



# **Gestion des Systèmes d'Information**

## **Département Informatique**

**Semestre 3 année 2**



## Table des matières

CHAPITRE 1 : DEFINITION D'UN SYSTEME D'INFORMATION.....	1
Les Hôtels Altéo .....	3
CHAPITRE 2 : SYSTEMES D'INFORMATION DANS UN CONTEXTE DE COMPETITION .....	4
Le Bug de la SNCF : comment l'évolution du système informatique interroge le système d'information, arme stratégique .....	6
CHAPITRE 3 : LES EFFETS DE L'IMPLANTATION D'UN SYSTEME D'INFORMATION .....	8
Un cas parmi tant d'autres... ..	13
CHAPITRE 4 : L'EVALUATION DE LA PERFORMANCE DES SYSTEMES D'INFORMATION ....	15
CHAPITRE 5 : LA SECURITE INFORMATIQUE.....	18
Le «hit-parade» des risques perçus par les entreprises.....	21
Les principes menaces pour les entreprises selon l'ANSSI .....	26

---

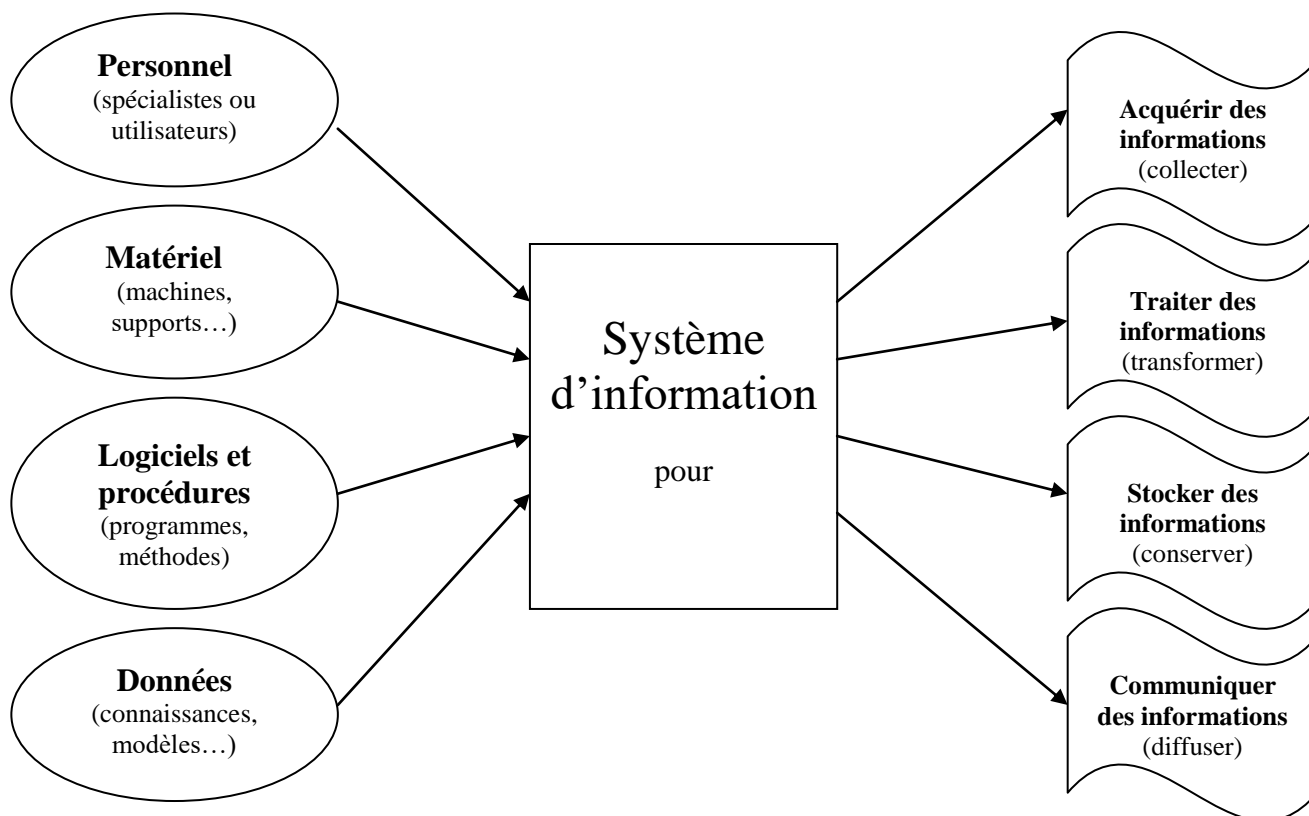
## CHAPITRE 1 : DEFINITION D'UN SYSTEME D'INFORMATION

---

### 1) Définition de R.REIX

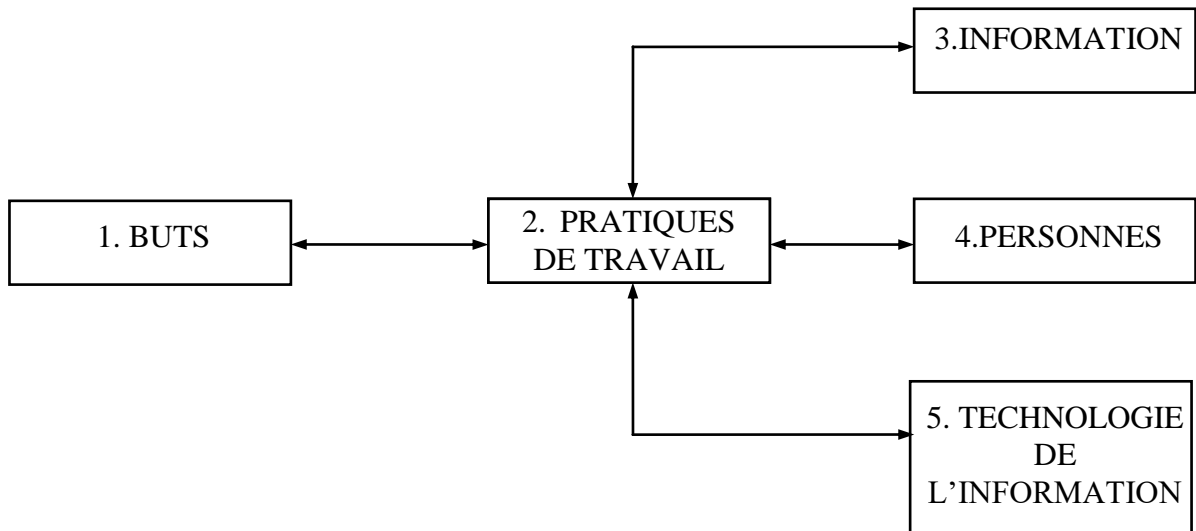
Un système d'information est un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures permettant d'acquérir, traiter, stocker, communiquer des informations (sous forme de données, textes, images, sons, etc) dans des organisations.

#### Les composants d'un système d'information d'après REIX



## 2) Définition d'Alter

« Un système d'information est une combinaison de pratiques de travail, d'informations, de personnes et de technologies organisées pour atteindre des objectifs dans une organisation »



## LES HOTELS ALTEO

(adapté de Steven Alter, "Information Systems, a Management Perspective")

Lors d'une de ses fréquentes visites à ses hôtels, le président de la compagnie ALTEO, monsieur Jacques Marti, en était venu à une constatation importante. Il s'était trouvé derrière le comptoir lorsqu'un employé avait refusé un client qui était prêt à payer 50 € pour une nuit. Ce soir là, toutes les chambres à 50 € étaient réservées. Quelques chambres à 70 € étaient vacantes et le resteraient sans doute. Les hôtels ALTEO venaient donc de perdre 50 € et Jacques Marti se demandait quelle était la politique de la compagnie qui avait amené l'employé à refuser l'accès au client alors qu'il restait des chambres disponibles.

Jacques Marti demanda à l'employé s'il n'était pas possible d'ajuster le tarif des chambres dans ces circonstances. L'employé lui répondit que personne ne lui avait dit de le faire et qu'il n'en aurait sûrement pas pris l'initiative sans instruction claire. L'employé pensait que le prix était le prix et qu'il n'avait pas l'autorité pour le changer.

Le président se demanda alors s'il ne serait pas intéressant d'adopter une politique de prix plus flexible pour accroître les revenus. Ceci pourrait être possible en utilisant l'information contenue dans le nouveau système informatique de réservation qui venait d'être installé. Les employés à la réservation du central téléphonique utilisaient ce système pour les réservations faites d'avance. Les employés des hôtels l'utilisaient également aux comptoirs pour les réservations sur place. Le système comprenait plusieurs informations notamment sur les tarifs standards, par saison, pour chacun des 5 types de chambres. Les réservations spécifient le type de chambre, les chambres sont assignées lorsque les clients arrivent. Le système comprend aussi des informations sur les rabais de quantité pour certaines grandes entreprises.

Pour rendre la tarification plus flexible, le prix des chambres dans le système de réservation pourrait être considéré comme un prix maximum. Si le système de réservation montrait à un moment donné que les chambres les moins chères seraient toutes occupées mais qu'il resterait des chambres plus coûteuses, il serait sensé de louer certaines des chambres de la catégorie supérieure au tarif le plus bas. Ceci pourrait amener à l'hôtel des gens qui auraient logé ailleurs autrement. Cela semblait une bonne idée mais Jacques Marti ne savait pas comment ce système fonctionnerait dans son organisation.

### Questions :

Discuter l'intérêt de la problématique, les avantages et les inconvénients du nouveau mode de fonctionnement.

## CHAPITRE 2 : SYSTEMES D'INFORMATION DANS UN CONTEXTE DE COMPETITION

---

L'internationalisation des marchés a rendu cette dernière décennie la compétition entre les entreprises de plus en plus vive.

Il faut être conscient aujourd'hui que dans ce contexte, un usage adéquat des SI peut constituer une arme stratégique fondamentale. De multiples exemples le démontrent : télévision par satellite, banque à distance, commerce électronique.... Mais le premier cas relevé dans l'histoire des systèmes d'information fut celui de Mac-Kesson :

**L'exemple de Mac-Kesson :** Dans la plupart des pharmacies, jusqu'à la fin des 70's, pour la gestion des stocks, un employé contrôlait l'inventaire, enregistrait les quantités à commander et envoyait par la poste la commande au distributeur. Le distributeur recevait la commande quelques jours plus tard, essayait de satisfaire la commande à partir des produits dont il disposait lui-même en stock, envoyait les produits disponibles à la pharmacie, et commandait les produits manquants à ses fournisseurs. Ce système de distribution n'était pas très efficace :

- il était sujet à des erreurs parce que le nom des produits et les quantités étaient enregistrés et transcrits plusieurs fois,
- il était lent à cause des délais postaux et de l'entrée de la commande dans le système informatique du distributeur et ces délais très longs obligeaient la pharmacie à garder des stocks importants.

Mac-Kesson, un distributeur de produits pharmaceutiques, a le premier utilisé un système d'information pour changer ce processus. Ce système permettait aux pharmacies d'enregistrer leurs commandes en utilisant un terminal pas plus grand qu'une calculatrice de poche. Des étiquettes avec codes barres installées sur les tablettes rendaient même inutile pour certains clients l'écriture du nom du produit. Les commandes enregistrées sur le terminal étaient transmises par téléphone au système informatique de Mac-Kesson et y étaient automatiquement enregistrées. Cette stratégie innovatrice donna à Mac-Kesson un avantage concurrentiel décisif.

Cela lui permit :

- de réduire ses propres coûts (par exemple, le nombre d'employés à l'entrée des commandes est passé de 750 à 15)
- de réduire les coûts de transaction de ses clients,
- de leur fournir un meilleur service (délais plus courts, moins d'erreurs...)

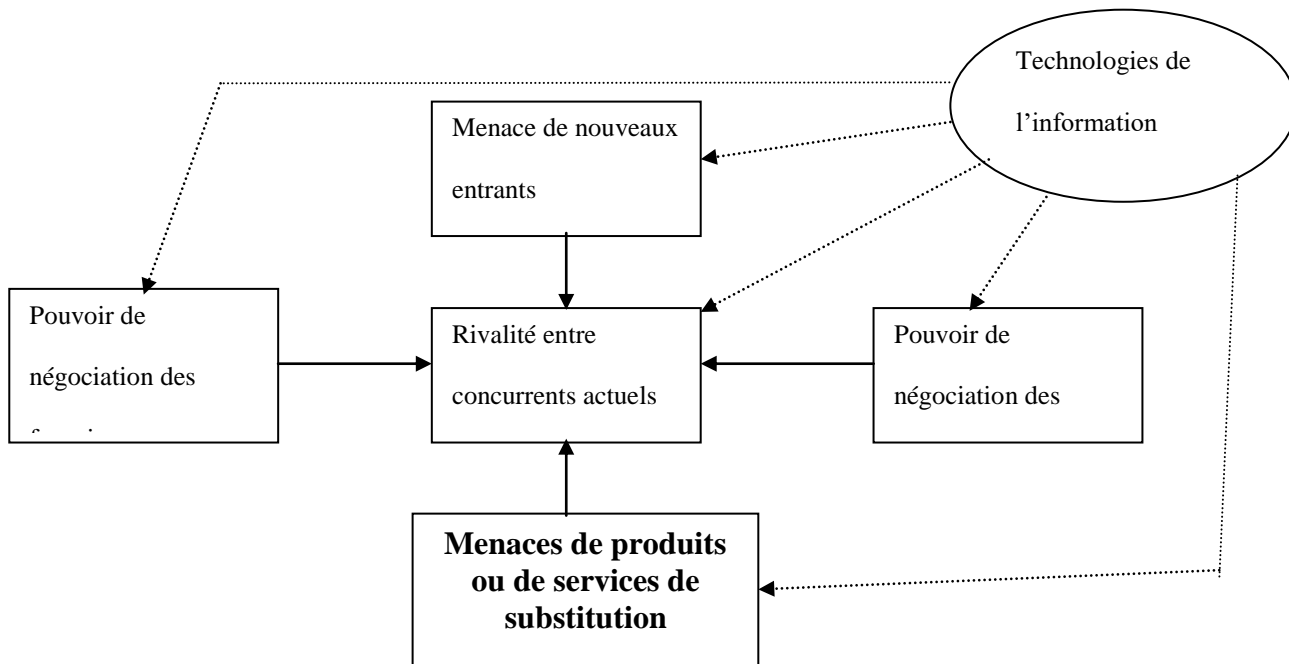
Au total, de 1975 à 1987 les ventes de Mac-Kesson ont grimpé de 424% (essentiellement grâce à des gains de parts de marché) alors que ses dépenses d'opération n'ont augmenté que de 86%.

Cet exemple certes ancien mais qui fait référence démontre les SI peuvent influencer chacun ou presque de ces niveaux et notamment sur les points clés de la compétitivité, à savoir les coûts et la qualité du produit et du service rendus aux clients (délais, nombre d'erreurs).

Bien entendu, la compétitivité des entreprises dépend de beaucoup de facteurs, de leur rentabilité (résultat/moyens mis en œuvre), de leur productivité, de leur position sur le marché, de leur savoir-faire, de la compétence du personnel, des dirigeants, de leur capacité à innover, de la qualité des produits, de la qualité des services rendus aux clients, de leur flexibilité (capacité à s'adapter)...

En fait Porter repère cinq forces essentielles de la structure concurrentielle :

- la rivalité inter-firme dans le secteur,
- le pouvoir de négociation avec le client,
- le pouvoir de négociation avec les fournisseurs,
- la menace de nouveaux entrants dans le secteur,
- la menace de produits ou de services de substitution.



Pour faire face à l'action de ces 5 forces l'entreprise peut adopter des stratégies génériques :

- de domination par les coûts (produire à des coûts durablement plus faibles que les concurrents)
- de différenciation (offrir des produits ou des services différents de ceux des concurrents)

Et l'exemple de Mac-Kesson démontre les SI peuvent influencer chacun ou presque de ces niveaux et notamment sur les points clés de la compétitivité à savoir :

- les coûts
- la qualité produit ou du service rendu aux clients (délais, nombre d'erreurs...).

**Conclusion :** Les aspects stratégiques des technologies de l'information décrits rapidement ci-dessus démontrent qu'il est indispensable d'élargir notre vision traditionnelle des SI : un système d'information ne sert pas qu'à gagner un peu de temps et d'argent en calculant la paye sur machine au lieu de le faire à la main, le SI de l'entreprise peut au contraire être décisif pour sa survie, le choix des ressources à affecter aux SI n'est pas qu'un simple problème technique, c'est un problème de politique générale de l'entreprise, le responsable du service « système d'information » fait partie de l'équipe de direction.



## **Le Bug de la SNCF : comment l'évolution du système informatique interroge le système d'information, arme stratégique<sup>1</sup>**

Dimanche 3 décembre 2017, à la suite de travaux d'extension d'un poste d'aiguillage, un bug informatique a paralysé la gare Montparnasse à Paris, entraînant l'annulation de 30% des TGV et des retards importants : des milliers de voyageurs se sont retrouvés sans transport ou bloqués dans les wagons. La cause ? Une erreur de codage d'un nouveau système informatique, mis en place dès samedi, et destiné à augmenter de 20% le nombre de trains au départ de la gare. Un nouveau dysfonctionnement qui intervient quatre mois après une première panne dans cette même gare.

En effet la Gare Montparnasse dessert la banlieue parisienne et les lignes de l'Ouest de la France. Or deux nouvelles lignes de trains à grande vitesse vers Rennes et Bordeaux ont été mises en service au printemps 2017. Cela a nécessité une modernisation majeure des équipements techniques : l'extension d'un poste d'aiguillage, et un nouveau système informatique gérant ce surplus de données de trafic. « Sur une petite portion, entre la Gare Montparnasse et Châtillon [en proche banlieue parisienne], il fallait changer le logiciel qui gère les aiguillages et les signaux (...). Ce changement de logiciel avait pour objectif d'augmenter de 20% la capacité d'accueil des trains au niveau des voies à la Gare Montparnasse. La panne est intervenue après la reprise de la circulation, à 12h15. Après la mise en service de ce nouveau logiciel, le système s'est bloqué », nous a indiqué la SNCF.

Cet incident a fait la une de titres de l'actualité dès le lendemain, alors même que la SNCF a eu du mal à communiquer sur ce nouvel incident pour ne pas créer de mouvement de colère des passagers. Mais à l'heure des réseaux sociaux, c'est difficilement compréhensible. L'image de la SNCF est désastreuse, alors qu'elle a de très bonnes performances. Comme ils n'ont pas d'information, les gens échangent entre eux sur les réseaux sociaux, et la situation dégénère. Le manque de communication interne accentue le problème. En cas de crise, des agents sont déployés en gare pour calmer les voyageurs. Mais ils sont parfois moins informés que les voyageurs, ce qui renforce la colère des clients. A la suite de l'incident du mois de décembre, la Ministre des Transports a demandé aux dirigeants de la SNCF d'accélérer la mise en œuvre d'un programme d'information baptisé « Rob.In » pour « apporter des améliorations à la fois dans la robustesse et dans l'information des voyageurs » d'ici 2020, qui sera déployé à partir du 1er janvier 2018. Le ministère des Transports note que la SNCF devra rendre compte régulièrement devant les conseils de surveillance et d'administration du groupe public

Mais, pour parvenir à atteindre cet objectif, la SNCF aurait intérêt à passer d'une culture d'usagers à une culture client. En effet, les agents de la SNCF considèrent souvent encore les voyageurs comme des usagers, dociles et patients. Mais ce sont aujourd'hui des clients qui ont des exigences. La communication de la SNCF n'est plus du tout adaptée au marché des transports. C'est une vraie révolution culturelle que l'entreprise doit amorcer. Or les agents SNCF raisonnent comme des ingénieurs. Au moment d'une panne, ce qui compte pour eux, c'est de résoudre le problème. La communication n'est pas une priorité. Ils considèrent qu'ils ne vont pas mobiliser de l'énergie à informer des usagers qui, de toute façon, ne comprennent rien. Ils ont la volonté de communiquer une information exacte. Mais, comme en situation de panne, la situation évolue en permanence, ils préfèrent attendre la résolution du problème. La meilleure solution pour la SNCF serait de faire preuve d'empathie. Elle doit comprendre que le voyageur a besoin de comprendre ce qu'il se passe. Il faut noter que par ailleurs, est annoncé pour décembre 2017 le passage de Voyages-SNCF.com en Oui.SNCF. Ce changement reflète une stratégie numérique et d'innovation menée avec de nombreux partenaires, start-ups et grands acteurs de l'Internet comme Google et Amazon.

---

<sup>1</sup> Cette étude de cas a été réalisée par A. Mazars-Chapelon, Université de Montpellier, à partir d'articles du Monde Informatique, d'Ouest France et de France Culture (4 et 5/12/2017)



Questions :

1. Quel est l'objectif affiché par la SNCF quand elle décide d'implémenter une nouvelle version de son système informatique au centre de l'incident de début décembre 2017 ? Vous pourrez mobiliser la grille d'analyse des 5 forces de Porter pour en éclairer l'enjeu stratégique.
2. Pourquoi la SNCF a-t-elle tant de difficultés à tenir les passagers informés alors qu'elle s'est dotée de nouveaux outils pour communiquer (site Internet, appli, réseaux sociaux) ?
3. Quelles sont les risques stratégiques induits par ces dysfonctionnements ?
4. Quelle évolution du système d'information recommanderiez-vous à la SNCF pour se prémunir de risques futurs ? Vous pourrez vous appuyer sur les composantes du SI selon Alter pour justifier votre réponse.

## CHAPITRE 3 : LES EFFETS DE L'IMPLANTATION D'UN SYSTEME D'INFORMATION

---

Si les organisations mettent en place des système d'information (SI) c'est essentiellement parce qu'elles pensent que ceux-ci vont améliorer leur fonctionnement. Pourtant cette mise en place pose parfois des problèmes importants et les échecs sont nombreux. Certains échecs sont liés à des problèmes techniques (le système marche mal, il est peu puissant...) mais beaucoup d'entre-eux proviennent de causes organisationnelles et humaines. En effet « Un système d'information est une combinaison de pratiques de travail, d'informations, de personnes et de technologies organisées pour atteindre des objectifs dans une organisation » (Alter, 1991). Il est donc clair qu'un système d'information n'est pas seulement un système informatique, c'est aussi des pratiques de travail, des informations et ... des personnes. Ainsi, l'objet de l'exposé est d'une part de montrer l'effet prévisible des systèmes d'information sur les plans stratégique, organisationnel et humain et d'autre part de mettre en évidence les risques de résistance à la mise en place d'un SI et les moyens à mettre en oeuvre face à ces risques.

### I. LES EFFETS ATTENDUS PAR LES DIRIGEANTS

Les entreprises qui utilisent les SI en attendent nécessairement une amélioration de leur efficacité et de leur efficacité. Il est sans doute impossible de raisonner en terme de déterminisme simple : **l'usage d'une technologie n'entraîne pas nécessairement les mêmes effets quelle que soit l'organisation et quelles que soient les conditions d'utilisation**. En revanche il est possible de s'interroger sur les effets potentiels de ces technologies sur tous les aspects organisationnels et humains du fonctionnement des organisations.

#### A. Une amélioration de la productivité

L'amélioration de la productivité, et particulièrement celle des services administratifs a été une des premières justifications de l'utilisation de l'informatique dans les entreprises. L'idée est que pour certains travaux, le remplacement de l'homme (ou son assistance) par des systèmes informatiques moins coûteux et plus fiables permettrait des gains de productivité (exemple : travail de secrétariat). Les systèmes d'information ont en outre un impact sur la qualité de ce qui est produit. Deux exemples en témoignent :

- si l'introduction de la lecture optique aux caisses des grandes surfaces a considérablement augmenté le nombre d'articles enregistrés à l'heure, elle a aussi permis de réduire le nombre d'erreurs par 1000 (avant une erreur tous les 300 enregistrements, maintenant une tous les 300000)
- les distributeur de billets augmentent la productivité des banques (moins de salariés) mais offrent de plus une disponibilité bancaire en dehors des heures d'ouverture.

On constate en outre parfois une redéfinition du champ d'activité des entreprises. Par exemple, American Airlines qui avait développé pour son propre usage un système perfectionné de réservation de places vend les services de ce système à d'autres compagnies aériennes. A l'heure actuelle, les profits tirés de cette activité sont plus élevés que ceux tirés de l'activité première, le transport de passagers.

#### B. Une amélioration de la prise de décisions

Pour décrire le processus décisionnel, la littérature a souvent fait appel au modèle très connu proposé par Simon. Ce modèle comporte trois étapes : **l'intelligence du problème** (le décideur étudie l'environnement économique, technique, social et politique pour identifier les situations appelant décision), **la phase de**

**modélisation, de la conception des solutions** (le décideur doit "inventer, développer, analyser diverses actions envisageables"), et enfin **le choix final** (le décideur "sélectionne une action parmi celles qui sont recensées").

Dans la mesure où le nombre de données recueillies est plus élevé, la communication plus facile entre les individus, les temps de traitement plus réduits, l'effet le plus vraisemblable sera une identification plus rapide et plus précise des problèmes (la surveillance continue des ventes réalisées liée à un modèle de déclenchement de commandes géré par ordinateur permet au gestionnaire d'identifier plus vite et mieux les produits à problèmes). La mise en place d'indicateurs d'alerte calculés en permanence soulage les décideurs dans leur **phase d'intelligence** (au sens de Simon). De même, grâce à leurs capacités de traitement, les SI permettent une amélioration **de la phase « modélisation »** c'est-à-dire d'identification des solutions possibles et de **la phase de choix** (système expert, SIAD). Les technologies apportent des capacités de stockage, des possibilités d'interrogation multiples rendant l'information plus accessibles, des moyens de conservation de l'expérience accumulée...

Exemple : Grâce à un système de messagerie électronique il est possible de consulter rapidement plusieurs centaines de personnes quelle que soit leur position géographique. Il est donc normal de penser que l'usage des technologies de communication et d'aide à la décision conduit à des décisions de qualité plus élevée.

### C. Une amélioration de la compétitivité

L'internationalisation des marchés a rendu cette dernière décennie la compétition entre les entreprises de plus en plus vive. Bien entendu, la compétitivité de l'entreprise dépend de nombreux facteurs : flexibilité, rentabilité, capacité d'innovation, qualité des produits et services. L'introduction d'un SI peut permettre d'agir favorablement sur ces facteurs : grâce au système d'information on peut réduire les coûts, augmenter la qualité des produits, des services aux clients. Ils peuvent permettre à l'entreprise de se différencier, d'attirer les clients, de les fidéliser, d'augmenter les parts de marché... On peut donc être plus compétitif que ses concurrents grâce aux SI. Il faut être conscient aujourd'hui que dans ce contexte, un usage adéquat des SI peut constituer une arme stratégique fondamentale. L'exemple de l'entreprise Mac-Kesson illustre ce type d'utilisation (cf chapitre 2 : les systèmes d'information dans un contexte de compétition).

Michael Porter (1984) repère cinq forces essentielles de la structure concurrentielle :

- la rivalité inter-firme dans le secteur,
- le pouvoir de négociation avec le client,
- le pouvoir de négociation avec les fournisseurs,
- la menace de nouveaux entrants dans le secteur,
- la menace de produits ou de services de substitution.

Pour faire face à l'action de ces 5 forces l'entreprise peut adopter des stratégies génériques de domination par les coûts (produire à des coûts durablement plus faibles que les concurrents) et/ou de différenciation (offrir des produits ou des services différents de ceux des concurrents).

Cet exemple certes ancien mais qui fait référence démontre que les SI peuvent influencer chacun ou presque de ces niveaux et notamment sur les points clés de la compétitivité, à savoir les coûts et la qualité du produit et du service rendus aux clients (délais, nombre d'erreurs). Le document fourni en Annexe (extrait de l'ouvrage de PORTER) fait ressortir les impacts possibles de l'introduction d'un système d'information sur l'état des cinq « forces concurrentielles » qui s'exercent dans le secteur où l'entreprise est présente.

## D. La redéfinition des rôles et des tâches des individus

La mise en place des SI dans les organisations a souvent modifié l'éventail des rôles dans l'organisation. De nouveaux emplois sont apparus (programmeurs, analystes...) d'autres ont disparu (comptables teneurs de livres...). Les impacts des SI sur les rôles et les tâches des individus sont très variables :

- **Au niveau des compétences** : les SI peuvent avoir des effets positifs ou négatifs sur les compétences requises des individus. Pour certains, les SI ont permis de prendre des décisions plus rapides avec des données plus fiables et en plus grande quantité et donc de manière plus rationnelle, moins intuitive. Ils peuvent de même profiter de l'expertise fourni par les SIAD ou les systèmes experts. Sans doute prennent-ils grâce à cela de meilleures décisions. Pour d'autres, les SI ont eu l'effet inverse, spécialement lorsqu'il s'agissait de systèmes conçu pour automatiser une grande partie du jugement dans le travail. Prenons l'exemple d'un réceptionniste d'hôtel qui jusqu'à présent décidait lui-même de l'opportunité de louer à partir d'une certaine heure les chambres les plus chères à des prix moins élevés et à qui l'on fournit maintenant un SIAD qui prend les décisions à sa place. La conséquence de cela est que le réceptionniste perd de son pouvoir et le travail peut maintenant être accompli par une personne moins compétente. De même, dans un restaurant quelconque, le cuisinier doit surveiller le niveau de cuisson ce qui demande certaines compétences non requises chez **Mac-Donald's** où un SI et plus précisément un Bip, signale au « cuisinier » que les frites sont prêtes.

### Exemple de McDonald : Utiliser les systèmes d'information pour contrôler le travail

« McDonald emploie 500 000 jeunes adultes à la fois, mais beaucoup d'entre eux ne restent pas longtemps. Pour obtenir des résultats constants avec ce personnel, McDonald a défini de façon très précise leur travail. A titre d'exemple, un système informatique est utilisé pour que les frites McDonald soient toujours parfaitement dorées et servies dans des portions égales. L'employé jette un bac de frites dans la graisse et appuie sur un bouton. Un système informatique contrôle la cuisson des frites et déclenche une sonnerie quand celle-ci est finie. Il n'y a plus qu'à retirer les frites et utiliser une cuillère conçue spécialement pour qu'un sac de 100 livres de pommes de terre donne entre 400 et 420 portions de frites. Plusieurs jeunes employés disent qu'ils ont quitté McDonald parce qu'ils avaient l'impression de devenir des robots . Chaque étape de leur travail était contrôlée par des "timers". »

Pas besoin d'avoir un diplôme de l'école hôtelière, il suffit d'avoir des jambes et des mains et d'effectuer les mouvements nécessaires aussi vite que possible.

- **Au niveau de la variété des tâches** : les SI peuvent soit étendre soit réduire la variété des tâches des individus au travail. Lorsque qu'un SI permet d'automatiser des tâches routinières, il peut contribuer à augmenter la variété des tâches d'un individu en lui permettant de consacrer plus de temps à la partie la plus intéressante de son travail (exemple : le comptable qui met deux ou trois fois moins de temps pour la saisie peut peut-être maintenant consacrer plus de temps à la partie analyse...). Par contre il arrive qu'un système réduise la variété des tâches en confinant l'employé à une seule tâche, souvent la saisie.

- **Au niveau de l'autonomie du salarié** : l'autonomie dans un travail est le degré de liberté que les individus ou les groupes ont dans la planification, l'organisation et le contrôle de leur travail. Certains systèmes sont conçus pour réduire l'autonomie (exemple Op. cité du réceptionniste). Il faut noter par ailleurs que les personnes travaillant sur des réseaux peuvent ressentir un fort sentiment de contrôle, ils pensent que toutes leurs opérations sont enregistrées et peuvent ainsi être examinées. Mais la tendance générale semble à **l'enrichissement des tâches** et à plus d'autonomie par le développement de l'auto-

contrôle. Grâce à l'outil informatique, l'opérateur peut constater le résultat de ses actions, utiliser le diagnostic d'un SIAD ou d'un système-expert...

- **Au niveau des relations professionnelles :** les SI peuvent causer une augmentation ou une diminution des interactions sociales au travail. Des emplois qui nécessitent de passer des journées entières devant un ordinateur à accomplir des tâches répétitives ont tendance à réduire les interactions sociales. Par contre un système qui permet de réduire le temps passé à remplir des formulaires peut donner plus de temps à la partie du travail d'un individu qui nécessite des contacts avec les autres. En outre, les SI permettent de communiquer (ex : messagerie électronique)

## II. LES RISQUES DE RESISTANCES A L'IMPLANTATION D'UN S.I.

Si certains individus voient dans la mise en place d'un système d'information un progrès important dont ils vont profiter, d'autres y voient un risque de devoir changer leurs habitudes et une source de frustration et risquent de fait d'opposer une résistance. Il existe de multiples façons de résister à un système : ne pas l'utiliser, le critiquer sans cesse, demander toujours d'autres améliorations, introduire de fausses données, le saboter, modifier ou altérer les programmes, provoquer des pannes...

Eviter ou du moins gérer cette résistance implique tout d'abord de bien la comprendre : Pourquoi certains individus, dans certaines situations, sont-ils réticents à la mise en place ou à la modification d'un SI ? Comment éviter ou limiter ces résistances? Les chercheurs en Systèmes d'Information ont distingué deux raisons essentielles aux résistances observées dans les entreprises : des raisons techniques et des raisons humaines.

### A. Des raisons techniques

Une des causes de la résistance peut être l'insuffisance de la qualité, de la performance du système (peu convivial, trop complexe d'utilisation, inadapté aux besoins des utilisateurs, pas assez puissant, pas assez rapide, il commet des erreurs). Il peut en résulter une sous-utilisation du système (certains terminaux restent parfois inutilisés...) ou un coût important d'amélioration du système mis en place.

Pour limiter ces problèmes, une attention particulière doit être portée à la planification et au développement des systèmes d'information. Pour éviter cela, il est important de faire participer les utilisateurs à la conception pour qu'ils fassent part de leurs remarques (sur la convivialité par exemple) avant la mise en place définitive. Pour favoriser l'adéquation du système d'information aux attentes des utilisateurs et ainsi minimiser les risques de résistances, il apparaît souhaitable de :

- S'assurer que le système traite le bon problème de la bonne façon (faire participer les utilisateurs à la conception, faire des prototypes, prévoir des supports et des modifications...)
- Garder un système simple, facile d'utilisation (éviter ou tout au moins cacher les complexités, travailler sur la convivialité, l'ergonomie...)
- Minimiser les problèmes techniques (pannes, lenteurs.... ) pour éviter de perdre la confiance des utilisateurs...

### B. Des raisons humaines et sociales

Tout projet d'informatisation est un facteur de changement dans l'organisation. Or, naturellement, les individus n'aiment pas changer, cela nécessite obligatoirement un effort supplémentaire et entraîne au

moins un certain temps une période d'inconfort. Tout **changement organisationnel** est donc difficile à gérer. Lewin et Schein ont proposé un modèle de gestion du changement organisationnel en trois phases : Dégeler - Changer - Regeler. Leur constat est que souvent on occulte la première et la troisième. La première phase constitue toute la préparation au changement : il faut que les personnes impliquées soient convaincues du bien fondé de ce changement. La troisième phase est celle de la consolidation du changement : il s'agit de s'assurer que les nouvelles méthodes, les nouveaux outils sont bien intégrés dans les pratiques de travail, que les personnes ne sont pas revenues à leur anciennes habitudes.

Outre le fait que l'informatique pose souvent des problèmes de réduction de personnel, l'introduction des nouvelles technologies de l'information modifie les modes opératoires (la façon de faire) et les savoirs faire. Le travail devient moins physique, plus abstrait. La surveillance des machines sur écran de contrôle est un travail plus abstrait que l'observation directe dans le bruit et la poussière. De même, Le dessin assisté par ordinateur (CAO) ne procure pas les mêmes sensations que la planche à dessin. Cet éloignement des aspects concrets de la tâche et cette uniformisation apparente des postes de travail procurent chez certains une perte d'identité, une perte de savoir-faire. Le métier et la relation au métier en sont modifiés.

Les caractéristiques des utilisateurs sont souvent source de résistances : on observe souvent que les personnes plus âgées acceptent plus difficilement l'informatisation. Le sentiment d'être plus contrôlé (si on travaille sur réseau) constitue également une cause de résistance. Le manque de formation, de compétence est source de découragement et donc de résistance. Il est donc impératif, pour diminuer les risques d'échec avant de mettre en place un système d'information, de former les futurs utilisateurs. De même la non consultation, la non participation des futurs utilisateurs pendant les phases de conception et de mise en place, est une cause de résistance importante, cela peut les « vexer », ils peuvent mal comprendre l'intérêt du projet... Il est impératif pour la réussite du projet que les concepteurs travaillent en collaboration avec les utilisateurs.

Enfin, une cause importante de la résistance est la perte de pouvoir perçu : le pouvoir appartient à ceux qui ont l'information et ceux qui sont peu à l'aise face à l'outil informatique vont perdre du pouvoir au profit de ceux qui sauront exploiter le système : ils peuvent pour cela être réticents à sa mise en place.

En conséquence, pour vaincre la résistance des utilisateurs et non-utilisateurs, il est souhaitable de :

- Favoriser l'implication (faire participer les utilisateurs, savoir leur « vendre » le système, leur montrer qu'il va leur apporter quelque chose de positif...).
- Favoriser la compréhension par des actions de formation
- Contrôler l'utilisation (obliger(?), favoriser, et aider)
- Favoriser le travail d'équipe entre personnel SI et utilisateurs (formation des informaticiens à la gestion, à la Bureautique selon les besoins des utilisateurs, organiser des plages de travail en commun...)

**Conclusion** : la conséquence de tout cela est que l'on doit considérer les SI comme **des systèmes socio-techniques** où il faut optimiser conjointement les paramètres techniques et les paramètres sociaux relatifs aux individus qui travaillent dans les organisations sans quoi l'échec est inévitable.



## Un cas parmi tant d'autres...



Michel, un spécialiste de l'informatique, venait tout juste de terminer un mandat de développement d'un système informatisé pour la gestion des ressources humaines de la petite entreprise pour laquelle il travaillait. Alors qu'il profitait de la fin de ce mandat pour remettre ses connaissances à jour en lisant une revue spécialisée, il reçut la visite de son supérieur immédiat à son bureau

*"Bonjour Michel, lui dit monsieur Boucher, j'ai parlé à monsieur Parent ce matin et je pense que je l'ai convaincu de nous laisser développer un système de journal général pour lui."*

Monsieur Parent est le chef comptable de l'entreprise. Cela faisait déjà plusieurs années que monsieur Boucher essayait d'automatiser les écritures au journal général de monsieur Parent, c'est-à-dire le report des opérations quotidiennes (paiement des factures, sortie de fonds, etc.).

*"Je voudrais que vous le rencontriez demain matin. Déterminez ce dont il a besoin puis faites la conception et programmez le système."*

*"Pas de problème, monsieur Boucher. C'est formidable que vous l'ayez finalement convaincu."*

*" Vous savez comment sont les comptables. Ils ne veulent jamais changer. Ils ne semblent pas se rendre compte que nous sommes au 21ème siècle. Mais je lui ai dit que nous allions lui donner un système de comptabilité vraiment moderne et qu'il l'aurait d'ici deux mois."*

Michel eut du mal à en croire ses oreilles.

*"Pensez-vous vraiment que cela ne prendra que deux mois?" dit-il.*

*"Ca ne peut pas être très compliqué. Les comptables ne sont pas des gens très compliqués. Enfin, bonne chance et tenez-moi au courant. "*

Michel prit un crayon, un bloc de papier et parcourut rapidement un de ses anciens cours de comptabilité qu'il avait suivi à l'université. Le lendemain matin, il se rendit au bureau de monsieur Parent afin de déterminer les spécifications du système qu'il devait développer. Après avoir répondu à quelques questions intéressantes de monsieur Parent sur l'informatique et sur ce que lui, Michel, pensait qu'un système informatisé devait accomplir, il commença à prendre des notes se rapportant à la comptabilité du journal général de l'entreprise. Michel n'obtint pas beaucoup d'information car monsieur Parent devait passer à la banque en rentrant chez lui.

Michel fut ensuite occupé pendant deux jours par la modification d'un programme qu'il avait réalisé deux mois plus tôt pour le système de gestion des ressources humaines.

Puis, à partir de ses notions de comptabilité générale et des renseignements obtenus de monsieur Parent, il fit la conception d'un système informatisé de journal général.



Une semaine après avoir parlé pour la première fois à monsieur Parent, il estima que le temps était venu de lui soumettre la conception générale qu'il proposait. Le premier rendez-vous fut annulé à cause de l'arrivée imprévue d'un visiteur important. Une deuxième tentative avorta à cause d'une réunion convoquée à la dernière minute, réunion à laquelle monsieur Parent devait absolument assister. Enfin, un troisième rendez-vous fut annulé à cause d'une urgence. En désespoir de cause, Michel décida d'entreprendre la conception détaillée du système. Comme il disposait de peu de temps, Michel commença à programmer aussitôt après avoir terminé la conception détaillée d'une section du système ; de toute manière, il n'aurait pas eu suffisamment de temps pour tenir des réunions de projet. Environ sept semaines après le début du projet, monsieur Boucher lui demanda comment avançaient les travaux.

« Michel, où en êtes-vous avec votre système de journal général ? »

« Tout va très bien, monsieur Boucher. J'ai terminé à 95%. »

« Parfait. Continuez dans la même voie. N'hésitez pas à venir me voir si vous avez besoin d'aide. »

Mais Michel savait par expérience que les problèmes étaient la dernière chose dont monsieur Boucher voulait entendre parler. Il continua donc à travailler par lui-même. Il obtint d'un des assistants de monsieur Parent une liste des opérations pour une durée d'un mois (75 seulement !) et il construisit un fichier pour tester ses programmes. Il compléta le système quelques jours avant l'échéance des deux mois.

Lorsque monsieur Parent passa manuellement les écritures du mois suivant au journal général, Michel utilisa en parallèle le nouveau système afin de le tester. Mais plusieurs cas d'espèces n'avaient pas été prévus dans le système ; il s'agissait d'éléments que Michel, étant donné les circonstances, ne pouvait pas connaître. Michel apporta les corrections nécessaires afin que ses totaux correspondent à ceux de monsieur Parent.

Le mois suivant, il y eut d'autres problèmes dont l'un força Michel à refaire la programmation d'une partie importante du système. Il s'agissait à nouveau d'un élément qu'il ne pouvait pas prévoir et cela l'obligea à retarder la livraison du système d'un autre mois.

Le mois suivant, tout sembla bien marcher jusqu'à ce que monsieur Parent parle à Michel de la possibilité de faire des corrections après clôture. Michel se remit donc au travail pour ajouter cette fonction au système. Mais le mois suivant amena encore une situation d'exception ! Ce fut le dernier car Michel quitta l'entreprise deux semaines plus tard ; il avait trouvé du travail dans une autre entreprise.

Monsieur Parent utilise toujours son système manuel tandis que le remplaçant de Michel tente de comprendre le système tant bien que mal en l'absence d'une documentation du fichier et des programmes...



Décrire l'évolution souhaitée du système d'information de l'entreprise en reprenant les différentes composantes d'un système d'information selon la définition d'ALTER  
Quelles sont les erreurs que vous détectez dans ce cas ?

Comment expliquez-vous l'attitude du comptable ?

Comment vous y seriez-vous pris pour que ces erreurs ne soient pas commises ?

## CHAPITRE 4 : L'EVALUATION DE LA PERFORMANCE DES SYSTEMES D'INFORMATION

L'évaluation des SI renvoie aux problèmes de contrôle. Or, on associe généralement deux sens distincts au mot "contrôle" :  
- le premier tient à **l'idée de surveillance**. En ce sens, contrôler signifie vérifier que les choses se déroulent conformément à ce que l'on souhaite (exemple : les examens de contrôle),  
- le deuxième sens, plus large, est associé au **concept de maîtrise** (" je contrôle la situation " signifie je la maîtrise).  
C'est dans cette double logique que l'on parle du contrôle des SI.

**L'enjeu du contrôle** des SI dans les entreprises est variable, mais il est toujours important : par exemple, **les coûts informatiques représentent 0.5% du chiffre d'affaires dans la distribution mais plus de 10% dans les banques**. A l'intérieur d'un même secteur, ces coûts peuvent varier de 1 à 4.

**Dans ces conditions, l'amélioration du contrôle de la gestion des SI constitue désormais un objectif clairement annoncé par la plupart des entreprises.**

La mise en place d'un système d'évaluation dans une entreprise implique que des réponses soient apportées à deux questions fondamentales :

- Quels sont les buts et les cibles du système de contrôle : **quand et quoi contrôler ?**
- De quelles informations pertinentes, de quels outils doit-on disposer pour cela : **comment contrôler ?**

### I. Quand et quoi contrôler

#### 1.1 Le moment du contrôle : quand contrôler ?

La pluralité des objectifs du contrôle s'explique par la diversité des contextes de contrôle. Sans viser un recensement exhaustif, nous pouvons décrire quelques situations couramment observées.

##### a) Evaluation prévisionnelle ; Etude d'opportunité ; Elaboration d'un schéma directeur

L'objectif est alors de repérer les moyens en matériels, logiciels et personnel nécessaires à l'implantation d'un projet et **d'évaluer l'intérêt économique**, la praticabilité technique et organisationnelle de ce projet.

##### b) Evaluation post- implantation

Lorsqu'un projet d'informatisation a été réalisé, on procède dans les mois qui suivent à une évaluation ponctuelle. Celle-ci a pour but de **vérifier dans quelle mesure les objectifs du projet ont été atteints** et quelles sont les mesures à prendre pour le rendre encore plus performant.

##### c) Contrôle de la gestion du système informatique

Dans ce cas, l'objectif est de contrôler l'évolution de ses coûts (matériels, logiciels, personnel), et/ou la qualité de son fonctionnement, et/ou la satisfaction des utilisateurs et ce, de manière régulière.

Ces quelques exemples sont révélateurs du caractère hétérogène des contextes et donc des objectifs du contrôle. Dans chacune de ces situations, les objets contrôlés d'une part et les perspectives du contrôle d'autre part seront différents.

#### 1.2 Les objets du contrôle : quoi contrôler ?

Selon les instants et selon les préoccupations dominantes, on peut contrôler :

- **les moyens utilisés** : le matériel, les logiciels, le personnel
- **le produit ou les services offerts** : la qualité de l'information fournie
- **les résultats** : l'amélioration du SI s'est-elle traduite par une amélioration des résultats de l'entreprise (baisse des coûts, hausse de chiffre d'affaires...). Mais sur ce plan il faut rester très prudent : **exemple : un grand hôtel** avait mis en place un système informatique perfectionné d'aide à la gestion des réservations et constaté une hausse sensible de son taux de remplissage. Pouvait-on en conclure que le passage d'un taux moyen de remplissage de 60% à 72% était le résultat de l'informatisation ? Pas obligatoirement car une étude plus approfondie sur une période plus longue montra que ce taux de remplissage avait été fortement influencé par la hausse du dollar par rapport au franc plus attractif pour les touristes américains.

**Conclusion** : Ces différents objets du contrôle à titre prévisionnel, en post-implantation ou en « contrôle continu » aboutissent à une très grande diversité des objectifs, à **une grande diversité du “ pourquoi ” du contrôle**. **Il semble évident que toute évaluation doit s'appuyer sur une réflexion préalable quand aux objectifs poursuivis**. Une fois que l'on sait quoi quand et pourquoi contrôler, il faut déterminer comment.

## II. Comment contrôler : les problèmes de mesure

L'exercice effectif du contrôle repose sur la possibilité de recueillir des informations pertinentes sur le fonctionnement du SI. Cette condition essentielle est pourtant difficile à satisfaire, **les concepts utiles ne sont pas des notions simples et leurs mesures concernant les SI soulèvent de nombreuses difficultés**.

### 1.1. Le choix des concepts clés : les différentes perspectives du contrôle

On retrouve ici trois perspectives dominantes possibles :

- **une perspective d'efficience** où l'on rapproche les résultats des moyens utilisés (exemple de l'hôtel : nombre de commandes gérées / montants investis...)
- **une perspective d'efficacité** où l'on rapproche les résultats des objectifs que l'on s'était fixé (accroissement réel du nombre de clients / accroissement prévu...).
- **une perspective de satisfaction** (c'est une vision particulière de l'efficacité organisationnelle exprimée aux travers des perceptions des utilisateurs. Ces perceptions peuvent bien entendu découler de causes multiples : image a priori de l'outil, utilisation plus ou moins agréable...) ou **d'utilisation** (mesure de l'attitude des utilisateurs).

#### a) L'analyse de l'efficacité (résultats/objectifs)

Mesurer l'efficacité pose deux problèmes essentiels :

- il faut d'abord que **les objectifs assignés au système aient été explicités avec précision**,
- il faut ensuite, à partir des résultats observés, **être capable de mettre en évidence la contribution effective du SI** à la production de ces résultats.

**Exemple de R.Reix** : une grande banque a choisi au niveau stratégique d'améliorer le service à sa clientèle (possibilité d'effectuer des opérations 24h/24) et de lancer des produits nouveaux (d'épargne ou de crédit). Pour cela, elle a décidé de recourir davantage aux technologies de l'information (en offrant ses services via des services automatiques en particulier) et assigné comme objectif prioritaire à la fonction système d'information la réduction des temps de construction de nouveaux systèmes. C'est par rapport à ces objectifs que sera mesurée l'efficacité (par exemple à l'aide du critère temps de développement moyen des projets). Mais si l'amélioration de la position concurrentielle de la banque est mesurable (hausse de la part de marché par exemple), il n'est pas simple d'isoler l'impact réel de la réduction des temps de développement des SI sur la variation de la part de marché qui peut découler également d'actions commerciales, de fautes de concurrents... Autrement dit, **la mesure de l'efficacité du système implique une hypothèse de séparabilité des effets** qu'il est souvent difficile de respecter.

#### b) L'analyse de l'efficience (résultats/moyens)

Une publication de l'association française des auditeurs internes montre les valeurs moyennes observées dans 3 grands secteurs d'activité pour les coûts informatiques :

	Industrie	Banque, assurance	Distribution
Coûts informatiques / Chiffre d'affaires	1.3%	10.2%	0.5%

Coûts informatiques / frais généraux	7.7%	14.5%	12.3%
---	------	-------	-------

Cela montre que les problèmes d'efficience ne sont pas à négliger quel que soit le secteur d'activité.

La mesure d'efficience dans l'entreprise peut se faire à deux niveaux :

- **Mesure d'efficience du système informatique** : il s'agit alors de rapprocher les résultats du système exprimés par des variables techniques (capacité, temps de réponse...) et le coûts des ressources engagées. Ceci ne pose pas de difficultés majeures : l'objet évalué est le système informatique en tant qu'outil (matériel et logiciel), il est assez facilement identifiable.

- **Mesure d'efficience en termes d'information** : L'objectif est dans ce cas d'évaluer le produit fourni par le service informatique : l'information. La difficulté méthodologique est ici nettement plus grande. En effet, **la valeur de l'information est essentiellement déterminée par son usage** et c'est alors très compliqué voire impossible à mettre en œuvre (c'est pour cela que certaines entreprises se limitent à des mesures beaucoup moins pertinentes mais beaucoup plus praticables telles que le volume d'informations produites ou le temps de réponse).

### c) L'analyse de l'utilisation ou de la satisfaction

Dans le cas où l'utilisation du système est facultative, la mesure de l'utilisation est un critère du succès (nombre d'utilisateurs / nombre d'utilisateurs potentiels ; fréquence, intensité, diversité, durée de l'utilisation).

Dans le cas où l'utilisation est obligatoire, ordonnée par la direction ou par les faits (saisie comptable), le niveau de satisfaction des utilisateurs est retenu. Cette satisfaction est généralement appréciée à l'aide d'échelle de Likert à 5 ou 7 degrés :

Totalement satisfait    1    2    3    4    5    Profondément mécontent

Il est à noter que plusieurs études ont démontré une très faible corrélation entre les mesures d'efficacité et d'efficience d'une part et les mesures de satisfaction d'autre part, c'est pourquoi ces différents types de mesure sont souvent associés. Autrement dit, la mesure de la satisfaction ne constitue pas un substitut mais plutôt un complément aux mesures d'efficacité et d'efficience.

Maintenant on sait que pour évaluer la performance des SI on regarde leur efficacité, leur efficience et la satisfaction ou l'utilisation des utilisateurs. Mais comment fait-on pour mesurer ces concepts, quels sont les critères retenus ?

### 1.2. Le choix des critères : les outils du contrôle

La diversité des objectifs du contrôle rend difficile la constitution a priori d'une liste de critères valables dans tous les cas. Afin de mieux comprendre comment les chercheurs procèdent pour évaluer les systèmes d'information, voici trois listes de critères extraites de publications classiques dans le domaine en fonction de l'objectif du contrôle :

## CHAPITRE 5 : LA SECURITE INFORMATIQUE

---

« Celui qui reconnaît consciemment ses limites est plus proche de la perfection » J.W. von Goethe

Le recours de plus en plus important aux technologies de l'information a fortement amélioré les performances des SI mais sans doute **aussi leur vulnérabilité**. Qu'arriverait-il à une société de ventes par correspondance si sa base de données client était détruite ? Comment pourrait fonctionner une compagnie aérienne si son service informatique était en panne ? Quelles seraient les conséquences pour une compagnie d'assurance de la perte de son fichier contrat ?

Des estimations évaluaient les pertes dues à des sinistres informatiques pour les entreprises françaises à 16 milliards pour l'an 2000. L'informatisation croissante explique sans doute que les chiffres des sinistres croissent régulièrement. **Il s'agit donc d'un enjeu particulièrement important qui nécessite une attention régulière de la part des responsables.**

Après avoir identifié les principaux risques auxquels sont exposés les systèmes d'information, nous décrirons les principales mesures liées à l'organisation de la sécurité informatique.

### I. L'identification des principaux risques informatiques

**Définition :** La sécurité d'un SI est sa non-vulnérabilité à des accidents ou à des attaques volontaires c'est-à-dire à l'impossibilité que ces agressions produisent des conséquences graves sur l'état du système ou son fonctionnement.

#### **A) les causes potentielles de sinistre (lire l'annexe)**

Nous distinguerons les causes de sinistres humaines des accidents.

##### **1.1 Les causes de sinistres humaines**

###### **a) les actes de malveillance**

###### **- La fraude**

Cette cause est en pleine expansion et demeure sous-évaluée : beaucoup de fraudes ne sont sans doute pas découvertes.

###### **Exemple :**

- Falsification de la gestion des acomptes fournisseurs (15),
- Modification de la cote des valeurs boursières (29),

###### **- Les vols matériels et immatériels**

Les vols de matériels se sont fortement développés avec l'apparition des micro-ordinateurs et des portables faciles à emporter (4).

Mais il peut également s'agir :

- de vols de données c'est-à-dire d'un détournement d'informations :
  - . copie d'un fichier client (3),
  - . d'un savoir-faire (19)

**et souvent, les vols de données s'avèrent plus dangereux et plus coûteux que les pertes matérielles.**

- de vols de logiciels : le piratage est très fréquent dans le cas des micro-ordinateurs, plus rare pour les grands systèmes.

#### **- Le sabotage**

Il peut s'agir d'actes de résistance à la mise en place d'un SI, d'actes de vengeance ou encore d'actes gratuits. Pour certains “ petits génies ”, cela constitue un jeu, un défi...

Le sabotage peut se manifester de plusieurs façons :

- le bris de matériel (7)
- les virus (17)
- La destruction ou la modification de données (21)

### **b) Les actes non volontaires et les autres risques**

#### **- Les erreurs**

Il peut s'agir :

- d'erreurs de saisies (16)
- d'erreurs de date (utilisation d'anciennes versions)
- d'erreurs de conception et de réalisation des logiciels (5)
- d'erreurs d'inattention ou autres (14)

#### **- La négligence**

Certains utilisateurs ne sont pas conscients de l'importance de l'information présente dans les machines et font preuve d'insouciance vis à vis notamment des impératifs de confidentialité. Des gens laissent traîner des listings, quittent leur travail en laissant une disquette dans l'ordinateur, choisissent leur prénom ou celui de leur copain ou copine comme mot de passe, il y en a même qui utilisent des mots de passe comme "test" ou "system" qui sont les mots de passe attribués par les fabricants d'ordinateurs en attendant que les clients le changent.

#### **- Les risques divers**

- **le départ d'un salarié spécialisé** qui a tout mis en place et qui est le seul à savoir comment le système fonctionne peut engendrer, si celui-ci n'a pas constitué de documentation précise et lisible, la nécessité de tout recommencer

- **les grèves** peuvent bloquer le fonctionnement du système

## **1.2. Les accidents**

### **a) La défaillance du système, les pannes**

Occasionnée par un défaut ou par l'usure, la défaillance du système peut coûter très cher à l'entreprise si on est obligé de tout arrêter pour faire la réparation nécessaire (2).

### **b) Les risques extérieurs**

Ils concernent la destruction des locaux, du matériel, des logiciels, des données à cause des incendies, de la foudre, des inondations, des tremblements de terre... (6) (9).

## B) Statistiques sur les sinistres : enquête réalisée pour le Clusif publiée en mai 2001

### 1) les causes de sinistres

Dans de très nombreux cas, les responsables « système d'information » ayant répondu à l'enquête sont en mesure de dire avec précision si l'entreprise a subi un des types de sinistres répertoriés, mais elles ne peuvent pas fournir une mesure d'occurrence précise (nombre de sinistres de chaque type) ni d'évaluation financière. Ainsi seules 10% des entreprises procèdent systématiquement à une évaluation financière de l'impact d'un sinistre, cette proportion montant à peine à 17% des entreprises de plus de 500 salariés. Un seul type de sinistre est systématiquement chiffré : le vol de matériel. Il est



normal que le vol de matériel soit le plus facile à mesurer : la disparition d'une immobilisation apparaît en comptabilité, et est donc nécessairement chiffrée. De plus, le recours à l'assurance rend obligatoire le dépôt de plainte.

La mesure la plus fiable que nous soyons en mesure de fournir sur la sinistralité informatique en France est celle de la survenance, c'est à dire le pourcentage d'entreprises ayant été touchées par un type de sinistre donné durant l'année 2000. Les estimations d'occurrence (nombre de sinistres) et d'impact économique seront données à titre indicatif (entre autres à cause du nombre important de non-déclarations et de non-mesures).

L'erreur d'utilisation (23,9%) apparaît sans conteste comme le sinistre identifié le plus courant. Il sera pourtant le plus difficile à chiffrer, car il est considéré comme un problème quotidien, «normal». La qualité parfois très relative des logiciels bureautiques standards combinée à la «formation sur le tas» est un des éléments d'explication.

Le faible taux de survenance des sinistres d'ordre logique (par opposition aux sinistres matériels), et notamment des attaques logiques ciblées, est à rapprocher de la faible ouverture des réseaux des



entreprises et du manque de surveillance des réseaux (pratiquée par seulement 31% des entreprises), ainsi que d'une amélioration de la protection antivirale du moins pour les plus grandes entreprises.

Enfin, les sinistres les moins courants n'en sont pas moins réels : si seules 0,4% des entreprises françaises déclarent avoir eu au moins un cas de fraude informatique, cela représente tout de même plus de 6800 entreprises touchées en France durant l'année 2000.

Par faute de réponses en nombre insuffisant pour une analyse statistique, nous ne pouvons pas déterminer de manière fiable l'origine de la malveillance (interne, externe ou inconnue).

## 2) Le «hit-parade» des risques perçus par les entreprises

Lorsque l'on interroge les entreprises sur les risques qui les inquiètent le plus pour l'avenir, il est surprenant de constater que 18% des entreprises déclarent qu'aucun risque ne les inquiète particulièrement. *On retrouve là le décalage entre une perception du risque global (nous sommes conscients que le risque existe), la perception du risque pour l'entreprise (la probabilité que nous soyons touchés est très faible) et l'état réel des sinistres.*

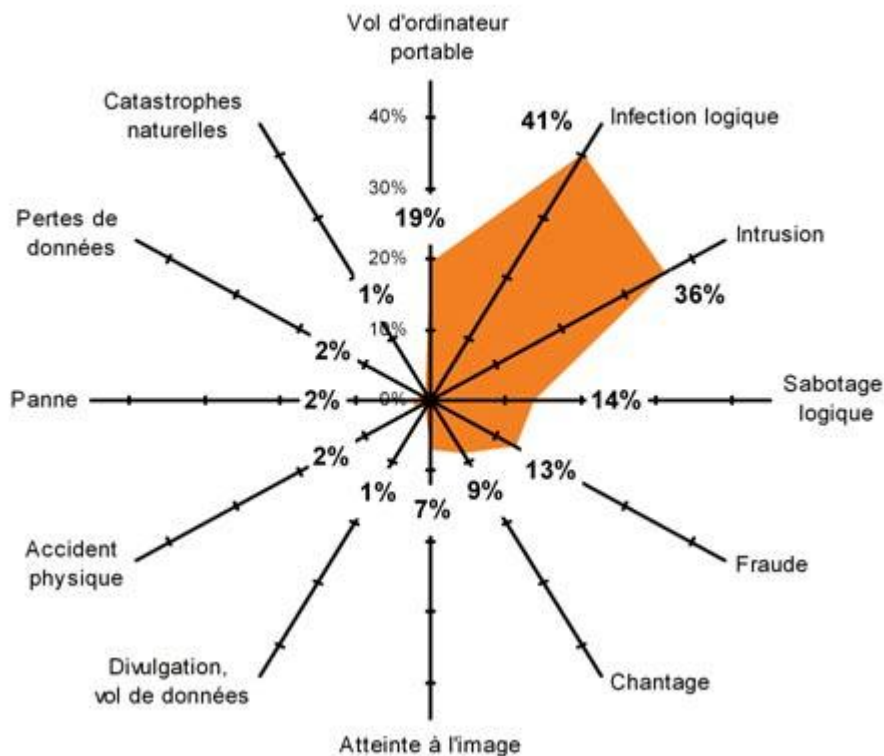
Parmi les entreprises qui déclarent craindre certains risques, les scénarios les plus médiatisés (virus et intrusion informatique) se placent en tête, loin devant les pannes et accidents, et ce contrairement à ce que montrent certains des tableaux précédents.

*Cette perception est à relier aussi à la conscience de la fragilité des mesures antivirales mises en place et au manque de surveillance des réseaux (mesure pratiquée par seulement 31% des entreprises).*

En revanche, seules les grandes entreprises et le secteur public affirment être préoccupés par le facteur humain. Ce dernier apparaît comme le grand absent de la perception du risque informatique et réseau tel qu'elle ressort de l'enquête.

Cette distorsion entre la réalité de la sinistralité et la perception qu'en ont les entreprises pose un réel problème quant aux méthodes à utiliser pour sensibiliser les entreprises sur les risques objectifs de sinistres. Nous sommes en fait confrontés à une problématique relevant plus des sciences de l'information et de la communication que de la technique informatique elle-même.

### Top 12 des risques cités par les entreprises



**Conclusion :** Les conséquences d'un sinistre (quel qu'il soit) pour une entreprise peuvent être énormes (utilisation d'informations inexactes, perte d'actifs, insatisfaction des utilisateurs, des clients...). Les questions d'organisation de la sécurité deviennent dans ce contexte essentielles.

## II. L'organisation de la sécurité

Les activités de gestion de la sécurité consistent essentiellement à analyser la vulnérabilité du système puis à définir les mesures adéquates. Après avoir décrit les principes de la démarche, nous présenterons les différentes mesures à prendre.

### 2.1. La démarche sécurité

Pour les responsables, la gestion de la sécurité se situe dans un avenir incertain. Certains sinistres résultent de combinaisons difficilement envisageables de causes variées, il faut estimer les événements en termes de possibilité, de vraisemblance, de plausibilité.

Une deuxième difficulté tient à l'incertitude quant au montant des pertes encourues si le sinistre se réalise. Le coût de la prévention doit en effet être ajusté en fonction de ce risque.

L'une des démarches les plus utilisées est la méthode MARION (Méthode d'analyse des risques informatiques et d'optimisation par niveau) proposée par le CLUSIF. Cette méthode a pour objectif la préparation d'un plan d'orientation soumis à la direction générale. Elle est articulée en six étapes :

**Etape 1 :** Analyse des risques : quels risques court-on ?

On essaie de déterminer qualitativement et quantitativement les risques encourus par le SI (il s'agit d'imaginer des scénarios de sinistres et de les décrire).

**Etape 2 :** Expression du risque maximum admissible : peut-on accepter ces risques ?

On essaie d'évaluer la capacité de résistance de l'entreprise face à ces sinistres : quelle perte peut-on raisonnablement accepter ?

**Etape 3 :** Analyse des moyens de la sécurité : quelle est la qualité de la sécurité actuelle ?

Il s'agit d'avoir une vision exhaustive et cohérente des moyens de sécurité existant.

**Etape 4 :** Evaluation des contraintes : quelles sont les contraintes majeures à respecter ? Certaines mesures de sécurité peuvent s'avérer inapplicables dans l'entreprise en raison de contraintes particulières :

- contraintes techniques (liées aux bâtiments, aux matériels...)
- contraintes humaines (problèmes de formation, de motivation, de convention collective...)
- contraintes financières (niveau maximum d'investissement)

**Etape 5 :** Choix des moyens : comment améliorer la sécurité ?

En tenant compte des contraintes, on essaie de trouver une solution de sécurité optimale en jouant à la fois sur la prévention (réduire la fréquence des sinistres) et la protection (réduire les conséquences de la réalisation d'un sinistre).

**Etape 6 :** Plan d'orientation : quel schéma d'action mettre en oeuvre ?

A partir des résultats de l'étape précédente, les orientations retenues sont mises en termes de budgets, de plannings, de description de solutions techniques à implanter.

## 2.2 Les mesures de sécurité

Il est très difficile de donner une liste exhaustive des mesures de sécurité susceptibles d'être appliquées à des SI. La description des causes des sinistres présentée dans le paragraphe précédent fournit un point de départ utile à la recherche de solutions concrètes. En effet, lorsque les causes de risques sont repérées, il faut choisir le type de parade à adopter. On peut jouer :

- **sur la prévention** : appliquer une parade à priori pour réduire ou éliminer le risque (ex : instaurer un contrôle d'accès aux locaux informatiques pour réduire les risques de vol ou de sabotage).

- **sur la protection** : définir a priori une parade qui appliquée après la réalisation du sinistre en réduira les conséquences dommageables (exemple : prévoir une copie de sécurité systématique des fichiers archivée dans un lieu différent réduit les dommages causés par un incendie du service informatique).

En définitive, les parades réduisent le risque à un niveau acceptable :

- en réduisant la possibilité de réalisation d'une menace,
- en limitant les dommages engendrés par la réalisation d'une menace,
- en permettant de détecter l'existence d'une menace,
- en transférant le risque à un tiers (assurance),
- en rendant possible la réparation des dommages engendrés par le sinistre (copie de fichiers par exemple)

A titre d'exemple, nous présentons quelques mesures parmi les plus souvent utilisées :

**a) La sécurité physique des ressources**

Elle concerne la protection des locaux informatiques, des matériels, des réseaux, des fichiers. Les principales mesures de prévention consistent à prévoir des locaux adaptés, une protection incendie et dégâts des eaux rigoureuse (ne pas mettre la salle informatique à côté des toilettes, la surélever...), une sécurité d'accès aux locaux : système d'identification à l'entrée (lecteurs de badges, serrures à codes...), alarmes...

La protection physique peut consister à répartir les matériels sur plusieurs sites et surtout prévoir systématiquement, ce qui n'est pas toujours fait, des copies de fichiers et de programmes.

**b) La sécurité logique des ressources**

Les dispositions de sécurité logique protègent les ressources immatérielles (données, programmes...) contre les erreurs et les malveillances.

- **Contre les malveillances** : Les systèmes informatiques, de plus en plus faciles à utiliser, sont désormais davantage exposés à des utilisations non-autorisées parce que les individus sont mieux formés et que les données et les programmes sont accessibles à travers de nombreux points des réseaux.

**Définition** : “un système sûr est un système qui, à travers l'utilisation de dispositifs spécifiques de sécurité, permet de contrôler l'accès à l'information de telle manière que seuls les individus dûment habilités puissent lire, écrire, créer ou détruire de l'information ” (National Computer Security Center).

On doit gérer l'accès des individus aux informations et aux programmes à l'aide de mots de passe (bien choisis et modifiés régulièrement) ou de le cryptage (qui consiste à transformer les informations contenues dans un fichier en les codifiant selon des formules mathématiques complexes), il faut gérer les droits de ces individus (un utilisateur peut avoir le droit de consulter une information mais pas de la modifier...). Ces systèmes doivent en outre conserver une trace de toute utilisation...

- **Contre les erreurs** : toute application doit normalement prévoir des procédures de contrôle protégeant contre les erreurs de saisie (exemple : dans un logiciel de comptabilité : débit doit être égal à crédit).

**c) Des mesures d'ordre général**

La sécurité des SI peut être grandement améliorée par des mesures d'ordre général tels que :

- la séparation des fonctions, qui est un des principes fondamentaux du contrôle interne. Il permet de réduire les risques d'erreurs et de malveillances (l'accord de plusieurs personnes est nécessaire pour que l'opération soit réalisée...),

- les opérations de recrutement des personnes sensibles (ingénieurs systèmes, administrateurs de données...) doivent s'accompagner de garanties sur les compétences et sur la moralité,

- La rotation des individus à un poste améliore aussi la sécurité (mais crée d'autres problèmes),


- Des actions de formation sont aussi utiles pour réduire les erreurs.

**d) L'assurance**

Les mesures de prévention et de protection ne peuvent totalement éliminer les risques. Il est donc conseillé de s'assurer pour couvrir les risques accidentels classiques (tels que le feu, l'eau, les vols...) et les risques informatiques classiques (fraude, détournement d'informations...). Les assurances couvrent en général à la fois les pertes matérielles, les frais de reconstitution d'informations (fichiers, programmes) et les pertes d'exploitation découlant du sinistre.

**Conclusion :** La sécurité informatique est un enjeu considérable, les statistiques montrent un accroissement de son importance. Dans la mesure où il peut mettre en jeu la survie de l'entreprise, où les mesures à prendre ne sont pas simplement techniques mais relèvent aussi de l'organisation et du contrôle, **la question de la sécurité n'est pas qu'un problème de spécialistes de l'informatique mais aussi un problème de gestionnaires.** Penser que la sécurité est totalement assurée par des dispositifs techniques est une utopie dangereuse. Sans réflexion organisationnelle, sans sensibilisation et formation des individus, elle ne sera pas efficace. Au total, l'étude approfondie des SI (tant sur le plan de l'évaluation ou de la sécurité que sur celui des impacts organisationnels et humains de la mise en place d'un SI) mettent en avant un phénomène nouveau : au début de l'informatique, les informaticiens sont apparus omniprésents et seuls capables de maîtriser l'ensemble des problèmes posés par l'outil informatique. Mais aujourd'hui, l'utilisateur, longtemps considéré comme un "client passif" se limitant à exprimer "maladroitement" des besoins confus, est devenu un partenaire actif dans la définition et la construction des SI. De ce fait, le succès des SI passent aujourd'hui certes par des informaticiens compétents mais aussi de plus en plus par des utilisateurs formés, motivés et consultés.

## Les principes menaces pour les entreprises selon l'ANSSI

ANSSI | Agence nationale de la sécurité des systèmes d'information

ENTREPRISE > PRINCIPALES MENACES

### PRINCIPALES MENACES

*La déstabilisation, l'espionnage, le sabotage et dans certaines conditions la cybercriminalité constituent les principales menaces traitées par le Centre de cyberdéfense.*

Perpétrées par une large palette d'acteurs, de l'individu isolé à des organisations offensives étatiques, les attaques se limitent rarement à une seule technique. Si les tendances généralement observées attribuent plutôt la déstabilisation (défigurations, divulgations de données et prises de contrôle) aux hacktivistes, le rançongiciel et l'hameçonnage aux cybercriminels, l'espionnage aux concurrents et aux États, on constate aussi que des attaques simples peuvent être le fait d'États et des attaques complexes le fait de groupuscules ou de structures criminelles organisées.

Les conséquences des attaques concernent une multiplicité d'enjeux. La portée financière dépasse de très loin des postes informatiques à remplacer ou des systèmes à repenser intégralement. Dénis de service, défigurations, exfiltrations et divulgations de données, prises de contrôle d'un système informatique : la crédibilité de l'organisation victime est en jeu... Ces quatre types d'attaques très employés par les hacktivistes visent essentiellement à porter atteinte à l'image de leur cible. Bien souvent, les attaques sont revendiquées en temps réel sur les réseaux sociaux ou des sites spécialisés.

La combinaison d'une attaque informationnelle (exploitation des réseaux sociaux pour amplifier) avec une attaque informatique maximise cette recherche d'atteinte à l'image.

Si elles sont souvent le fait d'hacktivistes, ces attaques sont parfois également commises, voire organisées pour les mêmes raisons de recherche d'atteinte à l'image ou de décredibilisation de leur cible par des concurrents, des employés mécontents, voire par des organisations étatiques.

Pour réaliser leur objectif, les attaquants choisissent différents types d'attaque selon le niveau de protection de leur cible et le contexte.

#### UNE FINALITÉ VOIRE UN PRÉALABLE : LA PRISE DE CONTRÔLE DU SYSTÈME

La prise de contrôle à distance d'un système informatique reste une finalité voire un préalable de nombreuses attaques informatiques constatées par l'ANSSI. En cas de révélation publique d'un tel événement, l'atteinte à l'image et à la crédibilité est également préjudiciable à sa victime.

L'attaquant exploite des vulnérabilités généralement bien connues ainsi que les faiblesses de la sécurité des systèmes informatiques : mauvaise configuration, non-application des mises à jour de l'éditeur... , qui constituent une surface d'exposition importante aux attaques.

<https://www.ssi.gouv.fr/>