RISQUES INFORMATIQUES

Maîtriser ou périr

Club de la Sécurité Informatique Belge (CLUSIB A.s.b.l.)
rue des Sols 8
1000 Bruxelles
Tel: +32 2 515.08.57 Fax: +32 2 515.09.85
e-mail: na@vbo-feb.be
site web: http://www.clusib.be

TABLE des MATIÈRES

PRÉFACE

« *C'est par l'expérience que la science et l'art font leurs progrès chez l'homme* »

Métaphysique livre I - ARISTOTE (384 - 322 avant notre ère).

Pendant longtemps, l'informatique demeura un outil réservé aux universités, aux grandes entreprises et aux pouvoirs publics. Comme toute technologie, son usage est loin d'être exempt de risques. Des défauts de sécurité informatique peuvent avoir un impact direct et grave pour les utilisateurs des systèmes. Néanmoins, si le recours à l'informatique à des fins privées et professionnelles ne cesse de croître, c'est que les avantages dépassent les inconvénients et qu'il est donc possible de maîtriser de manière raisonnable les risques y afférent.

Le caractère immatériel des systèmes d'information, la haute technicité des solutions mises en œuvre et le jargon volontiers manipulé par les technocrates rendent l'abord de cette discipline malaisé pour le non-initié et le conduisent souvent à penser qu'il s'agit là d'une matière à aucune pareille. Rien n'est moins vrai. Tous les principes applicables aux autres activités d'ingénierie sont parfaitement transposables à l'informatique, notamment ceux liés à la gestion des risques. Les risques liés à l'usage des systèmes d'information et de communication ne sont que quelques-uns des risques courus par une entreprise ou une organisation. Il convient donc de les ramener à leur juste proportion au sein de ceux-ci et de leur appliquer les techniques de gestion de risques qui présentent un caractère universel.

Celles-ci veulent que l'on apporte les réponses aux questions suivantes :

- Quelles sont les atteintes potentielles ?
- Quelles en sont les origines ?
- Quelles en sont les conséquences ?
- Quels sont les risques majeurs et les risques mineurs ?
- Comment les gérer ?

Voilà quelques-unes des interrogations que ce document se propose d'aborder.

1 LES ATTEINTES

Les **atteintes** aux systèmes d'information sont principalement de trois types :

- les atteintes à la disponibilité
- les atteintes à l'intégrité
- les atteintes à la confidentialité.

1.1 Les atteintes à la disponibilité

Au fur et à mesure qu'une organisation remplace ses anciennes procédures manuelles par des traitements automatisés, elle se rend de plus en plus dépendante de son informatique. Le retour vers les anciennes procédures ne pourra généralement plus être envisagé. En cas d'**indisponibilité** du système d'information, les conséquences deviennent vite insupportables. Le fonctionnement de l'organisation sera gravement handicapé voire paralysé.

Le temps pendant lequel l'indisponibilité d'un système d'information est supportable varie d'entreprise en entreprise en fonction de la nature des applications traitées. Selon le type d'application, une durée de quelques secondes (p.ex. pilotage de processus de fabrication industrielle), quelques minutes (p.ex. systèmes de réservation des compagnies aériennes), quelques heures, quelques semaines ou mois entraînera un préjudice important. D'autres applications par contre ne présentent qu'un caractère plus accessoire. Il est possible de s'en passer pendant plusieurs mois. Dans quasiment tous les cas, le préjudice causé augmente très rapidement avec la durée d'indisponibilité. Les systèmes dits « de production » doivent faire l'objet d'une attention prioritaire et constante.

La neutralisation des systèmes d'information et de communication est généralement le risque principal pour beaucoup d'entreprises et représente à lui seul près de la moitié des pertes dues à des sinistres informatiques.

1.2 Les atteintes à l'intégrité

Les atteintes à l'**intégrité** concernent les incidents qui ont pour effet que le système ne fonctionne plus selon les spécifications normales. On ne peut plus avoir confiance en les résultats qu'il produit car ceux-ci peuvent être erronés ou frauduleux.

Dans des cas extrêmes, l'atteinte à l'intégrité peut conduire à l'arrêt pur et simple de l'utilisation du système, ce qui ramène au cas décrit ci-dessus.

1.3 Les atteintes à la confidentialité

Le risque de divulgation d'informations confidentielles existe depuis toujours et se gérait avant l'arrivée de l'informatique par

1° la création de relations de confiance,

2° par le partage d'intérêts communs à garder certaines informations confidentielles et notamment l'intérêt de garder une longueur d'avance dans certains domaines : politiques, militaires, commerciaux, …

3° mais aussi par des contrôles de sécurité préventifs, dissuasifs, de détection, etc…

L'Histoire - de l'Antiquité à nos jours - fourmille de techniques diverses parmi lesquelles le chiffrement (non IT bien entendu) a une place importante. Jules César chiffrait ses messages critiques. Marie Stuart « perdit la tête » notamment parce que son chiffre s'était avéré trop faible face aux cryptanalystes anglais. Le « Grand Chiffre » de Louis XIV a résisté environ deux cents ans. Depuis son « craquage» au 19ème siècle, on a par exemple découvert que le « masque de fer » n'était pas le frère jumeau de Louis XIV comme la légende le voulait, etc…

Nous renvoyons à ce sujet le lecteur à la fascinante « Histoire des Codes Secrets » de Simon Singh.

Aujourd'hui, les systèmes « électroniques » d'informations, de par leur nature complexe, leurs possibilités d'échanges rapides et de duplication de messages, leur perméabilité difficile à maîtriser, ajoutent plusieurs couches de risques à la gestion d'une confidentialité adéquate.

Dans un monde d'échanges électroniques croissants, transportés, stockés et accédés par une diversité croissante de technologies (internet, technologies sans fil, smartphones,…) les CEO, les CIO et les CISO seront bien inspirés de se préoccuper constamment de la « sécurité des échanges électroniques » de leurs entreprises.

Nombre de systèmes gèrent des données ou des programmes au caractère très sensible. Leur divulgation à des tiers peut avoir des conséquences très dommageables. Les exemples abondent en matières médicale, financière, judiciaire,... Les entreprises confient leurs secrets à leurs ordinateurs : documents stratégiques, plans marketing, prix de revient, procédés de fabrication, travaux de recherche et de développement,... Des bases de données sont le fruit d'investissements considérables consentis en collecte et mise à jour de données. Certains systèmes détiennent un savoir-faire important : logiciels de pointe, systèmes-experts utilisés pour l'acceptation de risques de crédit ou d'assurance...

Les atteintes à la **confidentialité** peuvent dès lors mettre en danger la compétitivité de l'entreprise et se muer en risque majeur. En outre, elles exposent l'entreprise à des procédures basées sur la violation d'engagements contractuels de confidentialité ou de la législation sur la protection de la vie privée.

2. LES ORIGINES DES RISQUES INFORMATIQUES

Les risques trouvent leurs **origines** dans :

- les causes accidentelles
- les erreurs
- la malveillance.

2.1 Les risques accidentels

2.1.1 Risques matériels

C'est la destruction totale ou partielle d'un ou plusieurs composants d'un système d'information (matériel informatique ou de communication, supports de données, environnement tels que locaux, conditionnement d'air, alimentation électrique, installation téléphonique, …) suite à des événements comme un choc, la coupure de câbles électriques ou téléphoniques, l'incendie, l'inondation, la foudre, la tempête,…etc.

2.1.2 Pannes et dysfonctionnement de matériel ou de logiciel de base

Généralement, les interruptions de service consécutives à des pannes sont de courte durée mais ce n'est pas toujours le cas. Des défaillances de matériel ou de logiciels de base ont provoqué des arrêts de fonctionnement de serveurs importants s'étendant sur plusieurs jours ouvrables.

Les interruptions peuvent aussi résulter de pannes dont l'origine est externe à l'entreprise (réseau téléphonique, alimentation électrique, …).

L'impossibilité d'accéder au réseau Internet peut empêcher une organisation de recevoir ou d'émettre du courrier électronique ou faire en sorte qu'un site de commerce électronique ne puisse plus recevoir de commandes.

A ce niveau également, les CEO, les CIO et les CISO seront bien avisés de jauger régulièrement leur dépendance de la continuité du « réseau des réseaux » et d'envisager des solutions de continuité alternatives pour leurs processus les plus critiques, dans la mesure du possible bien entendu.

2.2 Erreurs

2.2.1 Erreurs de saisie, de transmission et d'utilisation de l'information

On a tendance à sous-estimer les erreurs de saisie de données. Même après vérification, elles atteignent couramment un taux de 0,5 %. A tort, on les considère comme une conséquence inéluctable de l'activité humaine, alors qu'elles sont à l'origine d'un nombre élevé de problèmes et de pertes pouvant être importantes. De bons contrôles de vraisemblance des données saisies sont une mesure indispensable.

La transmission de données, qu'elle se fasse par transport de supports ou par télécommunications, est sujette à altération de données ou détournements, sans compter les transmissions des mauvais fichiers.

D'une manière générale, les erreurs humaines de tous types sont une grande source de préoccupation. Des défauts organisationnels ou de communication interne, tels que la non-suppression d'un mot de passe attribué à une personne licenciée, peuvent être lourds de conséquences.

Mais l'informatique, qui peut être à l'origine d'un certain nombre de ces erreurs humaines, peut venir « à son propre secours », notamment si l'on a le bon sens de prévoir

- des contrôles de robustesse (limite d'un champ de saisie évitant un débordement dans les champs suivants),
- des filets de sécurité (« une date d'expiration » qui suspend automatiquement un utilisateur dont le contrat se termine à une date précise)
- etc…

2.2.2 Erreurs d'exploitation

Ces erreurs prennent des formes variées : effacement accidentel de fichiers, supports ou copies de sauvegarde, chargement d'une version incorrecte de logiciel ou de copie de sauvegarde, lancement d'un programme inapproprié, …

Il est souvent difficile d'identifier la cause exacte de ces problèmes : faute professionnelle, malveillance, erreur, négligence, laxisme, … Une analyse pointue des processus et des éléments endogènes ou exogènes, qui ont provoqué l'erreur, prendra du temps et risque d'être coûteuse pour l'entreprise.

Le recours à des systèmes automatisés de gestion des applications permet de réduire le rôle joué par les opérateurs humains et de faire baisser le nombre de ces erreurs.

2.2.3 Erreurs de conception et de réalisation

Alors que le nombre d'erreurs des deux catégories précédentes a tendance à se stabiliser et même à diminuer, les erreurs de conception et de réalisation sont en forte augmentation. Il suffit pour s'en convaincre de consulter les publications internationales qui recensent des dizaines de nouvelles vulnérabilités chaque semaine.

D'une part, des logiciels conçus et réalisés il y a bon nombre d'années sont toujours utilisés de manière opérationnelle. Leur documentation est souvent inexistante, incomplète ou mauvaise et n'est plus à jour. Leurs auteurs ne sont plus disponibles pour assurer la maintenance. La qualité de la programmation est généralement médiocre. Toute évolution, adaptation ou correction de ces logiciels devient dès lors une gageure, qui entraîne fréquemment des dysfonctionnements graves et imprévisibles.

D'autre part, on développe chaque jour de nouveaux logiciels de grande taille et d'une complexité sans cesse croissante. Les ambitions dépassent quelquefois l'état de l'art ou la compétence de leurs auteurs. Les développements s'appuient souvent sur des bibliothèques de composants ou des logiciels de base eux-mêmes truffés d'erreurs. L'application de méthodologies rigoureuses supportées par des outils performants et une approche systématique de contrôle de la qualité permettent de réduire les erreurs de conception et de réalisation.

Les défaillances des logiciels résultent souvent des lacunes de la maintenance. Chaque nouveau développement entraîne des charges de mise à jour du logiciel pendant toute sa durée de vie. Il est fréquent que la maintenance annuelle se chiffre à 20 % du coût de développement initial d'un logiciel. Il n'est donc pas rare de voir la maintenance cumulée exiger 70 ou 80 % des efforts des équipes de développement-maintenance.

Leurs conséquences des erreurs de développement et de conception sont souvent dramatiques et peuvent mettre en péril aussi bien la survie du client que du fournisseur. Les litiges relatifs à la fourniture de services et systèmes informatiques se multiplient à un rythme inquiétant. Nombre de ceux-ci demeurent inconnus car ils font l'objet de transactions amiables, assorties souvent de paiement de dommages et intérêts substantiels, ou de procédures d'arbitrage, par nature confidentielles.

Les erreurs de conception dans la configuration et le paramétrage des systèmes de protection engendrent de grosses vulnérabilités. Il y va par exemple d'ordinateurs coupe-feu (« firewalls ») ne filtrant rien ou prou ou encore qui soient mal placés dans le réseau.

Des faiblesses dans la conception de la protection logique, telles que des mots de passe communs à plusieurs personnes ou trop faciles à découvrir (par raisonnement logique, par « craquage » ou piratage, par observation illicite ….) créent également des brèches dans la sécurité.

2.3 Malveillance

Les actes malveillants à l'encontre des systèmes d'information et de communication, décrits ci-après, sont désormais des actes criminels sanctionnés pénalement par la loi du 28 novembre 2000.

2.3.1 Vol et sabotage de matériel

Les vols portent principalement sur les petits matériels, tels que les ordinateurs portables et les supports informatiques (disques de serveurs, …). La disparition d'un PC ou d'un serveur peut être lourde de conséquences au cas où celui-ci n'a pas fait l'objet d'une copie de sauvegarde récente et complète ou encore lorsque celui-ci contient des données ou programmes confidentiels.

Dans les grandes gares ou aéroports, il ne se passe pas de journée sans qu'un ou plusieurs portables ne soient volés. Ces outils des cadres contiennent le plus souvent des données confidentielles de l'entreprise. Le vol d'un portable peut également permettre de prendre connaissance des mots de passe et des informations nécessaires pour se connecter au réseau interne de l'entreprise.

Le sabotage va de l'endommagement d'un appareil isolé aux attentats terroristes détruisant toute une infrastructure.

L'utilisation de matériels hors standards du marché aggrave les conséquences d'un vol ou d'un sabotage dans la mesure où l'obtention de matériels de remplacement peut

s'avérer plus difficile. Cette dimension du risque (diminution de sa capacité à réagir) devrait être prise en compte par le CIO dans ses choix technologiques.

2.3.2 Fraudes

La pratique des fraudes est aussi vieille que le monde. L'informatique y a cependant ajouté de nouvelles dimensions :

- le montant moyen des fraudes informatiques est sensiblement plus élevé que celui des fraudes traditionnelles ;
- le manque d'enregistrements visibles réduit les chances de détection par observation fortuite ;
- programmes et données peuvent dans bien des cas être modifiés sans laisser de traces et être effacés avec une rapidité extrême. Il n'est pas rare qu'un fraudeur efface les fichiers comportant les traces de ses méfaits, ainsi que toutes ses copies de sauvegarde ;
- la sécurité est souvent sacrifiée au profit de l'efficience ;
- la complexité de certains systèmes est telle que les utilisateurs ne disposent plus de la compétence requise pour vérifier l'exactitude des résultats produits ;
- les contrôles organisationnels classiques (séparation de fonctions et de connaissances, doubles contrôles, …) ont été négligés lors de l'introduction des nouveaux systèmes ;
- de nombreux systèmes informatiques ont été réalisés sans prendre la sécurité en compte lors de leur conception ;
- le personnel technique peut contourner des contrôles essentiels.

Les fraudes informatiques conduisent à des détournements de *biens* et de *fonds*. Elles peuvent également avoir pour conséquence le sabotage du fonctionnement :

- des *exécutants*, que l'on induit en erreur (p.ex. livraison à des clients dont l'insolvabilité a été masquée, acceptation de risques tarés dans une compagnie d'assurances par manipulation de l'historique des sinistres, …) ;
- des *gestionnaires*, en basant le contrôle de gestion sur des états incorrects, ce qui peut conduire à ne pas prendre des décisions qui s'imposeraient ou à prendre des décisions inappropriées qui pourraient avoir des conséquences désastreuses (p.ex. rentabilité des départements et produits, situations de trésorerie, …).

2.3.3 Sabotage immatériel

Le sabotage immatériel concerne l'altération ou la destruction, totale ou partielle, des données, des programmes ou de leurs sauvegardes. Ses conséquences peuvent être aussi graves et parfois même davantage que celles d'un sinistre matériel, car il peut

provoquer des destructions en profondeur et avoir pour effet de neutraliser pendant un temps long le fonctionnement du système informatique.

Le sabotage immatériel recouvre diverses notions :

- la modification non autorisée de programmes ;

- le cheval de Troie qui est une partie de programme pernicieuse ajoutée à un autre programme dont le comportement externe paraît normal ;

- les bombes logiques, qui sortent leurs effets destructeurs de données ou de programmes lors de la réalisation d'un événement (p.ex. survenance d'une date particulière, destruction de fichiers lorsque le matricule de l'auteur licencié disparaît du fichier du personnel,…). Une forme particulièrement dommageable de bombe logique consiste à altérer graduellement un nombre limité d'enregistrements d'une grande base de données. Lorsque le problème est découvert, parfois au terme de nombreux mois, il y a fort à parier que l'entreprise ne disposera plus d'aucune copie de sauvegarde fiable et devra procéder à un contrôle exhaustif et coûteux de l'entièreté de la base de données ;

- les virus et vers, fortement médiatisés, qui agissent comme des bombes logiques mais qui ont, en outre, la faculté de se reproduire et faire perdurer les infections. L'Internet et le courrier électronique leur ont fourni des voies royales de propagation ;

- les logiciels espions (« spyware »). Lorsqu'un utilisateur consulte licitement des sites Internet, il peut lire une page intéressante, mais qui cache des parties malveillantes permettant à ces dangereux logiciels espions de s'installer dans le poste de travail et de migrer sur le réseau interne tout en communiquant des informations-clés vers l'extérieur. Techniquement, ces pages dangereuses sont beaucoup plus difficiles à détecter que les virus dans les mails.

Le recours intensif à l'Internet a fait apparaître de nouvelles formes d'actes malveillants, dont voici quelques exemples :

- le déni de service, qui se traduit par l'indisponibilité d'un site web. Il se provoque en inondant et en saturant le serveur ou le réseau par une masse énorme de messages rendant impossible l'accès normal aux ressources. Ces messages proviennent le plus souvent de réseaux de PC mal protégés, encore appelés « botnets ». Il s'agit de réseaux de PC « zombies », dont l'auteur malveillant a pris le contrôle. Ces réseaux peuvent comporter des dizaines de milliers de PC, appartenant bien souvent à des propriétaires, qui n'ont pas installé les mesures de sécurité élémentaires que sont des logiciels « firewall » et des logiciels anti-virus ;

- le remplacement de la page d'accueil d'un site web par un renvoi automatique sur le site d'un concurrent ou sur un site à caractère pornographique ;

- le renvoi de la page d'accueil vers celle d'un site qui y ressemble très fortement, mais qui est en fait celui d'une organisation malveillante, qui tentera ainsi de voler

des données personnelles (données d'identité de l'utilisateur, données relatives à des comptes bancaires ou à des cartes de crédit, mots de passe, etc.) ;

- la modification des prix du catalogue d'une entreprise de vente exclusivement par Internet ;

- la modification de l'adresse e-mail pour les commandes sur Internet et son remplacement par l'adresse du concurrent ;

- le dépôt, dans la boîte d'envoi du système de messagerie d'un service Relations publiques d'un message annonçant l'ouverture d'une instruction judiciaire à l'encontre de l'entreprise. Le message devait être envoyé aux agences de presse ;

- le blocage du central téléphonique (ordinateur) empêchant toutes les communications téléphoniques intérieures et extérieures. Les techniques de téléphonie par Internet (VoIP) devront faire l'objet de mesures de protection adéquates.

2.3.4 Indiscrétion, détournement d'informations

Il s'agit d'actes qui ont pour effet que des personnes non autorisées ont accès aux informations maintenues par le système informatique. Ces informations peuvent être des données ou des programmes (correspondances, contrats, secrets industriels, plans commerciaux, calculs de prix de revient, offres, données personnelles, financières, médicales, …). Au fur et à mesure que des données de plus en plus confidentielles sont confiées à des ordinateurs, ceux-ci deviennent les cibles privilégiées de cette forme actuelle d'espionnage industriel.

Les systèmes-experts font l'objet d'une convoitise particulière car ils contiennent une part essentielle du savoir-faire et de la politique suivie par une organisation.

Ces accès non autorisés aux données confidentielles de l'entreprise peuvent être perpétrés par des tiers qui font une intrusion dans le réseau de l'entreprise. Toutefois, le propre personnel de l'entreprise est souvent à l'origine de ces méfaits. Il devient courant qu'un employé quitte une entreprise pour se faire engager par un concurrent ou pour démarrer une activité concurrente, non sans avoir pris soin de copier les fichiers essentiels qui lui procureront un avantage concurrentiel et déloyal. La multiplication de supports amovibles de petite taille mais de grande capacité de stockage, tels que les sticks mémoire ou les disques portables à interface USB, a grandement facilité la mise en œuvre de ces actes de copiage. Parfois, les fichiers sont même exportés en annexe à des courriers électroniques transmis par le propre système de messagerie de l'entreprise victime.

2.3.5 Détournement de logiciels

La copie de logiciels pour PC est une activité qui bat toujours son plein nonobstant les succès récents de poursuites judiciaires engagées contre les pirates et la diminution de l'attrait du copiage résultant des baisses de prix consenties par les éditeurs de logiciels.

La responsabilité de l'entreprise est engagée si elle permet le copiage ou l'utilisation de logiciels copiés et ce, en vertu de la loi sur les droits d'auteur des programmes du 30 juin 1994.

Les conséquences pour les entreprises prises en flagrant délit de détention de programmes illicites sont lourdes. Elles devront en effet s'acquitter de :

- L'acquisition des licences manquantes ;
- Le paiement d'indemnités pouvant s'élever à 200 % du prix des licences ;
- Le défraiement des frais de la procédure (frais de justice, d'huissier, d'expert judiciaire, etc.).

2.4 Grève, départ de personnel stratégique

Le personnel est un maillon indispensable dans la chaîne qui assure le fonctionnement d'un système d'information. L'indisponibilité, une épidémie ou la disparition d'un membre de personnel-clé peut provoquer l'arrêt du système et par voie de conséquence celle de toute l'activité de l'entreprise.

3. LES CONSÉQUENCES DES RISQUES INFORMATIQUES

Les conséquences d'atteintes aux systèmes d'information sont multiples :

3.1 Les pertes directes

Elles correspondent de manière directe à une disparition d'actifs. Elles entraînent des écritures de redressement comptable s'il s'agit d'actifs appartenant à l'entreprise (détournement de fonds ou de biens) ou un décaissement s'il s'agit d'actifs appartenant à des tiers (comptes clients, dépôts, …). Si ces actifs sont nécessaires pour poursuivre le fonctionnement de l'entreprise (stock, outils de production, …), ils devront être remplacés généralement dans l'urgence.

Dans les *pertes directes matérielles*, on trouve des postes tels que :

- équipements informatiques ;
- équipements télématiques ;
- environnement (électricité, eau, climatisation, …) ;
- bâtiments ;
- logiciels ;
- données.

Dans les *pertes directes immatérielles*, on trouve des postes tels que :

- le contenu des logiciels ;
- le contenu des données.

3.2 Les pertes indirectes

Les conséquences indirectes d'un incident dépassent généralement de loin les pertes directes.

Dans les *pertes indirectes matérielles*, on trouve des postes tels que :

- les frais de reconstitution de données et d'archives ;
- les frais supplémentaires, définis comme la différence entre le coût total de traitement informatique après sinistre et le coût total de traitement informatique qui aurait été normalement supporté pour effectuer les mêmes tâches dans la même période, si aucun sinistre n'était survenu (p.ex. location de matériel de remplacement, environnement de secours, travail sous-traité, personnel temporaire, primes spéciales et heures supplémentaires, frais de transport, …) ;
- les frais financiers ;
- les intérêts sur comptes à recevoir ;
- les pertes d'exploitation ;
- le manque à gagner (reconstitution du bénéfice normal en l'absence de sinistre) ;
- la perte de matières périssables ;
- les frais d'étude et d'expertise ;
- la responsabilité vis-à-vis de tiers (p. ex. non respect d'obligations contractuelles suite à une neutralisation du système informatique, demandes de dédommagement formulées par des personnes lésées par la divulgation de données de nature confidentielle, telles que données médicales, financières, …).

Les *pertes indirectes immatérielles* contiennent des postes tels que :

- l'atteinte à l'image de marque (et donc le risque de fuite de la clientèle, etc.)
- la perte de marchés potentiels ;
- l'affaiblissement de la capacité concurrentielle ;
- le retard technologique.

Ces pertes indirectes immatérielles sont particulièrement pernicieuses car leurs effets ne se font généralement sentir qu'à plus long terme, ce qui fait qu'on les appelle parfois *pertes futures*.

Les défauts de sécurité peuvent susciter la méfiance de partenaires ou clients lorsqu'ils prennent connaissance des incidents de sécurité informatique.

L'étude du préjudice consécutif à un sinistre doit amener à se poser les questions suivantes :

- est-il chiffrable ?
- est-il prouvable ?
- est-il réparable ?
- est-il assurable ?

4. LE COÛT DES ATTEINTES À LA SÉCURITÉ

Il existe peu de données statistiques relatives aux pertes engendrées par des sinistres informatiques. La réticence des entreprises à déclarer les sinistres dont elles sont victimes tient à diverses causes :

- craintes d'effets sur l'image de marque de l'entreprise ;
- non-couverture par un contrat d'assurance ;
- peu d'espoir d'obtenir réparation des dommages subis ;
- impossibilité de remédier rapidement aux défaillances dans certains cas;
- désagréments causés par l'enquête ;
- identification et condamnation de l'auteur d'actes malveillants incertaine.

Néanmoins, le Club de la Sécurité Informatique Belge a mené en 1998 et en 2004 des enquêtes de grande envergure auprès des entreprises belges, portant respectivement sur 680 et 550 entreprises. Les rapports de ces enquêtes publiés par le CLUSIB contiennent une grande richesse de données relatives aux mesures de protection mises en œuvre par nos entreprises, de même qu'aux incidents de sécurité dont elles ont été victimes.

5. LA GESTION DES RISQUES

Les mesures de sécurité informatique se construisent au départ d'une gestion des risques, pour laquelle il existe plusieurs approches possibles. Elles se résument toutes à quelques aspects essentiels.

Un risque est la potentialité d'une menace donnée d'exploiter une vulnérabilité d'une entité et donc d'occasionner un dommage à l'entreprise.

La gestion des risques consiste :

- à identifier les risques (menaces, potentialité, probabilité de survenance) ;
- à les évaluer selon des critères propres à chaque entreprise, tenant compte tant des faiblesses des protections (exposition aux risques, vulnérabilités) ainsi que des conséquences potentielles pour l'entreprise (impact, enjeu).

Cet examen tiendra compte de la capacité de l'entreprise à réagir en cas d'impact, capacité qu'il faudra qualifier avec la plus grande objectivité.

Il faut ensuite définir les moyens de protection adéquats, modulés selon une analyse coûts/bénéfices. Certains risques peuvent être transférés en les couvrant par exemple par des assurances ou en sous-traitant certaines applications.

En toutes circonstances, il est essentiel que toutes les parties concernées par les risques contribuent activement à l'évaluation de ces derniers, notamment par l'identification des menaces potentielles ou en évaluant les conséquences possibles. En

particulier, chaque constat de faiblesse en sécurité informatique doit être signalé en vue de l'étudier de manière adéquate et de prendre les éventuelles mesures nécessaires.

La gestion des risques doit être un processus permanent. La réévaluation des risques doit intervenir en temps opportun : de manière périodique ou lors d'événements tels que le lancement d'une nouvelle application, la modification dans la configuration des réseaux, la réorganisation d'un département, la mutation de responsables, etc. Tout ceci va donc requérir une méthode de « gestion du changement » adéquate.

5.1 Risques majeurs et risques mineurs

Le risque informatique n'est qu'un des nombreux dangers que court l'entreprise. Aussi, il doit être maîtrisé et géré comme ces autres risques par une approche méthodologique rigoureuse. Des mesures adéquates et cohérentes doivent être prises.

Un arbitrage doit être fait entre les conséquences financières des sinistres et le montant des investissements de sécurité à consentir. La sous-sécurité est dangereuse. La sur-sécurité est un gaspillage.

Une saine gestion des risques implique que l'on établisse la distinction entre risques majeurs et mineurs.

Les **risques majeurs** sont des risques de vie ou de mort pour l'organisation. Ils ont généralement un taux de fréquence extrêmement bas mais leurs conséquences sont catastrophiques. S'ils se matérialisent, l'entreprise ne survivra pas car les conséquences dépassent sa capacité financière ou sont telles que l'entreprise n'atteindra plus ses objectifs généraux. Ils sont totalement INACCEPTABLES. L'assurance est inadéquate pour se protéger contre pareils risques. Plus de la moitié des entreprises dont les bâtiments ont été totalement détruits par un incendie n'existent plus trois ans après le sinistre. Elles sont tout simplement "*out of business*". Ceci n'est pas dû au fait qu'elles n'étaient pas ou mal assurées mais bien parce qu'elles ne disposaient pas d'un plan de survie. L'assureur donne une indemnisation mais il ne peut restituer à l'entreprise les données et programmes perdus. Que faire lorsque les programmes et données indispensables au fonctionnement de l'organisation ont été détruits ? Comment reconstituer la situation comptable, les fichiers clients, fournisseurs et articles, les prix de revient, les modèles ou gammes opératoires de la production, ...? Plusieurs entreprises belges ont perdu l'entièreté de leurs données, suite à la conjugaison de sinistres et de systèmes de sauvegarde de données défectueux à l'insu de leurs utilisateurs.

La seule réponse aux risques majeurs est la mise en œuvre d'un plan de survie, qui permettra à l'entreprise de restaurer, dans des délais acceptables, la situation qui prévalait avant le sinistre et de poursuivre ses activités. Ce plan doit être périodiquement testé pour valider son bon fonctionnement. L'expérience a montré que même dans des environnements où ces plans sont régulièrement testés, il subsiste toujours des imprévus et des difficultés lorsqu'il faut mettre le plan en exécution suite à un sinistre réel et non simulé.

Les **risques mineurs** ont le plus souvent une probabilité de survenance plus élevée mais leurs conséquences sont moindres et temporairement acceptables. Ces risques

peuvent être traités par des mesures de prévention et le recours aux assurances. L'amortissement économique de ces mesures sera évalué par rapport à la probabilité et la gravité des sinistres. Les très nombreux incidents que l'on rencontre au quotidien sans même qu'ils ne soient répertoriés dans les statistiques vu leur fréquence élevée sont à ranger dans cette catégorie.

5.2 Méthodologie de gestion des risques

Les diverses approches méthodologiques de gestion des risques se doivent toutes d'aborder les étapes suivantes :

- identification des risques, par raisonnement, imagination et simulation de scénarios ;
- évaluation des conséquences financières et non financières des sinistres ;
- détermination de la capacité financière de l'entreprise ainsi que de ses objectifs généraux ;
- répartition des risques en risques majeurs et mineurs ;
- évaluation du niveau de sécurité existant (audit) ;
- examen des mesures envisageables pour :
    - éliminer les risques, si possible (élimination) ;
    - réduire la probabilité de survenance (prévention) ;
    - limiter l'amplitude (protection) ;
- étude du plan de survie réalisable pour réagir vis-à-vis des risques majeurs ;
- arbitrage pour les risques majeurs entre :
    - le plan de survie réalisable ;
    - les mesures de prévention possibles ;
    - la remise en cause éventuelle des objectifs généraux ;
- équilibrage pour les risques mineurs des mesures en fonction des contraintes de l'entreprise et de leur rapport qualité/coût ;
- recours à l'assurance pour :
    - financer le plan de survie ;
    - transférer les risques résiduels ;
- formalisation des mesures ci-dessus sous forme d'un plan pour l'amélioration de la sécurité pour les années à venir.

5.3 Interdépendance du traitement des risques

Le traitement d'une catégorie de risques aura souvent des répercussions sur celui des autres catégories. Les mesures de prévention mises en œuvre pour un type de risque peuvent avoir des effets bénéfiques pour d'autres. Par exemple, la conservation de copies de sécurité en divers endroits extérieurs à l'entreprise pour se protéger contre les conséquences d'un incendie permettra également de maîtriser une neutralisation provoquée par une attaque extérieure, voire une occupation de l'entreprise.

Inversement, les mesures prises pour limiter certains risques peuvent en aggraver d'autres. La protection contre l'intrusion tend à réduire le nombre des accès, tandis que l'évacuation du personnel en cas d'incendie demande leur multiplication. Corollairement, la multiplication des endroits de conservation des copies de sécurité accroît les risques d'accès non autorisés à celles-ci.

5.4 Recours à l'assurance

Le recours à l'assurance ne paraît pas logique si l'entreprise ne dispose pas d'un plan de survie ; il ne semble pas utile si le coût des sinistres est supportable (notion de franchise). Il est nécessaire dans tous les autres cas, à condition que les garanties proposées soient adaptées aux besoins mis en évidence lors de l'étude des risques informatiques.

La réalisation d'une bonne couverture en matière de risques informatiques est loin d'être une chose évidente. Les compagnies d'assurances actives dans ce domaine sont peu nombreuses. Les contrats proposés présentent souvent des restrictions (p. ex. exclusions, plafonds d'intervention, franchises). La souscription d'une série de contrats isolés peut donner une fausse impression de sécurité alors qu'il existe trous et redondances entre les garanties souscrites.

Le conseil de spécialistes, notamment de courtiers qualifiés, n'est pas un luxe dans ce domaine où le recours à des contrats «sur mesure» s'avère souvent être la solution la plus appropriée.

Les garanties, auxquelles on peut souscrire, portent notamment sur :

- les matériels ;
- les logiciels ;
- les frais de reconstitution de données ;
- les frais supplémentaires ;
- les pertes d'exploitation ;
- la reconstitution du bénéfice ;
- les frais financiers et les intérêts sur comptes à recevoir ;
- les fraudes ;
- la responsabilité civile ;

etc.

6. L'IDENTIFICATION DES RISQUES

6.1 Découpe en centres de risques

Les risques doivent nécessairement être identifiés pour l'ensemble de l'entreprise. Le domaine à couvrir est donc très vaste. C'est pourquoi l'étude des risques sera grandement facilitée si l'entreprise est découpée en centres de risques. Une découpe envisageable consiste à considérer comme centres de risques les environnements suivants :

- les applications elles-mêmes
- les centres de traitement des applications
- le développement des applications.
- le réseau qui permet les échanges des données traitées par les applications
- les risques propres aux Tiers (échanges et responsabilités externes)
- etc.

Chaque centre de risque pourra lui-même être découpé en sous-centres de risques et ainsi de suite. L'avantage de cette approche est qu'elle permet de déléguer l'application de la méthode d'analyse et de traitement des risques aux responsables hiérarchiques. Ceux-ci doivent étudier, chacun à leur niveau, les risques et les parades, bien entendu, avec l'appui et le conseil de spécialistes qui les guideront dans leurs travaux.

6.2 Inventaire des risques

L'identification des risques est toujours une tâche délicate pour le non-spécialiste. De prime abord, il se croit souvent faussement sécurisé et ne peut imaginer les vulnérabilités auxquelles le système, dont il a la charge, est exposé. Lorsque le spécialiste lui suggère quelques scénarios réalistes, il devient angoissé à l'excès.

L'approche par scénarios a le mérite d'être parlante et concrète. Il est souhaitable de l'appliquer car elle permet de réfléchir aux conséquences d'un certain nombre de situations qui pourraient réellement survenir, ainsi qu'aux parades à mettre en œuvre. Il existe d'ailleurs des glossaires de scénarios-types particulièrement utiles pour cet exercice.

Par contre, cette approche fait courir le risque de sombrer dans le syndrome de la ligne Maginot, qui fait que l'on croit avoir imaginé tous les cas de figures. En effet, au même titre que les check-lists de sécurité, ces glossaires de scénarios ne concernent que des cas connus et sont donc orientés vers le passé. Chaque jour voit naître des scénarios qui ne s'étaient pas encore produits auparavant. Particulièrement en matière de criminalité informatique, l'imagination des malfaiteurs est sans bornes et très largement supérieure à la capacité inventive des meilleurs spécialistes de sécurité.

C'est pourquoi il est indispensable d'avoir une réflexion plus générale, qui consiste aussi à réfléchir aux conséquences. On ne doit donc pas ne se préoccuper que du « *comment* ?» mais aussi du « *quid si cela se passe ?* ».

Pour **chaque application**, il conviendra de se poser les questions suivantes qui ont trait aux aspects fondamentaux de disponibilité, intégrité et confidentialité :

- quelles seraient les conséquences pour l'organisation si cette application était indisponible pendant une période de quelques secondes, minutes, heures, jours, semaines, mois, ...? (atteinte à la DISPONIBILITE);
- quelles seraient les conséquences les plus lourdes d'une erreur ou le montant maximal d'une fraude dans cette application ? (atteinte à l'INTEGRITE) ;
- quelles seraient les conséquences les plus graves d'une divulgation à des tiers des données ou des programmes de cette application ? ou encore des

données relatives au système de sécurité protégeant cette application ? (atteinte à la CONFIDENTIALITÉ).

Les risques liés aux **centres de traitement** présentent le plus souvent un caractère global aux effets cumulatifs, voire multiplicateurs. En effet, la neutralisation d'un serveur ou la destruction d'un centre de traitement affectera toutes les applications dont l'exploitation en dépend. On se posera à cette fin les mêmes questions que celles suggérées ci-dessus.

Il devient de plus en plus courant que l'informatique soit une arme concurrentielle et revête un caractère stratégique pour les organisations. Au delà de la simple amélioration de l'efficacité opérationnelle, les nouvelles applications jouent un rôle crucial dans les politiques commerciales en mettant de nouveaux produits et services à disposition des clients, agents, distributeurs, fournisseurs,... Un retard ou une neutralisation du **développement des applications** se traduit alors directement en pertes de marché. Il faut en évaluer la portée.

Lorsqu'on évalue financièrement les conséquences des risques, on ne cherche pas de fausse précision. Seul l'ordre de grandeur importe, afin de déterminer si on a affaire à un risque majeur ou à un risque mineur et de faire un classement relatif grossier des risques. On parlera par exemple de sinistres de moins de 10.000, 20.000, 50.000 EUR, de moins de 100.000, 200.000, 500.000 EUR, de moins de 1, 2, 5 millions EUR et ainsi de suite….

On remarque ainsi que le rôle du spécialiste de la sécurité est de catalyser la réflexion des utilisateurs mais que ceux-ci sont les seuls à être réellement qualifiés pour évaluer les conséquences des risques identifiés par eux ou par les spécialistes auxquels ils font appel pour les guider sur le plan méthodologique, sur le plan des risques techniques complexes, etc.

7. TRAITEMENT DES RISQUES

7.1 Les risques d'atteinte à la disponibilité

Tout système d'information devient indisponible dès qu'un des composants nécessaires à son fonctionnement cesse d'être disponible. Se prémunir contre les risques de neutralisation implique dès lors d'assurer une redondance suffisante des éléments critiques, de telle sorte que la défaillance de l'un d'entre eux ne conduise pas à une neutralisation du système. Les systèmes de réservation de places d'avion ou de paiements électroniques font largement usage de ce principe. Le terme "composant" est à prendre au sens large, car il convient d'y inclure tous les éléments indispensables au fonctionnement du système d'information (matériel, logiciel, données, communications, conditionnement d'air, personnel, énergie,...).

Il conviendra de ne pas réunir les composants redondants dans un même espace, où ils pourraient tous être neutralisés simultanément, par exemple suite à un incendie ou une grève. Il faudra donc les placer en des lieux suffisamment séparés, parfois de plusieurs

kilomètres (p.ex. des bâtiments trop contigus pourraient être touchés par un même sinistre tel qu'une chute d'avion).

Quels que soient les moyens de prévention déployés, l'éventualité d'un sinistre catastrophique ne peut jamais être écartée.

Il conviendra donc d'envisager :

- Une sécurisation de la configuration informatique, dans le cadre d'un plan de recouvrement (DRP – Disaster Recovery Plan). Différentes procédures sont à élaborer et à mettre en pratique, par exemple pour les copies de sauvegarde (des fichiers et des programmes), le dédoublement de matériel, les contrats de maintenance avec les fournisseurs, etc.

  Diverses solutions peuvent être envisagées telles que :

  - plusieurs sites de traitement propres à l'entreprise, de sorte qu'un site puisse reprendre les activités d'un autre site neutralisé ;
  - contrat avec une entreprise spécialisée qui met son centre à disposition en cas de sinistre ;
  - centre de calcul mobile (camion équipé) ;
  - centre de calcul transportable (analogue aux salles de tennis « gonflables »)

  Chacune de ces solutions entraînera des frais supplémentaires qu'un contrat d'assurance approprié pourra utilement financer. La solution la plus appropriée doit être recherchée pour chaque cas précis en fonction des contraintes de la situation.

- Une adaptation des activités professionnelles, dans le cadre d'un plan de continuité (BCP – Business Continuity Planning). Les procédures sont à élaborer avec les utilisateurs afin d'avoir la créativité suffisante pour les bonnes solutions alternatives en cas d'arrêt temporaire ou prolongé des services de l'informatique.

  A titre d'exemple, la panne temporaire d'un serveur de transactions avec un ou plusieurs partenaires identifiés peut facilement être couverte par l'envoi de fax ; pour cela, il faut un accord avec le partenaire pour pouvoir mettre immédiatement la procédure en œuvre, en cas d'urgence.

L'élaboration d'un plan de survie comportera les étapes suivantes :

- recensement des applications vitales pour le fonctionnement de l'entreprise ;
- définition des priorités des applications pour le redémarrage ;
- recensement de l'actif informatique ;
- définition des procédures et lieux de stockage des éléments nécessaires pour les applications vitales (données, programmes, etc…) ;
- choix des solutions de secours ;

- formalisation du plan de secours ;
- essais et simulations périodiques du plan de secours.

Lors du recensement de l'actif informatique, on attachera une attention particulière à tous les éléments présentant un caractère d'unicité ou dont le remplacement pourrait s'avérer problématique.

Dans tous les cas, certaines situations extrêmes doivent être résolues, dans le cadre d'un plan catastrophe par exemple.

7.2 Les risques d'atteinte à l'intégrité

Des modifications volontaires ou accidentelles dans des informations peuvent avoir des conséquences désastreuses pour l'entreprise. Ces atteintes peuvent résulter d'actes d'origine interne, risque qu'il ne faudrait nullement sous-estimer, mais également d'intrusions en provenance de l'extérieur.

Ces risques ne peuvent se comprendre qu'en s'interrogeant sur la signification profonde des systèmes d'information. Pour connaître la réalité du monde qui nous entoure, on a le choix entre *l'observation directe* (p.ex. comptage de pièces en stock, inventaire physique des titres d'un portefeuille, …) ou le *recours à un système d'information*, qui donne une *image* de la réalité (fiche de stock, relevé de portefeuille, …).

L'observation directe est souvent impraticable ou trop coûteuse. Le système d'information s'impose alors pour des raisons économiques. Les images des objets de la réalité sont mémorisées sous forme de données et mises à jour lors de la survenance d'événements qui les modifient.

L'exploitation d'un système d'information repose sur une sorte de contrat de confiance qui doit être partagé par tous les utilisateurs. Cette condition purement subjective consiste à accepter l'idée que les données du système donnent une image complète et fidèle de la réalité.

Dès qu'un utilisateur met en doute la fidélité d'une image fournie par le système, le recours à l'observation directe de la réalité s'impose (inventaire physique, comptage,…).

Aussi longtemps qu'une fraude ou qu'une erreur n'est pas détectée, le consensus des utilisateurs reste entier. Des prestations continuent à être effectuées et des décisions continuent à être prises, tous ignorant que la réalité n'est plus correctement reflétée.

La confiance revêt un caractère absolu. Un manque répété de fiabilité de l'information fournie par le système entraînera son rejet et/ou son abandon par les utilisateurs.

Chaque composant du système d'information peut connaître des défaillances qui mettront en péril l'intégrité des résultats qu'il fournit. Il en va ainsi des données elles-mêmes, des programmes, des utilisateurs, des équipements, etc.

La *fiabilisation* exploitera les principes de la *redondance*, en effectuant des vérifications croisées entre les deux types de « processeurs » utilisés, à savoir les processeurs *humains* et les processeurs *automatisés*. Il apparaît ainsi quatre axes de contrôle :

- l'homme contrôle l'homme (contrôle interne) ;
- l'homme contrôle le système (contrôles fonctionnels) ;
- le système contrôle le système (contrôles techniques) ;
- le système contrôle l'homme (contrôles conceptuels).

Le *contrôle interne* veille à mettre en place une organisation sécurisée :

- principe de la double intervention (p.ex. double signature, double saisie de données, lancement d'un ordre et confirmation de son exécution,…) ;
- principe d'autorisation (p.ex. plafond financier d'autorisation de signature) ;
- principe des privilèges minima nécessaires et suffisants pour exécuter la fonction ;
- définition claire et précise des responsabilités ;
- séparation de fonctions (exécuter, approuver, contrôler) ;
- séparation du savoir ;
- rotation de fonctions ;
- formation du personnel ;
- etc...

Les *contrôles fonctionnels* comprennent toutes les actions que les humains doivent accomplir en amont et en aval de l'ordinateur pour vérifier le bon fonctionnement des traitements effectués par celui-ci : calcul et vérification de totaux de contrôle, examen des bilans des traitements (nombres d'enregistrements lus, traités, rejetés, totaux financiers des mouvements traités, …).

Les *contrôles techniques* ont pour but de vérifier le bon fonctionnement des traitements et transmissions de données (p.ex. contrôles de parité, sceaux électroniques pour vérifier la non-altération de données lors de transmissions, …). Par définition, ils sont indépendants de la nature des applications concernées.

Les *contrôles conceptuels* sont comme leur nom l'indique strictement non-technologiques. Ils ont pour but de détecter toutes les situations du monde réel qui sont *impossibles* ou *peu plausibles*, car en violation de lois physiques, biologiques, humaines (p. ex. égalité débit-crédit en comptabilité, vraisemblance du taux de change entre devises, plausibilité d'une date de naissance, …).

L'examen de nombreux cas d'erreurs et de fraudes connus montre que la plus grande partie d'entre elles eût pu être détectée, si le système d'information avait vérifié de manière extrêmement poussée les violations de ces *contraintes d'intégrité conceptuelles*. Ces contraintes sont :

- statiques : elles doivent être vérifiées à tout moment, (p. ex. vraisemblance d'une date de naissance) ;

- dynamiques : elles doivent être vérifiées lors de la survenance d'un événement, induisant un changement des données du modèle, (p.ex. pourcentage d'augmentation entre ancien et nouveau salaire).

Ces contraintes devront idéalement pouvoir être définies dans le dictionnaire de données des systèmes de gestion de bases de données définissant les objets modélisés par le système d'information, en lieu et place de les incorporer, comme souvent le cas, dans les programmes d'application, ce qui en rend le contrôle très difficile.

Cette mesure devrait permettre à tous ceux (auditeurs, réviseurs, utilisateurs, …) préoccupés par la fiabilité d'un système d'information de vérifier que les contrôles d'intégrité des données ont été mis en œuvre de manière adéquate, correcte et complète, en vue de déceler et d'empêcher les données erronées ou frauduleuses.

II convient d'attirer l'attention sur le fait que la différence entre une erreur et une fraude ne réside que dans l'intention de celui qui commet l'acte. Les systèmes de contrôle ne sont ni des psychologues ni des psychiatres. Ils ne peuvent donc établir une distinction entre ces deux manifestations. Par conséquent, ce seront exactement *les mêmes mécanismes* qui serviront à détecter les erreurs et les fraudes. Réduire la probabilité de survenance d'erreurs fournira simultanément une protection efficace contre les fraudes.

Éliminer totalement les erreurs et les fraudes n'est pas un objectif réaliste. Le coût correspondant serait infini. Toutefois, comme tout ce qui est idéal, il s'agit d'un objectif vers lequel il convient de tendre. Dans la vaste majorité des systèmes actuels, le point des retours décroissants est loin d'avoir été atteint. Le coût de la protection demeure le plus souvent inférieur à celui de la non-protection. Face à la dépendance croissante des entreprises de l'informatique et à l'activité sans cesse accrue des professionnels du crime en col blanc, des investissements importants s'imposent, si l'on veut contenir les pertes résultant d'erreurs et fraudes *dans des limites supportables*. Pareil objectif est réaliste.

La journalisation de l'identification des auteurs, des accès aux systèmes, aux applications ou aux fichiers représente une dissuasion envers la malveillance et donc un moyen de réduire les risques de perte d'intégrité. Bien plus, de tels traçages permettent souvent de remonter aux causes de la perte d'intégrité.

7.3 Les risques d'atteinte à la confidentialité

Les systèmes et réseaux interconnectés facilitent le copiage des informations sans laisser de trace depuis et vers n'importe où dans le monde. Des informations critiques ou délicates peuvent tomber entre des mains malveillantes ou entre celles de concurrents. Cela peut intervenir par piratage du site Internet (dépôt de programmes espions, etc.), par divulgation de mots de passe, de manière directe par la prise de contrôle à distance des systèmes ou des applications, ou encore de bien d'autres façons.

Il faut donc :

- *identifier* toutes les informations qui ne peuvent être rendues publiques;
- les *classifier* selon l'impact ou les conséquences que subirait l'entreprise en cas de divulgation ;
- envisager les solutions potentielles pour les *protéger*.

La stratégie à suivre est, en tous points, identique à celle suivie pour maîtriser les autres risques : prévenir, détecter et protéger.

- **Prévenir** en mettant une barrière aux accès non autorisés. Ceci implique une politique de *contrôle d'accès* telle que chaque maillon de la chaîne d'accès aux données puisse être *identifié* et *authentifié*. Chaque élément devra donc décliner non seulement son identité mais également un moyen supplémentaire permettant au système de contrôle d'authentifier cette identité, afin de déceler les usurpations d'identité. Pour les personnes, l'identification se fait le plus souvent en donnant un nom d'utilisateur ou un numéro de compte d'imputation. L'authentification se fait par quelque chose que l'utilisateur *sait* (p.ex. mot de passe), *détient* (p. ex. carte à puce) ou *est* (p.ex. empreinte digitale) ou une combinaison de ces techniques (p.ex. carte à puce, mot de passe et empreinte digitale) ou encore *fait* (mouvement et clic de souris, biométrie de la frappe appelée aussi « the fist of the sender », etc.). Ces moyens d'identification et d'authentification doivent être confidentiels, personnels et individuels.

  Le contrôle doit cependant s'étendre aux autres composants : est-ce bien tel PC ou tel serveur, telle ligne téléphonique, tel programme, … ?

  La prévention requiert de définir une *politique d'autorisation*, qui précise quel *sujet* peut exécuter quelle *action* sur quel *objet* (p.ex. tel utilisateur peut travailler sur telle station de travail, tel programme peut être déclenché au départ de telle station de travail, tel programme peut accéder à tel fichier, …).

- **Détecter** grâce à des systèmes de détection d'intrusion et en effectuant une *journalisation* systématique de tous les accès et opérations effectués sur le système, ainsi que de toute modification apportée aux prérogatives de sécurité des utilisateurs. Ce journal sera analysé régulièrement pour détecter d'éventuels profils de comportements anormaux. Les tentatives de violation des règles de sécurité devront donner lieu sur le champ à alerte et réaction : verrouillage de l'accès et démarches pour intercepter l'intrus.

- **Protéger** en chiffrant les données et programmes sensibles du système. Ceci est l'expression d'une stratégie de repli, qui suppose à juste titre qu'aucune politique de prévention aussi judicieuse soit-elle n'est totalement fiable. Par conséquent, il convient de limiter les dégâts si d'aventure un intrus parvenait malgré tout à s'introduire dans le système informatique. Ceci implique de transformer les données sous forme chiffrée, que seul celui qui connaît la clé de chiffrement peut déchiffrer. Les clés de chiffrement doivent elles-mêmes faire l'objet d'une protection particulière et être changées à une fréquence appropriée.

Les techniques de chiffrement sont appliquées de longue date pour préserver le secret des communications militaires ou diplomatiques. Elles doivent au terme de l'analyse des risques., chaque fois que c'est nécessaire après avoir aussi tenu compte des protections déjà en place, être appliquées pour tout fichier informatique considéré comme sensible.

7.4 L'intégration de la sécurité dans les applications informatiques

Les applications elles-mêmes doivent comporter les dispositifs de sécurité internes nécessaires (cryptage des informations critiques mémorisées sur le site, fonctions de contrôle d'intégrité et de niveau des services, alertes diverses en cas de détection de défaut de sécurité, etc.). Souvent, la bonne sécurisation dans les applications est plus efficace et permet des économies dans la configuration du réseau. C'est donc *dès la conception* de l'application qu'il faut définir les besoins de sécurité et envisager les mécanismes optimaux pour la sécurité de l'information et des processus.

Dans les applications, il faut, par exemple, identifier les transactions qui ont un caractère critique ou sont susceptibles d'être contestées. La mise en œuvre de mécanismes de *non-répudiation* permet alors de prouver la matérialité de la transaction (date, heure et contenu) et, le cas échéant, d'authentifier les expéditeur/destinataire du message et de tracer la transaction. En cas de litige, et sous certaines conditions légales, ces preuves devront pouvoir être produites en justice.

8. LA GESTION DES INCIDENTS DE SECURITE

8.1 La gestion de l'après-sinistre

La gestion de l'après-sinistre consiste à mener une série d'actions :

- investiguer l'incident (circonstances, technique utilisée, causes, auteur, dommages, …) ;
- prendre les actions permettant à l'organisation de continuer à assumer ses fonctions vitales dans les meilleurs délais après un sinistre (plan de survie) ;
- éventuellement, déposer plainte auprès des autorités judiciaires. Il existe dans tout le pays des COMPUTER CRIME UNITS de la Police Fédérale, qui disposent de spécialistes et d'experts qualifiés pour mener des investigations relatives aux systèmes d'information et de communication. Ces CCU sont coiffés par la cellule fédérale, à laquelle il est possible de s'adresser 24 heures sur 24 :

  FEDERAL COMPUTER CRIME UNIT (FCCU)
  Rue du Noyer, 211
  1000 BRUXELLES

  Tel. 02 / 743.73.84 (permanence 24/24 heures et 7/7 jours).

- conserver sous scellés les moyens de preuve et pièces à conviction. La collecte des preuves est l'affaire de spécialistes, disposant des outils *inforensiques* adéquats, permettant de faire des copies « fidèles » des preuves qui pourront être exploitées de manière incontestable en justice. Il n'est pas rare que

lorsqu'une entreprise licencie un membre de personnel pour faute grave, les informaticiens maison opèrent des recherches et contrôles sur le PC de cette personne. Ces actions, qui se déroulent après le licenciement, modifieront la date de dernier accès de nombreux fichiers. Il en résulte que les preuves seront à coup sûr et à juste titre contestées devant le Tribunal et risquent fort de devoir être écartées des débats.

- prendre les dispositions pour éviter la répétition de l'incident ;
- mener une campagne d'information pour minimiser l'impact de l'incident sur l'image de marque de l'entreprise ;
- réparer l'éventuel dommage causé aux tiers.

Dans la pratique, les crises résultant d'atteintes aux systèmes d'information peuvent être extrêmement complexes à gérer (p.ex. bug complexe inconnu). Plus le temps passe, plus l'impact d'un incident, d'un problème ou d'une crise générale grandira. Il en va ainsi comme de certains incendies, qu'un verre d'eau peut éteindre 10 secondes après le départ du feu, alors qu'un seau d'eau est nécessaire après 1 minute et que seuls les pompiers pourront maîtriser le feu après 5 ou 10 minutes.

Dans certains cas, la complexité d'une crise sera telle que l'entreprise sera sortie de la crise par différents moyens avant que le diagnostic final de la cause profonde de l'incident n'ait pu être établi. Comme l'entreprise ne peut attendre le résultat de ce diagnostic, elle devra gérer la crise avec d'autres armes que le processus automatisé existant et qui est défaillant.

L'entreprise peut tenter d'agir *préventivement* en réunissant, en cas de signes de crise probable, un comité de gestion préventive de crise. C'est la démarche qui lui coûtera le moins cher car elle lui donnera une chance d'éviter un sinistre.

Si les signes annonciateurs de crise ne sont pas perceptibles, il faut que le monitoring des systèmes et de la sécurité soit suffisamment élaboré pour déceler un *impact* et déclencher les alertes utiles qui permettront

i) de prendre des mesures conservatoires

ii) au management de réunir un comité de crise

iii) d'instaurer des relais sur le terrain

iv) de procéder au diagnostic de l'incident (de sa gravité d'abord et de ses causes ensuite), d'activer un plan de contournement (plan de contingence) et de gérer la crise dans la durée, opérations de retour à la normale incluses.

La démarche concrète de gestion de crise proposée ci-après fait appel à huit processus ou *savoirs* interactifs :

1. le savoir ***tactique et organisationnel*** (qui fait quoi quand ?) : c'est le rôle du chef de la cellule de crise. Le pilotage et la coordination opérationnelle sont les clés

les plus critiques pour sortir de la crise. Le pilote doit garder la main sur toutes les actions à décider.

2. le savoir ***schématique*** (qui est capable de schématiser le problème dans son ensemble ?). Concrètement, il faut faire appel aux personnes compétentes, les réunir autour de la table de crise, procéder « au tableau » à la schématisation fonctionnelle et technique de la crise, identifier ce qui fonctionne et ce qui ne fonctionne plus, évaluer les alternatives de contournement, établir le planning des tâches à réaliser sur la ligne du temps, etc. Ce schéma va considérablement aider le pilote-tacticien et les équipes d'intervention. C'est un outil indispensable trop souvent oublié pour définir les actions de crise à entreprendre.

3. le savoir ***d'expérience*** : faire appel aux personnes expérimentées fait gagner un temps considérable.

4. le savoir ***méthodologique*** (à tout niveau du processus de crise, appliquer la bonne méthode pour ne pas se tromper de chemin et sortir plus sûrement de la crise). La présente démarche en 8 points est déjà en soi une méthode et est inspirée de l'expérience de praticiens de la gestion des risques informatiques, mais aussi de celle provenant d'autres disciplines (ex : *Philippe Perrenoud - Université de Genève – Psychologie des sciences de l 'éducation)*

5. le savoir ***procédural***, qui suppose que les procédures essentielles de récupération de la situation soient accessibles en cas de sinistre.

Au cas où cela ne suffit pas et cela suffit rarement dans la réalité, être prêt à activer :

6. un savoir dit de ***recherche d'information*** (rechercher les pièces manquantes de la solution de réparation, de contournement, etc.) Certains seront plus créatifs que d'autres pour trouver l'information nécessaire.

7. un savoir ***heuristique*** : dans certains cas, la sortie d'une crise peut requérir un ensemble d'opérations itératives du type « essais et erreurs ».

8. un savoir de ***gestion d'exception*** : sortir de l'impasse d'un système complètement bloqué peut parfois être fait en s'écartant des standards, règles et procédures, en sacrifiant temporairement un flux dans un processus, etc.

Le rôle du chef de la cellule de crise (le « pilote ») sera donc d'arbitrer et d'activer tactiquement avec le plus grand discernement l'enchaînement de ces 8 savoirs.

Ces 8 savoirs sont autant de solutions possibles. Au plus leur combinaison est judicieuse, au plus vite l'entreprise sortira de la crise.

Lors d'un débriefing final, le pilote pourra identifier quel savoir aura été performant et quel autre aura été insuffisant. A cette occasion, il pourrait ainsi apparaître que le savoir procédural a montré des faiblesses comme une mise à jour insuffisante des procédures insuffisante, mais qu'heureusement le savoir d'expérience et/ou le savoir heuristique auront pu compenser ces manquements. Il devrait en résulter comme décision la nécessité d'améliorer dorénavant la qualité des procédures critiques de récupération.

Le pilote se rappellera que chaque décision tactique prise par la cellule de crise est un pas *nécessaire*, *urgent* et *parfois unique* pour sortir de la crise. Il devra donc veiller à sécuriser chaque opération décidée (p.ex. une erreur d'encodage peut aggraver la crise ou faire perdre des heures d'efforts à des équipes d'informaticiens qui commencent à fatiguer).

Inutile de préciser que ce pilote doit être préalablement préparé à la gestion de ces 8 savoirs.

8.2 La communication de crise

Pour qu'un incident endommage l'image de marque de l'organisation, il faut que d'une part, cet événement soit connu à l'extérieur et que d'autre part, cette information induise des réactions négatives auprès de ceux qui en prennent connaissance.

Tout dépendra donc de la manière dont l'entreprise informera son propre personnel, ses actionnaires, les autorités, les médias, les clients, les concurrents.

La manière, éventuellement tendancieuse, dont la presse informera le public ainsi que les confidences de «gens bien informés» peuvent représenter un risque considérable.

Un plan d'information des médias doit être disponible pour réagir, sans délai, si besoin en est, face à n'importe quel incident, permettant ainsi de contrôler les effets négatifs potentiels sur l'image de marque de l'organisation.

La preuve a été faite qu'un incident, a priori néfaste, pouvait être exploité et transformé en élément positif de publicité. C'est ainsi qu'un incendie détruisant complètement un centre de calcul d'un grand constructeur d'ordinateurs, fut mis à profit pour éditer une brochure illustrée sur les causes, le déroulement et les conséquences du sinistre, ainsi que sur des recommandations à usage des responsables de centres de calcul.

La communication de crise est un métier à part. Il est recommandé de faire appel à des agences spécialisées et des professionnels du domaine.

8.3 Le suivi des incidents

Tous les incidents informatiques doivent être signalés immédiatement, certains demandant une réaction immédiate. Les incidents relevés doivent faire l'objet d'une analyse ; le cas échéant, par un groupe de personnes désignées à cet effet, encore appelé CSIRT (Computer Security Incident Response Team).

Un rapport périodique doit être adressé à la direction générale, reprenant non seulement les aspects statistiques, mais aussi les recommandations nécessaires. Pour se conformer à la politique européenne en la matière, ces rapports d'incidents doivent être globalisés en interentreprises (CISRT sectoriels ou nationaux, souvent appelés

CERT – Computer Emergency Response Team[1]) pour qu'ensuite la globalisation nationale puisse contribuer valablement à une surveillance globale européenne.

9. LA POLITIQUE DE SECURITÉ

9.1 Les responsabilités du chef d'entreprise

Le chef d'entreprise doit, bien sûr, se préoccuper de la bonne sécurité informatique au même titre que les autres aspects qualité des activités de son entreprise.

Les entreprises et leurs activités sont de plus en plus dépendantes de leurs systèmes d'information. Les perturbations aux systèmes, quelles qu'elles soient, peuvent entraîner des impacts directs ou indirects importants, qui vont jusqu'à mettre en question leur survie. Pour répondre aux contraintes sociales, légales et économiques, qui reposent sur des textes européens (directives, recommandations, etc.) et sur la législation et la réglementation belges, les entreprises doivent protéger suffisamment mais raisonnablement leurs systèmes d'information contre toutes les menaces potentielles, qu'elles soient humaines ou techniques, internes ou externes, logiques ou physiques ou encore accidentelles ou malveillantes.

A noter également que les défaillances de sécurité informatique peuvent avoir des conséquences graves, tant pénales que civiles, et impliquer directement la responsabilité du chef d'entreprise. C'est notamment le cas lorsque les défauts de sécurité informatique entraînent des dommages à des tiers.

De par la personnalité juridique des organisations, le conseil d'administration et les directions générales sont responsables des conséquences directes ou indirectes d'un incident de sécurité informatique, telles que dommages à des tiers, divulgation d'informations confidentielles, responsabilité sociale, etc. Leurs rôles consistent principalement à :

- définir les objectifs de sécurité (identifier ce qui est confidentiel, définir les niveaux de disponibilité des services fournis aux tiers, etc.) ;
- concrétiser la politique de sécurité dans un document diffusé à toutes les personnes concernées (police de sécurité) ;
- instaurer l'organisation du support à la sécurité informatique ;
- arbitrer les risques à couvrir et assumer les risques acceptables ;
- fournir les moyens pour une sécurité suffisante (ressources financières, humaines et logistiques) ;
- approuver l'organisation de la sécurité et en faciliter le bon fonctionnement ;
- approuver et faire appliquer les procédures de sécurité ;

[1] CERT est un nom déposé par la Carnegie Mellon University

- vérifier périodiquement la bonne transmission des instructions et leur bonne mise en œuvre ;
- s'assurer de l'évolution des besoins et des mises à niveau des réponses correspondantes ;
- distribuer les rôles et responsabilités en matière de sécurité (inventaires des risques, études et développement, gestion générale et administration courante) en les affectant aux fonctions existantes dans l'organisation (utilisateurs des systèmes, informaticiens, responsables divers en matière de sécurité, ressources humaines, logistique interne, services techniques, production, etc.) ;
- inciter et faciliter l'acquisition et la maintenance des connaissances en sécurité, d'un niveau suffisant, selon les besoins propres à chacun.

Une sécurité informatique de niveau adéquat ne peut se concevoir sans que l'autorité suprême de l'entreprise ne s'implique dans les processus de sécurité et de gestion des risques.

9.2 La contribution du personnel à l'amélioration de la sécurité

La politique de sécurité est l'ensemble des dispositions que l'entreprise prend pour assurer la sécurité de ses systèmes informatiques, notamment en induisant les nécessaires modifications de comportement individuel.

Elle relève de la direction générale de l'entreprise et doit couvrir tous les départements, y compris le département informatique.

La sécurité informatique doit faire partie de la culture de l'entreprise, en s'inspirant par exemple de la recommandation de l'OCDE « *Lignes directrices de la sécurité informatique : Vers une culture de sécurité (2002)* ».

Chacun peut et doit contribuer à la sécurité informatique. La politique de sécurité et les procédures doivent être formalisées dans un ou plusieurs documents suffisamment diffusés. Ces documents (polices de sécurité) doivent induire le comportement individuel par une description adéquate des rôles et responsabilités, des droits et devoirs qui incombent à chacun. Afin de prouver la bonne information, on pourra exiger un accusé de réception du document de chaque membre du personnel. Pour toutes les données revêtant un caractère de confidentialité, il sera exigé un engagement individuel et explicite de confidentialité.

Tous les employés doivent être avertis de ce qu'une simple imprudence peut entraîner des conséquences majeures pour l'entreprise. La lecture inconsidérée d'une disquette ou d'un CD-ROM ou une connexion extérieure par modem, par exemple, peut introduire un virus qui va affecter le site Internet, par migration dans le réseau. Plus pernicieux que les virus, les « chevaux de Troie » sont de petits programmes qui désactivent certaines protections internes du réseau ou ajoutent des mots de passe de manière à ouvrir les portes pour une attaque majeure des systèmes par l'extérieur.

9.3 La politique de sécurité

Comme évoqué ci-dessus, la politique de sécurité va construire un cadre de comportement individuel. Elle est donc essentielle. La promulgation de cette politique est donc une des premières tâches de l'autorité de l'entreprise et doit se faire avec tout le soin nécessaire. La mise en œuvre de la politique commence par des activités de sensibilisation et doit se poursuivre de manière permanente, pour que chacun atteigne et conserve le niveau de connaissances suffisant. Ces connaissances couvrent les dangers, les impacts potentiels, les mesures de sécurité à maîtriser, avec les procédures correspondantes. La politique de sécurité relève de la direction générale de l'entreprise et couvre tous les départements, y compris le département informatique.

9.4 Un comportement de « bon père de famille »

La meilleure sécurité n'est pas atteinte par une pléthore de moyens techniques tels qu'antivirus, firewalls ou autres systèmes. Il existe un juste compromis entre les risques potentiels et les mesures de sécurité à prendre pour les éviter ou les réduire. Comme en matière d'assurances, il existe des risques qu'il est raisonnable de ne pas couvrir. La politique de sécurité informatique a donc aussi pour objectif de définir le niveau de sécurité raisonnable, en tenant compte notamment des impacts potentiels et des coûts nécessaires pour les éviter. Ce niveau de sécurité est à définir selon de multiples critères, notamment le contexte et les possibilités humaines, financières ou technologiques. Les critères à prendre en considération sont donc propres à chaque entreprise.

Cette politique de sécurité doit donc devenir la base de référence pour une gestion des risques informatiques en bon père de famille.

Les dispositions importantes de la politique de sécurité sont à reprendre dans le règlement de travail ou dans une convention collective d'entreprise à faire signer par chaque employé.

9.5 Une information adéquate

Les sources d'information sont nombreuses, mais pas toujours fiables. La recommandation de l'OCDE susmentionnée est certainement un document de base.

La FEB et les associations professionnelles publient des dossiers précisant certains aspects de la sécurité informatique.

Il existe des normes d'aide à la gestion de la sécurité. Trois normes ISO sont utiles pour les responsables d'entreprise :

- ISO 13335-1:2004: « *Le management de la sécurité des technologies de l'information et des communications* »
- ISO 17799-2005: « *Code de pratique pour la gestion de la sécurité d'information* »)

- ISO/IEC 27001:2005 *« Systèmes de gestion de sécurité de l'information - Exigences ».*

Utilisées avec discernement, ces normes peuvent déjà être d'une grande utilité dans la construction d'une politique de sécurité. Quelques autres normes analogues sont en préparation par l'ISO. Elles sont élaborées avec l'objectif premier d'être des outils d'aide pour les responsables d'entreprise et pour les personnes concernées par la politique de sécurité. Toutes les questions sur les normes peuvent être adressées à la NBN (Bureau de Normalisation), un service public ayant notamment cette mission dans ses attributions. Toutes les normes publiées peuvent être consultées sur place, gratuitement.

A noter que la plupart des normes de sécurité sont élaborées sur un plan international, sans tenir compte de la culture ou de la législation propre à chaque pays ou secteur d'activités. Les modalités d'application de ces normes ne peuvent en aucun cas justifier des infractions. La réglementation en vigueur reste d'application stricte, prioritairement par rapport aux modèles normatifs.

Le CLUSIB (Club de la sécurité informatique belge) organise, quant à lui, des séances d'information et publie des documents d'intérêt. L'objectif de cette association sans but lucratif, sous l'égide de la FEB et d'associations professionnelles, est d'aider les responsables d'entreprise dans leurs tâches relatives à la sécurité informatique.

10. QUELQUES THÈMES PARTICULIERS

10.1 La sécurisation des applications Internet

Si les applications sont externalisées, il y a lieu de s'assurer que le niveau de sécurité installé globalement par le fournisseur est suffisant. En tout état de cause, les informations, applications ou services mis sur le site sont à limiter aux stricts composants nécessaires.

Les applications elles-mêmes doivent comporter les dispositifs de sécurité internes nécessaires.

Si les applications sont hébergées sur des systèmes de l'entreprise :

- les réseaux doivent être segmentés selon les différents niveaux de sécurité. Les segments sont protégés les uns des autres par des dispositifs de sécurité (tels que ‘gateways’, ‘firewalls’, etc.) ;
- le site Internet proprement dit doit être isolé des autres réseaux par des dispositifs spécifiques (DMZ – Demilitarized Zone) ;
- les communications et accès transitant par des réseaux extérieurs (ou non sous contrôle) doivent être protégés de manière spécifique (ex.: VPN – Virtual Private Network et/ou utilisation d'un système de détection des intrusions IDS – Intrusion Detection System) ;

- la connexion d'un système interne protégé à un autre système du monde extérieur (p. ex. via un modem) ne peut se faire sans le respect de procédures précises ;
- la connexion de l'extérieur à un système interne (ex.: employé en voyage se connectant par téléphone ou par Internet) nécessite des protections spécifiques (système de « remote access control » exigeant, par exemple, une identification/authentification forte de l'appelant).

10.2 Le commerce électronique

Internet offre des opportunités exceptionnelles pour les entreprises d'informer le monde entier sur les produits et services qu'elles peuvent offrir et permettre de les acheter en ligne. Le « shopping » électronique offre un moyen facile aux entreprises et aux particuliers de rechercher les meilleures propositions.

La conclusion des transactions nécessite cependant qu'il soit satisfait aux conditions suivantes :

- les parties concluantes doivent pouvoir être **authentifiées** de manière sûre;
- il faut pouvoir vérifier **l'habilitation** des personnes à l'origine de la transaction;
- la **confidentialité** de la transaction doit être garantie;
- **l'intégrité** et la **non-altération** des messages doivent être assurées;
- **la non-répudiation à l'émission et à la réception** doit être certaine; un émetteur ne peut nier avoir émis un message; le récepteur ne peut nier l'avoir reçu; ceci fait généralement appel à une journalisation par un tiers de confiance, encore appelé notaire électronique.
- la continuité des flux et systèmes en ligne, qui s'appuient très souvent sur des prestations de Tiers. Le niveau de qualité à garantir sera défini par un Service Level Agreement.

10.3 La protection de la vie privée

La journalisation des opérations réalisées sur un système d'information, comprenant l'identification des utilisateurs, est souvent nécessaire pour l'imputation des transactions, dans des buts d'analyses historiques ou de recherche en cas de fraudes. À noter que l'enregistrement de ces données ayant un caractère personnel est soumis à des dispositions légales et réglementaires, telles que la loi sur la protection des données à caractère personnel du 8 décembre 1992, l'Arrêté Royal du 13 février 2001 ou la Convention collective de travail n°81 (ces textes sont disponibles sur le site de la Commission de la protection de la vie privée, www.privacycommission.be)

Les traitements des données à caractère personnel sont soumis à déclaration à la Commission. Les plaintes en matière de vie privée et les questions relatives à l'application de la loi du 8 décembre 1992 peuvent être adressées directement à la

Commission par mail ou par téléphone (service de première ligne : FR : 02/213.85.99; NL : 02/213.85.98).

11. QUELQUES RÉFLEXIONS EN GUISE DE CONCLUSION

Il n'est évidemment pas possible de donner dans un espace aussi limité un aperçu complet de toutes les techniques permettant de maîtriser efficacement les risques informatiques. Par ailleurs, au fur et à mesure que la technique évolue et que la nature des menaces change, les moyens de lutte doivent être adaptés.

Un bon niveau de sécurité informatique ne peut être atteint qu'au terme d'un programme pluridisciplinaire dans lequel agiront de concert la direction générale, les responsables de tous les départements de l'entreprise et l'ensemble du personnel. Les responsables de départements informatiques, juridiques et assurances seront particulièrement impliqués dans ce processus. Le recours aux services de consultants est fréquent dans ce domaine très spécialisé.

Si la mise en place d'un programme de maîtrise des risques informatiques peut faire l'objet d'un effort ponctuel, il est indispensable que ce programme fasse l'objet de révisions annuelles. Il faut demeurer flexible dans un environnement changeant.

Ce qui importe c'est la sécurité des systèmes d'information et des informations et non la sécurité informatique. Dès lors que les chefs d'entreprise délèguent aux techniciens les problèmes de sécurité, on risque de tomber dans la myopie technologique en perdant de vue les objectifs généraux de l'entreprise. La fiabilité de l'organisation informatique risque d'être considérée comme une fin en soi. Le danger est réel de vouloir se protéger contre des risques mineurs en ignorant parallèlement certains risques majeurs, non pas de l'informatique, mais de l'entreprise.

Un programme de sécurité entraînera des actions à une multitude de niveaux :

- éthique professionnelle ;
- ligne de conduite de la direction ;
- procédures administratives ;
- contrôle interne ;
- politique du personnel (au recrutement, pendant l'emploi et au départ) ;
- programmes d'audit ;
- contrôle de qualité des applications informatiques ;
- etc.

La sécurité n'est en fait qu'une des facettes de la qualité d'un système d'information, au même titre que la convivialité, la facilité de maintenance, l'efficacité, etc. C'est au tout premier stade du développement d'un projet informatique que les exigences en matière de sécurité doivent être identifiées et précisées, afin que la phase de conception permette d'imaginer une solution qui y réponde de manière adéquate. Il est souvent difficile voire même impossible de protéger a posteriori des systèmes où la sécurité n'a pas été prise en la conception. Le contrôle de la qualité, et donc de la sécurité, s'effectuera à tous les stades du développement : spécification des besoins, conception, réalisation, tests, réception, …

Si la sécurité impose de recourir à des moyens techniques, elle reste avant tout un problème humain. Sensibiliser, motiver, communiquer, former sont des tâches essentielles.

« *Faire passer le message* » de la sécurité est une des choses les plus difficiles qui soit. Voici quelques conseils utiles pour y parvenir :

- créer l'adhésion en optant pour la méthodologie exposée plus haut, qui requiert une très large participation de tous les responsables aux divers échelons de l'entreprise ;
- des priorités devront être fixées ; elles devront faire l'objet d'un large débat devant déboucher sur un consensus autour du programme retenu ;
- il importe de rechercher des appuis auprès de personnes déjà sensibilisées à la nécessité d'une bonne sécurité informatique ;
- les responsabilités doivent être clairement définies, à tous les niveaux ;
- l'exemple fait tache d'huile.

Dans chaque organisation, il faut quelqu'un qui prenne en charge la sécurité. Toutefois, seules les grandes organisations pourront se doter d'un ou plusieurs responsables affectés exclusivement à cette fonction.

Le responsable de la sécurité est avant tout aujourd'hui un **Risk Manager** qui doit être prêt à gérer les risques, sans nécessairement faire appel dans tous les cas à des mesures de sécurité.

Il doit donc pouvoir décrire des points d'arbitrage, les arbitrer s'il en a le mandat, et sinon organiser leur arbitrage. Il est a priori la référence et le recours pour chacun dans l'entreprise et doit se former en permanence à ses processus pour les comprendre et en analyser les risques avec plus de pertinence.

L'entreprise étant friande de projets nouveaux lui permettant de se développer, de s'adapter ou de se reconstituer progressivement et différemment, le responsable de sécurité se doit d'être présent au sein de chaque projet informatique et de faire en sorte de produire le livrable « risques et sécurité » de chaque projet avec la collaboration de toutes les personnes concernées. Au travers de chaque projet sécurisé adéquatement, l'entreprise acquiert aussi, sinon une culture, du moins de sains réflexes de gestion de ses risques IT et de ses responsabilités en matière de sécurité.

Le responsable de la sécurité a une tâche importante, lourde et souvent ingrate :

- il doit sortir de sa tour d'ivoire et être présent sur le terrain, en relation directe avec les utilisateurs ;
- il a des tâches administratives (recommandations, lignes de conduite, normes de sécurité, ..) ; toutefois, l'objectif n'est pas de produire du papier ;
- il doit respecter dans ses actions un équilibre entre le court et le moyen terme ;
- il doit agir de manière réaliste ;

- il doit faire ce qui peut être réalisé et ne pas tenter de remonter à contre-courant ;
- il doit se concentrer sur ses résultats et non sur ses efforts ;
- il ne doit pas espérer tout savoir et ne doit pas hésiter à avoir recours à des spécialistes internes ou externes ;
- il se méfiera des check-lists lorsqu'il procède à des audits ; si on ne se fie qu'à elles, on risque de négliger des aspects nouveaux ou fondamentaux. Elles ne sont utiles qu'après avoir procédé à un exercice de réflexion personnel et critique ;
- il ne tombera pas dans le syndrome de la ligne Maginot. Il ne sert à rien de mettre sur pied des défenses coûteuses qui peuvent facilement être contournées par ailleurs ;
- il ne s'imaginera surtout pas qu'il existe une sécurité absolue (syndrome du Titanic, considéré comme insubmersible avant son voyage d'essai) ;
- il aura l'intelligence de considérer que l'ennemi contre lequel il se bat est plus intelligent que lui ;
- enfin, à tout moment, il se souviendra de ce que ceux qui n'apprennent pas de l'histoire sont condamnés à la revivre.

* * * * * * * * * * * * * * * * * *