



# LE FACTEUR HUMAIN

- Olivier GOMAS
- Yves RAISIN
- Richard ROZIER



Mercredi 06 avril 2005

- Contexte
- Cartographie des risques
- SSI : Facteurs clés de succès
- Documents de responsabilisation des différentes catégories d'utilisateurs
- Communication à mettre en œuvre
- Actions de pérennisation de la sécurité

- 
- LE FACTEUR HUMAIN AU CŒUR DE LA SECURITE
    - Le maillon faible de la sécurité informatique est souvent le facteur humain
    - La sécurité informatique commence par l'éducation de l'utilisateur aux bonnes pratiques informatiques

- **La principale menace** contrairement à ce que l'on pourrait penser, **ne vient pas de l'extérieur mais il s'agit bien du facteur humain c'est-à-dire de l'utilisateur.**
- **La sécurité des systèmes est affaire de tous** dans l'entreprise mais elle nécessite plus particulièrement par les acteurs concernés une technicité et un savoir faire spécifique (informaticien, administrateur réseaux et systèmes, chef de projet informatique et manager)
- **La sensibilisation du personnel à tous les niveaux sur les enjeux, les menaces, les attitudes à observer et les procédures est une composante essentielle du dispositif de protection.** Des actions d'information et de sensibilisation sont menées sur le terrain et souvent intégrées dans des sessions de formation à caractère plus générale.



## **Le facteur humain**

Le management : une nécessaire prise de conscience

Les risques internes liés au facteur humain :

Panorama des risques internes, enjeux associés pour l'entreprise,  
populations les plus exposées

SSI : facteurs clés de succès

- Pourquoi :
  - Responsabilité juridique et pénale des dirigeants :
    - protection des informations nominatives, perte des données & absence de mesures de protection du SI, contrefaçons (piratage logiciel), protection de la vie privée (correspondance), infractions commises en utilisant les ressources de l'entreprise, obligations liées au contrôle fiscal des comptabilités informatisées, Loi LSF & SOX Act, ...
  - La montée en puissance du risque lié au SI

## La SSI : un des moyens permettant à l'entreprise d'atteindre ses objectifs

- Comment
  - Sensibiliser via l'analyse de risques
    - Classification des actifs, menaces, vulnérabilités : **Risques & Enjeux**
  - Intégrer le management et la couverture du risque dans la stratégie globale de l'entreprise
  - Soutenir la mise en œuvre et la diffusion de la PSSI

# Risques internes liés au facteur humain

## Petit panorama (non paranoïaque)

Menaces	D	I	C	exemples de risques	conséquences
<b>Sinistres Physiques</b>					
INCENDIE	X	X		vandalisme (conflit social) par attaque directe ou indirecte (altération moyens détection ou de lutte), négligences dans le transport ou le stockage, renversement de nourriture ou de boissons	destruction de biens, atteinte à la sécurité personnes, perturbations fonctionnement, perte de données
DEGATS DES EAUX	X	X			
POLLUTION	X	X			
SINISTRE MAJEUR	X	X			
DESTRUCTION DE MATÉRIELS OU DE SUPPORTS	X	X			
<b>Perte de services essentiels</b>					
DÉFAILLANCE DE LA CLIMATISATION	X			conflit social, vengeance entraînant le sabotage des équipements, la saturation bande passante ; erreurs de dimensionnement ; absence de maintenance des équipements	perturbation ou arrêt de fonctionnement
PERTE D'ALIMENTATION ENERGETIQUE	X				
PERTE DES MOYENS DE TÉLÉCOMMUNICATIONS	X				
<b>Perturbations dues aux rayonnements</b>					
RAYONNEMENTS ÉLECTROMAGNÉTIQUES	X	X		ludique ou vengeance : brouillage des communications ; absence de coordination dans choix et installations des équipements (brouillage des communications, dégagement de chaleur, ...)	destruction de biens, perturbations ou arrêt de fonctionnement
RAYONNEMENTS THERMIQUES	X	X			
<b>Défaillances techniques</b>					
PANNE MATÉRIELLE	X	X		absence de maintenance des équipements ; erreurs de dimensionnement, d'exploitation ; absence de procédures de qualification ; bases de données non archivées à périodicité régulière ; pas de suivi des ressources (indicateurs alerte) ; processus de maintenance et développement non sécurisé ; absence de documentation ; connaissances non partagées ; non maîtrise des évolutions du SI ; défaillance fournisseurs, TMA ; pb coordination entre différents prestataires (infogérance vs TMA) ; personnalité, crainte licenciement ou vengeance du personnel SI (absence de doc ou protégée)	dysfonctionnements, interruptions de service, indisponibilités, altération ou perte de données
DYSFONCTIONNEMENT DU MATÉRIEL	X	X			
SATURATION DU SYSTÈME INFORMATIQUE	X				
DYSFONCTIONNEMENT LOGICIEL	X	X			
ATTEINTE A LA MAINTENABILITE DU SI	X				

# Risques internes liés au facteur humain

## Petit panorama (non paranoïaque)

Menaces	D	I	C	exemples de risques	conséquences
<b>Compromission des informations</b>					
ÉCOUTE PASSIVE			X	vente de matériel, d'informations (vengeance, avidité, chantage) ou exploitation d'information à des fins de nuire ; personnalité (abus de pouvoir) ; installation de bombes logiques par vengeance ; absence de protection des locaux, du matériel, des documents ; absence d'une procédure de destruction des documents confidentiels (réutilisation en brouillon, poubelles), de destruction des supports ; divulgation par erreur de destinataire de messagerie, réponses à des sollicitations sans vérification origine (social engineering), absence de règles de diffusion des documents selon leur sensibilité ; absence de gestion des habilitations & droits d'accès ; absence de discrétion dans les lieux publics ; absence de protection des laptops ; interventions de tiers non contrôlées ; utilisation de NTIC perso non protégées	divulgation interne et externe, atteinte à la vie privée, dysfonctionnements (matériel de maintenance), destruction ou altération de données, altération de traitements, destruction des protections
VOL DE SUPPORTS OU DE DOCUMENTS			X		
VOL DE MATÉRIELS	X		X		
RÉCUP. SUPPORTS RECYCLES OU MIS AU REBUS			X		
DIVULGATION			X		
INFOS SANS GARANTIE DE L'ORIGINE	X	X			
PIÉGEAGE DU MATÉRIEL		X	X		
PIÉGEAGE DU LOGICIEL	X	X	X		
<b>Actions illicites</b>					
COPIE FRAUDULEUSE DE LOGICIELS			X	Copie de logiciels pour utilisation perso ou vente, utilisation de logiciels copiés ou téléchargés sans acquittement des licences ; mauvaise gestion ou perte des preuves d'acquisition de licences ; destruction ou modification de données suite à conflit ou vengeance (par abus de droits ou usurpation de droits) ; constitution & utilisation de fichiers de données nominatives, utilisation de solution de chiffrements hors législation	atteinte à la vie privée, fraude
UTILISATION LOGICIELS CONTREFAITS OU COPIES	X				
ALTÉRATION DES DONNÉES		X	X		
TRAITEMENT ILICITE DES DONNÉES			X		
<b>Compromission des fonctions</b>					
ERREUR D'UTILISATION	X	X	X	absence de motivation, professionnalisme ; mauvaises conditions de travail ; absence de documentation ; absence de formation ; absence de procédures d'habilitations et de gestion des droits d'accès ; compétences ou habilitations uniques ; mauvaise planification des congés ; conflit social ; arrêt de traitement sans information des responsables (sauvegardes) ; évolutions logicielles sans information ni validation des utilisateurs ;	perte ou altération de données, pertes ou interruptions de services, fraude, perte des moyens de protection, divulgation
ABUS DE DROITS	X	X	X		
USURPATION DE DROITS	X	X	X		
ATTEINTE A LA DISPONIBILITE DU PERSONNEL	X				

### Les enjeux pour l'entreprise :

**compétitivité, conformité réglementaire, pertes financières, image de marque, cohésion sociale, ...**

# Risques internes liés au facteur humain des populations plus exposées

---

- Dirigeants : la détention d'informations très confidentielles, de plus en plus équipés en TIC, de plus en plus nomades ; contrôles plus délicats
- Nomades : un accès à distance au réseau de l'entreprise, une exposition plus forte au piégeage logiciel et matériel, au vol et à la divulgation
- Informaticiens : des droits souvent larges et un accès aux informations confidentielles, la disponibilité et l'intégrité de l'information fortement dépendantes de leurs pratiques
- Stagiaires : un accès souvent large à l'information, une sensibilité moindre à la confidentialité : moins concernés par la culture d'entreprise, une culture universitaire de partage des informations

### ■ Politique d'entreprise & gouvernance du SI

<b>Management &amp; organisation</b>	<ul style="list-style-type: none"><li>Politique d'entreprise, règles de morale et d'éthique appliquées et connues</li><li>Dialogue social permanent, personnel motivé évoluant dans de bonnes conditions de travail</li><li>Organisation définie et adaptée, responsabilités claires et connues de tous</li><li>Gestion des conflits entre personnes</li></ul>
<b>Gouvernance du SI</b>	<ul style="list-style-type: none"><li>Politique Qualité, standards et normes</li><li>Processus de maintenance et développement sécurisé</li><li>Documentation existante (logiciels, exploitation des équipements, ...) et maintenue à jour</li><li>Personnel SI formé, connaissances partagées</li><li>Gestion du parc matériel et logiciel ; licences</li><li>Suivi des pannes &amp; indicateurs préventifs de dysfonctionnements</li></ul>
<b>Formation des utilisateurs</b>	<ul style="list-style-type: none"><li>Documentation des applicatifs existante et maintenue à jour</li><li>Personnel formé, connaissances partagées</li></ul>

### ■ Management de la SSI

<b>PSSI</b>	<ul style="list-style-type: none"> <li>Politique de sécurité des systèmes d'information formalisée et diffusée</li> <li>Soutien de la Direction à l'application de la PSSI</li> </ul>
<b>Classification des actifs informationnels</b>	<ul style="list-style-type: none"> <li>Actifs informationnels identifiés et classifiés selon leur niveau de sensibilité</li> <li>Procédure et gestion des habilitations et droits selon le besoin d'en connaître</li> <li>Personnel sensibilisé aux risques, à la protection des informations &amp; documents confidentiels</li> <li>Engagement individuel à la protection des informations à caractères sensibles, devoir de discrétion</li> </ul>
<b>Protection physique</b>	<ul style="list-style-type: none"> <li>Sensibilisation à la protection des locaux, matériels, et équipements de sécurité</li> <li>Sensibilisation à la nécessaire vigilance lors de l'intervention de tiers sur les équipements et dans les locaux</li> </ul>
<b>Exigences d'utilisation</b>	<ul style="list-style-type: none"> <li>Chartes des exigences d'utilisation des SI et des conditions d'utilisation licite de l'information</li> <li>Formation / sensibilisation au bon usage des SI, droits et devoirs</li> <li>Sensibilisation au risque de sanctions</li> </ul>
<b>Contrôle et suivi</b>	<ul style="list-style-type: none"> <li>Sensibilisation du personnel au devoir d'alerte</li> <li>Traitement, suivi et centralisation des incidents de sécurité</li> <li>Audit du respect des mesures de sécurité (procédures et règles de protection, exigences d'utilisation)</li> </ul>
<b>Gestion de crise</b>	<ul style="list-style-type: none"> <li>Procédures de gestion et d'information formalisées et testées</li> <li>Personnel formé à l'utilisation des moyens de secours</li> </ul>



**Documents de responsabilisation des  
différentes catégories d'utilisateurs du  
Système d'Information**

Mercredi 06 avril 2005

- Les fichiers informatiques doivent être sécurisés et « confidentialisés » face à des intrusions externes ou à des indiscretions internes
- Les fichiers informatiques constituent des **actifs** de l'entreprise qu'il convient de « sauvegarder » et de protéger
- L'existence de mesures d'organisation et de protection du système d'information de l'entreprise doit être démontrable (auditable)

## La responsabilité Pénale

### Article 226-17 du Code Pénal

« Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000 € d'amende »

## La responsabilité Civile (Art 1384 Code Civil)

**La responsabilité civile du dirigeant\* est engagée si par une faute caractérisée de sa part – telle l'absence de sauvegarde – l'entreprise subit une perte de données qui lui soit très dommageable.**

**La responsabilité civile est également engagée face à une absence avérée de mesure d'organisation ou de protection du système d'information de l'entreprise.**

**(\*) : ou du délégué ayant reçu pouvoir officiel du dirigeant (ex: responsable informatique)**

- L'obtention et le maintien d'un niveau de sécurité satisfaisant au sein de toute entité nécessite qu'existe un document regroupant l'ensemble des modes opératoires requis pour y arriver.
- La Politique de Sécurité s'applique, à travers toute la hiérarchie, à l'ensemble des personnes concernées par la maîtrise d'ouvrage, la maîtrise d'œuvre et l'exploitation du Système d'Information du Groupe.
- Elle vise principalement à offrir un cadre de référence destiné à :
  - ✓ Mettre en évidence les objectifs, les besoins, les obligations et les engagements sécurité du Groupe vis à vis de son propre patrimoine
  - ✓ Définir et formaliser l'organisation mise en place en matière de sécurité
  - ✓ Définir les rôles et attributions des acteurs concernés

- Elle a pour objet d'opérer un transfert de la responsabilité pénale du chef d'entreprise vers le préposé délégataire
- Le système d'information devient de plus en plus complexe et il s'avère être une source potentielle de responsabilité pénale pour l'entreprise et son dirigeant au titre d'infractions variées :
  - En matière de contrefaçon (piratage de logiciels au sein de l'entreprise)
  - En matière de respect de l'obligation de sécurité afférentes aux données nominatives (Article 226-16 à 226-24 du nouveau code pénal)
  - Toutes les infractions pénales et civiles susceptibles d'être commises par les salariés sur le réseau en utilisant les moyens de l'entreprise (Article 1384 alinéa 1 du code civil)

## Conditions de validité d'une délégation de pouvoir

---

- Elles ne font l'objet d'aucune disposition légale et c'est la jurisprudence qui a construit son régime juridique.
- Un chef d'entreprise peut s'exonérer de sa responsabilité pénale s'il rapporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue :
  - Des compétences nécessaires (techniques mais également juridiques)
  - De l'autorité nécessaire (pouvoir de commandement)
  - Des moyens nécessaires (budgets)
- De plus, la délégation doit être précise et revêtir un caractère de permanence (personne n'occupant pas temporairement le poste)
- Le chef d'entreprise est tenu d'informer le salarié des conséquences produites par la délégation de pouvoir

- La **sub-délégation** est possible aux mêmes conditions vues précédemment – ainsi un DSI pourrait déléguer en partie ses pouvoirs à un RSSI. Il faut cependant veiller au principe de **non-cumul** des délégations de pouvoir.
- Sur la **forme**, aucune règle ne prévaut ; la jurisprudence admet même la validité d'une DP verbale dès lors que celle-ci est dépourvue d'ambiguïté.

Néanmoins le DSI ou le RSSI ont intérêt à exiger un écrit très précis quant à l'étendue de sa mission et quant au champ exact de la délégation de pouvoir.

- Le contrat de travail contenant une clause d'engagement de confidentialité
- Le règlement intérieur – rarement lu et incomplet
- Les chartes de bonne conduite concernant l'utilisation du S.I permettant de :
  - Identifier les particularités et les contraintes liées à l'activité et à la structure de l'entreprise
  - Tenir compte des pratiques et risques induits (utilisation de modem autonome, téléchargement, forums de discussion, contournement des mesures de protection physique et logique, devoir d'alerte...)
  - Définir les règles d'utilisation des ressources professionnelles et les sanctions prévues
  - Sensibiliser et former les utilisateurs aux risques liés aux S.I
  - Informer sur les lois et réglementations en vigueur

- Respecter le principe de proportionnalité (L120-2 Code du travail)
- Consultation des instances représentatives du personnel lors de l'introduction de nouvelles technologies (CE, CCE, CHSCT L432-2 du CT)
- Information préalable des salariés (L121-8 du CT)
- Déclaration à la CNIL de tout dispositif constituant un traitement automatisé de données personnelles

- Les chartes spécifiques informaticiens :
  - L'administrateur informatique doit assurer le fonctionnement normal des systèmes d'exploitation et des réseaux et veiller à leur sécurité
  - Il ne peut en aucun cas intercepter les messages privés
  - Il n'a pas à exploiter volontairement ou sur ordre de sa hiérarchie, le contenu de la messagerie des salariés (CNIL 2004, correspondance privée, article 8 CEDH, article 9 code civil)
  - L'administrateur est tenu au secret professionnel

## ■ Les chartes spécifiques managers :

- Guide de bonne conduite post IPO (Initial Public Offering) avec notamment le risque du délit d'initié
- Gestion des droits octroyés aux prestataires extérieurs (signature des chartes, gestion des comptes)
- Idem pour la gestion des droits sur mobilité inter-services (exemple conservation des privilèges d'un commercial allant au marketing)
- Bonnes conduites à tenir sur le secret des affaires et la confidentialité de l'information (lieux publics, protection des documents confidentiels,...)
- Communication des ces bonnes conduites à leurs collaborateurs

- Les accords de secret ou CDA (Confidential Disclosure Agreement)
  - accords dont l'objet est la confidentialité des informations transmises par l'une ou l'autre des parties ou faisant l'objet d'un échange mutuel.
  
- Les clauses de confidentialité
  - Paragraphe d'un contrat (Achat, Prestation informatique) dont l'objet principal n'est pas la confidentialité mais qui traite cette question.

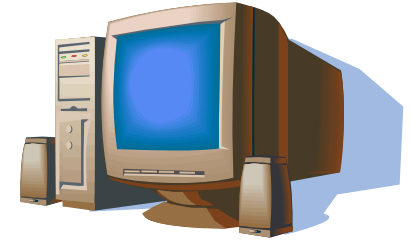
Ces documents sont indispensables et leur signature est préalable à tout démarrage de services ou de prestations avec des partenaires externes

## ■ Objectifs de la Communication

- SENSIBILISER LE PERSONNEL A LA SECURITE
- RESPONSABILISER LES UTILISATEURS



## ■ Objectif par profil d'utilisateur



### – Pour tout utilisateur

- **Connaître la démarche à suivre en cas de problème informatique**
  - Processus de résolution des problèmes les plus fréquents
  - En cas de non résolution savoir où et à qui s'adresser
- **Application et connaissance de la charte**
  - Obligations de l'utilisateur en terme de confidentialité, de sécurité
  - Règles d'utilisation des moyens informatiques
  - Conditions d'accès

- **Les bonnes pratique en terme de sécurité**

- Procédure informatique évolutive permettant de s'adapter à l'évolution de la demande de l'utilisateur
  - Évolutive: aisément adaptable en fonction des besoins, possibilité d'ajout ou de suppression d'instructions élémentaires
  - Diffusable: pouvant être diffusée rapidement et à grande échelle sur les postes des utilisateurs
  - Opérable: exécutable dans l'environnement des utilisateurs
  - Traçable: pouvant être suivie et analysée tout au long de son cycle de vie

## – Pour le service informatique

- **Leur responsabilité dans la définition et l'implémentation d'une politique de sécurité**
  - Obligation légale de sécuriser les données nominatives stockées sur un système d'information (Art.226-16 à 2226-24 du Nouveau Code Pénal)
  - Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment d'empêcher qu'elles ne soient déformées, endommagées, communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000€ d'amende (Art.226-16)
- **Les standards de sécurité**

## – Pour la Direction de l'entreprise

### ▪ **Leur responsabilité**

- L'entreprise sera présumée responsable des personnes et des biens sous sa dépendance et des biens dont elle a la garde
- Pour s'exonérer il faut prouver que la cause est exogène
  - « On est responsable non seulement du dommage que l'on cause de son propre fait, mais encore de celui qui est causé par des personnes dont on doit répondre ou des choses que l'on a sous sa garde » Art 1384 Alinéa 1 du code civil

### ▪ **Les impacts en termes de perte financières, de parts de marché, d'image de marque, de savoir-faire, de poursuite judiciaire**

- Il est nécessaire de chiffrer ces coûts pour en avoir une meilleure vision

## ■ Les moyens de communication

### – Lettre de bienvenue

- Pour les nouveaux utilisateurs
- Informations pratiques

### – Édition d'un guide de la sécurité informatique

### – Charte d'utilisateur

- La charte du bon usage des systèmes d'information doit être à la base de toute politique globale de SSI
- Elle a pour but de formaliser les droits et les devoirs de chacun face à l'outil informatique

### – Le management de la qualité

- Car basé sur les processus métier des services



## – Séminaires, Réunions et Présentations

- Moyen formel d'informer les utilisateurs
- Elles peuvent être organisées de façon régulière suivant les besoins
- Après toute modification et mise à jour
- Permet aux utilisateurs de trouver des réponses, d'échanger des informations et de s'impliquer.
- Elle peuvent être animées par des intervenants externes
- Suivant les besoins spécifiques de l'entreprise

## – Informations sur le site INTRANET de l'entreprise

- Possibilité de consulter des informations dès la connexion sur le site de l'entreprise
- Moyen de communication permanent
- Les informations pourront être facilement et rapidement mises à jour
- **Enquêtes de satisfaction et tests de niveau**

- Les actions de pérennisation dépendant largement de l'activité et du système d'information de l'entreprise
  
- D'un point de vue général, il convient de se poser un certain nombre de questions relatives à la sécurité afin de détecter les points faibles de l'entreprise et la où elle devra fournir des efforts. Pour une efficacité maximale cette analyse doit être effectuée le plus souvent possible.

## – Politique de sécurité informatique

L'entreprise a-t-elle une politique de sécurité de l'information?

- Son objectif étant de protéger ses biens matériels et immatériels (informations)
- Pour une efficacité maximale il est nécessaire:
  - **D'obtenir un soutien clair de la direction générale**
  - De solliciter la participation des différents niveaux hiérarchiques
  - De communiquer la pertinence des procédures de sécurité et leurs avantages dans un langage simple « orienté métier »
  - **Mettre en place les nouvelles procédures de façon progressive et non brutale**
  - Prendre en compte les besoins réels de l'organisation afin de mettre en place des procédures réalistes en fonction du niveau du risque

## – Procédures informatiques

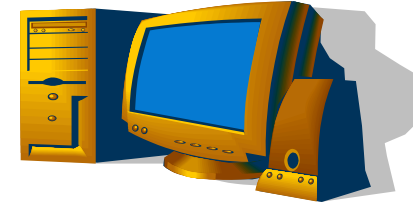
Les procédures de connexion au réseau local (LAN) sont-elles hiérarchisées?

- Sont-elles changées régulièrement?
- Sont-elles réservées à une seule personne?

## – Charte informatique

Existe-t-il une charte de sécurité des systèmes d'information dans l'entreprise?

- Pour être juridiquement valide elle doit être négociée avec les partenaires sociaux et sa publicité doit répondre à un certain formalisme imposé par le droit du travail et la jurisprudence
- Est-elle respectée? Si non, pourquoi?
  - Son non respect peut être dû au fait qu'elle soit méconnue des utilisateurs ou qu'elle impose des contraintes inappropriées ou inacceptables.



## – Matériel informatique

- L'ensemble du matériel informatique de l'entreprise est-il régulièrement recensé dans l'objectif de s'assurer que toutes les machines soient autorisées?
- Il est important d'avoir une vision exhaustive de son parc pour éviter la connexion de machines parasite qui peuvent être à l'origine de problèmes ( défaut de confidentialité, virus, usurpation de droits, envoi de faux mails, etc...)
- **L'usage d'un modem personnel pour se connecter au réseau Internet via le RTC (par exemple) doit être strictement interdit car cette pratique engendre d'importantes vulnérabilités pour le réseau interne.**

## – Pc Portables

- Y a-t-il des consignes particulières pour les utilisateurs de pc portables?

Les pc portables constituent actuellement une vulnérabilité majeure pour les entreprises (Vols du matériel et propagation de virus sur le réseau de l'entreprise)

**Il faut veiller à: - faire des sauvegardes régulières**

- tenir à jour les antivirus
- installer un mot de passe efficace

## – La continuité de l'activité

- Plan de reprise
- Plan de continuité

## – Les Mots de passe

- Les mots de passe sont-ils obligatoires?
  - Sont-ils changés régulièrement?
  - Quelles en sont les conditions?
- Les Mots de passe doivent être strictement personnel, unique et suffisamment « solide » pour résister aux nombreux outils qui permettent de les forcer
- Ils ne doivent jamais être notés près d'un ordinateur et doivent être changés régulièrement
- **Il s'agit d'un basique qui doit permettre de sensibiliser quotidiennement les utilisateurs sur le respect des règles de sécurité**

## – Réactivité du Responsable Informatique

- Quel est le degré d'information du Responsable Informatique concernant l'évolution relative à la sécurité informatique
- Comment se tient-il informé?

- La sécurité des systèmes d'information (S.S.I.) est très évolutive: la menace est protéiforme, des vulnérabilités apparaissent chaque jour ainsi d'ailleurs que de nouvelles parades...

**- Pour ne pas avoir trop de retard, il est indispensable de pouvoir consacrer du temps à des travaux de veille (abonnement à des revues spécialisées, participation à des clubs, forums sur Internet, contacts avec des spécialistes, etc....)**

**Le facteur humain dans la sécurité des systèmes d'information, c'est ...:**

**... une équipe de management et un personnel formé, sensibilisé, responsabilisé  
avec la connaissance de la sensibilité des informations,  
la confiance dans l'organisation, dans le SI, la sécurité du SI ...**

**... la même exigence pour les partenaires de l'entreprise :  
fournisseurs, sous-traitants, intervenants extérieurs, ....  
à qui sont confiées des informations confidentielles,  
et/ou de qui dépend la continuité de l'activité de l'entreprise,  
quel que soit le domaine d'activité du partenaire (production, mktg, design, SI, ...)**