un complément financier vis à vis de la solution technique informatique et télécoms que constitue le PCA. L'assurance PEI couvre en fait la reconstitution des médias et les frais supplémentaires.

En pratique au départ, faute de PCA et de manière transitoire, l'assurance perte d'exploitation informationnelle peut être utilisée seule pour couvrir les risques d'indisponibilité du système d'information. Par contre si la couverture d'assurance PEI est obtenue sans PCA établi et testé, la compagnie d'assurance refuse contractuellement de prendre le risque pendant une durée supérieure à un an. En effet quelques semaines ou au plus quelques mois sont nécessaires en pratique, pour bâtir un PCA. La solution technique informatique et télécoms reste malgré tout le pivot du redémarrage du système d'information. L'assurance PEI constitue seulement un complément monétaire nécessaire pour couvrir le risque financier après sinistre.

En terme d'enjeu financier : Que se passe t-il si le système d'information est indisponible pendant une assez longue durée? Cela peut coûter très cher à l'entreprise. En cas de sinistre, les pertes totales peuvent s'accroître de 20% par jour et atteindre près de 1 million d'euros au quotidien. Il s'agit là d'un cas réel dans une entreprise ou l'indisponibilité du système d'information ne peut excéder la journée (salle des marchés).

En pratique, si le système d'information redémarre en 30 jours, en 10 jours ou en 1 jour les besoins de financement en frais supplémentaires et reconstitution des média couverts par l'assurance PEI ne sont pas du tout de la même hauteur. D'où la nécessité de bien calculer et valider au départ le temps de redémarrage et les dégâts potentiels sur les media de l'entreprise. Ensuite il est prudent de majorer ces capitaux en cas de sinistre d'une portée exceptionnelle. La couverture assurance PEI dépend donc directement de la durée de redémarrage en phase de croisière du système d'information de l'entreprise.

La fiche 1 : Disponibilité / Accessibilité aborde les notions de haute, moyenne et basse disponibilité du système d'information selon le métier de l'entreprise. Par contre, pour la reconstitution des médias, la conservation des données présente un caractère essentiel pour pouvoir reconstituer les données numériques manquantes, y compris donc la voix (opérateurs des salles de marché) et les images. Une étude très précise est à entreprendre ne serait-ce que pour chiffrer le montant plafond des capitaux demandés à la Compagnie d'Assurance pour la reconstitution des médias et cela varie fortement selon les scénarios de sinistre retenus.

Recommandations

Méthodologie résumée pour s'assurer en perte d'exploitation informationnelle (PEi)

Classifier l'information	Effectuer une classification en terme de durée de conservation, des informations gérées par l'entreprise et constituant le patrimoine informationnel, mais également en terme de sensibilité (confidentialité - valeur) et d'accessibilité.
Bâtir des scénarios de sinistre	Sinistre total et sinistre partiel ayant pour cause un accident ou de la malveillance. Il y a donc quatre scénarios de sinistre à étudier.
Déterminer le montant du sinistre brut	Addition des montants de pertes directes et indirectes.
Déterminer le montant du sinistre net	On soustrait du montant du sinistre brut, les capitaux assurés pour la cible concernée.
Estimer les montants frais supplémentaires (FS) et reconstitution de médias (RM)	En fonction des différents scénarios envisagés, calculer le montant plafond des frais supplémentaires (FS) et de la reconstitution des média (RM) du fait du sinistre. L'on retiendra le sinistre avec les montants de pertes FS et RM les plus élevés.
Fixer le RMT	Le risque maximum tolérable par scénario de X euros est fixé par la direction de l'entreprise.

Préambule

«… le facteur de production absolument décisif,
la ressource réelle qui commande tout,
ce n'est plus le capital, ni la terre, ni le travail.
C'est le savoir…»[1]

L'intelligence économique a longtemps été perçue comme un concept flou. Compris par certains dans son acception anglo-saxonne - assimilée au renseignement - elle a, depuis une décennie, donné lieu, dans notre pays, à de multiples essais de définitions. Ainsi, elle a été tour à tour soit présentée comme une stratégie, un processus, une méthode, soit examinée sous l'angle des fonctionnalités, des techniques et des pratiques. En France, l'intelligence économique (IE) est « enfin » considérée aujourd'hui comme une véritable politique publique au service des intérêts des entreprises. Une politique de sécurité économique, de compétitivité et d'influence assise sur une mutualisation des informations publiques et privées. Dans son statut premier de politique publique, l'intelligence économique peut être définie au plan national et européen comme un *«… Mode de gouvernance dont l'objet est la maîtrise de l'information stratégique et qui a pour finalité la compétitivité de l'économie et la sécurité des entreprises*[2] *»*.

La compétitivité des entreprises repose désormais sur leur capacité à mobiliser de nouvelles compétences stratégiques telles que la création de savoir (et sa diffusion rapide dans les processus de production), telles que la capacité à favoriser la mise en réseau (et sa coordination par l'usage des technologies), telles que la maitrise de l'information (et sa capacité d'absorption par toutes les parties prenantes).

Dans la compétition internationale actuelle, le seul véritable avantage concurrentiel, défendable et durable, réside pour l'entreprise, dans sa capacité à maîtriser l'information, en temps réel, à tout moment et en tous lieux pour construire et faire évoluer sa base de connaissance stratégique.

L'alignement entre l'entreprise et ses environnements, allié à la mise en œuvre opérationnelle de nouvelles formes de coopérations, revêt une dimension stratégique de première importance. La captation et la réponse aux stimuli de l'environnement, la lecture des évènements, la production de décisions qui en découlent sont de nature à permettre aux dirigeants d'optimiser la performance de leur firme en créant des opportunités stratégiques et en identifiant des niches d'innovation.

«… Pour relever un tel défi, l'entreprise doit engager une politique d'intelligence économique, laquelle englobe la mise en place d'une fonction d'observation et de surveillance en vue de détecter, d'analyser et de suivre tous les signaux susceptibles de conforter, d'infléchir ou de remettre en cause sa stratégie ou les décisions prises[4]*...»*

Force ou zone de fragilité potentielle, la capacité à créer de la connaissance stratégique à partir de l'information est au centre de la compétition économique et des stratégies cachées. Elle est le chaînon essentiel qui permet de construire et d'influencer l'image globale de l'entreprise. Dès lors que cet actif immatériel devient le facteur essentiel d'avantages concurrentiels pour l'entreprise, il peut également s'avérer être un redoutable vecteur de menaces et un non moins redoutable instrument de dépendance. Savoir gérer les risques et opportunités liés à cet actif immatériel nécessite de porter une attention particulière au patrimoine informationnel de l'entreprise.

«… Pour une entreprise ou une organisation, l'IE est l'ensemble des moyens qui, organisés en système de management par la connaissance, produit de l'information utile à la prise de décision dans une perspective de performance et de création de valeur pour toutes les parties prenantes[3] *…»*

1 Peter Drucker « Au-delà du capitalisme » - Dunod (1993)
2 Alain Juillet, discours lors de la création du « Cercle IE » du CPA - Executive MBA d'HEC le 9 juin 2004
3 Définition retenue par l'Association Française pour le Développement de l'IE (AFDIE) dans son ouvrage « Modèle d'IE » - Economica (2004)
4 Extrait du Rapport CIGREF « Veille stratégique » Sept. 1998

Contexte

Gérer les risques informationnels en entreprise, revient d'abord à prendre la mesure de l'enjeu. En effet, on ne peut surveiller et protéger que ce que l'on a conscience de posséder ou besoin d'acquérir.

Plus la nouvelle compétence des firmes relève de l'intangible, plus elle devient sensible et vulnérable. Face aux nouveaux types de menaces qui pèsent aujourd'hui sur les actifs matériels et immatériels des entreprises, tout dirigeant doit anticiper, contrer, voire riposter afin de protéger activement ses patrimoines technologique et informationnel.

Identifier les ressources informationnelles et percevoir leurs interactions, oblige à l'analyse des différentes composantes d'un nouveau type de capital définit comme « immatériel »[5] . Au cœur de ces actifs immatériels, les Systèmes d'Information et les processus organisationnels occupent une place essentielle, tant en termes de volume qu'en termes de leviers stratégiques et de performance. Dans une économie en réseaux, l'information, la connaissance et leurs modes d'articulation deviennent déterminants. C'est ce qui fonde la démarche d'Intelligence Economique d'Entreprise (IEE).

L'entrée dans une économie du savoir génère des changements tant pour l'organisation interne des entreprises que pour leur environnement externe. Pour rester compétitives, elles font évoluer leur périmètre d'activité (fusions, acquisitions), elles nouent des alliances stratégiques avec d'autres acteurs publics et/ou privés (contrats R&D et d'ingénierie, brevets et licences), voire elles font appel à des savoir-faire et des expertises « hors les murs » (externalisation, offshore).

Ces nouvelles modalités de fonctionnement sont certes synonymes d'agilité et souvent porteuses d'efficacité, mais elles sont également sources de nouveaux défis (problèmes d'intégration, de fragmentation et de transferts de connaissances etc.) qui peuvent fragiliser la capacité d'apprentissage de l'entreprise dans la durée.

«… *En fait, les tendances en cours vont dans le sens d'une complexification croissante des processus de création de connaissances et, en même temps, dans le sens d'une codification accrue, grâce notamment au progrès permis par les TIC. Par conséquent, le savoir est de plus en plus susceptible d'être transféré dans un cadre aussi bien intra firme qu'au delà des frontières de la firme…*»[6]

Transférer le savoir entre firmes génère en effet des risques: perte de contrôle direct, abandon de certains droits de propriété, dépendance pour récréer en interne les compétences préalablement sous-traitées et à les recombiner en cas de changement stratégique. Mais surtout, transférer le savoir entre firmes, requiert l'existence d'une capacité d'apprentissage collectif qui permet d'assimiler et d'exploiter le savoir ainsi produit. La tendance lourde à se concentrer sur un cœur de compétences induit de fait l'émergence d'une division cognitive du travail, dans laquelle les processus de production sont décomposés en blocs de savoirs. Dès lors, les mécanismes d'apprentissage de la firme nécessitent une forte dimension interactive entre réseaux d'acteurs et impliquent le développement de nouvelles formes de coordination autour des activités de conception, de réalisation et de commercialisation.

5 «… le capital immatériel est la détention d'un savoir, d'une expérience concrète, d'une technologie d'organisation, de relations avec les clients et des compétences professionnelles qui confèrent à l'entreprise un avantage compétitif sur le marché…» D'après Edvinson et Malone
6 « La France dans l'économie du savoir » - La documentation Française

Pour ce faire, il revient au dirigeant de mettre en place des processus qui permettent de susciter des interactions entre les différents savoirs individuels, de façon à générer de nouveaux savoirs collectifs qui seront à l'origine d'innovations (notamment organisationnelles) dans l'entreprise. Par l'apprentissage collectif et la coopération, l'IE - dans le but d'éclairer le processus décisionnel - articule la maîtrise des techniques d'accès et de traitement de l'information à la gestion des connaissances (comme fondement de l'Intelligence collective).

«… *La gestion des connaissances est un ensemble de modes d'organisation et de technologies visant à créer, collecter, organiser, stocker, diffuser, utiliser et transférer les connaissances dans l'entreprise. Connaissances matérialisées par des documents internes et externes, mais aussi sous forme de capital intellectuel et d'expériences, détenus par les collaborateurs ou les experts d'un domaine…*»[7]

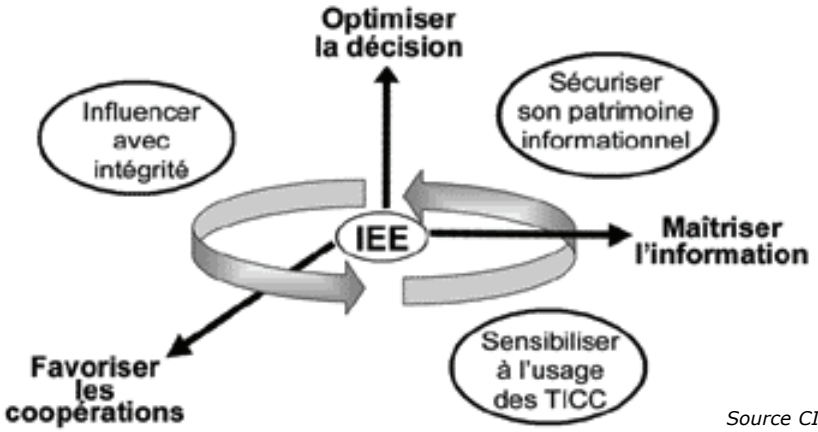
L'IE s'inscrit donc clairement dans la grande mutation du passage d'une économie industrielle à une économie de réseaux fondée sur la connaissance. Dès lors, au sein même des entreprises, les formes classiques de management sont aujourd'hui mises en doute dans leur capacité à coordonner des actions collectives.

L'IE d'Entreprise comme culture managériale !

Orientée vers la maîtrise de l'information, l'optimisation de la décision et la promotion des coopérations, l'Intelligence Economique d'Entreprise est d'abord une affaire de culture managériale, c'est-à-dire une volonté singulière de penser, de décider et de coopérer afin de mieux agir collectivement.

De ce fait, l'Intelligence Economique d'Entreprise (l'IEE) a pour finalité «…*la maîtrise, par le dirigeant, des informations stratégiques nécessaires à la décision et favorables à l'action coopérative, c'est-à-dire utiles au renforcement de son pouvoir d'influence sur ses environnements et de son leadership sur l'ensemble des parties prenantes de l'entreprise*…».

Dans sa dimension organisationnelle, l'Intelligence Economique d'Entreprise présente de ce fait quelques caractéristiques majeures destinées à renforcer les processus de coordination.



Source CIGREF

La compétitivité de l'organisation dépend donc fortement de sa capacité à gérer de manière efficace des processus transversaux. Pour permettre une gestion optimale de la connaissance, elle doit s'appuyer sur une infrastructure informationnelle dont les systèmes d'information constituent la clé de voûte.

7 Rapport CIGREF - octobre 2000 - « Gérer les connaissances »(www.cigref.fr)

L'IE d'Entreprise : le SI au cœur de la démarche !

Véritables systèmes nerveux de l'entreprise, les Systèmes d'Information peuvent radicalement accélérer le développement d'une culture collective et collaborative de l'information, grâce à leurs performances techniques et leurs ramifications transversales.

La multiplication des informations, des compétences et des savoirs nécessaires pour résoudre des problèmes de plus en plus complexes, exige une coordination étroite entre les différentes parties concernées.

◆ Un SI adapté à la démarche d'IEE

Le SI permet à l'entreprise d'optimiser ses modes de fonctionnement en fournissant aux différents acteurs concernés, les outils de coordination entre les tâches des diverses unités de l'organisation. Cette nécessaire coordination oblige le système d'information à tout mettre en œuvre pour protéger les données, récupérer, stocker, traiter, et diffuser à bon escient l'information, fondement du savoir et de la connaissance de l'entreprise.

Pour Patrick Romagni et Valérie Wild, la définition d'un système d'information adapté à la démarche d'Intelligence Economique est la suivante : « *Ensemble organisé de procédures permettant, à tout moment, de donner aux décideurs une représentation de la place de l'entreprise dans son environnement et sur son marché. Il produit de l'information pour assister les individus dans les fonctions d'exécution, de gestion et de prise de décision*[9]».

◆ La nouvelle compétence des firmes

Face à la complexité croissante de l'environnement économique, technologique, social et politique (liée à l'apparition de nouveaux acteurs), à l'enchevêtrement et à l'interdépendance des niveaux d'actions (local, national, européen et international), cette nouvelle compétence s'exerce au cœur d'une réalité économique de plus en plus immatérielle. Philippe Zarifian[10] décrit la compétence comme : « *la faculté de mobiliser des réseaux d'acteurs autour des mêmes situations, à partager des enjeux, à assumer des domaines de co-responsabilité* » ou bien encore « *une intelligence pratique des situations qui s'appuie sur des connaissances acquises et les transforme avec d'autant plus de forces que la diversité des situations augmente* ». Dès lors, le dirigeant découvre l'opportunité de « voir la réalité autrement » en prenant acte qu'au début de ce IIIème Millénaire, notre économie classique, bâtie sur « l'énergie matière » mute vers une nouvelle économie fonctionnant sur « l'énergie information », ce qui transforme et redéploye la valeur créée par les entreprises.

Au regard de ce nouveau défi, l'objectif désormais poursuivi par l'entreprise est de détenir une triple capacité :

- **Capacité à « influencer avec intégrité »** son environnement par des actions de communication et de lobbying.

- **Capacité à gérer et exploiter l'information** pour produire de la connaissance à visée stratégique, organisationnelle et opérationnelle, en vue de la rendre utile non seulement au dirigeant, mais aussi à toutes les « parties prenantes », acteurs internes et externes qui contribuent à la compétitivité de l'entreprise et de l'économie.

- **Capacité à sécuriser ses patrimoines informationnels** constitués non seulement d'infrastructures technologiques mais surtout d'informations, de savoirs et de connaissances.

« La mise en place d'une démarche d'intelligence économique efficace passe obligatoirement par une réflexion sur l'organisation interne et sur les systèmes d'information[8] *».*

8 Enquête de l'IHEDN - Economica, 2000
9 Romagni Patrick et Wild Valérie, L'intelligence économique au service de l'entreprise, Les Presses du Management, 1998
10 Philippe Zarifian - Objectif compétence

En recherchant et en partageant ses informations, l'entreprise accroît potentiellement sa vulnérabilité. Dès lors, le risque informationnel est double : d'abord la captation ou le détournement d'informations stratégiques et ensuite, la probabilité d'une information avérée ou pas, susceptible de modifier ou d'influencer l'image, le comportement et la stratégie de l'entreprise.

Dans ce contexte nouveau, l'Intelligence Economique d'Entreprise met en œuvre :

- d'une part une stratégie de sécurité de l'information (aspects organisationnels et humains, sécurité des systèmes d'information, utilisation du droit, choix de partenaires, prestataires et fournisseurs de confiance, maîtrise de la divulgation de ses propres données au travers des sites Internet, documentations, relations avec ses partenaires... etc.),

- d'autre part une démarche informationnelle défensive active (gestion de la réputation, contre-désinformation, etc.). Les problèmes de déstabilisation ou de rumeur nuisent à l'image de marque de l'entreprise. Véhiculées ou amplifiées par Internet, ces attaques peuvent être contrées par une stratégie de communication, des discours adaptés. Néanmoins, anticiper ces attaques, c'est être en mesure de les détecter. Cette connaissance des menaces et des parades, doit alors permettre de définir des possibilités de contre-offensive.

- Enfin, une action d'influence sur le cours d'événements extérieurs, par des actions de communication maîtrisée et de lobbying à différents niveaux, en particulier aux niveaux européen et international, en amont de l'élaboration de conventions, de règlements, de normes[11], de chartes…

◆ Protection du patrimoine technologique

La sécurité des systèmes d'information (SSI) déborde le cadre de l'entreprise. Elle est désormais un enjeu national stratégique, politique et économique [12].

Les 6 recommandations du Rapport Lasbordes

Ces 6 recommandations « 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 ».

Axe 1 :	Sensibiliser et former à la sécurité des systèmes d'information
Axe 2 :	Responsabiliser les acteurs
Axe 3 :	Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence
Axe 4 :	Rendre accessible la SSI à toutes les entreprises
Axe 5 :	Accroître la mobilisation des moyens judiciaires
Axe 6 :	Assurer la sécurité de l'Etat et des infrastructures vitales

11 Rapport « A armes égales » remis au Premier ministre par le Député B. Carayon - Juillet 2006
12 « Sécurité des systèmes d'information, un enjeu majeur pour la France » - Rapport au Premier ministre - Janvier 2006

Pour l'entreprise, ses patrimoines, qu'ils soient intellectuel, technique, scientifique, informationnel ou économique constituent des actifs stratégiques. La défense de ces actifs est devenue un enjeu vital dans un environnement mondialisé et de plus en plus concurrentiel. Or, ces patrimoines sont aujourd'hui au cœur des systèmes d'information (SI) informatisés de l'entreprise.

Les risques liés à l'informatique, et susceptibles de porter atteinte au patrimoine de l'entreprise, se classent en trois catégories :

- les **menaces**, pesant sur les actifs à protéger,
- les **vulnérabilités** de ces actifs,
- leur **sensibilité**, définie selon le degré de disponibilité, de confidentialité et d'intégrité des données.

◆ Les menaces

On constate un phénomène d'intensification des menaces dû à leur diversité, leurs imbrications, leur vitesse de propagation qui s'explique par des interconnexions et une interaction grandissantes. Les conséquences de ces menaces, qu'elles émanent d'actions malveillantes ou de risques mal maîtrisés, peuvent peser lourdement sur les différents métiers de l'entreprise. Les dommages se déclinent souvent en termes financiers, en impacts logistiques ou sur l'image de l'entreprise, etc.

Elles peuvent être de nature humaine, physique ou logique :

- humaine : usage abusif d'Internet, violation des correspondances, de la propriété intellectuelle, traitement non-déclaré de données personnelles, rumeurs, usurpation d'identité, fraudes, etc.
- physique : sinistres (incendies, inondations, sabotages, vols de matériels), défauts / dysfonctionnement systèmes, risques liés à l'introduction de nouvelles technologies (nomadisme, wifi, etc.).
- logique : malveillance (interne et externe), attaques (vers, virus, phishing, spamming, etc.), vol / perte / suppression / altérations d'informations, manque de connaissances et de sensibilisation des acteurs, criminalité / terrorisme, etc.

En septembre 2005, le CIGREF a réalisé une enquête[13] auprès de ses membres, afin de connaître leurs degrés de sensibilité selon les types de menaces :

100%	les malveillances internes ou externes liées à l'utilisateur
94%	les atteintes aux données personnelles
87,5%	les attaques telles que virus, vers, phishing, spamming… qui laissent apparaître des failles favorisant les intrusions ou la manipulation des données
75%	l'intrusion dans le SI, ouvrant illégalement l'accès à des données ou à des programmes et entraînant le vol, la perte, la suppression ou l'altération des données
74%	la violation du secret des correspondances
74%	les usages juridiquement non-conformes du SI, tels que la violation du secret des correspondances
68%	le non respect des règles d'archivage
65%	la cybersurveillance
65%	le non respect de la propriété intellectuelle
62,5%	les sinistres, tels que le vol, l'incendie, le dégât des eaux, entraînant une perte de matériel et/ou de données

13 Enquête réalisée dans le cadre des auditions menées par le Député P. Lasbordes sur la Sécurité des SI

Les vulnérabilités

Les innovations technologiques, le développement de l'entreprise étendue, l'évolution des méthodes de travail (connexion à distance, travail collaboratif, etc.) oblige le système d'information à s'adapter pour faciliter le travail en réseau de toutes les parties prenantes (clients, fournisseurs, donneurs d'ordre, partenaires, pouvoirs publics). Cette interdépendance de l'ensemble des acteurs augmente le degré de vulnérabilité du SI. La multiplication des interconnexions est source de nouveaux risques pour l'entreprise, ajoutés à ceux provoqués par le déploiement du nomadisme.

De multiples sources de vulnérabilité en découlent, émanant :

- de l'entreprise elle-même : externalisation, informations non classifiées, absence de traçabilité,

- de l'individu : non respect des réglementations, ignorance ou sous-estimation des risques, inadaptation des compétences à certaines fonctions critiques, inconscience et ignorance de menaces liées aux contacts d'affaire, multiplication des acteurs,

- des logiciels: complexité croissante souvent source d'erreurs difficilement détectables, éventuelles failles délibérées (back doors),

- des réseaux de communication : entreprise étendue, nomadisme,

- de l'écosystème informatique : concurrence, dépendance vis-à-vis de fournisseurs, etc.

La sensibilité

La sensibilité porte sur la vulnérabilité des technologies présentes dans le SI : systèmes d'exploitation, logiciels, processeurs, périphériques, etc. Elle peut viser également des zones ou des points spécifiques du SI. Elle augmente les risques, notamment sur la divulgation ou la modification des données, leur origine, leur disponibilité, la répudiation de transactions financières ou l'authentification des utilisateurs, le contournement des contrôles des accès…

Quelle que soit l'origine des failles du système d'information, celles-ci représentent autant de risques contre lesquels l'entreprise doit se prémunir grâce à une politique de sécurité adaptée.

Protection du patrimoine Informationnel

La définition d'une politique optimale de sécurité du système d'information suppose une prise en compte globale des dimensions de sécurité et de sûreté. Elle est définie et pilotée par un Responsable de la Sécurité des Systèmes d'Information (RSSI) qui veille également à sa bonne application et à son respect. Elle implique aussi le Directeur des Systèmes d'Information (DSI), les auditeurs internes, les risks managers et les juristes.

Mettre en place une politique globale de sécurité et de gestion des risques permet à l'entreprise de se prémunir contre les risques susceptibles de porter atteinte à tout ou partie de son patrimoine, de garantir l'intégrité de son système d'information. Abordée de manière globale et systémique, elle sensibilise tous les utilisateurs à l'ensemble des problèmes de sécurité : protection et sécurisation des données, des réseaux informatiques, des systèmes d'exploitation, des applications, des télécommunications, et sécurité physique.

La sécurité des systèmes d'information en vigueur dans les grands groupes suit l'évolution des risques. Elle est régulièrement auditée et ajustée, ce qui permet notamment de mettre l'accent sur l'industrialisation et l'intégration des processus de sécurité (gestion des correctifs, gestion des identités, prise en compte du risque fournisseur…), le renforcement du reporting (lié aux nouvelles exigences réglementaires), la généralisation de la formation et de la sensibilisation des utilisateurs (responsabilisation).

Adaptée à la culture de l'organisation, cette politique doit être homogène, toujours équilibrée entre usages du SI et contraintes. Globale mais sélective et ciblée, elle se doit d'être pragmatique, synthétique et compréhensible. Elle sera d'autant mieux vécue si elle s'accompagne d'un volet « formation » destiné à sensibiliser les utilisateurs.

◆ La démarche

La démarche ne se limite pas à la seule approche technique (architecture). Elle s'oriente vers une gestion organisationnelle, méthodologique et humaine des failles. Deux temps pour définir une politique globale de sécurité des systèmes d'information :

- en amont : analyse de risques, définition d'une charte d'usages des ressources informatiques, classification et traçabilité des informations, etc.
- en aval : audits et contrôles internes / externes, tests d'intrusions, reporting et tableaux de bord, ajustement, formation continue, etc.

La démarche consiste à définir les règles et procédures organisationnelles visant la protection du patrimoine de l'entreprise. Elle intègre à tous niveaux la sensibilisation et la responsabilisation des utilisateurs à l'usage des ressources informationnelles. Ainsi, une bonne politique SSI s'accompagnera par exemple d'une charte d'usages. Les ressources technologiques offrent chaque jour davantage de potentialités mais elles créent des risques liés à des utilisations non-conformes. Ces comportements peuvent générer des failles dans le système d'information menaçant la sécurité du patrimoine de l'entreprise.

Afin de mieux appréhender ces risques liés aux mésusages des technologies, il est souhaitable de compléter une bonne politique de sécurité par des règles déontologiques spécifiques au système d'information[14]. Ces règles n'ont pas d'objectif moralisateur, pas plus celui de standardiser les comportements, mais bien de donner des repères sur les conduites que l'entreprise attend de ses collaborateurs.

14 Rapport CIGREF - Déontologie de l'usage des SI - 2006

Pour conclure

L'alignement entre l'entreprise et ses environnements, allié à la mise en œuvre opérationnelle de nouvelles formes de coopérations, revêt une dimension stratégique de première importance. La captation et la réponse aux stimuli de l'environnement, la lecture des évènements, la production de décisions qui en découlent sont de nature à permettre aux dirigeants d'optimiser la performance de leur firme en créant des opportunités stratégiques et en identifiant des niches d'innovation.

Grâce aux TICCC[14] et à la nouvelle alchimie de l'intangible qu'elles diffusent au sein de l'entreprise, nous sommes entrés aujourd'hui de plain-pied dans une économie postindustrielle marquée par une très forte valorisation des actifs immatériels comme le savoir, la connaissance et l'intelligence collective partagée.

«… *le traitement informatisé des données devient pour la production de connaissances ce que l'électricité, puis les robots ont représenté pour la production matérielle*[16] …»

Dès lors, au même titre que son patrimoine physique se pèse, se mesure et se compte, l'entreprise doit veiller et protéger son « capital immatériel ».

Les stratégies de différenciation, de plus en plus complexes, amènent les entreprises à considérer l'information comme une « ressource stratégique » à part entière, génératrice de valeur. L'information est « *intégrée comme bien immatériel à l'outil de travail. Elle est à ce titre une source collective de profit et une des garanties de la pérennité de l'entreprise*[17]».

En alimentant tous les rouages de l'entreprise, l'information joue donc un rôle moteur dans son fonctionnement. A l'état brut, les gisements d'informations sont considérables. C'est la maîtrise de leurs flux en temps réel, à tout moment et en tous lieux qui est bel et bien devenue, pour le dirigeant, un enjeu majeur en termes de performance et de compétitivité en créant la connaissance stratégique, à vocation opérationnelle.

Dans ce contexte, le système d'information est jugé «… *comme une ressource critique pour le déploiement des capacités d'innovation, le management des activités en réseaux et le maintien d'une identité organisationnelle forte*[18]…».

L'enjeu de la protection des patrimoines technologiques et informationnels de l'entreprise est donc bien la maîtrise des risques liés au cycle de l'information dans un contexte d'entreprise étendue et dans un environnement géopolitique incertain. Certes, l'Intelligence Economique d'Entreprise n'est pas, une fin en soi, mais un moyen pour atteindre les objectifs vitaux que sont la sécurité, la compétitivité et l'innovation permanente. Ces objectifs vitaux sont de la responsabilité première des dirigeants[19].

15 Technologies de l'Information, de la Communication de la Connaissance et de la Coopération
16 Le Cercle des Economistes
17 Œuvre collective du Commissariat Général du plan, 1994, Intelligence Economique et stratégie des entreprises, La documentation française, Paris
18 Bounfour A. Epinette G. « Valeur et Performance des Système d'Information : Une nouvelles approche du capital immatériel de l'entreprise». Dunod, 2006
19 Extrait d'un texte publié sous le titre « Gestion des risques informationnels dans l'entreprise et sécurité des systèmes d'information » - ouvrage collectif sous la direction d'Alice Guillon : « IE et gestion des risques » Pearson, juillet 2007

Index

L'ensemble des mots-clés utilisés dans l'ouvrage est repris ici dans l'ordre alphabétique.

Les références indiquées renvoient aux numéros des fiches, suivi de la lettre C pour la partie " Contexte ", E pour " Enjeux ", R pour " Recommandations " ou S pour " Solutions envisageables " et Préf. pour Préface, Fich. pour Fiches, Int pour Introduction.