# Management de la Sécurité de l'Information

***Vision résumée***

## Introduction

*Avez-vous déjà rencontré des difficultés avec vos informations ?*

*Vous êtes-vous déjà posé la question sur la sécurité – l'insécurité – les dangers de l'internet ?*

*Vous êtes-vous déjà inquiété de ce que vous pourriez faire si le degré de confiance dans les informations que vous recevez ou celles que vous produisez en venait à disparaître ?*

### L'information

Vos informations dans vos activités peuvent être comparées au sang circulant dans l'organisme humain. Ce facteur 'métabolique' de vos activités doit occuper la première place dans votre esprit, bien avant les questions d'argent. Car celui-ci ne remplit les caisses que si vous avec livré un produit ou un service qui a répondu aux besoins de vos client.

Ce besoin est une information de base. Votre offre que vous présentez pour répondre à cette demande (produit ou service, prix) en est une autre

L'information est donc tout ce qui entre dans tous vos processus (d'échange, de transformation ou de stockage) tout autant que ce qui en sort.

La qualité des données ***et des processus*** vous permet d'atteindre vos objectifs de façon efficace, rentable et durable. C'est la sécurité qui vous garantit cette maitrise et la vraie continuité de vos activités contre les défaillances et les actes délibérés.

Notons que l'information est bien plus que la donnée informatisée. Cette donnée n'a une signification que dans le contexte de sa collecte et de son utilisation. C'est cette signification qui lui apporte sa vraie valeur.

L'information peut se présenter sous des formes variées, être enregistrée sur tout support (papier, électronique, pierre). Elle peut être transmise par différents moyens (l'informatique, les télécommunications, … la voix humaine, etc.).

### Le problème

L'insécurité est indissociable des risques… et les risques existent toujours.

Il ne suffit pourtant pas d'en faire le simple inventaire, encore faut-il se décider à les gérer… Souvent le constat d'insécurité fait suite à une catastrophe que l'on admet comme ''ayant pu être évitée''.

Nous faisons face à un regrettable retard par rapport aux événements…

La plupart des entrepreneurs, pourtant soucieux de la sécurité de leur entreprise, se contentent de se rassurer à bon compte en faisant l'acquisition d'un outil de protection (une application ou du matériel).

Sur base de quelques conseils glanés, ils s'autorisent à faire l'impasse sur la réflexion de fond.

Il semble que seul soit abordé le volet commercial et financier du problème. Ils n'ont aucune attitude de protection face à l'éventualité d'une catastrophe touchant leur entreprise.

## Prévenir avant de guérir

Mettre en regard les faiblesses de protection de ses données et les moyens que l'on se donne pour y remédier est une démarche responsable et exigeante.

Les bonnes questions à se poser sont clairement :

- Sommes-nous sûr de traiter avec la 'vraie' personne, celle qu'elle prétend être ?
- L'information que j'échange arrivera-t-elle bien 'intacte' à la destination voulue ?
- Un intrus peut-il s'introduire dans mes systèmes informatiques sans que je m'en aperçoive, avec tous les dégâts directs et indirects que cela entraînerait ?

Les conséquences de cet attentisme sont doubles pour les experts : elles leur laissent le désagréable sentiment de ne pouvoir réagir qu'en mettant un emplâtre sur une jambe de bois. Mais, et surtout, il leur apparaît clairement que le remède utilisé semble « en retard d'une guerre » quant aux dangers 'à venir'.

On a des réactions statiques en réponse à des attaques mobiles et dynamiques.

Il serait sage de chercher à s'attaquer à la stratégie de l'ennemi plutôt que de se contenter de contrer sa technique offensive.

La plupart du temps, les 'sinistrés' se contenteront donc de répondre ponctuellement, en mettant en place des systèmes d'évitements calibrés en fonction du récent accident.

*Si l'on ose un parallèle avec une personne désirant perdre du poids, il est de notoriété publique que chacun préfère tester différentes propositions 'dites miraculeuses', plutôt que de se remettre en question quant à sa façon de se nourrir, quant à son hygiène de vie ou ses habitudes trop sédentaires.*

Et par le fait d'une étrange alchimie, l'angoisse va s'en trouver momentanément apaisée, alors même que le problème subsiste, et que les causes se renforcent.

**Le danger n'a donc pas été écarté.**
**Il a été déplacé, dans le temps ou dans l'espace.**

Il est évident que la solution ne cadrait pas avec les véritables causes induisant le problème.

## Alors…Que faire ?

*Abraham Maslow*, sociologue et psychologue américain des années 1950, a publié le résultat de ses recherches sur le comportement humain dans sa « pyramide des besoins ».

Il constate que la Sécurité vient en seconde place, juste après la Survie.

Nos entreprises veillent de très près à leur sécurité financière, et c'est évidemment une bonne chose. Elles évitent de se pencher sur leur survie à long terme après grave imprévu majeur.

Mais elles font souvent l'impasse quant à la sécurité de 'leur pain quotidien' : à savoir, leur métier et ce qui s'y rapporte.

Seul l'aspect mercantile semble concerné au plan de la continuité et de l'expansion financière des affaires.

La vraie question concernant un éventuel 'désastre' en entreprise, c'est de savoir quelle est sa potentialité d'occurrence et quelles conséquences en dériveront. Dans tous les cas, il ne s'agit pas de se contenter de s'en tenir à l'aspect matériel, visible, concret et palpable des nuisances.

Après une catastrophe – qu'elle soit advenue à titre personnel ou qu'elle ait frappé une connaissance –, les statistiques montrent que seule une entreprise sur cinq, ayant réussi son redémarrage, est parvenue à conserver son activité au-delà de deux ans.
La résilience non préparée est donc souvent de très courte durée…

Par ailleurs, en ressources humaines, il est souvent tristement constaté que le personnel ne fait généralement guère partie du programme de résilience. Or, ces spécialistes, l'avenir prouvera à leurs employeurs qu'il n'est pas si aisé de les remplacer !...

Cette préoccupation basique ne semble toutefois pas rentrer dans la sphère de préoccupation et d'inquiétude du management. La compétence en elle-même n'est donc pas prise en compte, avec toutes les conséquences en cascade que cette 'négligence' laisse entrevoir.

Pour les gestionnaires avertis, ceux qui avaient déjà eu la sagesse de se pencher sur le concept même de 'risques', il semble naturel d'être mis en garde contre de graves effets secondaires.

Il s'agit d'attirer leur attention quant à la possibilité de trouver des solutions tant en amont qu'en aval, en réduisant au maximum les possibilités d'occurence, et en s'efforçant le cas échéant, d'en atténuer la gravité.

Pour atteindre ces objectifs, il faudrait :

1. Agir avec excellence et
2. Conserver la fidélité de ses clients tout en cherchant à en 'recruter' de nouveaux.

Comme dit dans l'introduction, tout métier – qu'il soit celui de menuisier ou celui de médecin – collecte, exploite, mémorise et produit des informations.

Quel que soit le travail, cette synergie génère de la réflexion, augmente les connaissances et permet de prendre des décisions ; elle permet en toute logique, ensuite, de mener des actions et d'en mesurer les résultats.

Nous avons la conviction qu'une entreprise qui jouit d'une grande renommée est celle qui répond aux besoins de chacune des parties prenantes qui se sont engagées durablement.

Les intérêts représentés sont ceux du «cadre sociétal», des clients, du personnel, des investisseurs, des patrons, du personnel, des partenaires et des fournisseurs.

## Gérer l'information

La première action, simple, est de gérer cette information 'en bon père de famille'. Les deux points difficiles à circonscrire sont :

1° La quantité, qui est souvent astronomique
2° Une information qui est 'immatérielle', difficilement localisée car stockée sur un ou plusieurs serveurs ou supports.

Faisons un simple parallèle avec notre consommation alimentaire : comment 'gérons-nous' la nourriture consommée ? Que ce soit le sandwich du déjeuner quotidien, le repas entre copains ou le dimer gastronomique prévu pour cinquante convives lors d'une grande occasion.

- Où et comment en faire l'acquisition (collecte) ?
- Comment les séparer en catégories d'utilisation et ne pas briser la chaine du froid ?
- Comment les inventorier, pour toujours savoir ce dont on dispose (inventaire et catégorisation) ?
- Comment déterminer leur valeur réelle (classification : nutritive, diététique, gustative, de présentation *car nous mangeons autant avec les yeux qu'avec la bouche*) ?
- Comment et où les stocker ? Comment séparer le périssable de la conservation à long terme (stockage) ?
- Comment les déplacer et les remettre à ceux qui les utiliseront (transfert, échange) ?
- Comment les utiliser de la meilleure façon (préparation et consommation – exploitation) ?
- Comment se débarrasser des restes et des déchets (mise au rebut - évacuation) ?
- Que faire des mets et provisions non utilisés ?
- Comment gérer les vivres périmés ?

## Déterminer la valeur

En termes d'informations, nous parlons de classification. Cette mesure de valeur utilise quatre facteurs :

- La **valeur propre** - le coût d'acquisition et de gestion
- La **valeur d'usage** – la valeur pratique quant à ce que vous voulez en faire
- La **valeur d'attraction** – l'inclination à prendre un renseignement chez vous plutôt que de l'acquérir ailleurs (chez un fournisseur plutôt qu'un autre ; c'est la valeur d'usage de ceux qui travaillent contre vous, y compris la valeur d'un usage malsain dirigé à votre encontre), tout en considérant sa motivation, son désir de la subtiliser et sa capacité à le faire, et son intérêt à vous la trafiquer.
- La **valeur de perte** – la gravité des conséquences qui sont liées à la perte physique de cette information ou à la perte de qualité intrinsèque de votre point de vue… (ce qui se passerait si l'information ne répondait plus à vos attentes).

La valeur de perte se mesure à l'aide de ce que l'on peut appeler des axes de sensibilité :vos objectifs et vos enjeux. Les trois critères classiques de sécurité sont :

- La **confidentialité** ;
- La **disponibilité** ;
- L'**intégrité** (c'est très souvent le critère le plus exigeant).

Les évènements redoutés correspondants, car impactant vos objectifs et vos enjeux, sont :

- La **modification intempestive** (dont les conséquences non évaluées peuvent déboucher sur de véritables catastrophes).
- L'**indisponibilité** au moment et à l'endroit où vous en avez spécifiquement besoin. En effet, la disponibilité prompte et instantanée fait partie des critères de valeur.
- La **divulgation** ou la diffusion non contrôlée de l'information à trop large spectre, lui permet d'être perçue par ceux qui n'ont pas à la connaître.

Personne n'est en mesure de parier sur le futur, mais il est toutefois possible d'imaginer les principaux scénarios capables d'affecter vos données. Vous en évaluerez prospectivement le juste degré des retombées négatives.

## Gérer les risques

Les risques se gèrent, comme toute chose, en travaillant sur une évaluation de vraisemblance d'occurrence, et de gravité quant aux conséquences.
Rappelons-nous que nous traaillons avec des perceptions, des incertitudes et des probabilités.

Le processus simplifié de gestion des risques est le suivant :

- Déterminer l'objet de notre inquiétude –
  Quelles sont les informations et les processus qui ont le plus de valeur à nos yeux ? D'où l'importance de focaliser notre attention sur l'essentiel.

- Déterminer le contexte de leur utilisation – les lois, règlements et contrats dont nous dépendrions. Il s'agit d'être cohérent et exhaustif.
  - Induiraient-elles des contraintes ?
  - Des dispositions sont-elles à prendre ?
  - Des objectifs majeurs sont-ils impliqués ?
  - Des protections juridiques ou des dispositifs de défense préventive (démarche juridique telle que le recours à un avocat) sont-elles à envisager?

- Estimer le risque – Quel degré de vraisemblance et de dommage direct et immédiat peut-on supposer?
  Ici, il est permis d'être (un peu) paranoïaque…
  La question « ***Et si… ?*** » est conseillée et encouragée !

- Evaluer le risque – Cet éventuel dommage peut-il avoir un effet sur vos objectifs, vos valeurs, vos enjeux ?
  A ce stade, il s'agit d'être réaliste.
  Cette phase est souvent omise, qui répond à la question : «***Et alors …?***»…

L'évaluation des risques aboutit à l'élaboration d'une liste hiérarchisée des risques jugés inacceptables.

- Traiter le risque – Déterminer ce que vous pouvez et voulez faire pour rendre ces risques 'acceptables'.
  ***Soyons pragmatiques, et retroussons nos manches pour mettre en œuvre les décisions qui s'imposent.***

Ce processus de gestion des risques peut être rapide et efficace ; nul besoin de le complexifier car c'est une dépense excessive et inutile.

Il faut savoir si le risque vaut l'investissement qu'il génère.

## La sécurité de l'information

Trop souvent, la sécurité est considérée comme une contrainte car elle est synonyme d'obstacle, de dépense. Ma conviction, c'est qu'une focalisation sur ce qui est **Important et Urgent**, vous affranchit de certaines contraintes ; la sécurité vous rend plus autonome ; elle vous libère de vos craintes, des surprises désagréables, des évènements insupportables…..

Considérons la sécurité sous son angle positif : elle s'apparente bien plus à la souplesse salvatrice du baudrier et des accessoires de l'alpiniste qu'à la rigidité statique du coffre-fort.

La sécurité se doit d'être un investissement qui vous libère d'inutiles préoccupations ou angoisses ; elle soutient la qualité, l'efficacité, la rentabilité et la durabilité de votre entreprise. L'investissement portera ses fruits à bien des niveaux. Les résultats ne manqueront pas de se faire sentir plus tôt que vous n'osiez même l'envisager.

## Conclusion

Ceci est une réflexion consciente que tout chef d'entreprise, et que chacun même, devrait s'imposer lorsqu'il désire consolider son projet et en assurer la réussite quelles que soient les circonstances.

Cette approche se donne pour vocation de n'être qu'un résumé et une adaptation voulue des recommandations quant au développement personnel, appliqué au cadre de la gestion de votre entreprise et de son 'patrimoine informationnel'.

*Nous ne vivons pas dans un monde philanthropique !...*

Le monde virtuel auquel internet nous donne accès, secondé par les merveilles de l'informatique, nous apporte de nombreux avantages. Mais ne perdons toutefois pas de vue qu'il s'accompagne inévitablement de nombreuses menaces qui peuvent s'avérer être une permanente épée de Damoclès qui génère un spectre d'incertitudes.

Ces permanentes épées de Damoclès, ces spectres génèrent à tout le moins une sérieuse inquiétude que l'on se doit de gérer.

A très bientôt.

***Plus en sécurité avec vos informations***
***Jean-Luc Allard***

Spécialiste dans le domaine de la gestion de l'information, de ses risques et de sa sécurité depuis 20 ans, je mets mes compétences patiemment acquises à votre service.

www.misis.be - jeanluc.allard@misis.be
www.info-attitude.com