

La Modélisation du Risque

**Présentation générale
du modèle d'analyse de risque
et de sa métrique**

INTRODUCTION

L'analyse de risque est un processus souvent mis en œuvre par le Responsable de la Sécurité des Systèmes d'Information.

Ce processus s'appuie sur trois éléments :

- Une démarche de management.
- Un modèle de risque.
- Une métrique des risques.

La démarche proprement dite est décrite dans divers documents disponibles sur le site de 2SI et dans des documents du Clusif (Club de la sécurité des systèmes d'information français).

Nous décrivons ici, sur un plan relativement théorique, le modèle de risque et sa métrique.

Une description plus approfondie et plus détaillée du modèle et de sa métrique se trouve dans la bibliothèque du site de 2SI, sous le nom de l'ouvrage initialement paru aux *Editions d'Organisation* : "*Le Risque Informatique*"

Des présentations plus pragmatiques sont également disponibles dans la partie bibliothèque du site (Mehari : Les outils du management de la sécurité et Mehari et le management de la sécurité).

LA MODÉLISATION DU RISQUE

La mise en évidence des paramètres caractéristiques des risques qui permettront de les évaluer au mieux ensuite, s'appuie sur une modélisation générale du risque.

Un risque peut être vu comme le déroulement d'un scénario.

Les paramètres caractéristiques dépendent des phases de ce scénario et nous allons donc tout d'abord décrire ces différentes phases.

Phases d'un sinistre

Le déroulement chronologique typique d'un scénario de risque est le suivant :

- L'entreprise possède un certain nombre de moyens ou de biens, matériels ou immatériels, que nous appellerons ses ressources ou actifs. Ces ressources représentent pour l'entreprise des enjeux et peuvent être la cible d'agressions diverses de la part d'agresseurs qui peuvent être des événements naturels ou des êtres humains, agissant volontairement ou non.

On peut les répartir en plusieurs types : les biens matériels, les supports d'informations, de données et de programmes, les programmes, les informations et données, enfin le personnel. La valeur des ressources comporte deux éléments : la **valeur intrinsèque**, que l'on pourra estimer par son coût de remplacement, et la **valeur d'usage**, dont la mesure prendra en compte les coûts engendrés par son indisponibilité, son altération, sa divulgation ou son détournement.

- Nous appelons **menace** une agression potentielle qui ne s'est pas manifestée, toute action possible d'une personne ou tout événement potentiel susceptible de conduire à un changement non souhaité d'une ressource du système d'information, quel que soit son type. Tant que l'agression ne s'est pas concrétisée, tant qu'aucune action n'a été entreprise ou qu'aucun événement déclencheur n'est intervenu, la menace restera potentielle. Toute entreprise est ainsi soumise à un ensemble de menaces potentielles.
- Le passage à l'action, c'est-à-dire la mise à exécution de la menace, se concrétisera par une **agression**, qui peut comporter deux étapes :
 - Une première étape où la source de l'agression, l'auteur, humain ou non, progresse jusqu'à la ressource sans dégradation, sans détérioration.
 - Une deuxième étape où il y a effectivement changement, détérioration, dans la constitution ou l'état d'une ressource du système d'information.

Les finalités défensives concernant ces deux étapes sont nettement différentes : pendant la première étape d'agression, on cherchera à stopper l'agression ou à l'empêcher, à la prévenir, alors que, pendant l'étape suivante qui correspond à des détériorations de ressources, l'on s'attachera à restreindre l'ampleur du sinistre, à en limiter les conséquences.

Une agression peut être caractérisée par son *type* et par les *vulnérabilités exploitées*.

- Les conséquences de l'agression sont des **détériorations** des ressources - au sens de changement d'état de ces dernières - subies par l'entreprise; elles sont provoquées pendant la deuxième étape de l'agression.

Les détériorations peuvent être caractérisées par deux paramètres ou attributs, le *type* et l'*évolutivité*

- L'agression qui était la cause des détériorations a pu être détectée ou non, les

détériorations le seront inévitablement à un moment ou à un autre, ce qui donnera lieu à une réaction, automatisée ou non, de la part du système et plus généralement de l'entreprise. Une cellule de crise, par exemple, pourra être créée pour prendre les meilleures décisions en fonction de la situation constatée et, d'abord, stopper la progression des détériorations.

- Les détériorations de ressources vont entraîner des dysfonctionnements de l'entreprise, plus ou moins importants. Il s'agit donc des conséquences ressenties non plus au niveau du système d'information mais à celui de l'entreprise elle-même.
- Quelles que soient les détériorations estimées ou constatées, une fois l'évolution du sinistre stoppée, on doit entrer dans une phase de *reconfiguration* : il s'agit des mesures destinées à assurer la continuation de l'activité, et à minimiser les dysfonctionnements. Par exemple il est encore possible, en cas de destruction partielle du matériel, d'utiliser le matériel restant pour traiter les applications les plus prioritaires, c'est le mode de fonctionnement dégradé, ou, en cas de destruction totale, de transférer les traitements sur un système de secours.
- L'arrêt ou la suppression des dysfonctionnements sont obtenus par la *restauration* des ressources ayant subi des dommages, ce qui permet de revenir à un état stable, proche de l'état normal initial, suivant le niveau de performance retrouvé. Il peut s'agir de la correction d'une erreur sur une donnée ou dans un logiciel, ou la reconstruction d'un centre de traitement, opération beaucoup plus longue. Enfin, il est des cas où la réparation s'étend sur une très longue période, comme par exemple après la divulgation à des concurrents de données commerciales confidentielles, dont le cycle de vie s'étend sur plusieurs années.
- Les dysfonctionnements et les frais de réparation ou de restauration se traduisent par des pertes pour l'entreprise qui toutefois ne seront évaluées qu'après une dernière étape constituée par la récupération éventuelle d'une partie des pertes auprès de l'assurance ou par recours à une action judiciaire contre les tiers responsables du sinistre.

Globalement, nous présenterons le déroulement d'un scénario de risque comme la concrétisation d'une menace se traduisant par une agression des ressources de l'entreprise, entraînant leur détérioration, ce qui provoque des dysfonctionnements occasionnant des pertes. Nous appellerons *modèle de scénario de risque* le modèle relationnel représenté figure 1.

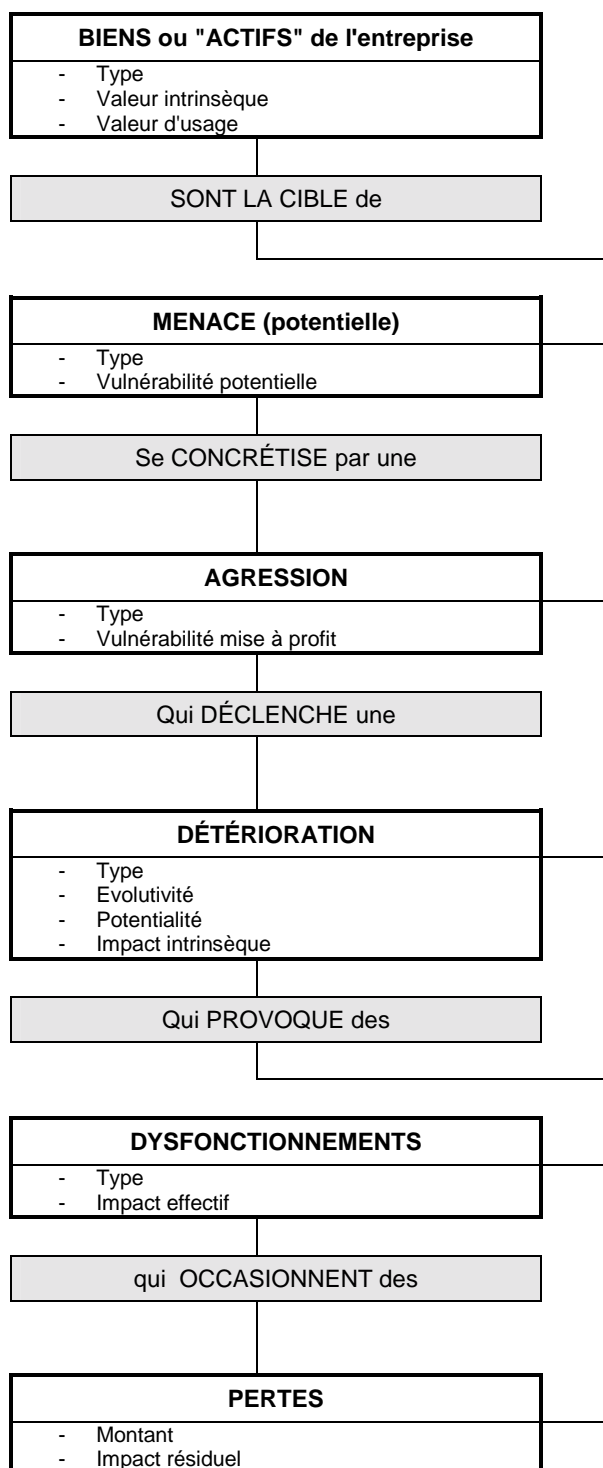


Figure 1

Mesures de sécurité

A chaque phase du sinistre, des mesures de sécurité peuvent avoir une influence sur son déroulement et vont donc aider à caractériser le risque.

En considérant les éléments conceptuels du modèle relationnel précédent comme des niveaux, nous organiserons les mesures de sécurité en niveaux parallèles, chaque niveau représentant une classe de mesures, comme indiqué sur la figure 2.

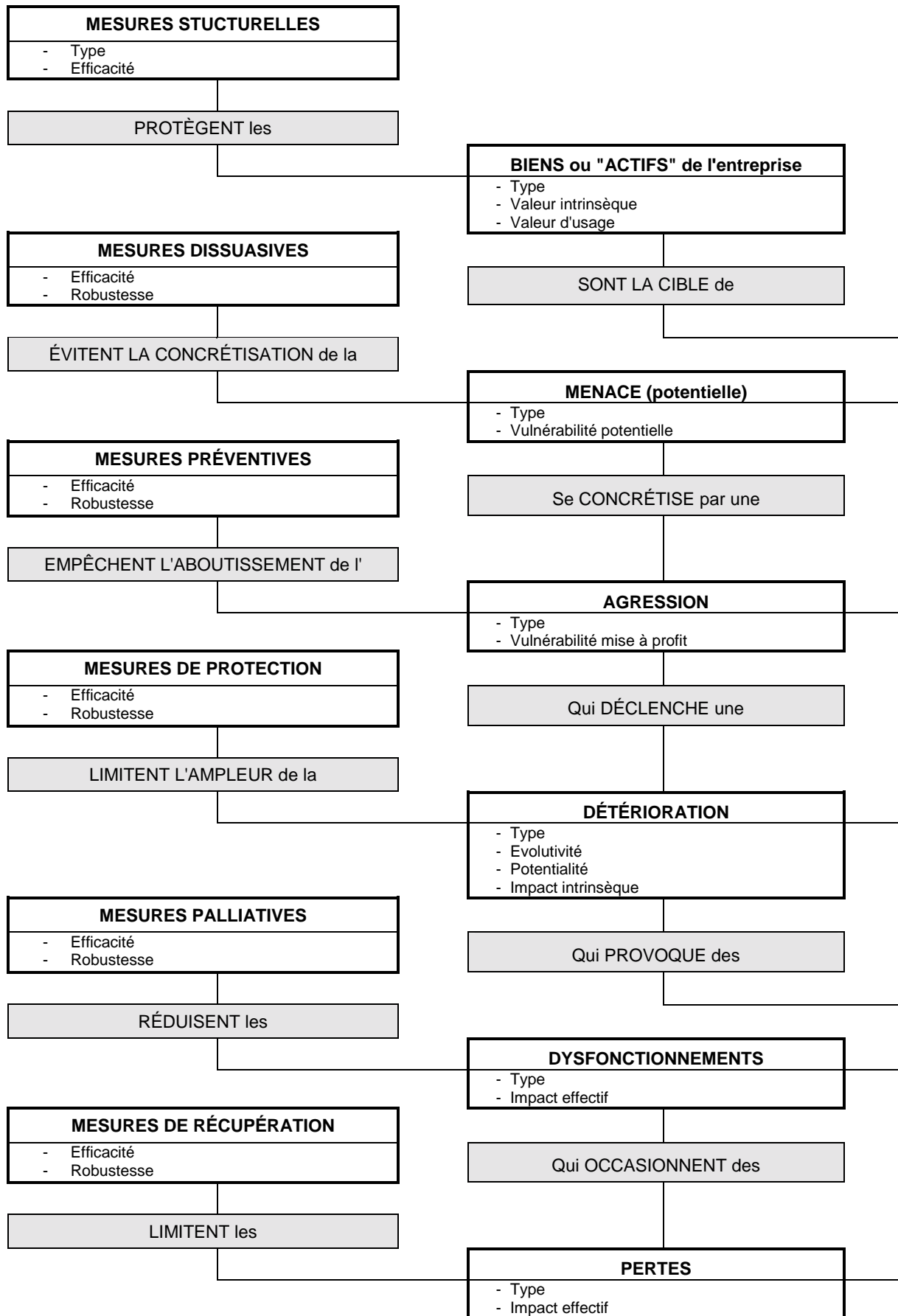


Figure 2

Ce découpage permet un regroupement des mesures en six grandes familles :

- Les **mesures structurelles** qui jouent sur la structure même du système d'information, pour éviter certaines agressions ou en limiter la gravité ; on distingue la *fragmentation* de l'information, qui permet de limiter l'impact de l'agression à un fragment plutôt qu'à la totalité de l'information, l'occultation des ressources, par exemple cacher l'existence ou la localisation d'un site informatique, la *réduction de la valeur* des ressources, par exemple en n'autorisant le transfert automatique de fonds - sans procédure d'autorisation spéciale - que dans le cas de sommes limitées, et les *mesures structurelles d'organisation*, qui regroupent ce que l'on pourrait appeler les mesures positives de motivation.
- Les **mesures dissuasives** qui permettent, dans le cas d'agresseurs humains, d'éviter qu'ils mettent à exécution la menace potentielle en déclenchant l'agression. Il s'agit essentiellement d'augmenter le risque que prendrait l'agresseur s'il lui prenait envie de tenter sa chance. Ce risque est lié à deux facteurs, d'une part le risque d'être découvert : ce risque est accru par la mise en place de moyens de *détection* et de *trace* suffisamment complets et précis pour pouvoir remonter jusqu'à l'agresseur et l'identifier sans ambiguïté, d'autre part l'ampleur des *sanctions encourues*.
- Les **mesures préventives** : celles qui permettent d'empêcher les détériorations ou d'éviter qu'une agression n'atteigne des ressources du système d'information ; elles incluent des mesures de *barrage*, par exemple clôture ou blindage, les *contrôle d'accès*, qui autorisent l'accès de manière sélective, la *détection-interception*, qui arrête directement l'agression avant qu'elle ne provoque un sinistre et le *masquage de l'information* qui est une technique utilisée pour assurer la confidentialité de données lors de leur stockage ou de leur transport, en particulier par chiffrement ou cryptage.
- Les **mesures de protection** qui, sans empêcher les détériorations, permettent tout au moins d'en limiter l'ampleur. On distingue surtout la chaîne *détection-réaction* qui comprend une phase de *détection* suivie d'une phase de *réaction* permettant de limiter les détériorations, les mesures *anti-propagation* qui empêche l'agression de se propager à d'autres ressources que les premières atteintes et la *certification des données et programmes* basée soit sur des redondances ponctuelles soit sur des processus de contrôle d'intégrité.
- Les **mesures palliatives** qui agissent une fois les détériorations accomplies, et qui permettent, d'une part d'en limiter les conséquences au niveau de l'entreprise, d'autre part de restaurer les ressources détériorées pour retrouver l'état initial. On distingue les mesures atténuant les dysfonctionnements et celles ayant pour objet la restauration des ressources détériorées. Les premières sont constituées de différentes sortes de *reconfiguration*, dynamiques (redondances, clusterisation) ou statiques (secours) ; les secondes sont constituées de *réparation*, de *correction* et de *reconstruction*.
- Les **mesures de récupération** qui visent à récupérer une partie du préjudice subi par *transfert des pertes sur des tiers*, par le biais des *assurances* ou de dommages et intérêts consécutifs à des *actions en justice*, dans le cas d'agresseurs humains.

Modélisation et caractérisation d'un risque

Modéliser et caractériser un risque consiste ainsi, d'une part à décrire précisément les différentes phases du scénario de risque et leurs paramètres caractéristiques, d'autre part à identifier les mesures de sécurité effectivement en place susceptibles d'avoir une influence sur ces paramètres, en s'appuyant sur la décomposition générique des mesures efficaces à chaque phase du scénario.

L'ÉVALUATION DU RISQUE

Globalement, pour évaluer quantitativement un risque, il est bien clair que la gravité des conséquences du sinistre est tout à fait essentielle. C'est ce que nous appellerons l'« *impact* » du sinistre.

L'impact, cependant, ne peut suffire à décrire un scénario.

On sent bien, intuitivement, que certains risques peuvent être considérés comme courants, d'autres comme exceptionnels, et qu'entre les deux il n'y a pas de discontinuité. On sent également qu'il est naturel, à impact équivalent, d'attacher une plus grande priorité aux risques courants qu'à ceux qui sont exceptionnels.

Il nous faut donc un paramètre pour décrire ce côté plus ou moins plausible, pour ne pas dire probable, du sinistre éventuel. C'est ce que nous appellerons la « *potentialité* ».

Ces deux paramètres, potentialité et impact, sont caractéristiques de phases différentes dans le scénario de sinistre.

Tant que l'action de l'agression n'a pas été jusqu'à un début d'impact, c'est-à-dire tant que nous sommes dans la première partie de la phase d'agression, on peut parler de potentialité. Ceci ne veut pas dire que l'action n'ait pas commencé, mais que les détériorations ne sont pas déclenchées, elles restent potentielles et peut-être est-il encore possible de les empêcher.

Une fois que les détériorations ont commencé, on est entré dans une phase où il ne s'agit plus de potentialité mais de réalité, de gravité des conséquences du sinistre.

En résumé, en adoptant une approche par scénario, nous avons vu apparaître :

- Une première phase du scénario, constituée par l'agression, sur laquelle nous reviendrons, qui comprend à la fois une source ou un sujet déclenchant, humain ou non, des vulnérabilités exploitées ou voies d'accès, et des ressources atteintes, donc le « *qui* », le « *quoi* », et le « *comment* ». Nous caractériserons cette phase, du point de vue de la sécurité, par un paramètre de « *potentialité* ». Ce paramètre de potentialité, que nous définirons en détail, vise à quantifier la possibilité, la plausibilité, que ce scénario concerne l'entreprise.
- Une deuxième phase du scénario, constituée de la fin de l'agression et des actions menées alors par l'entreprise, qui dépend en grande partie de l'entreprise et des moyens qu'elle met en œuvre. Nous caractériserons cette deuxième phase du scénario, dégradation et recouvrement, par un paramètre d'« *impact* » du scénario sur l'entreprise. Ce paramètre d'impact vise à quantifier la gravité du dommage subi par l'entreprise, dommage qui résulte de l'agression.

Les deux paramètres du scénario de sinistre, l'impact et la potentialité, sont représentatifs du risque de l'entreprise face à la menace correspondante.

La potentialité et les facteurs de risques correspondants

La potentialité d'un risque sera vue comme une caractéristique non mathématique permettant de différencier des risques ou des scénarios de risques en fonction de leur vraisemblance pour l'entreprise, de leur possibilité de réalisation, de leur pertinence, de leur plausibilité. L'intérêt d'une approche méthodologique de la potentialité est de remplacer l'intuition globale par un raisonnement analytique de facteurs de risque. Ces facteurs de risques qui vont permettre l'évaluation de la potentialité sont les suivants.

L'exposition naturelle

Ce facteur vise à mettre en évidence, quand il s'agit d'une agression humaine, que le risque est d'autant plus fort que le scénario de sinistre représente un *enjeu* pour l'agresseur, et qu'en fonction de cet enjeu, l'entreprise représente une *cible* particulière. Il s'agit bien de la plus ou moins grande exposition de l'entreprise à ce type de risque.

Pour les scénarios de sinistres qui ne mettent pas en jeu une volonté humaine, l'exposition naturelle correspond aux conditions qui rendent plus ou moins potentielle la naissance d'un événement qui va conduire au sinistre.

L'impunité de l'agresseur

Pour les agressions volontaires, le deuxième facteur à prendre en compte est celui des risques pris par l'agresseur.

En effet, ayant eu l'idée d'une agression, la question que va se poser l'agresseur avant d'arrêter sa décision est d'analyser les risques personnels qu'il va devoir prendre.

Plus grand est le risque pris par l'agresseur et moins est potentiel le scénario de sinistre.

L'impunité de l'agresseur est caractérisée à la fois par *l'imputabilité*, c'est-à-dire par les possibilités de remonter jusqu'à l'auteur d'une action suite à sa détection, par les *sanctions*, c'est-à-dire par les conséquences qui peuvent en découler pour l'auteur lui-même et par la *perception* qu'il a lui-même de ces deux premiers éléments, perception qui est nécessaire à l'effet de dissuasion.

La trivialité des conditions de survenance

Le stade ultérieur pour un acte volontaire, une fois la décision de passer à l'action prise, est celui de la réalisation et de la propagation de l'agression depuis sa conception jusqu'au moment où elle va effectivement toucher l'entreprise, c'est-à-dire détériorer des ressources.

Il s'agit donc, pour ces actes volontaires, de leur faisabilité, c'est à dire des conditions dans lesquelles l'agresseur va pouvoir accéder à ce qui va devenir la cible du sinistre. Ce sont donc les possibilités d'atteintes non autorisées ou non prévues des ressources qu'il faut analyser à ce niveau.

La trivialité des conditions de survenance dépend de trois paramètres : la « *capacité requise* » qui qualifie le fait que l'agresseur doit être « *capable* » de mener à bien le scénario d'agression, les « *moyens requis* » qui recouvrent toutes les ressources qui devront être mobilisées pour arriver au déroulement du scénario. Il peut s'agir de moyens matériels, de moyens financiers, mais aussi de temps et le « *hasard* », certains scénarios mettant en cause un facteur « *chance* ».

Pour les scénarios ne faisant pas intervenir une action humaine déterminée, la trivialité des conditions de survenance est un facteur caractérisant à la fois l'ampleur du phénomène, par exemple l'ampleur d'un incendie, l'ampleur d'une crue ou d'une inondation, un taux d'erreur, etc. et la banalité des concours de circonstances qui peuvent faire aboutir le scénario.

Évaluation de la potentialité

L'analyse des facteurs de risque permet, dans un premier temps d'évaluer chacun de ces facteurs sur une échelle simple à quatre niveaux (faible, moyen, fort, très fort).

Ces évaluations directes, à la fois intuitives et réfléchies, permettent de se faire une première idée des conditions de réalisation du risque.

Dans un deuxième temps, à la lumière de ces évaluations, on portera un jugement sur le niveau résultant de la potentialité.

Des grilles de décision, établies par un comité d'analyse avec l'appui de personnes ayant l'expérience de ce type d'évaluation, permettent d'aider au jugement global sur le niveau de la potentialité du risque, en se basant sur les évaluations des facteurs de risque. Ces grilles sont aussi une garantie de stabilité et de cohérence des décisions.

L'impact et les facteurs de risques correspondants

Les conséquences sur l'entreprise d'un scénario de sinistre sont mesurées par son impact.

Il s'agit de l'impact sur l'entreprise des détériorations et des dysfonctionnements que ces dernières ont engendrés.

En effet, l'impact d'un scénario de sinistre est double : il faudra restaurer les ressources de l'entreprise détériorées et il faudra, en attendant cette restauration, subir les conséquences des dysfonctionnements engendrés par les détériorations.

La valeur intrinsèque des ressources et leur classification

Dans de nombreuses entreprises, une classification des informations a été effectuée et, si ce n'est déjà le cas, elle devra l'être un jour.

Une telle classification reflète la valeur intrinsèque des ressources, c'est-à-dire l'impact maximum d'une perte de disponibilité, d'intégrité ou de confidentialité, en l'absence de toute mesure de sécurité.

C'est évidemment le point de départ de l'évaluation de l'impact effectif d'un scénario de risque, compte tenu des mesures de sécurité mises en place.

L'évaluation de cet impact effectif sera faite en se basant sur des facteurs de risques spécifiques qui sont décrits ci-après.

L'expansibilité des détériorations

Ce facteur met en évidence qu'une détérioration initiale limitée peut se propager plus ou moins rapidement et qu'en fonction de cette possibilité voir de cette propension à s'étendre, l'impact sera d'autant plus sévère.

Il peut tout aussi bien s'agir de phénomènes naturels, l'incendie par exemple, que de propagation d'erreurs ou de contamination de fichiers.

L'impréparation de la situation de crise

Ce facteur vise à qualifier le fait qu'un manque de préparation à une situation de crise augmentera les conséquences directes et indirectes des détériorations.

Cela est le cas pour la restauration des ressources atteintes : mieux on se sera préparé à cette éventualité, plus vite on pourra le faire et moins graves en seront les conséquences.

En ce qui concerne les dysfonctionnements induits, ce facteur met en exergue que plus la réaction sera improvisée et plus graves et plus durables seront les dysfonctionnements au niveau de l'entreprise.

L'impréparation du recours sur des tiers

Ce facteur vise à qualifier le fait qu'en l'absence de possibilités de recours sur des tiers, par le biais d'assurances ou de poursuites pénales, l'entreprise subira seule l'intégralité des conséquences du scénario de risque, si celui-ci se matérialise.

Evaluation de l'impact

L'analyse des facteurs de risque ci-dessus permet, dans un premier temps d'évaluer chacun de ces facteurs sur une échelle simple à quatre niveaux (faible, moyen, fort, très fort). Ces évaluations directes, à la fois intuitives et réfléchies, permettent de se faire une première idée des conséquences du risque.

Dans un deuxième temps, à la lumière de ces évaluations, on portera un jugement sur le niveau résultant de l'impact.

Des grilles de décision, établies par un comité d'analyse avec l'appui de personnes ayant l'expérience de ce type d'évaluation, permettent d'aider au jugement global sur le niveau d'impact du risque, en se basant sur les évaluations des facteurs de risque. Ces grilles sont aussi une garantie de stabilité et de cohérence des décisions.

Facteurs de risque et effets des mesures de sécurité

Il y a un parallèle évident entre les facteurs de risques évoqués ci-dessus et la typologie des mesures de sécurité présentée plus haut dans le modèle de risque.

En fait, chaque facteur de risque reflète directement l'absence de mesures de sécurité correspondant à cette phase du scénario de risque.

Les mesures de sécurité auront donc un effet direct, selon leurs types, sur les facteurs de risques correspondants.

Gravité du risque

Partant des évaluations de la potentialité et de l'impact du risque, on pourra établir une évaluation globale du risque.

Pour ce faire, on peut préparer un cadre servant de support à la prise de décision, en remplissant un tableau qui indique le niveau d'« *acceptabilité du risque* » d'un scénario caractérisé par sa potentialité et son impact.

On définit ainsi une gravité résultante du scénario de risque, sur 4 niveaux : le niveau 4 est souvent défini comme intolérable et réclamant des actions très urgentes, le niveau 3 comme étant inadmissible mais les actions correspondantes pouvant être planifiées sur une certaine période, le niveau 2 étant tolérable et le niveau 1 étant considéré comme insignifiant.

Une telle grille peut aussi servir de support à la définition d'objectifs de sécurité et son élaboration doit être faite à haut niveau et a valeur d'orientation stratégique.

Nous donnons ci-dessous, à titre d'exemple, une grille de décision montrant une certaine dissymétrie pour manifester la volonté de l'entreprise de s'occuper prioritairement des sinistres extrêmement graves, c'est à dire pouvant entraîner la mort de l'entreprise, même si la potentialité d'un tel sinistre est faible.

GRAVITÉ DU RISQUE				
IMPACT	POTENTIALITÉ			
	Insignifiante	Faible	Moyenne	Très forte
Extrêmement grave	3	4	4	4
Très grave	2	3	3	4
Moyennement grave	1	1	2	2
Peu grave	1	1	1	1

Table d'acceptabilité des risques ou de définition d'objectifs de sécurité