Sécuriser vos informations

Guide de démarrage

eBook
offert
par **Jean-Luc Allard**
du site
www.info-attitude.com

Bonjour à vous

Merci d'avoir téléchargé cet eBook qui est une mise en bouche sur un domaine qui me tient à cœur depuis plus de vingt ans et semble peu prisé.

Ce Guide de Démarrage vous permettra de mieux appréhender la problématique de sécurité de l'information et de savoir comment une sécurité bien adaptée peut à la fois vous éviter une quantité de dépenses inutiles et vous apporter des gains là vous ne les attendez pas.

Il devrait vous apporter les éléments de base afin que, dans le monde fort insécurisé que nous connaissons, vous obteniez ***« l'assurance suffisante que vos informations (de valeur) sont à l'abri des évènements inacceptables. »***

La sécurité – ou la protection – de l'information est importante car elle nous apporte la confiance dont nous avons besoin pour l'utiliser au jour le jour. Après tout, à quoi sert une information à part accroitre nos connaissances, prendre des décisions et agir ? L'information est le sang de notre vie privée, sociale et professionnelle. Son acquisition, sa mémorisation, son échange, sa transformation sont notre unique tâche quotidienne.

Ma mission — tant celle de mon activité professionnelle que de mon blog — est de construire cette confiance dans les informations que nous manipulons et dans les manipulations que nous leur faisons subir.

Ma vision est que la protection adéquate de l'information est le seul moyen de construire cette confiance et de nous libérer des incertitudes dans lesquelles le monde moderne nous plonge. Comme les freins d'une voiture vous permettent d'aller vite, l'application du principe de précaution en rapport aux informations est libératoire.

La sécurité (dans tous les domaines) est plus une question d'attitude et d'habitudes que de technologies. Avez-vous déjà tenté de conduire sans utiliser vos freins ? Ce n'est pas aussi facile qu'on pourrait le croire…

Tout au long de votre lecture vous apprendrez une série de concepts et d'actions de base vous permettant de voir de manière plus claire les dangers auxquels nous sommes tous soumis (voir Chapitre II - pages 8 et 9).

Vous trouverez dans cet eBook des actions simples et efficaces, tout autant que des pistes pour aller plus loin si le jeu en vaut la chandelle… Parce que toutes les informations ne doivent pas être protégées à un niveau élevé ! (voir Chapitre V - pages 29 à 39).

Les informations contenues dans le texte repris dans la photo de couverture ont été bien protégées :

- *sur la durée (sculptées dans la pierre) – Disponibilité*
- *sur le contenu (très difficiles à modifier sans que cela se voie) – Intégrité*
- *sur la signification et la valeur (les hiéroglyphes n'ont été déchiffrées qu'au début du XIXe siècle) – Confidentialité*
- *sur sa dédicace complète – Traçabilité.*

Disponibilité, Intégrité, Confidentialité et Traçabilité sont les quatre critères fondamentaux en sécurité de l'information. Nous verrons ensemble comment assurer ces critères et nous apporter la confiance nécessaire à une utilisation consciente, cohérente et satisfaisante des informations.

(Crédit Photo page de couverture : Dreamstime)

Partagez ce guide autour de vous !

Ce guide a été créé dans le but d'être lu par un maximum de personnes. Je le propose gratuitement car je souhaite que tout le monde puisse y avoir accès et en profiter. Je vous invite donc à l'offrir en cadeau à votre entourage.

Vous êtes libre de le publier où bon vous semble (par email, sur les réseaux sociaux, aux abonnés de votre newsletter, sur votre blog, etc.)

Cependant, vous n'êtes pas autorisé à le vendre, ni à l'intégrer dans des offres punies par la loi (chaîne de lettres, système pyramidal, etc.)

Amicalement, Jean-Luc

Qui suis-je ?

Je m'appelle Jean-Luc ALLARD.

Enfant, je rêvais de devenir médecin et mon père m'appelait 'Docteur Paillasse' car je ne savais pas me lever le matin. J'ai donc changé d'option et suis devenu ingénieur en électronique.

C'est sous l'uniforme d'officier de la Force Aérienne belge que j'ai été plongé, par habitude, dans la sécurité de l'information et des communications.

Mon activité professionnelle est, depuis 1995, exclusivement dédiée à la sécurité de l'information, la gestion des risques et les politiques de sécurité. L'opportunité de représenter mon pays dans les groupes de travail de l'OTAN à ce sujet, les intérêts d'une entreprise émergente dans des contrats porteurs à l'étranger et l'industrie belge auprès de l'ISO (depuis 2005) pour ce qui concerne « le management de la sécurité de l'information » (série ISO/IEC 2700x) ont été l'occasion d'une explosion de mes connaissances et de mon plaisir à jouer dans ce bac à sable.

Actif au sein de l'ISACA, j'ai participé à la rédaction de la publication « BMIS[1] » Business Model for Information Security et je conserve (depuis 2000 et 2002) les certifications CISA et CISM.

Retour aux origines ?

En fait, je ne suis pas tellement éloigné de mon rêve d'enfance… je soigne les processus informationnels qui sont peu efficaces et efficients ainsi que les informations en danger. C'est une activité entre le psy et le développement personnel focalisé sur quelque chose de particulièrement virtuel et volatile, mais que nous manipulons tous les jours, sans y faire trop attention.

Mon rêve dans la vie est de créer et répandre l'harmonie et l'équilibre. Ce qui se marie bien avec mon amour de la musique et du chant choral (comme choriste et chef de chœur). Autant que la recherche de la sécurité…

J'aime le travail bien fait et vite fait. J'apprécie donc le fait de travailler dur dans les phases de développent et de mise en œuvre afin de disposer, ensuite, d'une activité simple, rapide et efficace, ce qui me permet de découvrir d'autres horizons.

[1] Ce document est accessible - en anglais uniquement - à cette adresse : http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

Sécuriser vos informations
Guide de démarrage

Table des matières

I. Pourquoi devez-vous sécuriser vos informations

Nous vivons dans un monde fortement insécurisé. J'en veux pour preuve l'agressivité – croissante – de tous : adultes et enfants, au travail, sur la route et à la maison, ainsi que le repli sur soi ou l'individualisme à outrance.

Ce qui importe, c'est de créer un environnement de sécurité – une bulle où nous nous sentons en confiance - qui nous soit propre, en tenant compte de notre situation (ou contexte), de nos besoins et de notre perception des risques.

Le propos de ce guide concerne l'information et tout ce qui lui est rattaché.

Que l'on soit une personne privée ou une organisation (personne morale – PME ou plus grande entreprise), il est question de se créer une 'zone de confort' et une 'zone de contrôle' dans lesquels nous maîtrisons les informations et leur utilisation. Les informations y résident, entrent, sortent et disparaissent.

La gestion adaptée des risques doit permettre d'identifier ce qui est inacceptable ainsi que l'urgence d'agir. C'est un des seuls moyens de considérer la sécurité comme un aspect « positif » et non comme une contrainte, et de recevoir l'acceptation de tous ceux qui sont impliqués : décideurs, investisseurs, gestionnaires et utilisateurs.

Ce *Guide de Démarrage* vous permettra de mieux appréhender la problématique de sécurité de l'information et de savoir comment une sécurité bien adaptée peut à la fois vous éviter une quantité de dépenses inutiles (coût des réparations et dédommagements) et vous apporter des gains là vous ne les attendez pas (économies et rentrées d'argent grâce à la confiance que vous inspirez).

Le Retour sur Investissement (ROI) d'une 'bonne' sécurité de vos informations dépassera vos espérances que vous soyez une personne physique ou une organisation.

II. Pourquoi vos informations ne sont pas en sécurité

Le concept même d'information est flou et on le sent virtuel. Cela ne facilite pas son étude et son contrôle.

Parallèlement, les actifs liés à l'information et qui supportent toutes les actions de base ne sont pas toujours bien identifiés ni pris en compte, alors qu'ils sont les premiers exposés aux problèmes.

Enfin, ce que l'on fait avec l'information et ce dont on a besoin pour le faire sont peu définis, mal compris et peu maîtrisés.

Le concept, approches et méthodes de gestion des risques, pourtant fort développées et efficaces dans de nombreux domaines, sont mal compris et mal appliqués en ce qui regarde d'information.

Le concept de sécurité est mal interprété et considéré comme un obstacle, une contrainte, une dépense dont on se passerait bien. Il s'ensuit que la sécurité de l'information est peu ou pas considérée et, quand c'est le cas, on ne s'intéresse qu'à la sécurité informatique. Comme si information et l'informatique étaient synonymes.

Je fais souvent le parallèle avec la sécurité routière. Qu'est-ce qui prime : une voiture bien conçue et en parfait état ou la protection des usagers 'faibles' – les êtres humains ?

Le résultat en est un manque de cohérence dans la gestion tant de l'information que de sa sécurité et de la gouvernance à ce sujet.

Cependant, notre monde économique, culturel, politique et virtuel d'aujourd'hui est particulièrement insécurisé et incertain. Pour les spécialistes, on est, depuis deux décennies au moins, en pleine guerre de l'information. Ne sommes-nous pas submergés d'informations au point de ne plus savoir à laquelle se fier ?

Beaucoup de ceux qui s'inquiètent de ces questions sont enfermés dans des croyances limitantes qui affirment : « De toute façon, on ne peut rien y faire… ».

D'autres, plus optimistes, répondent : « Je n'ai pas d'inquiétudes à ce sujet… », « J'ai déjà fait ce qu'il fallait… » ou « Est-ce vraiment important et grave ? »

Un troisième groupe dort sur ses deux oreilles en pensant que « Ca n'arrive qu'aux autres… »

Big Brother

Ceux qui ont lu « 1984 » de Georges Orwell avec son 'big brother', ou qui ont vu (entre autres) « Traque sur Internet » avec Sandra Bullock et « Firewall »

avec Harison Ford pensent sans doute que ce n'est que du cinéma. Je peux vous affirmer que ce n'est pas vraiment le cas.

Qui n'a pas été choqué par les scandales Wikileaks et Snowden et ces histoires des Etats-Unis qui espionnent les citoyens, les industries et les gouvernements européens. Ils y gagnent naturellement les marchés au détriment de l'Europe, nous ralentissant dans nos efforts de nous relever de la crise économique causée par un dysfonctionnement américain.

Connaissez-vous la cause de cette crise économique ? Simplement le fait qu'on a confié (sans vrai contrôle humain) des décisions à des ordinateurs. Des décisions basées sur des formules (des processus) mal conçus et utilisant des facteurs imprécis. Un de ces facteurs a dépassé les limites prévues et tout s'est emballé par un effet d'avalanche. C'est un très sérieux problème de sécurité de l'information.

Nous sommes 'tous fichés', nous le savons.

Nos déplacements sont enregistrés et exploitables. Il suffit d'interroger les relais de téléphones portables. On peut vous localiser dans un rayon de 1 km.

Avec votre carte de banque ou de crédit, que l'on peut suivre 'en direct', on sait dans quel magasin vous êtes et ce que vous achetez.

Les caméras sont partout et on peut vous identifier au volant commentant une infraction ou dans les parages d'un cambriolage.

Sur internet, on se trouve dans une sorte de zone de non-droits – enfin, c'est un sentiment général. Un no mans land.

Laissez-moi vous raconter quelques histoires vraies…

Vider votre compte en banque

Il suffit de disposer de papiers vous identifiant avec votre adresse et des éléments concrets, comme une facture d'électricité, pour introduire à la police une déclaration de perte ou de vol de papiers d'identité et de passer à la banque déclarer la perte de votre carte de banque.

> ***Trois ans pour des escroqueries commises grâce à une usurpation d'identité***
> Le tribunal correctionnel de Tournai a condamné mardi par défaut Elise M. à une peine de trois ans de prison et à payer 1.500 euros à la partie civile pour des faits d'escroquerie et de vol commis grâce à une usurpation d'identité. En juillet 2007, la prévenue avait volé le sac à main de la dame qui l'avait prise en stop le long des boulevards à Tournai et elle avait utilisé les papiers d'identité de la victime pour contracter des prêts à tempérament et acheter des objets à crédit. Elle a finalement été interpellée quand elle s'est présentée dans une banque

pour retirer 6.000 euros. La jeune femme était en état de récidive. Pendant deux ans, la victime a multiplié les démarches pour dénoncer ce vol mais les policiers sont restés sceptiques avant que, finalement, une plainte pour usurpation d'identité soit prise en considération par les policiers de Tournai. (b)

***Faits divers - Un inconnu a usurpé l'identité du député wallon Écolo et lui a vidé son compte en banque* –**

Vendredi 16 mars 2012

Découverte un peu par hasard sur le réseau social Facebook, ce jeudi matin, l'information interpelle. « À la banque puis à la police pour déclarer une usurpation d'identité et un compte en banque pillé ! » Premier réflexe de compassion : encore un ami qui va passer une bonne journée. Puis, plus égoïstement : bien content que ça ne me soit pas arrivé.

Passé le côté anecdotique, l'envie d'en savoir plus survient. La victime n'est pas n'importe qui puisqu'il s'agit de Manu Disabato, député wallon Écolo de Frameries. Comment a-t-il pu se faire détrousser de la sorte ?

« Mercredi midi, je suis sorti et je me suis rendu à un distributeur automatique afin de chercher de l'argent pour m'acheter à déjeuner, relate l'élu. Soudain, le distributeur avale ma carte et me signale un prétendu problème technique. J'essaie alors avec ma carte Visa mais elle m'est restituée par l'appareil. »

Intrigué mais décidé à en savoir plus, Manu contacte immédiatement sa banque. Loin de se douter de ce qu'il allait y apprendre.

« On m'a dit qu'une personne s'était présentée à l'agence Fortis Banque de Schuman, à Bruxelles, en prétendant être moi. Cet homme avait un duplicata et affirmait s'être fait voler son portefeuille contenant tous ses papiers et cartes bancaires. Il a donc fait opposition sur ma carte bancaire et a demandé une carte temporaire sur mon/son compte. Une fois la carte obtenue, il a effectué un premier retrait. »

Mais l'homme avait de la suite dans les idées. Il n'allait pas en rester là. « Il s'est rendu dans une deuxième agence Fortis, poursuit Manu Disabato. Là, il a demandé, avec sa carte temporaire, à augmenter à 5.000 euros par semaine ma capacité de retrait. Ca a été accepté sans le moindre problème et l'homme s'est servi. »

C'est bien ce qui interpelle la victime. Comment peut-on aussi facilement faire confiance à quelqu'un qui introduit une telle requête ? Pourquoi n'y a-t-il pas plus de contrôles ? Et comment l'escroc a-t-il su que le député était chez Fortis ? L'homme est activement recherché. Les bandes vidéo des différentes banques vont être saisies et étudiées par la police. Côté financier, « ma banque devrait normalement me rembourser », espère le député.

Usurper votre identité et vous interdire toute vie sociale

Je me rappelle d'une histoire qui s'est passée en France en 2012…

Un homme avait perdu ou s'était fait voler son portefeuille avec tous ses papiers d'identité et ses cartes de banque. Un escroc s'en est servi pour vider son compte en banque, contracter des crédits que le plaignant – seule personne contactée par la banque puisqu'elle disposait de son adresse – ne pouvait pas rembourser. Il s'est retrouvé interdit bancaire. Il a également perdu son travail. Par une action parallèle de l'escroc, le plaignant s'est retrouvé impliqué dans des délits dont il a du se défendre. Il ne pouvait cependant pas redemander une nouvelle carte d'identité. Il s'est même retrouvé dans l'impossibilité – à cause de l'existence de deux personnes ayant la même identité – d'hériter de ses parents.

Choquant, non ?

L'ex de Delarue dépose plainte

Elisabeth Bost, l'ex-épouse et mère du fils de Jean-Luc Delarue a porté plainte, pour « usurpation d'identité », après avoir reçu dans les heures suivant la mort de l'animateur deux messages provenant de sa boîte mail. Plusieurs éléments laissent penser que ces mails n'ont pas été écrits par Delarue. Le ton des messages, très agressif, ne correspondait en rien aux mails que Jean-Luc Delarue envoyait à celle dont il était séparé depuis 2010. (afp)

Passer avant vous en vous volant vos idées

Est-il besoin de revenir sur de nombreux cas d'espionnage industriels permettant à un concurrent de vous voler vos idées et de gagner le marché (ou la place) que vous convoitez sans avoir supporté les frais de recherche et développement ?

Comment peut-on expliquer le nombre d'attaques (violentes et très lucratives) de fourgons blindés malgré les itinéraires aléatoires employés, sans s'interroger sur la manière dont les braqueurs ont été informés ? L'envoi de l'itinéraire se faisait par email ou par fax, deux moyens faciles à écouter.

Plagiat …

Ma fille aînée s'est trouvé confrontée à un problème inattendu qui lui a coûté cher…

Pendant la rédaction de son mémoire de fin d'études, elle copie des extraits de textes provenant de sources externes. Lors de la finalisation de son travail, un court extrait – de trois lignes – se retrouve coupé de sa source et de sa référence.

Bilan : Zéro pour plagiat !

Ou comment une petite erreur peut coûter cher…

Perte de documents/mauvais classement

Qui se souvient de l'information relayée il y a quelques années de cet employé anglais qui avait oublié ou perdu ou s'était fait voler une mallette contenant des DVD répertoriant toutes les données de sécurité sociale de dizaines de milliers de citoyens britanniques ?

Et cette erreur de manipulation d'un technicien des chemins de fer belges qui a exposé sur la partie publique du site internet, toutes les coordonnées de leurs clients ?

Facebook, l'autre côté du miroir

Facebook est notre 'vitrine' gratuite. On y dit tout et n'importe quoi… et à n'importe qui. N'avez-vous pas déjà entendu ce genre d'histoires ?

> *« Deux jours après être partie en vacances, mon appartement a été cambriolé… »*

Un homme se répand en critiques sur son employeur avec lequel il est en train de se séparer. De futurs employeurs font des recherches et trouvent son profil. Voyant les motifs et le mode des critiques, ils refusent de l'engager.

Eh oui, si la parole est d'argent, le silence est d'or !

10.000 comptes Twitter « hackés »
Le Soir, Mardi 12 juin 2012
Une équipe de développeurs Web a utilisé un faux site Internet pour dérober 10.000 comptes Twitter dans le but de montrer les dangers d'une connexion avec un compte Facebook ou Twitter à un site ou à une application…

Pervers au téléphone et sur internet

Il piégeait des adolescentes sur internet, leur demandant de se dénuder
Un homme de 32 ans comparaissait jeudi devant le tribunal correctionnel de Namur pour avoir attenté aux mœurs de jeunes filles mineures, pour harcèlement par téléphone ou sur internet, et pour viol sur l'une d'elles.
Le jugement est attendu pour le 21 février. (b)

Harcèlement sur Internet

Une adolescente de 14 ans se suicide parce qu'un copain a mis une photo d'elle nue sur Facebook…

Vous souvenez-vous du scandale des photos du Prince Harry lors d'une fête entre étudiants ?

Comme quoi l'amitié est souvent relative…

Le suicide d'une ado bouleverse le Canada

Le Soir, Mardi 16 octobre 2012

harcèlement - Son histoire est sur YouTube

Montréal

De notre correspondant

Les hommages à Amanda Todd fleurissent partout au Canada », titre la chaîne de télévision nationale CTV News. « Le monde pleure Amanda Todd », ajoute The Vancouver Sun. Le journal consacre toute sa Une à cette jeune fille de 15 ans qui a mis fin à ses jours mercredi dernier après des années de harcèlement à son école, mais aussi sur internet. Diane Sowden, l'avocate de Carol Todd, la mère d'Amanda, confie au quotidien : « Tout a commencé par un prédateur qui ciblait une pré-adolescente sur internet. Il lui a demandé des images d'elle et par la suite, il s'en est servi pour effectuer du chantage. »

Depuis quelques années, Amanda Todd, adolescente de Port Coquitlam, bourgade de la banlieue de Vancouver, en Colombie-Britannique, a vécu un véritable enfer. Elle raconte son histoire dans une vidéo qu'elle a postée sur YouTube au début du mois de septembre, avant de se suicider le mois suivant. Amanda cache son visage par des feuilles de papier qu'elle fait défiler devant la caméra. Sur ces feuilles, elle a écrit avec un stylo-feutre noir tous ses malheurs. La jeune Canadienne explique que c'est en 2007 qu'elle a commencé à utiliser une webcam pour parler avec ses amis. Elle rencontre un homme sur internet. Celui-ci lui demande de lui montrer ses seins. Elle accepte, mais elle refuse manifestement certaines de ses demandes. L'homme se venge. Il fait circuler des photos et des vidéos de l'adolescente sur le web, les envoie à ses professeurs, ses amis. La petite internaute devient la risée de son école.

Elle change d'établissement plusieurs fois. Rien n'y fait. Elle est parfois battue. Des enfants l'encouragent au suicide. Amanda Todd est désespérée. Elle déprime. Elle se drogue. Elle boit. Elle tente plusieurs fois de se suicider. Et finit malheureusement par y parvenir.

Le cas de cette ado de l'Ouest du Canada n'est pas isolé dans le pays, même si le plus souvent les conséquences ne sont pas aussi dramatiques. Selon l'enquête « Jeunes Canadiens dans un monde branché », que mène l'organisme Réseau éducation médias depuis des années, plus du tiers des élèves interrogés ont déclaré avoir été victimes de cyber-intimidation au cours de l'année scolaire. Les menaces prennent la forme de courriels haineux ou de harcèlement par messagerie instantanée. Ce sont aussi des vidéos compromettantes de

la victime, prises avec un téléphone portable et diffusées sur internet. Les cyber-intimidateurs les plus acharnés n'hésitent pas à bâtir un site Web pour dénigrer leurs victimes. Le Premier ministre de l'Ontario, Dalton McGuinty, a décidé d'ajouter la cyber-intimidation à la liste des comportements répréhensibles dans les écoles et désormais, les intimidateurs sont expulsés.
A la suite du décès d'Amanda Todd, Ottawa a promis de réfléchir à une stratégie nationale contre le cyber-harcèlement. Les députés canadiens devaient étudier le sujet ce lundi à la Chambre des communes.
La Gendarmerie royale du Canada (GRC) a décidé, elle, de prendre les choses au sérieux. L'enquête pour retrouver l'homme qui a harcelé la jeune fille mobilise une vingtaine d'enquêteurs. Le sergent Peter Thiessen, de la GRC, a déclaré : « Les équipes des crimes majeurs de Port Coquitlam et de Ridge Meadows travaillent ensemble, interrogent et passent en revue les facteurs potentiels qui ont contribué à sa mort. »
Selon Carol Todd, la police aurait repéré un suspect « aux États-Unis. Mais elle ne l'a jamais retrouvé. Ces gens sont très forts pour masquer leurs traces. »
Lundi, plusieurs centaines de milliers de personnes avaient rendu hommage à Amanda sur une page Facebook consacrée à sa mémoire. Mais le cauchemar a continué après sa mort. Des messages haineux se sont glissés entre les condoléances.

(Tous les extraits dans les encadrés ci-dessus sont repris des Archives du journal **Le Soir** (Belgique) - http://archives.lesoir.be/ avec les mots-clés : harcèlement internet, danger d'internet, usurpation d'identité. Recherche réalisée le jeudi 20 février 2014 au matin.)

Je pourrais allonger la liste presque à l'infini…

Etes-vous satisfait et 'à l'aise' avec cette situation ou voulez-vous, au moins, vous protéger, vous et vos proches, de ce genre d'évènements ? Alors…

Que faut-il faire ?

Avant de répondre à cette question, voyons ensemble ce qu'il ne faut pas faire… et ce que, malheureusement, bon nombre de professionnels font.

III. L'erreur fondamentale que vous faites

L'erreur fondamentale est la prise en compte partielle du problème qui apporte une réponse insuffisante et un faux sentiment de sécurité.

L'insécurité de notre monde d'aujourd'hui n'est pas due qu'à sa virtualisation (« Internet et télévision »). Elle est économique, sociale et informationnelle. Elle est alimentée par les tensions politiques et le terrorisme. Cela pousse chacun à se réfugier dans sa bulle et à avoir un comportement individualiste.

Cela se traduit par une approche individuelle - 'objet' - de ce que l'on fait. La sécurité d'un objet qui ne prend pas en compte l'environnement dans lequel il se trouve n'est pas efficace. Et la sécurité est rejetée en bloc comme une contrainte et une dépense inutiles.

Informatique seulement

La prise en compte partielle du problème, essentiellement – voire uniquement – sur les moyens informatiques s'avère souvent catastrophique. Je ne nie pas que l'informatique soit 'le' jouet du moment et qu'on lui confie tout. Je veux dire que 50% de notre traitement de l'information (mémorisation/stockage, communication/transfert et exploitation/utilisation) se fait encore par nous, êtres humains et le papier (avec un crayon ou un Bic). Et ce n'est pas prêt de changer !

Bien sûr l'informatique et l'internet apportent leur lot de dangers, mais nous, avec nos bavardages et les papiers que l'on laisse traîner, sommes également des dangers ambulants. Certaines de nos erreurs 'humaines' feront perdre tout le poids et l'investissement que nous avons consentis sur nos ordinateurs.

Les voitures sont de plus en plus sûres et protègent le conducteur et ses passagers en cas d'accident (prévisibles par le constructeur lors d'un usage 'normal). *Cela signifie-t-il qu'il est idiot de vouloir aller 'à pied' ?* Un piéton qui traverse sans faire attention ne sera pas protégé et vous en subirez en partie les conséquences.

Professionnel seulement

Il est bien de faire attention aux informations professionnelles – principalement les 'secrets de fabrication', le 'secret médical' ou professionnel – parce que notre sécurité d'emploi est en jeu.

Mais souvent une grande quantité d'informations 'bureau' ne sont pas protégées ou pas assez. On pense qu'elles n'ont pas assez de valeur. Et les règles internes au travail ne disent pas clairement ce que l'on ne peut pas faire ni, surtout ce qu'on doit faire – et comment – pour protéger les informations.

Nous ramenons ce laxisme à la maison.

Ainsi, nous ne tenons pas assez compte des informations personnelles, privées et 'à caractère personnel' (personnalisables).

La sécurité de l'information doit être prise dans son sens 'global', universel et systémique. Tout ce qui se fait – ou ne se fait pas – a une influence sur le reste. Une information, même infime, qui attire notre attention, ou celle d'un importun, peut changer toute notre vie.

Les 5 mauvaises habitudes de la sécurité de l'information

Les solutions faciles

Mettre en place la sécurité de l'information adéquate n'est pas 'facile' et demande du travail ; un sérieux effort au début et ensuite de l'entretien.

Les solutions toutes faites,

Les solutions toutes faites ne répondent pas à votre besoin. On ne la trouvera pas dans un livre, mais dans **votre** réalité.

Les solutions 'one size fits all',

Ce n'est ni du 'prêt à porter' ni du 'taille unique' ! Il faut tailler **votre** sécurité à **votre** besoin dans **votre** contexte. Vous risqueriez de vous retrouver avec un bazooka pour tuer une mouche.

Les solutions 'one shot'…

Les solutions 'une fois pour toutes' ne marcheront qu'un temps.

Tout change tout le temps… on le voit bien avec la technologie et la situation économique. Il en va de même de vos informations, de leur valeur, des menaces qui pèsent sur elle et de vos solutions de sécurité.

Une 'bonne' solution d'aujourd'hui peut s'avérer insuffisante demain, surtout si elle repose sur la technologie. *Vous avez remarqué le besoin de mettre à jour très régulièrement votre antivirus…*

Les solutions 'lourdes'

On vous proposera plein d'outils, mais peu de techniques et encore moins de 'principes' vous permettant de fixer vous mêmes vos objectifs.

Ces outils sont lourds et dépassent souvent (largement) votre besoin et votre capacité de les utiliser correctement. Avez-vous déjà remarqué comme vous n'utilisez qu'une partie des fonctionnalités des logiciels de traitement de texte que vous avez acheté si cher ? C'est exactement la même chose.

Cette façon de faire crée un rejet de la sécurité ; à l'opposé de ce que chacun recherche.

L'obligation de faire appel à des spécialistes

Les rares méthodes et techniques disponibles vous poussent à faire appel à des spécialistes. Ils vous coûtent cher et vous imposent 'leur' vision des choses et surtout 'leurs' solutions.

Ce qu'il **vous** faut ce sont des principes simples, des techniques faciles à mettre en œuvre de façon régulière – un peu comme un bon bricoleur. Pas besoin d'être un 'pro' pour réaliser quelque chose de solide et de présentable.

C'est que je vous propose dans les pages qui suivent.

IV. Les 2 premières étapes indispensables pour sécuriser vos informations

Gérer l'insécurité

Aujourd'hui, on n'est pas plus en sécurité qu'avant… Nous sommes en pleine guerre de l'information.

N'êtes-vous pas submergés de toutes parts (médias et internet) par des informations 'vraies' au point que vous ne pouvez plus en faire le tri ? Le moindre petit incident à l'autre bout du monde est diffusé partout. Tout cela nous est-il bien utile ?

> *Nous sommes surinformés.*

A qui faire confiance ? Aujourd'hui, il ne faut plus être 'une autorité' pour écrire un livre qui se vend. Tout le monde peut se considérer comme un 'expert'. « 36 régimes pour maigrir sans danger… mais les autres sont un désastre. »

> *Nous sommes mal informés et désinformés (on nous ment et on nous fait croire plein de choses), surtout par les politiciens.*

Avec les livres, les magazines, les sites et articles internet… on ne sait plus à quel saint se vouer, et il y en a tant qu'on ne sait même plus comment les classer et les ranger.

> *« Une chatte n'y retrouverait pas ses jeunes. »*
> *Je connais des ordinateurs où il est impossible de retrouver quoi que se soit… comme une chambre d'adolescent où tout traîne par terre.*

On entend tellement de choses. Même le blog 'www.info-attitude.com' vous signale que 'l'ennemi a des oreilles' et qu'il faut faire attention à ce qu'on dit et écrit.

Que faire ? Comment s'en sortir ? Comment gérer cette insécurité ?

Déterminer les responsabilités :

Vous êtes responsables de vos actes… qu'ils soient conscients ou non. Je ne crois pas qu'il soit besoin d'en dire plus.

Vous êtes responsables de vos réactions à ce qui se passe… Rien ne vous empêche d'avoir une vision positive ou négative de ce qui vous arrive. Celui qui considère un échec comme une opportunité de s'améliorer a une vision différente de la majorité. Dans le domaine de la sécurité de l'information, c'est un avantage.

Vous êtes responsables de ce qui vous arrive, car on attire ce sur quoi on se focalise. Les coaches de conduite automobile vous le confirmeront : si vous dérapez sur la route, ne regardez pas l'arbre sur le bord de la route, mais partout ailleurs ! Sinon, c'est l'arbre que vous atteindrez !

Ne vous focalisez donc pas sur l'insécurité, les dangers, les risques et le reste, mais sur les solutions et sur l'assurance suffisante qu'elles répondent à vos besoins.

Vous avez quatre options face à l'insécurité

- l'ignorer
- la fuir
- la combattre
- ne rien faire.

Quel que soit votre choix, il faudra vous attendre à en assumer les conséquences.

Mais qui décide et qui agit ?

Qui est 'propriétaire' de l'information ? Vous avez acquis l'information (la connaissance) de haute lutte, progressivement, par l'apprentissage et l'étude ; vous l'avez achetée ; vous l'avez conçue, inventée, découverte par votre travail.

Qui concerne-t-elle ? Ces informations parlent de vous : votre santé (votre dossier médical), votre argent (toutes vos informations financières et économiques), votre compétence (vos évaluations), vos intentions, opinions (en questions de politique, de philosophie et de religion).

Ces deux catégories d'informations ont une forte influence sur vous, vos relations ou votre employeur. **C'est donc à vous, lui ou elle de décider.**

Et si cette information nous est confiée ? Le médecin, l'avocat et toutes les professions libérales vivent des informations que nous leur confions… pour nous assister ou nous guérir. Mais il y a également les informations qui vous sont confiées 'en confiance' lors de vos relations privées ou professionnelles. **Faites comme si c'était les vôtres.**

Il est assez facile de s'imaginer qui décide s'il s'agit de *votre* maison, de *votre* voiture, de *votre* GSM, de *votre* compte en banque. Sachez que l'information que *vous* manipulez peut être aussi importante, voire plus.

Les 6 clés à utiliser dans votre sécurité

Ce sont plus que des définitions, souvent fermées. Ce sont des portes ouvertes vers des avenirs meilleurs.

L'information

La donnée est une information brute, formatée et codée dans un langage convenu (par exemple : un texte en français ou des données financières).

L'information est une donnée qui, dans un contexte particulier, a une signification et une valeur (par exemple : ce texte en français est une lettre d'amour de votre conjoint à quelqu'un d'autre que vous ; cet ensemble de chiffres est une copie des comptes financiers de votre concurrent).

L'accumulation et l'organisation des informations créent la connaissance, le savoir.

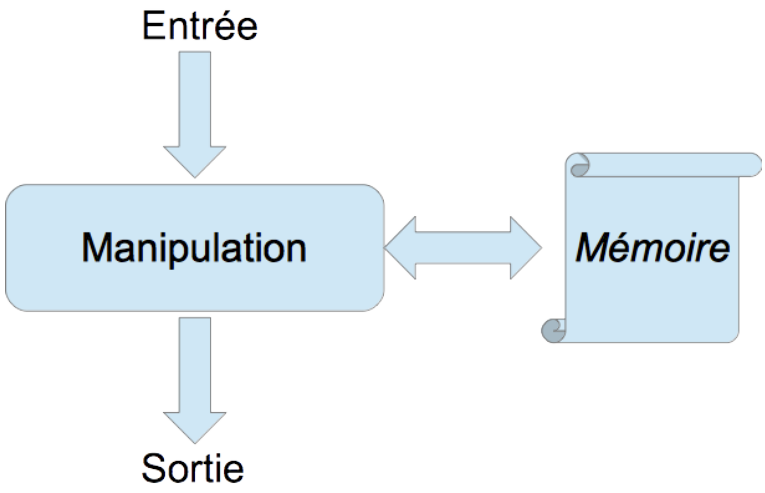
La connaissance mise en œuvre par la pratique est la compétence, la science, le savoir-faire.

La compétence consciente et réfléchie est la sagesse, le savoir-être.

L'information conduit à des décisions et des actions et permet de mesurer la réalisation des actions.

Le processus informationnel

C'est le procédé par lequel une information (d'entrée) est transformée en une autre (de sortie) par une manipulation quelconque : synthèse, traduction, développement, etc. L'information d'entrée démarre le processus et l'information de sortie en est le 'produit' ou le résultat.



- La préparation du pain est un processus complexe car certains éléments peuvent varier en fonction de la nature de la farine, ainsi que de la température et de l'humidité externes.

- Le choix de votre lieu de vacances est un autre exemple de processus (plus simple) sur les informations
- La préparation d'une dissertation au départ d'une recherche sur internet est un processus déjà plus complexe
- Un calcul mathématique ou scientifique.

Les actifs informationnels

L'information est stockée, mémorisée sur un *support* : l'esprit de l'homme, le papier et l'informatique.

L'information est communiquée par un *canal* : la voix, la poste et les réseaux de (télé)communication.

L'information est manipulée, traitée par des *moyens* : l'homme, l'informatique ainsi que tous les outils et machines conçues et construites par l'homme

Ce sont les trois types d'actifs informationnels sans lesquels l'information ne saurait être utile et exploitée. On les appellera actifs primaires.

Le système d'information

Le Système d'information est l'ensemble des ressources et moyens destinés à gérer et traiter l'information. Il comprend le processus ainsi que tout ce qui est nécessaire à son exécution :

- l'acteur (l'homme) ou les acteurs impliqué(s),
- les fournisseurs et destinataires de l'information 'source' et 'produit',
- les actifs primaires : supports, moyens et canaux de communication
- les actifs secondaires :
  - l'environnement physique dans lequel ils sont mis en œuvre (le bâtiment et les locaux)
  - l'énergie nécessaire (électricité, chauffage, etc.) et, enfin,
  - le contexte général (social ou économique) qui donne les règles et les contraintes.

On voit que cela dépasse de loin l'informatique, bien que les deux soient souvent confondus.

Une équipe au bureau (par exemple lors d'une réunion), une PME, une classe, votre famille sont des systèmes d'information.

Le risque

Le risque est un scénario d'attaque simple présentant une menace qui exploite une (ou plusieurs) faiblesse(s) pour causer un dommage à un bien (ici les informations).

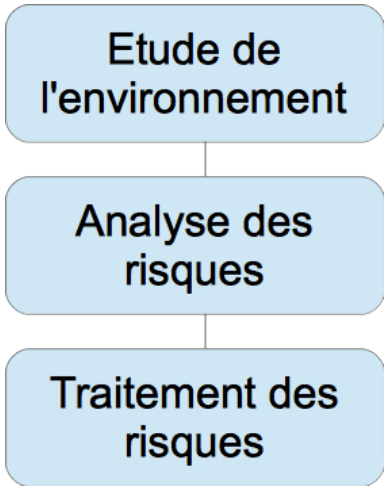
Le risque porte un 'nom' qui détermine l'élément prépondérant : la menace ou le dommage.

Le danger (regardez les panneaux triangulaires rouges le long de la route) indique un risque dont les conséquences sont potentiellement (très) graves.

Le risque touche d'abord les actifs informationnels (parfois au travers de l'environnement et le contexte), ensuite l'information.

Selon le degré de dommage à l'information, des *conséquences* plus graves sont possibles : les objectifs prévus ne seront pas atteints et d'autres choses seront touchés, comme vos enjeux et vos valeurs.

La gestion des risques consiste à contenir « en permanence » les *conséquences* dans des limites acceptables soit en jouant sur la survenance de l'événement soit sur l'étendue du dommage.



Le risque d'incendie couvert par une assurance ; le risque d'accident automobile limité à des dégâts matériels couvert par une assurance et un comportement prudent au volant ; un vol d'information qui n'a qu'un impact réduit sur les actions (quelques heures de travail perdues) ne sera pas couvert – voilà quelques exemples de risques limités à l'acceptable.

Les solutions de sécurité

Les solutions (ou mesures) de sécurité sont donc toutes les actions qui nous permettent de garder le risque dans des limites acceptables :

Les solutions de sécurité sont de trois ordres

- *La Prévention* : on agit avant que l'attaque ne se produise (on l'évite, on l'empêche, on en limite la probabilité ou la sévérité immédiate en cas de survenance
- *La Réaction* : on contre l'attaque quand elle se produit et on la fait cesser, de manière à limiter de manière active le dommage causé

- *La Correction* : on répare ou récupère ce qui doit l'être et reprend les activités là où elles se sont interrompues.

Exemples :

- *Prévention* : mise en place d'extincteurs avec exercices d'utilisation ; logiciel antivirus activé et régulièrement mis à jour ; mise au coffre des informations de valeur
- *Réaction* : déclenchement d'une alarme et envoi d'une équipe d'intervention pour arrêter l'attaque - appel des pompiers ; détection et éradication du virus ;
- *Correction* : remplacement de ce qui a été détruit avec l'argent de l'assurance ; récupération d'un fichier 'propre' dans les 'sauvegardes' pour reprendre le travail ; récupération ou rachat de ce qui a été dérobé ou détruit (éventuellement après jugement au tribunal).

Pour mettre en œuvre la protection de l'information en se fondant sur ces concepts, il faut prendre en compte 3 principes-clés – les règles - et gérer deux de ces concepts – vos actions prioritaires. Sans cela, les solutions de sécurité seront choisies « au petit bonheur », ce qui veut dire qu'elles ne répondront ni à vos attentes (en efficacité, en coût, en contraintes, en utilité.), ni à vos besoins.

Les 3 règles à respecter absolument :

Besoin d'en connaître[2]

A qui puis-je confier cette information ?

Que ce soit par pudeur ou par décence, par considération pour l'autre ou pour ne pas lui occasionner des réactions et des émotions non désirées ou désirables, certaines informations ne se communiquent pas à n'importe qui ou n'importe comment.

On connait le voyeurisme (les paparazzis et les scoops sur les People), la volonté de nuire et la méchanceté. Leurs auteurs font, le plus souvent, partie de notre cercle d'amis ou de relations.

Le principe de base du 'Besoin d'en Connaître' est de ne confier l'information qu'à celui (ou celle) qui doit la connaître afin de nouer une relation sereine et respectueuse, pour effectuer l'action ou le travail attendu ou convenu. *Qui a besoin de savoir votre état de santé ou de contenu de votre compte en banque – ou votre code d'accès ?*

[2] En jargon on parle de Need to Know (NTK).

Les autres ne sont pas mis 'dans le secret'. Certains voudront chercher à découvrir, à connaître cette information – quel qu'en soit le but – c'est pourquoi il convient de 'protéger' les informations et de chercher à maîtriser la liste de distribution.

Besoin d'utiliser

Vous ne donnez pas accès à votre voiture, votre compte en banque ou votre maison à n'importe qui. Et, chaque fois, vous donnez des consignes ou attendez un comportement respectueux de vos biens et avoirs.

Il est aussi important de ne pas permettre à n'importe qui de manipuler vos informations, celles qui vous concernent ou celles qui vous permettent de vous réaliser dans la vie.

Il vous appartient donc de donner accès à des personnes 'triées sur le volet' et à donner les directives indiquant ce que vous attendez et ce que *vous ne voulez pas* dans le travail, la gestion, la modification, la mise à jour et la destruction de vos informations.

Tous les autres n'ont ni l'accès et ni le droit de manipuler vos informations. Vous avez donc le droit de porter plainte et de vous faire dédommager s'ils le font. Si vous ne mettez pas ce principe en œuvre, vous n'avez aucun moyen de vous faire respecter et aucune base pour porter plainte.

Principe de précaution

Considérant l'illusion du 'risque zéro', il est raisonnable – on parle d'attitude 'en bon père de famille' – de prendre les mesures minimales pour que ces risques soient limités à ce que l'on peut supporter… autant que de se préparer à ce qui ne l'est pas.

Un des 'réflexes' dans notre société moderne est de prendre une assurance… mais c'est rarement suffisant. Il faut se comporter avec prudence, comme sur la route.

N'hésitons pas à écouter notre nature animale (notre cerveau reptilien), « faisons gaffe ».

Vos 2 priorités pour réaliser votre sécurité

Gestion des risques

La gestion des risques comporte 7 étapes. Ce n'est pas bien compliqué, mais oublier une étape vous mène à une impasse : solution trop chère et rejetée, solution inadaptée ou insuffisante.

Définition claire et précise du périmètre

Classer les informations dans la catégorie (et la sous-catégorie) adéquate est le premier pas vers le succès. Cela vous permet d'identifier bien clairement les informations qui devraient faire l'objet des principes ci-dessus et, partant, du système d'informations à protéger. En effet, protéger seulement l'information en oubliant le système qui l'entoure, c'est comme protéger un bijou, sans s'intéresser à tout ce qu'il y a autour et qui conduit à lui (votre chambre dans votre maison).

Chaque catégorie sera gérée et verra ses informations protégées au même niveau. La méthode employée varie avec l'actif primaire qui contient l'information.

Valeur de l'information

La valeur de l'information dépend, naturellement, de ce qu'elle vous coûte pour l'acquérir, la collecter, la classer, la gérer, la protéger. Mais elle vaut bien plus selon ce que vous en faites : augmenter vos connaissances, prendre une décision, mener une action, mesurer et évaluer le résultat de vos actions.

Il faut également tenir compte de la valeur que lui accorde celui qui veut se l'approprier : concurrent, jaloux, malveillant. Ce qu'il cherche est de vous embarrasser, vous isoler, vous bloquer ou vous détruire (en termes d'image, de relations ou de finances).

> *La valeur se mesure en termes de douleur si l'information est modifiée intempestivement, détruite ou inaccessible, ou si elle tombe entre des mains que vous n'auriez pas voulu.*

Il est important de protéger les informations de manière adéquate. Le classement et le rangement immédiats sont le premier choix. On pourra recommander de 'marquer' les informations de valeur de sorte que chaque utilisateur autorisé y apporte toute l'attention voulue.

Etude de la situation (le contexte, l'environnement)

> « ***Connais-toi toi-même, connais ton ennemi, ta victoire ne sera jamais mise en danger. Connais le terrain, connais ton temps, ta victoire sera alors totale***. » *Sun Tzu, l'Art de la Guerre (500 BC)*

Savoir qui vous êtes, où vous êtes, ce que vous voulez et tout ce qui peut vous empêcher de l'atteindre… est la troisième étape de la gestion des risques.

Décrire ses objectifs et ce dont on a besoin pour les réaliser ; identifier ceux qui nous bloquent la route – même ceux qui semblent en avoir l'intention – ainsi que les moyens qu'ils veulent utiliser ; étudier les contraintes et les conditions dans lesquelles on veut penser et agir.

C'est un des moyens les plus efficaces pour 'connaître le terrain' et identifier ce qui pourrait être ou devenir un obstacle ou une menace.

Analyse des risques

Estimer les risques est la première action dans l'analyse des risques.

> ***Et si*** *quelque chose arrivait, quelle serait le dommage?*

Listez les évènements qui vous seraient contraires, surtout – et d'abord – ceux qui vous sautent aux yeux et ceux qui vont vraiment vous faire « ****!@*** » - mal. Ensuite estimez leur probabilité (je vous fais grâce des autres termes qui apportent des nuances car celui-ci est bien compris) et la gravité des dommages immédiats et directs.

La seconde action dans l'analyse des risques consiste à **évaluer** les risques.

> ***Et alors,*** *quel mal cela ferait-il ? Quelles seraient les conséquences ?*

Revenez sur la valeur de l'information, sur vos valeurs, sur vos objectifs et ce que vous ne voulez pas perdre : votre réputation, votre argent, vos relations, votre emploi ; sur les suites possibles si vous vous trouvez en infraction avec les lois.

Cette évaluation vous permet d'éliminer de votre liste d'actions tout ce qui n'a pas ou très peu d'effet 'majeur'. Vous les prendrez en compte plus tard… au besoin. *Parce que la solution que vous choisirez vous couvrira peut-être automatiquement.*

Traitement des risques et le choix des solutions

> *Quels objectifs suis-je prêt à vouloir atteindre pour conjurer ce mal ?*

Troisième action : le choix des solutions.

Puisque ce qui peut se passer va vous faire mal, vous décidez de réagir soit pour éviter que l'événement ne se produise, soit vous veillez – par différents

moyens – à ce que la douleur soit (plus) supportable. Les solutions de sécurité sont préventives, réactives (quand l'événement se produit) et correctives.

Quels moyens suis-je prêt à engager pour y parvenir ?

Vous allez décider des moyens et techniques à mettre en œuvre, soit dès maintenant, soit quand les circonstances l'imposent. Il faudra, sans doute, dépenser de l'énergie et de l'argent… mais il faut le considérer comme un investissement : tout comme une assurance, une visite chez le médecin ou des médicaments.

Tout cela doit vous coûter bien moins cher que si l'évènement se produit.

Mise en œuvre des solutions

Comment m'organiser pour 'gagner' ?

Une fois la décision prise (et les moyens éventuellement acquis), il faut mettre les solutions en œuvre, les faire fonctionner (les utiliser) en suivant les directives – *vous devrez parfois les préparer vous même*.

Il ne faut pas chercher à tout vouloir mettre en œuvre d'un coup ou en même temps. Cela ne ferait que vous mettre dans une situation encore plus dangereuse.

Si vous voulez aller plus loin :

Si le système d'information que vous analysez est complexe et que c'est la première fois, le nombre de solutions à mettre en œuvre sera important. Cela prendra du temps et une gestion de projet sérieuse sera nécessaire.

N'hésitez pas à me contacter.

Gestion des solutions de sécurité

Comment m'assurer que je peux continuer à 'dormir sur mes deux oreilles' ?

La gestion des risques (les étapes précédentes) ne peut pas être un processus unique, réalisé une fois pour toutes. Tant de choses changent et il faut adapter ou remplacer les solutions.

Les solutions de sécurité ne sont pas universelles ni efficaces en permanence. Elles évoluent et celle qui était bonne hier risque de ne plus l'être demain (c'est relatif). Il faut donc mesurer l'efficacité de sorte de réaliser les corrections nécessaires pour rester couvert et garder les risques à un niveau acceptable.

Les solutions de sécurité se gèrent comme des actifs (ci-après).

Gestion des actifs

Comment m'assurer que je maîtrise assez ce que je protège ?

Il est essentiel de gérer les actifs - informations, les processus, le système d'information – de sorte que l'on sache bien où ils sont et dans quel état, ce qu'il faut changer ou remplacer, ce qui doit être éliminé ou détruit.

La gestion s'intéresse à l'acquisition, au classement, au stockage, à l'emploi correct, au transport, à l'entretien et à la mise au rebut en fin de vie.

Il convient d'établir

- un inventaire
- la personne responsable
- les règles d'utilisation correcte - soit de déterminer (au besoin par écrit) ce que vous faites en fonction de la valeur de l'information : plan de classement, conditions de stockage, règles d'emploi modes et conditions de transport, etc.
- les règles de restitution des actifs en fin d'utilisation, d'accord ou de contrat.

On commencera par la gestion des informations de grande valeur. Au besoin, on passera ensuite progressivement aux niveaux inférieurs.

La 'gouvernance'

Comment 'tenir la barre' si quelque chose d'important change ?

La gouvernance est l'ensemble des activités menées pour assurer l'utilité, le fonctionnement et la protection à long terme de ce que l'on gère. Elle repose, fondamentalement, sur trois groupes d'activités qui forment une boucle :

- l'évaluation de la situation
- la direction à donner pour corriger ou conserver ce qui doit l'être et
- la supervision de l'évolution, grâce à ces alarmes et des contrôles.

Maintenant que les fondations sont établies, voyons ce qu'il faut faire.

V. Propositions de solutions

Ce qui suit s'applique aux personnes (en privé) ainsi qu'aux PME ; tous deux manquent de temps et des ressources nécessaires à aller plus loin. J'indiquerai 'des pistes' pour ***'ceux qui veulent aller plus loin'****.*

Les Moyennes et Grandes Entreprises (ou organismes) commenceront par cela. Si un besoin existe d'aller plus loin – et ce sera souvent le cas suite à la nature et à la quantité d'information, à la complexité du système (ou des systèmes) d'information et à l'importance des choix informatiques – vous aurez besoin d'aide. Contactez-moi pour des informations supplémentaires (voir page 42).

En guise de préambule…

> ***Vous avez le choix de ne pas réagir et de ne pas prendre en compte le principe de précaution… mais vous êtes responsables de vos décisions***

« ***Prévenir vaut mieux que guérir*** ». *Sagesse populaire.*

Il est important d'être proactif. De décider de ne plus vous laisser dicter votre vie par les évènements. De toute façon, nous sommes responsables… Il faut décider de notre action préventive, réactive et corrective. Si vous choisissez de ne rien faire, il ne faudra pas vous plaindre.

> ***Le temps est irrécupérable, et il est souvent 'trop tard'.***

Vous devez agir au plus vite. Le temps que vous perdez ne se récupèrera jamais. Et vous risquez de perdre beaucoup plus que du temps.

> ***Vous devez construire votre potentiel et être proactif ; choisir les défis en fonction de vos capacités et des difficultés à agir ; avancer pas à pas dans votre ambition à vous améliorer et à être, à chaque fois, 'plus sûr qu'hier et moins que demain'***

Il faut des solutions simples et pragmatiques. Des solutions que vous pouvez facilement mettre en œuvre et contrôler. Des solutions qui ne seront pas des contraintes (ou au moins qui seront bien moins contraignantes que les conséquences si quelque chose se passe).

Allez-y petit à petit, pas à pas. Comme il s'agit de prendre de nouvelles (et bonnes) habitudes, il est déconseillé de trop vouloir faire d'un coup (« *Qui trop embrasse manque le train…* »). Prenez-en deux – maximum trois si elles sont vraiment élémentaires – en même temps. Pour les plus lourdes, allez-y une par une.

3 techniques rapides et efficaces

Trois actions assez faciles et rapides afin de vous mettre le pied à l'étrier. Ce sont les bases de toute l'attitude nécessaire pour vous donner « ***l'assurance que votre information est à l'abri des évènements (risques) inacceptables***. »

Gestion des informations

De quelle information parle-t-on ?

- Tout ce qui comporte des données à caractère personnel (nom, adresse + date de naissance, photo, numéro national ou de sécurité sociale, compte en banque, numéro de dossier pour la fourniture d'énergie et de téléphonie, informations de santé, etc.)
- Les factures, avis d'échéance pour les assurances – pendant au moins un à trois ans après règlement
- Les factures et tickets de caisse pour les garanties et la couverture en cas de vol/cambriolage et incendie
- Votre état financier, vos comptes, vos assurances (vol/incendie : car on y trouve un inventaire de vos avoirs de valeur ; vie : car il y un montant, un état de santé et l'identité des bénéficiaires, etc.)
- Tout ce qui vous permet en général
  - d'augmenter vos connaissances pour évoluer intellectuellement, socialement et financièrement
  - de prendre des décisions qui mettent en jeu votre réputation, vos relations et vos finances
  - de mener des actions qui vous font atteindre vos objectifs.
- Tout ce à quoi vous attachez une valeur sentimentale et émotionnelle (surtout dans la sphère privée.)

Classifier les informations

La classification sert à définir la valeur de l'information et, donc, de déterminer ce qui doit vraiment être protégé. Le niveau de valeur (ou de classification) indique le niveau de protection.

Il s'agit de mesurer le degré de douleur s'il y a **atteinte à la sécurité** :

- confidentialité : information tombant dans de mauvaises mains, y compris une *application* non autorisée
- intégrité : information modifiée de façon intempestive, non sûre – qui ne peut plus être considérée comme exacte et exhaustive
- disponibilité : information indisponible, inaccessible aux utilisateurs autorisés et dans les conditions définies

- traçabilité : incohérence ou absence d'historique essentiel ne permettant plus le contrôle et les vérifications indispensables.

Choisir des axes de sensibilité (indicateurs) :

- valeur (financière ou sentimentale) de l'information et des actifs touchés
- infraction aux lois (et ce qui en découle)
- perte d'image et de réputation (on peut créer des 'groupes' …)
- non atteinte des objectifs (et ce qui en découle)
- atteinte à la 'vie privée' (à vous de dire ce que vous voulez y mettre)
- atteinte à la qualité des soins médicaux reçus.

Je vous recommande d'en choisir au moins 3 pour avoir une vision '3D'.

Si vous voulez aller plus loin :

Contactez-moi pour une liste qui propose 18 axes pour les personnes privées et 36 pour les entreprises (quelle que soit leur taille).
Les moyennes et grandes entreprises devraient choisir 5 axes au lieu de 3.

Choisir des niveaux concrets de douleur :

Niveau	Niveau de douleur	Délai pour traiter
0	Aucun effet	Aucun
1	« Même pas mal ! »	Aucun
2	Supportable mais pas trop longtemps ou souvent	Surveiller, à long terme
3	Difficile à supporter	A court ou moyen terme
4	Totalement insupportable (potentiellement mortel)	Immédiatement, à très court terme

Ces niveaux et délais sont relatifs : c'est à vous de définir clairement ce qu'ils signifient pour vous.

Créer un tableau croisant les axes de sensibilité et les atteintes à la sécurité. Remplir chacune des cases par le niveau de douleur. La dernière colonne contient la valeur maximum obtenue sur la ligne : c'est votre **niveau de classification.**

Voici un exemple…

	Valeur	Image	Professionnel	Niveau
Confidentialité	0	1	2	**2**
Intégrité	2	3	1	**3**
Disponibilité	1	0	1	**1**

Si vous voulez aller plus loin…

Demandez-moi un tableau complet que vous pourrez le simplifier au besoin.
Le but est de prendre tout en compte de la manière la plus pragmatique possible.

Source : *Avez-vous confiance dans la source (là vous allez chercher l'information) et dans le canal par lequel cette information vous arrive ?*

Identifiez la source, son authenticité et son autorité. Il y a une (sérieuse) différence entre ce que vous obtenez d'une encyclopédie 'reconnue', ce que vous trouvez sur internet et les rumeurs qui courent …

Comment prenez-vous livraison de l'information ? Parfois un intermédiaire (connu ou caché) peut troubler votre assurance. C'est pour cette raison que les transactions bancaires par internet et GSM sont protégées par des codes et du chiffrement.

Attribuez une valeur (de 0 à 4) à votre degré de confiance dans chacun des indicateurs.

Pour les informations concernant les personnes, rappelez-vous « les trois filtres » de Socrate.

Classement/rangement : *Savez-vous où se trouvent les informations dont vous avez besoin ? Vous ne pouvez gérer ni protéger l'information si vous ne pouvez pas la contrôler.*

Au plus l'information est 'sensible' (voir classification ci-dessus), au plus vous aurez besoin de maîtrise.

Vous pourrez les classer selon plusieurs catégories, comme :

- Personnel (Privé, Médical, Sentimental, Etats d'Ame, Photos & vidéos, etc.)
- Connaissance : ce qui vous fait grandir intellectuellement et spirituellement
- Financier : Banque, Assurances, Prêts, Etat de vos finances, etc.
- Activités lucratives
- Activités de détente…

Faites un inventaire de ce que vous mettez dans chaque catégorie - tout comme vous le faites pour votre assurance vol ou incendie – et tenez-le à jour. Les inventaires électroniques donnent automatiquement la date d'entrée et de dernière modification. Cette donnée est souvent essentielle car il faudra rafraichir régulièrement les informations numériques.

> ***Si vous voulez aller plus loin…***
>
> Pour chaque groupe, vous pouvez créer des sous-groupes. A vous de voir si la classification s'applique au groupe, au sous-groupe ou à une information particulière.
>
> Le plus pratique est de choisir une information représentative du groupe ou du sous-groupe, de la classifier et de donner la même classification au (sous-)groupe qu'elle représente.

Traitement : *Comment contrôler l'évolution, la manipulation, la modification et la mise à jour de l'information ?*

Pour avoir une confiance suffisante dans le traitement, il est préférable de l'expliquer, de le décrire, voire de le documenter. Puisque nous sommes sûrs de ce qui rentre, nous le serons également de ce qui sort.

Ainsi, si nous confions le traitement à quelqu'un d'autre, nous pourrons même vérifier, au besoin, si le résultat correspond aux attentes et si le chemin indiqué a été suivi.

> ***Si vous voulez aller plus loin…***
>
> Une mini-formation est en préparation sur 'www.info-attitude.com'. Restez à l'écoute.

Nettoyage : *Que faites-vous quand les informations et les supports ne sont plus utiles ?*

Quand l'information ou les supports ne nous sont plus utiles, ils peuvent encore avoir de la valeur 'pour les autres' qui peuvent vous nuire d'une manière ou d'une autre. Il faudra donc non pas jeter les documents à la corbeille (qu'elle soit 'papier' ou dans l'ordinateur) ou les supports (disques durs d'ordinateurs, CD/DVD, clés-USB cartes mémoire). ***Il faut les détruire***.

N'hésitez pas à déchirer les papiers qui ont été 'sensibles' en petits morceaux que vous éparpillez dans la corbeille et dans la poubelle (merci aux communes et municipalités de nous forcer à trier nos déchets, nous avons donc au moins deux sacs pour jeter nos papiers).

On trouve des déchiqueteuses à de très petits prix. Je vous recommande d'en acquérir une.

Pour les supports (CD, DVD), n'ayez pas peur de les casser au marteau avant de les jeter.

Quand nous 'supprimons' un document informatique, il arrive dans la 'corbeille/poubelle'. Il ne faut pas se contenter de la vider, surtout pour les informations 'sensibles'.

> ***NOTE :***
>
> Quand vous faites un 'Delete/Effacer', le système se contente d'effacer non pas 'la table des matières' – ce qui n'empêche pas de lire, même s'il est plus difficile de s'y retrouver –, mais uniquement le numéro de page, ce qui rend l'espace mémoire à nouveau accessible. Les documents sont toujours là et assez faciles à récupérer avec une application spécifique.

Sur Mac, choisissez l'outil 'vider la corbeille en mode sécurisé' ; sur PC, choisissez l'outil 'Videz la poubelle' (Microsoft annonce que le document devient irrécupérable) ou installez le logiciel « C-Cleaner » (gratuit) qui vous donne des outils similaires – et bien d'autres.

Gestion des risques 'Fast&Furious'

La gestion des risques permet de déterminer précisément contre qui et contre quoi protéger ' de manière adéquate' les informations 'de valeur' sans s'imposer de contraintes inutiles.

> ***A RETENIR :***
>
> Nous gérons les risques en permanence. Nombre de nos actes sont réalisés pour éviter un dommage (perçu ou réel). Elle est essentiellement réactive. Cette gestion est naturelle, automatique, viscérale.
>
> Dans un domaine aussi intangible et virtuel que l'information, il est essentiel que la gestion des risques soit réfléchie et structurée.

Il est contre-productif de faire une gestion des risques longue et compliquée. Il est possible que les éléments de base aient changé en cours de route.

> ***Si vous voulez aller plus loin…***
>
> Adoptez la technique des archéologues qui n'attaquent jamais une fouille avec leurs instruments de précision, mais en différentes phases utilisant des moyens du plus gros au plus précis.

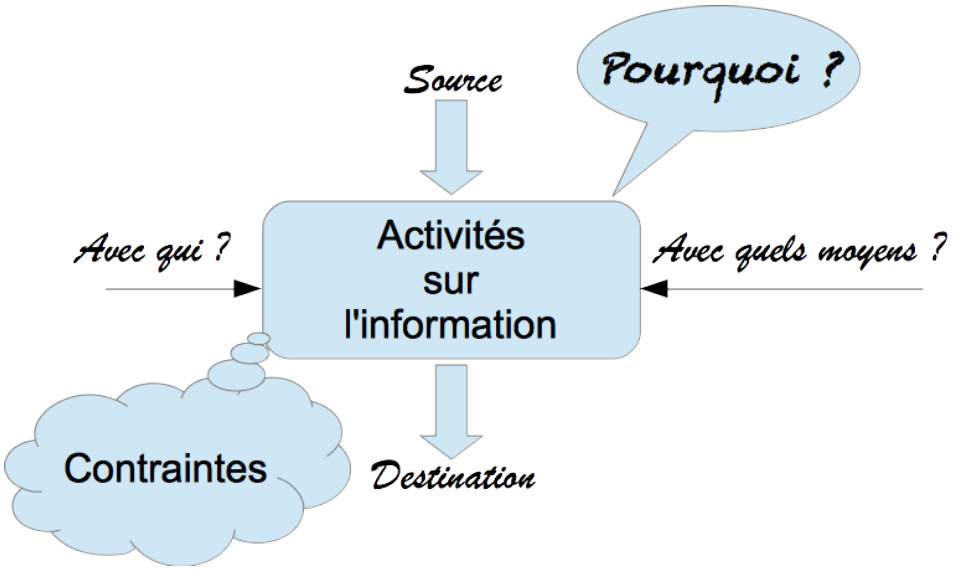
Une formation est en préparation sur 'www.info-attitude.com'. Restez à l'écoute.

Etudier le contexte

Faites une liste de vos informations les plus importantes – celles qui vous font réussir, gagner, atteindre ce que vous désirez.

Classifiez-les puis et choisissez le 'Top 5'.

Lister les Activités : *Que faites-vous avec l'information ? Pourquoi ? Avec qui et quels moyens ou outils ? D'où viennent-elles et où vont-elles une fois définies ?*



Par 'contagion', tout ce que vous venez de lister acquiert la même classification que l'information.

Dressez la liste des contraintes, difficultés, complexités que vous rencontrez en rapport avec ces informations. Trouvez-en au moins 5.

Evènements redoutés

Définissez quel effet peut avoir un événement 'contraire' sur chacun des axes de sensibilité (voir 'classification') sur votre Top 5 informations et les activités liées à cause des difficultés.

Vous disposez d'un petit inventaire qui vous permet de passer à la 3e étape.

Racontez – dans une courte histoire – ce qui peut se passer (concrètement), comment et pourquoi, pour que ces évènements redoutés se produisent avec la sévérité des conséquences qui en découlent.

Estimation des risques

Estimez la probabilité que ces évènements se produisent.

Vous pouvez utiliser ce tableau :

Niveau	Sévérité	Probabilité
0	Aucune	Totalement improbable
1	Légère	Improbable
2	Moyenne	Probable
3	Forte	Très probable
4	Très grave	Inévitable

Multipliez la valeur de la sévérité et de la probabilité pour chaque Scénario Redouté et classez ceux-ci du plus grand au plus petit.

La valeur « 8 » délimite, par exemple, ce que vous pouvez supporter et ce que vous ne voulez pas supporter.

Quel traitement du risque

Décidez si vous voulez Accepter, Refuser, Réduire ou Partager le risque.

- **Accepter** : vous ne faites rien (généralement ce qui est sous la limite de 8)
- **Refuser** : vous ne faites plus cette action sur cette information (supposons les valeurs 15 et 16)
- **Réduire** : vous regardez ce que vous pouvez faire pour ramener la valeur calculée sous la barre du '8'
- **Partager** : vous prenez une assurance.

Quelles solutions de sécurité

C'est pour moi, d'ici, la partie la plus épineuse. Je n'ai aucune idée de vos scénarios. Il y a cependant des éléments porteurs que l'on peut retirer des bonnes pratiques.

- **« clean desk »** (bureau propre) : mettez sous clé les informations sensibles quand vous ne pouvez pas les surveiller
- **« clear screen »** (écran vide) : ne quittez pas votre ordinateur sans activer l'économiseur d'écran que vous devez désactiver par mot de passe
- Mettre en place Besoin d'en connaître et le Besoin d'Utiliser (voir pages 23 et 24)
- Gérer l'information : assurez-vous que vous savez d'où viennent les informations, où elles se trouvent et où elles vont
- Gérer les accès : établissez la liste de ceux qui ont accès, les conditions et les clés pour accéder (voir ci-dessous)
- Coder ou chiffrer : rendez l'information incompréhensible pour les autres
- Vérifier les informations d'entrée et de sortie des 'processus'
- Créer et maintenir la confiance dans les personnes à qui on confie ses informations

- Classer et ranger les informations
- Classifier les informations
- *Etc.*

La 'force' de la solution dépend du niveau de classification de l'information. La priorité de mise en œuvre dépend, elle, du niveau de risque.

Vous pouvez *sentir* jusqu'à quel point une solution choisie va faire descendre la valeur de la probabilité ou de la sévérité.

Il n'est pas conseillé de se reposer sur une seule solution ou sur des solutions d'un seul type (par exemple informatique.) Une solution physique ou organisationnelle sera un complément hautement recommandé.

Attention :

La méthode présentée ci-dessus, très générique, n'est qu'un début si vous avez une vie compliquée, si vous gérez beaucoup d'informations de grande valeur et en milieu professionnel. Il faudra donc aller plus loin.

Pour les entreprises (quelle que soit leur taille), je vous propose de me contacter. Je vous procurerai des références (dont sont extraits les éléments ci-dessus). La majorité est en anglais, seules certaines ont été traduites en français.

Gestion de la sécurité

Une fois que les solutions sont en place, elles doivent être gérées comme les actifs et supervisées. Il n'est pas rentable de mettre une alarme en mode silencieux et de ne jamais y faire attention. Le feriez-vous avec votre réveil si vous avez un rendez-vous important tôt le lendemain matin ?

Les bases données pour la gestion de l'information sont généralement applicables.

Assurez-vous que les solutions évoluent avec les menaces, les risques et les changements (permanents) de l'environnement.

Si vous voulez aller plus loin…

Il faudra mettre en place un système cohérent et maîtrisé pour gérer la sécurité de l'information. Il y a des règles à suivre et même des normes.

Contactez-moi pour plus d'informations.

5 Solutions simples à mettre en place

Contrôle d'accès

Une fois le niveau de classification défini (au plus le niveau est élevé, au plus les contrôles seront 'serrés'):

- établir la liste de ceux qui auront accès
- déterminer les droits qu'ils reçoivent : lecture, écriture, modification, copie, déplacement, effacement
- déterminer les conditions d'accès et d'emploi, ainsi que les règles à appliquer (comme pour votre voiture ou votre argent)
- déterminer les moyens et clés d'accès (codes et mots de passe)
- mettre en place un système qui enregistre les demandes d'accès (avec les décisions) et d'activités sur les informations
- remettez tous ces contrôles en question de manière régulière.

C'est le point de départ de tous les autres contrôles si d'autres personnes doivent avoir accès.

Si vous ne communiquez l'information à personne, vous êtes seul responsable des problèmes qui se produisent.

Choisissez un bon mot de passe

On vous l'a sûrement déjà dit : choisissez un mot de passe solide que vous pourrez retenir et que les autres ne pourront pas deviner.

Pour être solide, il doit comporter ***au moins 8 caractères*** et un ***mélange de lettres, de chiffres et de signes***. Certains sites ou applications indiquent le niveau de votre mot de passe.

Ne l'écrivez pas et ne le mettez pas à côté de votre ordinateur… *vous ne mettez pas votre code PIN avec votre GSM ou votre carde de banque*. Cela donnerait au candidat intrus toutes les clés pour vous plumer.

Ne choisissez pas un seul et unique mot de passe sur votre ordinateur et une seul et unique code pour votre GSM et vos cartes de banque : vous donneriez un passe-partout unique au candidat voleur.

Ne choisissez pas…

Un nom ou prénom, votre identifiant, une date connus de tous ; votre numéro de plaque de voiture, votre hobby, votre film ou livre préféré, etc.

Comment le retenir ?

Choisissez quelque chose dont vous vous souviendrez et 'codez-le' à votre sauce.

Voyez dans cet article quelques trucs et astuces.

Contrôle de confidentialité

Taisez-vous (ou parlez tout bas) !

Mettez sous clés les informations importantes (haut niveau de classification) quand vous ne pouvez avoir un œil dessus. Gardez-les hors de vue des personnes non autorisées.

Codez vos informations dans un langage que les autres autour de vous ne connaissent pas (Espéranto, Navajo, Chinois, etc.) Chiffrez vos informations très importantes. Il existe des logiciels gratuits et très faciles d'emploi pour les personnes privées.

Voyez cet article pour aller un peu plus loin.

Contrôle de disponibilité

Faites des sauvegardes (des 'backups').

Faites plusieurs copies de nature différente (papier, informatique) sur différents supports. Au cas où l'un se perdait, vous auriez encore les autres.

Voyez cet article pour aller un peu plus loin.

Contrôle d'intégrité

Installez, activez et mettez à jour régulièrement (de manière automatique) votre antivirus)

Soyez vigilants et comparez (= relisez) les documents qui sont extraits de la mémoire de vos ordinateurs. Si vous gardez plusieurs copies – à éviter ! –, gardez-en une 'de référence' pour des comparaisons automatiques – les logiciels de traitement de texte possède cette fonction.

Chiffrez les informations, cela permet de détecter les modifications. Si elles sont modifiées, le déchiffrement ne sera plus possible (au moins à partir de l'erreur).

Voyez cet article pour aller un peu plus loin.

Contrôle de traces

Gardez des traces des mouvements et des changements des informations importantes (un peu comme des inventaires ou les extraits de compte en banque) et vérifiez-les régulièrement.

Les traces devraient être protégées en confidentialité, intégrité et disponibilité.

VI. A retenir

L'information est essentielle à notre vie personnelle et en société. Sans confiance suffisante, l'incertitude générera l'angoisse et le stress (au mieux).

Les solutions qu'on nous propose – pour autant que vous vous y intéressiez – sont incomplètes et inadaptées.

Nous avons vus les termes-clés : l'information, les actifs informationnels, le processus informationnel, le système d'informations, le risque et les solutions de sécurité.

Nous avons vu quels processus-clé de gestion nous devions mettre en œuvre : gestion de l'information, gestion des risques et gestion de la sécurité.

La protection (ou la « sécurité ») des informations c'est bien plus que le contrôle des accès.

Comme les informations sont surtout 'virtuelles' de par leur signification (votre perception) et leur valeur (celle que vous ou les autres leur attribuez), ***c'est votre attitude qui fera la différence.***

La sécurité, quel que soit son objet, est bien plus une question d'attitude que de technique. L'exemple de la sécurité routière en est un exemple flagrant.

Info-Attitude vous conduit vers la confiance dans les informations qui sont l'ADN de votre vie personnelle, sociale et professionnelle. Cette confiance se construit sur une protection – on parle de 'sécurité' – des attentes de qualité de l'information dont vous avez besoin pour augmenter vos connaissances, prendre des décisions et agir.

La sécurité devrait être considérée comme une aide pour oser … comme le harnais pour l'amateur d'escalade et d'alpinisme.

Agissez maintenant…

N'attendez pas une 'catastrophe' pour agir.

Que faire donc ?

- Identifier les informations
- Classifier les informations
- Déterminer le système d'information (avec tous les actifs concernés)
- Gérer les risques
- Gérer les solutions de sécurité.

En tout état de cause, restez connectés à mon blog http://www.info-attitude.com. Vous y découvrirez régulièrement de nouveaux articles, des produits et des offres.

Si vous voulez recevoir chaque semaine les articles que je publie et être informé des formations et autres services que je prépare, inscrivez-vous sur le blog.

Dites-moi de quoi vous désirez que je parle et ce sera l'objet d'un des prochains articles.

Merci encore et félicitation pour votre persévérance pour être arrivé à la fin de cet eBook qui n'est que le début de notre aventure.

Posez-moi toutes les questions qui vous viennent à l'esprit…

A bientôt, plus en sécurité avec vos informations…

Jean-Luc

Et après ?

Si vous souhaitez un entretien personnel…

- pour connaître vos besoins
- pour vous indiquer la marche à suivre
- pour vous aider à passer la première marche
- pour vous donner des références…

Je suis à votre disposition. Ecrivez-moi à l'adresse :

contact@info-attitude.com.