ORCA SECURITY
www.orcasecurity.fr

avril 08

Traitement sécuritaire de l'information

A chacun son regard pour sortir du brouillard

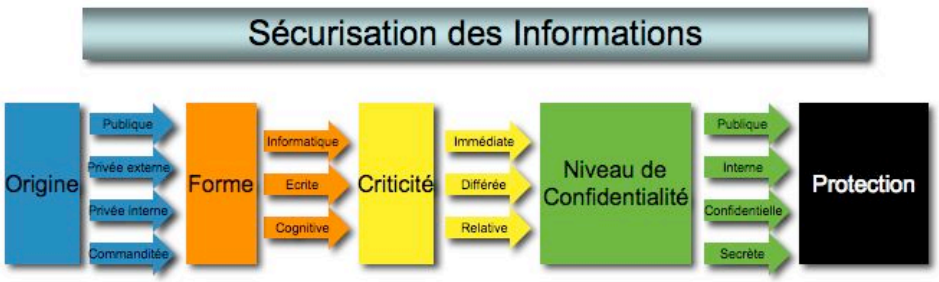
A l'heure où la circulation d'une information dépasse la vitesse du son pour atteindre l'autre bout de la planète en quelques secondes, à l'heure où la valeur de l'information n'a jamais eu autant d'importance, où sa diffusion peut en quelques instants détruire ou promouvoir une entreprise, nous entendons tous, et sommes parfaitement convaincus, qu'il faut protéger efficacement celle-ci.

Chacun a sa version de ce qu'est une information et comment la protéger. Notre étude n'a pas pour vocation de bouleverser la compréhension de ce qu'est une information telle qu'elle est comprise dans une approche d'intelligence économique ; nous souhaitons éclairer le débat sous un angle un peu différent.

- Comment y voir plus clair ?
- Comment mettre en cohérence l'information, la sécurité à y apporter et la structure de l'entreprise ?

A défaut de réponses « sur-mesure » inenvisageables par le nombre de cas à traiter, ou de réponses « prêt-à-porter » inutiles, nous essaierons ici une approche pragmatique du traitement sécuritaire de l'information et de proposer certaines clefs de réflexions aux dirigeants d'entreprises pour les éclairer et pouvoir engager des actions de sécurisation « à leur mesure ».

Piloter une entreprise c'est avant tout traiter de l'information.
On ne traite pas une information de la même façon suivant
son origine, sa forme, sa criticité, sa confidentialité, ou sa situation dans sa durée de vie.

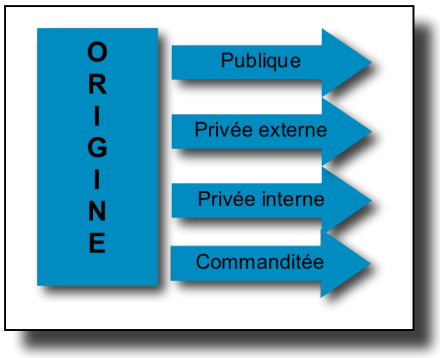


Par Laurent SCHMITTE, Président d'ORCA SECURITY

Sommaire

Le mode de sécurisation d'une information peut-il dépendre de son origine ? 3
Publique 3
Privée externe 3
Privée interne 3
Commanditée 3
Quelles précautions prendre en fonction de l'origine de l'information ? 3
Les informations publiques 3
Les informations privées collectées à l'extérieur 3
Les informations issues de l'entreprise 4
Les informations commanditées 4
Le mode de sécurisation d'une information dépend de sa forme. 4
Informatique 4
Orale, comportementale ou cognitive 5
Ecrite 5
Quelle sécurité pour quelle forme d'information ? 5
La sécurité informatique 5
Les informations intangibles 6
Les informations écrites 7
Quelle sécurité en fonction de la criticité de l'information ? 8
La criticité immédiate 8
La criticité différée 8
La criticité relative 9
Quelles mesures prendre en fonction de la criticité d'une information ? 9
La criticité immédiate 9
La criticité différée 9
La criticité relative 9
Le mode de sécurisation d'une information dépend de sa confidentialité. 10
Comment évaluer le niveau de confidentialité ? 10
Quelques solutions 10
La sécurisation d'une information doit-elle varier dans le temps ? 11
Une information n'a pas la même valeur dans le temps. 11
Types de variations 11
Conclusion 12

Le mode de sécurisation d'une information peut-il dépendre de son origine ?



Quelles sont les origines possibles de l'information ?

Publique

Il s'agit de toutes les informations publiées telles qu'articles, publicités, publications légales, communications audiovisuelles, diffusions sur Internet, conférences, petites annonces, lois et décrets, …

Privée externe

Nous recensons ici les informations résultant d'entretiens privés, de conversations, de courriers, de séminaires, ayant un lien direct ou sans lien apparent avec l'entreprise mais dont l'interprétation peut amener à son exploitation et qui peut donc avoir un impact sur l'image de la société.

Privée interne

Il s'agit de toutes les remontées d'informations obtenues lors des réunions, sessions de *debrieffing*, réunions de crise, pauses-café, et tout échange informel.

Commanditée

Ce sont les informations qui sont le résultat d'une analyse demandée par l'entreprise à un service ou un membre de l'entreprise, à un cabinet de conseil, un fournisseur, un avocat, …, dans un but déterminé, s'inscrivant dans un projet d'entreprise ou dans une démarche d'intelligence économique.

Quelles précautions prendre en fonction de l'origine de l'information ?

Les précautions à prendre peuvent être entrantes ou sortantes : quelles précautions prendre au moment où l'on reçoit l'information ; quel niveau de confidentialité attribuer à l'information offerte par l'entreprise ?

Les informations publiques

La précaution entrante à prendre est la validation de l'information. Ce n'est parce qu'elle provient d'un quotidien, du journal télévisé ou de la bouche d'un ministre qu'elle est avérée !
Il n'y a pas de précaution particulière à prendre quant au relais de l'information en interne ou en externe de l'entreprise, cependant l'information relatée peut être une fausse rumeur apte à mettre en péril l'équilibre financier ou l'image de la société ou d'un concurrent (affaire Perrier) ; en ce cas une gestion de crise s'imposera.
Si l'information publique se révèle être bénéfique pour l'entreprise, sa propagation doit être organisée par le service marketing et les forces commerciales.

Les informations privées collectées à l'extérieur

Il convient de prendre beaucoup de précaution vis-à-vis de la véracité de ce type de sources. Les informations ont pu vous être transmises dans le but de vous manipuler ou bien, au contraire, de vous faire plaisir avec le risque qu'elles soient largement amplifiées et donc

tout aussi dangereuse à retransmettre telles quelles (votre concurrent ne va pas bien et il va déposer le bilan, votre directeur commercial a postulé chez xxx, le marché que vous visez est perdu d'avance, …). Lors d'un entretien avec un client ou un prospect, il est toujours plus judicieux de ne pas évoquer une rumeur ; en la matière le silence est d'or.

Les informations issues de l'entreprise

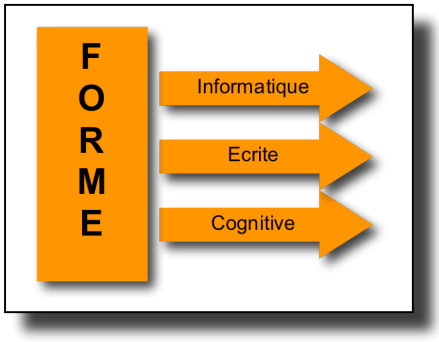
Elles sont réputées plutôt fiables. Attention toutefois à bien différencier rumeur et information valide.
Les seules précautions entrantes à prendre vis-à-vis de ce type d'information sont liées à la compétence de la personne ou des personnes qui les ont établies ou de leur lien réel avec la source. Pour éviter toute désinformation il convient de valider la fiabilité de la source plus que de la personne rapportant l'information.
Les mesures à prendre concernant la divulgation de ces informations sont relatives au niveau de confidentialité qu'elles requièrent (voir chapitre dédié).

Les informations commanditées

Ce sont des informations qui ont été vérifiées et validées par leur source (cabinet de conseil, comité de projet, …) ; elles sont le produit d'une réflexion compétente. A ce titre les précautions entrantes peuvent être de faible niveau ; attention toutefois car des experts peuvent toujours se tromper.
La diffusion de ces informations est très majoritairement soumise à des critères de confidentialité élevés. Elles auront besoin d'être protégées.
Le lieu où les réflexions se sont tenues (salle de réunion, bureaux, atelier, …) doivent aussi avoir été sécurisés :

- Des haut-parleurs dans les faux plafonds font d'excellents micros simplement en les branchant en entrée plutôt qu'en sortie sur l'amplificateur,
- un conduit de cheminée est aussi un tunnel d'écoute,
- un ordinateur équipé d'un microphone et connecté au réseau est tout autant une faille de sécurité
- l'usage des téléphones portables peut aussi devenir un enjeu
- …

Le mode de sécurisation d'une information dépend de sa forme.



Quelles sont les formes possibles de l'information ?

Informatique

Dans cette catégorie on recense notamment les fichiers de traitement, bases de données, fichiers vidéo ou audio, e-mails, et tous les fichiers du système informatique.
L'information est alors représentée par des fichiers ou des blocs, elle est stockée sur un support magnétique, optique, magnéto-optique ou mémoire ; disques, bandes, clefs USB, cartes mémoires, DVD-Rom, etc...

Les autorisations et les droits d'accès aux systèmes d'information sont des « méta data » de la sécurité qui conditionnent sa disponibilité. Une forme plus souple de la sécurité de l'information est aussi sa disponibilité. Cela peut être un effet secondaire de la sécurité de l'information : l'information inaccessible ne sert pas l'intelligence de l'entreprise qui la possède…

Orale, comportementale ou cognitive

Ces informations au service de l'entreprise correspondent au savoir-faire de chaque membre de l'entreprise, aux informations détenues par chacun qu'elles aient été formalisées ou pas. C'est le capital intellectuel de l'entreprise. C'est aussi la forme la plus délicate à traiter car l'intangible a cette particularité de n'avoir comme valeur que celle que veut bien lui donner son propriétaire et tant que cette information n'est pas partagée, elle ne peut profiter à l'entreprise et elle ne peut être protégée.

Ecrite

Il s'agit là de tout document papier, du simple Post-it au brevet en passant par tous types de courriers, notes de services, états informatiques, photos, schémas, …, ainsi que toutes les informations que l'entreprise livre et qui peuvent être imprimées et sauvegardées par tous, telles que celles affichées sur le site web de l'entreprise.

Quelle sécurité pour quelle forme d'information ?

La sécurité informatique

En raison des nombreuses informations et recommandations existantes sur le sujet, nous nous étendrons peu sur le sujet.

Observons toutefois quelques constatations surprenantes :

- Plus de 80 % des préjudices informatiques proviennent du personnel de l'entreprise alors que 80% des dépenses sont affectés à la protection de l'information vis-à-vis des menaces extérieures.
- Le propriétaire de l'information contenue dans un fichier informatique est l'utilisateur de cette information. Pourtant l'accès au contenu des fichiers est quasiment toujours accessible au personnel de la Production Informatique et tout aussi souvent au service Etudes de l'entreprise.
- Pratiquement tous les logiciels de sauvegarde copient les fichiers « en clair », c'est-à-dire non cryptés. Certains effectuent comme cryptographie une simple permutation d'octets. Il est beaucoup plus facile et moins coûteux de se procurer une copie des sauvegardes d'une entreprise plutôt que d'essayer de pénétrer son système informatique par le réseau.
- Les grosses baies de stockage disposent même parfois d'une option de maintenance à distance via une ligne téléphonique. Le constructeur vous jure qu'il ne peut pas accéder aux données, admettons, il peut toutefois reformater partiellement ou totalement la baie de stockage. Si vous avez mis en place un service de réplication immédiate sur un site distant, il y a fort à parier que l'effet sera propagé.
- Penser au pouvoir d'un supérieur hiérarchique sur un jeune ingénieur qui exigera de lui le « mappage » de la base Outlook d'un employé pour monitorer son courrier électronique en temps réel. Les conséquences pour l'individu et pour l'entreprise peuvent être catastrophiques.

Protéger l'accès à son système d'information est important, protéger la donnée elle même est encore plus indispensable, or, force est de constater que la cryptographie n'est, au mieux, utilisée que pour les échanges de mails et les paiements en ligne. Pourquoi ne pas l'utiliser pour protéger les fichiers sensibles : projets de R&D, fichiers du personnel, documents confidentiels, … ? Encore faut-il utiliser un système de chiffrement à la hauteur du niveau de protection désiré. Voir sur le Blog ORCA l'article sur les 48 millions de carte bancaires piratées → www.blog-intelligence-economique.fr

Les informations intangibles

Comment protéger l'impalpable ? Comment empêcher un employé de sortir ou répandre une information pouvant nuire à la société, de façon intentionnelle ou par négligence ?

Il y a 3 décennies un salarié faisait carrière dans son entreprise. Le modèle en la matière était sans nul doute la société Michelin. On travaillait chez Michelin, on était logé chez Michelin, on faisait ses courses dans les supermarchés de Michelin, on faisait du sport sur les terrains de Michelin, …, bref on vivait Michelin. Chacun s'appropriait l'entreprise, la défendait.
Aujourd'hui la valorisation de sa carrière passe par le changement régulier d'entreprise. On ne s'attache plus et il arrive même que l'on nuise publiquement aux intérêts de l'entreprise qui nous emploie.

Si il n'y a pas de recette miracle en la matière il y a toutefois des précautions et des actions à mettre en place :

- Recréer un esprit d'entreprise
- Récompenser la captation légale d'informations utiles sur la concurrence
- Définir un contrat de travail mettant l'accent sur la confidentialité de la vie en entreprise
- Accompagner ses futurs concurrents
- Cultiver le partage et la formalisation de la connaissance

Recréez un esprit d'entreprise

C'est la pierre angulaire de la conscience collective.

- ne dites plus « faites… », « il faut que vous… », dites « nous devons » « notre entreprise »
- la critique doit toujours être positive
- valorisez le travail de vos employés
- sachez dire « c'est bien, bon travail ! »
- partagez les repas avec tous vos employés
- récompensez l'esprit d'initiative, l'apport d'idées ou de nouveaux marchés
- établissez un outil de communication interne
- …

Récompensez la captation d'information utiles sur la concurrence

Sensibiliser son personnel à l'intelligence économique en récompensant la remontée d'informations sur un concurrent c'est par là même mettre un projecteur sur l'importance du silence à tenir quand on se trouve à l'extérieur de l'entreprise.

Améliorez le contrat de travail

Pour les commerciaux et les cadres, Il comporte souvent un paragraphe concernant la confidentialité des informations mises à la disposition du salarié, ce paragraphe doit être généralisé. Il existe également des politiques de sécurité de l'information et des formations pour s'y sensibiliser et s'y conformer avec clause réglementaire et unanime, annexe du contrat de travail.
Le contrat doit aussi comporter une clause exigeante concernant le comportement global de l'employé à l'extérieur de l'entreprise quand à toute déclaration ou dénégation de l'entreprise.
Le règlement intérieur de l'entreprise permet aussi de préciser certaines règles et bonnes pratiques.

Accompagnez vos futurs concurrents

Un commercial menace de quitter l'entreprise et de s'installer comme concurrent en risquant de partir avec une partie de votre clientèle ? Cela s'observe très (trop ?) régulièrement.

Pourquoi, plutôt que de laisser partir ce commercial de façon litigieuse, ne lui proposeriez vous pas de l'aider à s'installer en apportant 30 ou 50% du capital (en prenant soin d'avoir tout de même la minorité de blocage) ?
Si cela est possible vous avez tout à y gagner, si l'entreprise devient florissante vous rattraperez une partie de la perte de clientèle que vous auriez été amené à subir ; si l'entreprise ne décolle pas vous aurez très certainement évité un procès en prud'homme (devenu une habitude) et les exigences en terme d'indemnités de départ du salarié auront certainement été moindres.

Valorisez la connaissance
Le Knowledge Management (KM) est une démarche stratégique pluridisciplinaire visant à atteindre l'objectif fixé grâce à une exploitation optimale des savoirs de l'entreprise. Avec une telle démarche celle-ci part de son objectif et accepte de modifier éventuellement son mode de management.
Le KM permet entre autre de prendre des mesures de précaution du capital intellectuel de l'entreprise vis-à-vis de problématiques sociales telles que le « papy-boom » engendrant une perte de savoir-faire, le turnover, la délocalisation, la restructuration, … Le KM permet aussi d'Améliorer la qualité des produits, d'harmoniser les bonnes pratiques de fabrication, de fidéliser la clientèle, d'harmoniser la Gestion de la Relation Client.

Les informations écrites

Elles sont diffusées à un moment ou à un autre par l'entreprise par différents vecteurs

- les brochures commerciales et publicités
- les services de Relations Presse
- les sites webs
- les courriers divers sortant de l'entreprise

les brochures commerciales et publicités
La vocation des publicités étant une diffusion au plus grand nombre, elles ne sont confidentielles, pour en éviter la copie, que jusqu'à leur diffusion. Auparavant elles sont détenues par la société ou le service de communication et par l'imprimeur. Seule une clause de confidentialité dans le contrat avec le prestataire permet de limiter les risques.

Le services ou sociétés de Relations Presse
Elles sont toujours soumises à une déontologie de confidentialité. Le risque est donc lié à une mauvaise communication ou à une mauvaise interprétation d'un journaliste. Quand il ne peut y avoir de droit de regard sur l'article, seule une procédure de gestion de crise efficace peut limiter la casse ; d'où l'importance de la préparation des entretiens avec les journalistes. Tout ce que vous dites à un journaliste peut être retenu contre vous ; si vous ne voulez pas qu'il parle d'un de vos prospects chauds, ne lui dites rien !

Les sites webs
Comme pour les brochures commerciales, vous en maîtrisez le contenu, sauf que…

- il faut faire attention à ce qu'une nouveauté sur le site web ne soit pas malencontreusement accessible avant sa publication officielle.
- Il faut être prêt à ce que toutes les pages soient explorées et dépouillées par votre concurrent.

Les courriers divers sortant de l'entreprise
Le problème est ardu. Comment éviter qu'une note de service ou un document confidentiel ne se retrouve entre les mains d'un confrère ?
Nous suggérons une approche logique et une approche technologique.

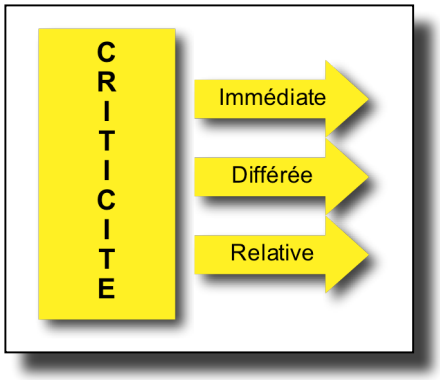
L'approche logique vous suggère de catégoriser les informations écrites en fonction de leur niveau de confidentialité : publiques, internes, confidentielles, secrètes (voir chapitre sur la confidentialité). Tout document devrait comporter de façon explicite ses conditions de diffusion.

L'approche technologique permet une traçabilité des documents édités.

- une **étiquette RFID** sur les documents originaux d'un contrat (émetteur passif de fréquences radios qui s'active à proximité d'une antenne, comme les systèmes anti-vol des magasins). Un photocopieur peut être programmé pour ne pas fonctionner à l'approche d'une étiquette RFID.
- un **papier filigrané** particulier ou un système de marquage du papier [1]
- un **papier non-photocopiable** [1]

L'un n'empêchant pas l'autre, nous vous conseillons de mettre en œuvre ces deux visions.

Quelle sécurité en fonction de la criticité de l'information ?



Une information est critique quand elle est absolument nécessaire au bon fonctionnement de l'entreprise. Le taux de criticité d'une information dépend de l'urgence dans la disponibilité de l'information. Nous avons retenu trois niveaux de criticité.

La criticité immédiate

Cela cible les informations les plus vitales à la vie de l'entreprise.
Elles sont généralement gérées par le système d'information.
Mais il y a aussi d'autres informations, non gérées par le système informatique et qui ont un taux de criticité immédiat :

- le code d'accès de la porte de l'usine ou de la salle informatique, il doit être connu de plusieurs personnes ou bien les locaux doivent avoir une 2e entrée.
- Le paramétrage des machines pour la fabrication d'une pièce à livrer en urgence
- La connaissance d'un incident sur un lieu de production ou chez un client
- …

La criticité différée

Cela concerne les informations dont on sait qu'elles sont incontournables mais pour lesquelles une certaine tolérance dans le délai de disponibilité est acceptable.
Là aussi beaucoup de ces informations sont gérées par le service informatique.
En dehors de ce contexte on peut aussi citer quelques exemples :

- les plans de fabrication de pièces de rechange dont on a encore quelques stocks
- le planning des congés d'été
- une loi de finance particulière ou une nouvelle réglementation
- …

[1] ORCA SECURITY propose ce type de produit

La criticité relative

Une information dont la criticité est relative ne signifie pas pour autant qu'elle n'est pas importante et ne nécessite pas d'attention particulière ; cela signifie simplement que si elle vient à manquer, la survie de l'entreprise ne sera pas en jeu.

Quelles mesures prendre en fonction de la criticité d'une information ?

Les précautions à prendre peuvent très onéreuses mais l'avenir de l'entreprise est en jeu. La principale difficulté réside dans l'identification de ces informations ainsi que dans l'évaluation de leur taux de criticité.

La criticité immédiate

Pour les informations qui sont gérées par le système d'information ; c'est le propriétaire de l'information qui doit indiquer au responsable d'exploitation informatique le taux de criticité des informations contenues dans les fichiers informatiques ; à ce dernier ensuite de mettre en place les procédures adéquates.
Les procédures à mettre en place s'inscrivent dans le cadre du Plan de Continuité d'Activité (PCA) ou de haute disponibilité et, pour certaines sociétés, dépendent de la législation : SOX (Sarbanes-Oxley), LSF (Loi de Sécurité Financière), LEN (Loi sur l'Economie Numérique), etc.) et de la réglementation (normes Bâle II, IAS, etc.).

Pour les autres formes de l'information, des procédures particulières doivent êtres mises en place :
- Un coffre-fort dans l'enceinte de l'entreprise,
- Un registre de consignes,
- Des assurances spécifiques aux risques identifiés,
- Le conseil et la prévention
- …

La criticité différée

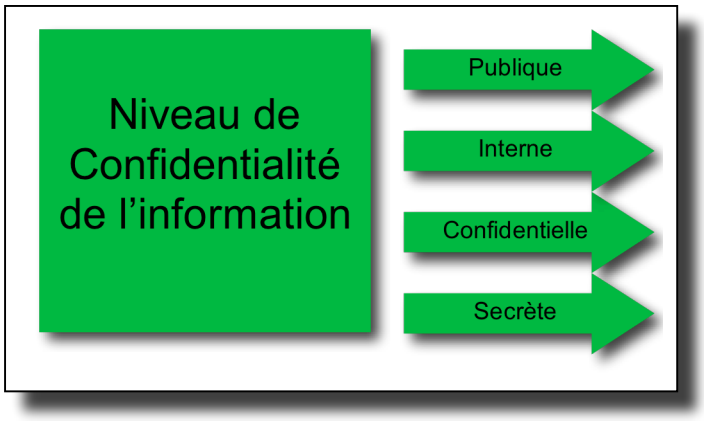
Même remarque concernant les informations gérées par l'informatique que pour la criticité immédiate.
Les informations numériques traitées par le système d'information et à criticité différée peuvent être préservées par un système de sauvegarde régulier (horaire, quotidien, hebdomadaire, … en fonction du taux de criticité). Les procédures à mettre en place dans ce cas de figure s'inscrivent dans le cadre du Plan de Reprise d'Activité (PRA) de l'entreprise.

Pour les autres formes de l'information, des procédures particulières doivent êtres mises en place :
- Un entreposage des documents dans un autre lieu que l'enceinte de l'entreprise.
- Une répartition des stocks dans des lieux géographiques différents
- Des réunions périodiques de partage des informations
- …

La criticité relative

Un archivage sécurisé (papier ou numérique) est souvent une bonne réponse au manquement de ce type d'information. La duplication des informations en des lieux géographiques différents est une garantie supplémentaire.

Le mode de sécurisation d'une information dépend de sa confidentialité.



Toute information doit être évaluée en terme de niveau de confidentialité, ce niveau devrait être attaché à tous types de communication. Seulement en terme de communication orale, nous savons tous qu'un secret partagé n'est plus un secret.

Pour les informations écrites ou sur support informatique, le marquage du niveau de confidentialité est beaucoup plus aisé ; ainsi on pourrait classifier les informations de la façon suivante :

- **Publique** : ouverte à tous (publicité, communiqués de presse, …)
- **Interne** : qui ne doit pas sortir du périmètre interne de l'entreprise mais qui est accessible à tous les employés (évolutions de la société, communication au personnel, nominations, …)
- **Confidentielle** : qui ne concerne qu'une branche ou un service de l'entreprise (Confidentiel Marketing, Confidentiel Ressources Humaines, …)
- **Secrète** : uniquement accessible aux personnes directement concernée (décision de comité directeur ou conseil d'administration, rapport de R&D, …)

Comment évaluer le niveau de confidentialité ?

Exactement de la même façon que l'on a évalué le taux de criticité de l'information : par l'appréciation de l'utilisateur. Seul le comptable de la société sait si les informations contenues dans tel ou tel fichier sont confidentielles ou non ; seul le commercial connaît la valeur de sa base de prospection, de sa base client etc…

Quelques solutions

Une clause dans le contrat de travail doit prévenir l'employé des risques encourus à la divulgation d'informations classifiées comme n'étant pas publiques.

Le marquage sur les documents papier comme « DOCUMENT CONFIDENTIEL » doit être bien visible, si possible toujours positionné au même endroit dans la feuille de papier et répété sur chaque entête ou bas de page.
L'utilisation de supports particuliers tels que papier filigrané ou non reproductible, un marquage systématique et encodé des coordonnées de la personne effectuant une impression, permettent aussi de participer activement à la confidentialité des informations contenues dans les documents.

Le marquage concernant les fichiers informatiques peut se faire de façon simple dans la codification du nom du fichier. La mise en place d'une normalisation des noms de fichiers est aussi un outil de simplification de recherche et des traitements. Ainsi, par exemple, le nom d'un fichier de comptabilité confidentiel pourrait prendre la forme suivante :

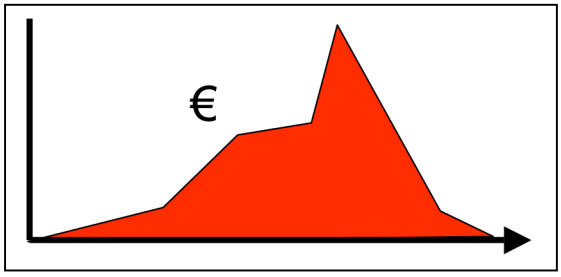
CPTA.PRSL.PARIS.CD.C.080439.doc
où

CPTA	= Comptabilité (identification du service utilisateur)
PRSL	= Personnel (concerne le personnel de l'entreprise)
PARIS	= lieu d'exploitation du fichier (en cas de diverses implantations)
CD	= Criticité Différée
C	= Confidentiel
080439	= numéro de référence du fichier
doc	= nature du fichier

Une telle normalisation permettrait de savoir que tous les fichiers qui ont « C » en 5e argument doivent être cryptés pour être inaccessibles aux personnes non autorisées. « CD » en 4e argument indiquera au service informatique que ce fichier doit rester sur un support disque ou une librairie robotisée pour être rapidement accessible.
A chacun sa norme en fonction de ses besoins.

La sécurisation d'une information doit-elle varier dans le temps ?

Une information n'a pas la même valeur dans le temps.



Certaines informations peuvent passer du niveau « Secret » au niveau « Publique » en quelques secondes, c'est le cas des annonces publiques : vente de la société, entrée en bourse, signature d'un contrat, démission d'un membre important de l'entreprise, publication des résultats annuels ou trimestriels…

Types de variations

Certaines informations ont une valeur relativement stable avec une tendance à croître ou à décroître régulièrement : une base de prospection (en fonction de son niveau de mise à jour), la liste des références clients, un brevet, les plans de conception d'un produit,…

D'autres ont une vocation à prendre presque indéfiniment de la valeur : une base d'intelligence économique (plus elle est renseignée, plus elle a de valeur), le fichier client, les résultats des travaux de R&D, …

Toutes ces évolutions de l'information sont très proches des traitements appliqués lors de la mise en place d'une stratégie d'ILM. ORCA SECURITY a publié un document entièrement consacré à cette approche. Il est disponible sur le site www.orcasecurity.fr, rubrique E-Librairie « Interactions en une politique d'Intelligence Economique et une stratégie d'ILM »[2].

Certaines informations prendront de plus en plus de valeur à chaque fois qu'elles seront diffusées : si l'information est que votre société est unique dans son savoir faire, cette information aura de plus en plus de valeur pour vous avec l'accroissement de sa diffusion. CQFD.

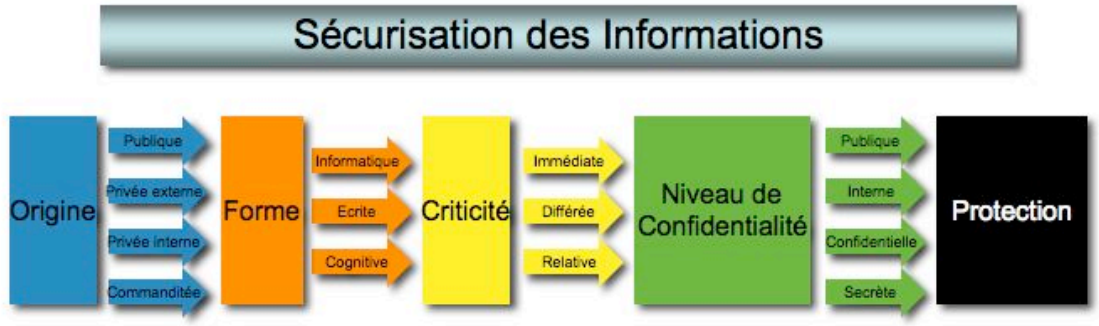
Le niveau de sécurité est donc à adapter en fonction de la valeur de l'information ou de l'effet escompté par sa disparition ou publication à un instant donné.

[2] ILM : Information Lifecycle Management, en français : Gestion du Cycle de Vie de l'Information

Conclusion

Adopter une règle de sécurité spécifique pour chaque cas de figure que nous avons envisagé peut s'avérer inexploitable pour une PME-PMI.
Néanmoins le regard porté sur les aspects de la sécurisation de l'information que nous avons évoqué oblige à prendre conscience de sa propre définition des meilleurs pratiques.

Il vous faudra probablement effectuer des choix ou des regroupements pour vous simplifier la mise en œuvre des procédures, quitte à développer certains aspects plus finement en fonction de vos besoins.



Forme, Origine, Criticité & Confidentialité varient dans le temps.

© ORCA SECURITY - 2008

Il n'y a bien évidemment pas de solution miracle et chaque entreprise doit appliquer des paramètres qui lui sont propres et qui lui permettront d'élever le niveau de sécurité des informations circulantes dans l'entreprise au degré qu'elle aura fixé. Un avis extérieur permettra une vision pragmatique de l'entreprise pour préciser ses objectifs dans le domaine.