

LE RISQUE INFORMATIQUE

AVANT PROPOS

Le Risque Informatique a été publié, à l'origine, en 1992.

Cette nouvelle version tient compte de l'expérience de mise en pratique du modèle de risque qui est exposé et des formations à la méthode Mehari que j'ai eu l'occasion de faire.

Par rapport à la version d'origine, le fond n'a pratiquement pas évolué, seuls quelques aménagements ont été apportés, pour une meilleure compréhension du modèle, d'une part, et pour que certains aspects de la métrique de risque restent homogènes avec les options prises par le Clusif¹ dans la méthode Mehari qui s'appuie sur ledit modèle.

Par ailleurs, la dernière partie de livre d'origine, qui traitait de la réduction du risque, n'a pas été reprise, la méthode Mehari traitant cet aspect de manière beaucoup plus approfondie.

Les deux premières parties du livre avaient été écrites par *Albert Harari* et moi-même. Je tiens à rendre encore hommage ici à Albert pour sa collaboration dans l'élaboration de ce modèle de risque et de sa métrique.

Jean-Philippe Jouas

¹ Club de la Sécurité des Systèmes d'Information Français

SOMMAIRE

Première partie LA MODÉLISATION DU RISQUE.....	9
INTRODUCTION	10
Chapitre 1 CARACTÉRISTIQUES D'UN MODÈLE DE RISQUE	11
I. PRÉSENTATION GÉNÉRALE.....	11
II. LE CHAMP DU MODÈLE DE SÉCURITÉ PROPOSÉ	13
RELATION ENTRE QUALITÉ, SÉCURITÉ ET PERFORMANCE	13
Qualité - rôle économique prévisible	13
Sécurité - accident ou risque imprévisible	14
Qualité et sécurité	14
III. OBJECTIF DÉCISIONNEL DU MODÈLE.....	15
Niveau stratégique ou schéma directeur	15
Niveau plan opérationnel	15
Niveau mise en œuvre et déploiement de solutions	16
Chapitre 2 LE SCÉNARIO DE SINISTRE	17
I. CHRONOLOGIE TYPE D'UN SINISTRE.....	17
II. LES RESSOURCES DU SYSTÈME D'INFORMATION	21
DÉFINITION.....	21
LES TYPES DE RESSOURCES.....	21
Les biens matériels.....	21
Les supports de données ou de programmes.....	22
Les processus et programmes	22
Les données et les informations	22
Le personnel.....	23
LA VALEUR DES RESSOURCES	23
La valeur intrinsèque des ressources.....	23
La valeur d'usage	23
III. LES MENACES ET LES AGRESSIONS	24
DÉFINITIONS	24
LES TYPES D'AGRESSION	24
Agressions physiques dues à des origines naturelles	25
Agressions physiques dues à l'environnement industriel	25
Agressions physiques d'origine accidentelle	25
Agressions logiques d'origines accidentelles	26
Les malveillances.....	26
Crises ou conflits origines de sinistres	26
LES VULNÉRABILITÉS	27
Les voies d'accès logiques	27
Les voies d'accès physiques	28
IV. LES DÉTÉRIORATIONS DE RESSOURCES.....	28
LES TYPES DE DÉTÉRIORATIONS.....	28
La compromission d'informations sensibles.....	29
Informations altérées ou faussées.....	29
Perte de disponibilité du service	30
L'ÉVOLUTIVITÉ.....	30
Les détériorations ponctuelles.....	30
Les détériorations évolutives	31
Les détériorations répétitives	31
V. LES DYSFONCTIONNEMENTS DE L'ENTREPRISE	31
TYPES DE DYSFONCTIONNEMENTS	31
Les dysfonctionnements opérationnels	31

Les dysfonctionnements intangibles	32
VI. LES PERTES	32
LES PERTES DIRECTES LIÉES AUX DÉTÉRIORATIONS	32
LES PERTES INDIRECTES ENGENDRÉES PAR LES DYSFONCTIONNEMENTS	33
LES PERTES TOTALES	33
Les pertes résiduelles	33
Chapitre 3 LES MESURES DE SÉCURITÉ	35
I. LES MESURES STRUCTURELLES	37
La fragmentation de l'information.....	37
L'occultation des ressources.....	38
La réduction de la valeur des ressources.....	38
Les mesures structurelles d'organisation.....	38
II. LES MESURES DISSUASIVES.....	39
III. LES MESURES PRÉVENTIVES	39
Le barrage	40
Les contrôles d'accès.....	40
La détection-interception	40
Le masquage des informations.....	41
IV. LES MESURES DE PROTECTION	41
La détection-réaction	41
Les mesures anti-propagation	42
La certification des données et programmes	42
V. LES MESURES PALLIATIVES.....	43
LES MESURES ATTÉNUANT LES DYSFONCTIONNEMENTS	43
La reconfiguration.....	43
LES MESURES DE RESTAURATION DES RESSOURCES DÉTÉRIORÉES	44
La réparation	45
La correction	45
La reconstruction	45
VI. LES MESURES DE RÉCUPÉRATION	45
Le transfert du risque sur des tiers	45
L'action en justice	46
Deuxième partie L'ÉVALUATION DU RISQUE.....	47
INTRODUCTION	48
Chapitre 4 LA POTENTIALITÉ	51
I. INTRODUCTION	51
II. LES NIVEAUX DE POTENTIALITÉ.....	53
Potentialité forte.....	53
Potentialité moyenne.....	54
Potentialité faible	54
Potentialité insignifiante	54
III. LA POTENTIALITÉ ET LES FACTEURS DE RISQUE	55
L'EXPOSITION NATURELLE	58
L'enjeu.....	58
Le ciblage.....	58
NIVEAUX D'EXPOSITION NATURELLE	59
Exposition naturelle forte.....	59
Exposition naturelle moyenne.....	59
Exposition naturelle faible	60
Exposition naturelle très faible ou réduite	60
L'IMPUNITÉ DE L'AGRESSEUR.....	60
L'imputabilité de l'action à son auteur.....	61
Les sanctions et conséquences de la découverte de l'action.....	61
NIVEAUX D'IMPUNITÉ DE L'AGRESSEUR	61
Impunité très forte (ou risque insignifiant)	61
Impunité moyenne (ou risque moyen)	62
Impunité faible (ou risque fort)	62
Impunité insignifiante (risque très fort)	63
LA TRIVIALITÉ DES CONDITIONS DE SURVENANCE	63

La capacité (requis).....	63
Les moyens (à mettre en œuvre).....	64
Le hasard.....	64
NIVEAUX DE TRIVIALITÉ DES CONDITIONS DE SURVENANCE.....	65
Forte trivialité des conditions de survenance (ou conditions de survenance standard).....	65
Trivialité moyenne des conditions de survenance (ou conditions de survenance non standard).....	65
Faible trivialité des conditions de survenance (ou conditions de survenance rares).....	66
Très faible trivialité des conditions de survenance (ou conditions de survenance exceptionnelles).....	66
IV. LA POTENTIALITÉ ET LES PROFILS D'AGRESSEURS.....	66
V. ÉVALUATION DE LA POTENTIALITÉ.....	67
Chapitre 5 L'IMPACT.....	69
I. L'IMPACT DES DÉTÉRIORATIONS ET DES DYSFONCTIONNEMENTS.....	69
QUELQUES NOTIONS INSTINCTIVES.....	69
UN NOMBRE LIMITÉ DE NIVEAUX DE GRAVITÉ.....	70
LA RELATIVITÉ DE L'ÉVALUATION DE L'IMPACT.....	71
II. NIVEAUX D'IMPACT.....	71
Impact extrêmement grave.....	72
Impact très grave.....	72
Impact moyennement grave.....	72
Impact peu grave.....	72
III. IMPACT INTRINSÈQUE ET IMPACT EFFECTIF D'UN SCÉNARIO DE SINISTRE.....	73
IV. L'IMPACT EFFECTIF ET LES FACTEURS DE RISQUE.....	74
L'EXPANSIBILITÉ DES DÉTÉRIORATIONS.....	75
La propagation du sinistre à d'autres ressources.....	75
Le renouvellement ou la répétition des détériorations.....	75
NIVEAUX D'EXPANSIBILITÉ.....	76
Expansibilité forte.....	76
Expansibilité moyenne.....	76
Expansibilité faible.....	76
Expansibilité insignifiante.....	77
L'IMPRÉPARATION DE LA SITUATION DE CRISE.....	77
La capacité de restauration des ressources.....	77
La capacité de reconfiguration.....	78
NIVEAUX D'IMPRÉPARATION DE LA SITUATION DE CRISE.....	78
Impréparation forte.....	78
Impréparation moyenne.....	78
Impréparation faible.....	79
Impréparation insignifiante.....	79
L'IMPRÉPARATION DU RECOURS SUR DES TIERS.....	79
Les assurances.....	79
Les actions en justice.....	79
NIVEAUX D'IMPRÉPARATION DU RECOURS SUR DES TIERS.....	80
Impréparation forte.....	80
Impréparation moyenne.....	80
Impréparation faible.....	80
Impréparation insignifiante.....	80
V. IMPACT ET CLASSIFICATION DES INFORMATIONS.....	81
V. ÉVALUATION DE L'IMPACT.....	81
Chapitre 6 EFFETS DES MESURES DE SÉCURITÉ.....	83
I. EFFICACITÉ DES MESURES DE SÉCURITÉ.....	83
EFFICACITÉ DES MESURES DISSUASIVES OU PRÉVENTIVES.....	84
EFFICACITÉ DES MESURES DE PROTECTION, PALLIATIVES.....	85
OU DE RÉCUPÉRATION.....	85
II. ROBUSTESSE DES MESURES.....	85
III. EFFETS DES SERVICES DE SÉCURITÉ.....	87
IV. EFFETS DU CUMUL DE SERVICES.....	88
Chapitre 7 LES CATÉGORIES D'AGRESSEURS.....	89
I. LES FILIÈRES D'AGRESSEURS.....	90
LE PERSONNEL ET LES PERSONNES ASSIMILÉES.....	90

Les utilisateurs accrédités	90
Les opérateurs accrédités	91
Les non accrédités	91
LES AGRESSEURS EXTERNES.....	91
Les pirates	92
Les malfaiteurs.....	92
Les espions.....	92
LES PHÉNOMÈNES NATURELS.....	92
II. LES NIVEAUX D'AGRESSEURS	93
NIVEAU STANDARD	93
NIVEAU MOYEN	94
NIVEAU IMPORTANT	94
NIVEAU TRÈS IMPORTANT	95
III. NIVEAUX D'AGRESSEURS ET TRIVIALITÉ DES CONDITIONS DE SURVENANCE.....	95
Chapitre 8 LE MODÈLE DE RISQUE.....	97
I. ÉVALUATION DU RISQUE	97
DISSYMÉTRIE DES ESTIMATIONS	97
DISSYMÉTRIE DES POIDS DES FACTEURS	98
II. L'AVERSION AU RISQUE	98

Première partie

LA MODÉLISATION DU RISQUE

INTRODUCTION

L'importance du système d'information pour l'entreprise, l'aspect stratégique de certaines de ses composantes et la complexité du problème de sa sécurité ne sont plus à démontrer.

Devant un ensemble complexe, l'approche scientifique a toujours été de découper cet ensemble en sous-ensembles plus simples à analyser et de procéder ainsi de proche en proche jusqu'à ce que l'objet isolé puisse être facilement compris, caractérisé.

Il est clair qu'à chaque étape de ce processus on opère une simplification, certains diront une réduction, dans les liaisons entre les sous-ensembles. On s'attache aux caractères principaux et on rejette les autres. C'est souvent à ce prix que l'on peut progresser, gagnant en clarté et compréhension ce que l'on perd en précision.

La vue synthétique à laquelle on aboutit par ce mode d'analyse est ce que nous appelons un « *modèle* ».

Le résultat auquel on parvient est une certaine vue de la réalité, ce que certains peuvent appeler une grille de lecture, qui est sans doute tronquée, mais qui permet une action plus efficace dans un domaine donné, si le modèle a été judicieusement élaboré.

Ce que nous allons aborder, dans cette première partie, est un modèle adapté à la gestion des risques liés aux systèmes d'information de l'entreprise.

Chapitre 1

CARACTÉRISTIQUES D'UN MODÈLE DE RISQUE

Telle que nous l'avons présentée, la modélisation se rapproche d'une technique d'analyse par décomposition, et revient à isoler certains éléments que l'on caractérisera par des propriétés spécifiques.

Nous allons, dans ce chapitre, présenter plus en détails certains aspects de la modélisation, en donner un exemple dans un domaine connexe à celui de la sécurité des systèmes d'information, et délimiter le champ d'un modèle adapté à notre sujet.

I. PRÉSENTATION GÉNÉRALE

Imaginons le scénario suivant :

Une association interprofessionnelle, comme il en existe tant, est reçue par l'un de ses membres, et, au cours de la visite traditionnelle, l'hôte ne manque pas de vanter les mérites du système d'information de son entreprise.

Les visiteurs assistent ainsi à une démonstration d'élaboration automatique de proposition commerciale par connexion à un serveur qui, sur la base des références et nombres d'articles et de prestations proposées, détermine les délais de livraison, les prix de référence, les concessions commerciales, etc.

Parmi les visiteurs, un concurrent regarde avec beaucoup d'attention cette démonstration et remarque que pour accéder au serveur, il suffit d'un mot de passe. Non seulement il le remarque, mais il note le nom sous lequel s'est identifié le démonstrateur, DEMO, et le mot de passe, 12345.

Rentré chez lui, il se connecte au serveur, constate qu'il a accès à un menu lui permettant également de modifier les éléments de référence, en particulier les délais et les prix de référence et en profite pour effectivement les augmenter.

Durant les mois qui viennent la société qui avait organisé la visite, perd des marchés, ses propositions étant jugées inacceptables.

Comment qualifier et résumer ce type de scénario ?

Selon les points de vue adoptés, nous pourrions avoir les réponses suivantes :

- C'est une altération de données (c'est-à-dire une perte d'intégrité). Cette typologie simple est celle que pourrait fournir un responsable de la classification des données en fonction de leur sensibilité selon trois critères, sur lesquels nous reviendrons, qui sont la confidentialité, l'intégrité et la disponibilité.
- C'est une altération malveillante de données. La qualification de malveillance ajoute une notion supplémentaire qui peut être utile, par exemple si une assurance couvre le risque de malveillance ou si on peut espérer se retourner contre l'agresseur.
- C'est une attaque logique. Ce genre de qualification reflète plutôt le point de vue de ceux qui veulent établir des statistiques ou des tendances de la sinistralité selon ses origines.
- C'est une erreur dans la spécification de l'application, qui n'aurait jamais dû rendre possible la modification distante des paramètres de référence, mais exiger une procédure très stricte pour ces mises à jour, par exemple depuis un poste physiquement déterminé, avec un double contrôle, etc. C'est le point de vue du « *propriétaire des informations* » qui, n'ignorant pas que le système d'information de l'entreprise est aussi utilisé pour son effet vitrine, se préoccupe de ce qui a pu lui échapper : la manière dont l'application a été spécifiée.
- C'est une erreur d'organisation de la circulation des personnes qui a permis qu'un visiteur découvre le mot de passe et le moyen d'accéder aux données sensibles.
- C'est un manque de robustesse du système de contrôle d'accès qui était inadapté à l'environnement d'un poste de travail : celui du démonstrateur. Ce point de vue est peut-être celui du responsable de la sécurité qui se dit que si le moyen de contrôle d'accès avait été une carte à microprocesseur, aucun visiteur n'aurait pu ainsi accéder aux données.

De tout ceci, il ressort que les points de vue sont variés et qu'ils sont, pour beaucoup, liés à une préoccupation particulière.

Dans cet exemple, purement fictif, les jugements variaient en fonction des objectifs des intervenants et de leurs activités qui se situaient à plusieurs niveaux :

- au niveau de l'organisation des visites : éviter qu'un visiteur puisse voir le mot de passe,
- au niveau du contrôle d'accès au système,
- au niveau de l'application : éviter qu'il soit possible de modifier une donnée de référence sans contrôle sérieux de la personne effectuant la mise à jour,
- au niveau des contrôles de sécurité de l'application, vérifications de cohérence, double contrôle, etc.

Un modèle utile à tous ces différents aspects nécessite que chacun puisse y trouver les concepts nécessaires à l'expression de son point de vue.

Une décomposition suffisamment fine en éléments discrets est donc nécessaire pour qu'un modèle soit pertinent. Ces éléments doivent, en outre, être adaptés aux types d'actions que l'on souhaite engager et de décisions que l'on souhaite prendre.

Un modèle et les concepts qu'il contient doivent donc être adaptés à un objectif.

II. LE CHAMP DU MODÈLE DE SÉCURITÉ PROPOSÉ

Avant d'aborder les éléments qui devraient figurer dans un modèle adapté à la sécurité des systèmes d'information, il convient d'en délimiter le champ, c'est-à-dire d'être clair sur la limite et la nature du problème à résoudre. En particulier, la ligne de partage entre le domaine de la qualité et celui de la sécurité mérite d'être nettement précisée.

RELATION ENTRE QUALITÉ, SÉCURITÉ ET PERFORMANCE

Il existe une relation certaine entre ces trois entités :

- on peut dire que la sécurité est un élément de la qualité, un produit non sûr et non fiable ne pouvant prétendre à un label de qualité,
- on peut dire que la qualité, à l'inverse, fait partie de la sécurité, un système ne pouvant être sûr de fonctionnement si la qualité de ses éléments est mauvaise,
- enfin les performances d'un système comme d'une entreprise varient dans le même sens que la qualité de leurs produits, et sont d'autant meilleures que leur fonctionnement n'est pas susceptible d'être entaché d'insécurité.

Notre propos ici n'est pas de lancer un débat théorique sur cette question, mais d'essayer d'éclairer le rôle de ces facteurs, et surtout d'en tirer une règle de conduite pratique pour la suite, en particulier, savoir à partir de quel point et jusqu'où on peut aller dans notre démarche de gestion des risques.

Qualité - rôle économique prévisible

La qualité d'un produit, d'un système ou d'un service est mesurée par son degré de conformité à ses spécifications, en supposant que lesdites spécifications sont elles-mêmes conformes aux besoins exprimés par les commanditaires, maîtres d'ouvrage et utilisateurs finaux. Les déviations possibles à cette conformité sont considérées comme courantes ou récurrentes et sont gérées par la « *fonction qualité* ». Deux éléments interviennent dans la qualité d'un produit, ce terme étant pris au sens large et pouvant, tout aussi bien, désigner un service :

- la qualité au niveau même du cycle de production et des divers processus qui interviennent dans l'élaboration de ce qui a été spécifié. Une phrase illustre bien les objectifs assortis à ce point de vue de la qualité : « *faire bien du premier coup* ». L'attitude moderne de la « *qualité totale* » est, en effet, d'anticiper, autant que faire se peut, les défauts de qualité pour pouvoir les éviter ou les traiter le plus en amont possible.
- la qualité du produit final obtenu, qui dépend non seulement du processus de production, mais encore du taux de contrôle, c'est-à-dire de l'effort consenti pour éviter que le client final ait à découvrir lui-même le défaut.

Dans notre domaine, si on prend pour exemple le cas du logiciel qui est un élément central dans l'analyse de la sécurité d'un système informatique, on distinguera les deux éléments suivants :

- la qualité au niveau du processus de développement, telle qu'elle peut être apportée, par exemple, par la mise en œuvre d'outils de génie logiciel,

- le contrôle de la qualité du logiciel, qui se fait a posteriori et met en œuvre des tests et des outils de métrologie. Il va de soi que ces contrôles ont une limite, en particulier économique, et qu'on ne pourra garantir par contrat qu'aucune erreur ne s'est glissée lors du développement. Ainsi les procédures de contrôle qualité et de recette du produit font-elles souvent partie des spécifications.

Le niveau de qualité, comme les déficiences potentielles du produit, sont ainsi des éléments prévisibles.

La qualité joue donc essentiellement un rôle économique : un produit de haute qualité non seulement se vendra mieux, mais les divers coûts de la non-qualité, retour au fabricant, réparation, échange, seront minimisés. A contrario, et toujours en gardant notre exemple précédent, il est souvent moins coûteux de tolérer quelques erreurs résiduelles dans un logiciel, qui sont passées au travers du tamis de l'assurance qualité, que de passer au peigne fin les programmes, instruction après instruction, pour diminuer encore le taux d'erreur. La seule question qui demeure sera de savoir si une erreur oubliée ne risque pas, dans un certain contexte, d'avoir des conséquences graves.

Sécurité - accident ou risque imprévisible

Par opposition à la non-qualité courante, une faille de sécurité entraîne un sinistre ressenti comme une rupture par rapport à un état antérieur, comme l'occurrence d'un événement ou d'un accident plus ou moins imprévisible, tout au moins quant à l'instant où il se produit, et dont les conséquences seront, elles, bien tangibles.

Entrent dans cette catégorie les catastrophes naturelles, les accidents ou concours de circonstances malheureux, les erreurs et les malveillances. La sécurité dans cette approche est la gestion des accidents-ruptures imprévisibles.

La question que l'on se pose est donc de savoir si on peut se limiter, dans l'analyse des risques de l'entreprise, aux failles de sécurité, sans se préoccuper des aspects liés à la qualité.

Qualité et sécurité

Si les problèmes liés à la qualité sont pris en compte, on peut se demander où et quand on pourra et on devra s'arrêter : qualité du personnel, qualité des cahiers des charges, qualité des spécifications, du choix des matériels et des techniques de programmation, qualité des bâtiments, qualité de l'organisation, et qualité du management. On risque ainsi de remettre en cause toute la structure et l'organisation de l'entreprise, dans le cadre d'une analyse des risques des systèmes d'information.

En réalité, tous ces éléments concourent effectivement à la plus ou moins grande sécurité des systèmes d'information et de l'entreprise elle-même. Ainsi à quel moment l'inexactitude, le caractère incomplet, la non-qualité d'une donnée est-elle une faille d'intégrité ? Dans la pratique, il faudra souvent se limiter à la détermination de problèmes potentiels de non-qualité bien identifiables quant à leurs conséquences concrètes dans le déclenchement d'un sinistre, surtout si les conséquences de ce sinistre sont potentiellement graves, ce qui est, en définitive, la rupture redoutée par rapport à un état antérieur. L'exemple typique est encore celui du logiciel intervenant dans des processus critiques, et dont on ne pourra faire l'économie de l'analyse de sa qualité.

D'autre part, on ne peut se dispenser d'apporter des améliorations progressives à la qualité dans tous ses aspects, notamment organisationnels, les faiblesses de l'organisation étant souvent la source implicite et invisible de ruptures flagrantes ; ce processus permet d'asseoir

la sécurité sur des fondations solides.

Cependant, la définition, la mise en place et le fonctionnement courant d'un système d'information qui réponde aux besoins de l'entreprise n'entrent pas, en général, dans les attributions de la fonction sécurité. De même, l'organisation des fonctions de l'entreprise, qui est souvent liée à celle des systèmes d'information, et le bon fonctionnement de l'entreprise au quotidien, ne sont pas du ressort de la fonction sécurité.

Nous considérons que la gestion de la sécurité est celle des ruptures potentielles dans le fonctionnement de l'entreprise, provoquées par des phénomènes naturels, par des accidents, par des erreurs d'utilisation ou de manipulation de données ou de ressources physiques, ou, enfin, par des malveillances, conduisant à ce qu'il est coutume d'appeler un « *sinistre* ».

Voilà ce que doit permettre d'analyser le modèle que nous proposons.

III. OBJECTIF DÉCISIONNEL DU MODÈLE

Dans le domaine de la gestion de la sécurité, plusieurs types d'objectifs peuvent être visés. Nous en décrivons brièvement trois, qui peuvent se définir comme trois niveaux de préoccupation non exclusifs, étant entendu que bien des variantes sont possibles.

Niveau stratégique ou schéma directeur

A ce niveau, l'objectif est double :

- sensibiliser la Direction de l'entreprise,
- définir un plan stratégique, c'est-à-dire la démarche de sécurité qui sera retenue par l'entreprise et l'organisation correspondante, les objectifs de sécurité justifiés par rapport à la stratégie de l'entreprise et la méthode de pilotage de la sécurité. Des études détaillées sont nécessaires, après cette étape, avant de pouvoir passer à une phase de mise en œuvre de solutions.

En termes de cible, une telle démarche s'adresse essentiellement à une Direction Générale.

En termes d'usage, une telle analyse est une action préliminaire d'orientation et de cadrage, voire de réorientation, et constitue un fondement stable qui n'est remis en question qu'en fonction des évolutions de l'entreprise.

Niveau plan opérationnel

A ce niveau, les objectifs sont de :

- définir les spécifications fonctionnelles des solutions de sécurité à mettre en œuvre, adaptées au contexte propre de l'entreprise et de ses diverses entités, c'est-à-dire avoir un support de décision quant au niveau des mesures à prendre,
- consolider ces analyses détaillées pour bâtir un schéma d'ensemble cohérent,
- justifier la nécessité de ces mesures auprès des utilisateurs.

Les cibles visées sont bien davantage le responsable de la sécurité des systèmes d'information (RSSI) et les responsables locaux d'entités autonomes, qui sont déjà convaincus

du besoin, mais qui demandent un outil d'aide à la décision. Cette aide leur est fournie par la modélisation fine des phénomènes intervenant dans la sécurité et par la proposition de « *services de sécurité* » adaptés à ces phénomènes. Ils souhaitent avoir, en outre, un outil capable d'effectuer une synthèse pour bâtir un plan opérationnel, annuel ou pluriannuel. Ils souhaitent souvent, enfin, que cet outil puisse leur servir à des fins didactiques, pour sensibiliser les utilisateurs, les faire adhérer aux objectifs et leur faire accepter les contraintes.

En termes d'usage, il s'agit donc d'une utilisation du modèle, de la méthode et des outils associés qui peut être permanente, pour l'analyse détaillée de risques particuliers, ou occasionnelle, pour la synthèse et l'élaboration du plan opérationnel.

Niveau mise en œuvre et déploiement de solutions

A ce niveau, l'objectif est de :

- déterminer les solutions à mettre en œuvre. Il s'agit d'une extrapolation du point de vue précédent, la seule différence, mais de taille, étant le niveau de détail des solutions proposées par la méthode. Au lieu de proposer des services, des mécanismes de solutions sont décrits et offerts,
- former les responsables locaux de sécurité et les opérationnels chargés de la mise en œuvre.

Si la cible est encore la responsable de la sécurité des systèmes d'information, elle s'étend aux opérationnels (service informatique, services généraux, audit, assurance, utilisateurs, etc.), en outre, l'objectif est légèrement différent, puisqu'il est aussi de former ces responsables. Cette autoformation leur est apportée par un niveau de détails très fin, tant dans la description des problèmes potentiels que des solutions éventuelles.

*

* *

Le modèle que nous visons recouvre les trois objectifs. Si les principes sont communs, ils seront déclinés, en pratique, de façon adaptée aux trois cibles différentes mais en assurant la nécessaire cohérence d'ensemble.

S'il est, en effet, possible d'appréhender les cibles par des méthodes différentes, la communication des résultats de l'une à l'autre ne se révèle pas aisée si l'ensemble n'a pas été structuré avec cet objectif.

Ayant précisé les objectifs, nous pouvons déjà en tirer quelques conclusions valables à tous les niveaux :

- pour pouvoir être un outil pédagogique, il est nécessaire que les risques soient présentés sous forme de scénarios facilement compréhensibles,
- pour être un outil d'aide à la décision, il convient d'associer une « *métrique* » du risque à chaque scénario.

C'est sur ces bases que le modèle de sécurité que nous allons maintenant présenter a été bâti.

Chapitre 2

LE SCÉNARIO DE SINISTRE

Nous allons maintenant présenter le scénario de sinistre comme une ossature générale sur laquelle vont s'articuler différentes vues que l'on peut avoir du problème sécuritaire et de ses solutions.

De manière générale, qu'un sinistre soit dû à une agression explicite ou qu'il soit le résultat d'une faiblesse associée à la non-qualité de tel ou tel élément d'un système, à la matérialisation de tel ou tel problème, le résultat concret à retenir est la rupture par rapport à un état antérieur considéré comme normal ou stable.

L'histoire d'un sinistre peut être décomposée en un certain nombre de phases caractéristiques, s'enchaînant l'une après l'autre. Par exemple, la chute de la foudre va déclencher un incendie qui va se propager, puis cet incendie sera éteint, puis le centre sera reconstruit, avant que l'activité ne puisse être reprise.

Nous appellerons « *scénario de sinistre* » l'ensemble de ces phases et étapes du déroulement d'un sinistre potentiel.

Nous commencerons par faire une description générale de ce scénario en fonction de sa chronologie, avant de le décrire par un modèle relationnel mettant en association différents types d'entités que nous serons donc amenés à définir et à décrire en détail.

I. CHRONOLOGIE TYPE D'UN SINISTRE

Décrivons d'abord le déroulement chronologique typique d'un tel scénario :

L'entreprise possède un certain nombre de moyens ou de biens, matériels ou immatériels, que nous appellerons ses ressources ou actifs (en anglais *assets*). 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.

— 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, il s'agit d'une menace qui reste potentielle. L'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* ».

L'agression, peut être immédiate, comme le vol d'un fichier, ou se dérouler en plusieurs étapes, comme l'écoute, par un pirate, du protocole de connexion d'un utilisateur sur des lignes de télécommunication afin de découvrir son mot de passe, suivie d'une connexion avec usurpation d'identité pour, finalement accéder à des données sensibles et les dérober.

L'agression a pour cible les ressources de l'entreprise.

- Les conditions locales favorables à la mise à exécution de la menace et à la réussite de l'agression constituent les « *vulnérabilités* » de l'entreprise vis-à-vis de ces dernières. Ces conditions dépendent de la perméabilité du système d'information vis-à-vis de l'agression et, plus généralement, des conditions d'accès aux différentes ressources qui lui sont liées.
- Les conséquences de l'agression sont des « *détériorations* » des ressources qui sont subies par l'entreprise.

Ces détériorations peuvent être progressives, comme dans tous les processus à caractère évolutif, par exemple dans le cas de l'incendie ou de la propagation d'une erreur, ou se répéter, comme par exemple l'intrusion dans un système d'information de la part d'un concurrent qui a obtenu un mot de passe et qui en profite pour détourner des informations confidentielles, de manière répétitive et régulière tant qu'on ne l'a pas découvert ou tant que le mot de passe n'a pas été modifié.

Pour ce qui concerne le risque informatique, ces détériorations sont subies, in fine, au niveau de son système d'information : perte de confidentialité et compromission d'informations sensibles, perte d'intégrité par l'altération d'informations sensibles, perte de disponibilité de ressources se traduisant par l'indisponibilité des traitements et des données. L'ampleur des détériorations sera, éventuellement, fonction de la rapidité de détection de l'agression et de l'efficacité de la réaction qui s'ensuit pour la confiner d'abord, et ensuite aboutir à son arrêt ; dans l'exemple du feu, détection du début d'incendie et déclenchement rapide de l'extinction.

- 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* » de la part de l'entreprise. Une cellule de crise pourra être créée pour prendre les meilleures décisions en fonction de la situation constatée et, d'abord, stopper la progression des détériorations.

Les détériorations du système d'information peuvent entraîner des dysfonctionnements de l'entreprise plus ou moins importants, par exemple perte de compétitivité ou mauvaises prises de décisions de la Direction Générale.

Les conséquences de ces dysfonctionnements ont un impact et un coût généralement plus élevé que ceux des détériorations directes.

- Quelles que soient les détériorations estimées ou constatées, une fois le sinistre arrêté, 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. Un autre cas de reconfiguration est la réorganisation d'un service pour améliorer la compétitivité de l'entreprise affaiblie par la divulgation d'informations alarmantes sur ses produits. Certains dysfonctionnements peuvent

s'arrêter d'eux-mêmes, au bout d'un certain temps, c'est en particulier le cas des effets de la divulgation d'informations confidentielles qui s'atténuent progressivement avec l'obsolescence croissante de ces informations. Dans le cas général, il faut réagir pour corriger ces dysfonctionnements, c'est-à-dire que plus tôt on aura estimé leur ampleur, meilleure sera la réaction.

- L'arrêt ou la suppression des dysfonctionnements, donc la limitation des dégâts, 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 restauration se traduisent tôt ou tard 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. On parlera alors de « *pertes résiduelles* ».

Globalement, nous présenterons le scénario de sinistre comme la concrétisation d'une menace se traduisant par une agression des ressources de l'entreprise, entraînant des détériorations du système d'information, ce qui provoque des dysfonctionnements occasionnant des pertes.

Nous appellerons modèle de scénario de sinistre le modèle relationnel représenté figure 1.

Nous verrons au chapitre 3 qu'à chacun de ces concepts correspondent des mesures de sécurité de nature spécifique qu'il importe de savoir choisir et de mettre en œuvre de manière appropriée.

Nous allons maintenant revenir sur les différentes notions ou « *entités* » présentées dans ce modèle, en donner des définitions et en décrire les principaux aspects.

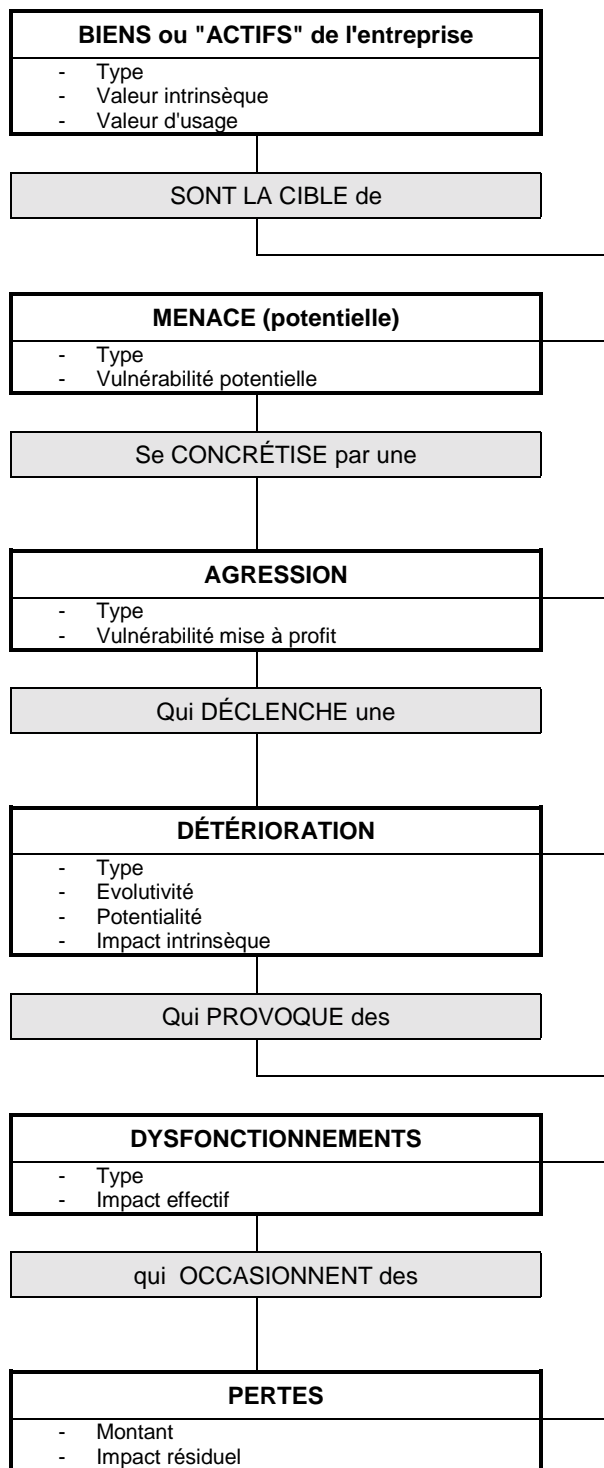


Figure 1

II. LES RESSOURCES DU SYSTÈME D'INFORMATION

Ce sont elles qui sont la cible des menaces potentielles, qui seront donc éventuellement celles de l'agression et qui pourront subir des détériorations.

En tant qu'entité, nous décrirons les ressources de l'entreprise tout en notant qu'au cours d'un même scénario de sinistre plusieurs ressources, de plusieurs types, peuvent être atteintes. Un programme, par exemple, peut être une cible primaire atteinte par un employé indélicat, et ce programme peut, à son tour, dégrader d'autres ressources, programmes ou données, qui constituent des cibles secondaires.

DÉFINITION

Les ressources que nous considérons sont tous les moyens, de quelque nature que ce soit, qui assurent ou qui participent à la saisie, au traitement, au stockage, à la diffusion et à la transmission des informations au sein de l'entreprise.

Une ressource peut être caractérisée par deux « *attributs* » : son type et sa valeur.

LES TYPES DE RESSOURCES

D'une manière générale, on peut répartir les ressources en plusieurs types :

- les biens matériels,
- les supports de données, d'informations ou de programmes,
- les processus ou programmes,
- les données et les informations,
- le personnel,

Les biens matériels

Il s'agit, bien sûr, des bâtiments et locaux informatiques ainsi que des équipements informatiques, mais aussi, plus généralement, de toute ressource matérielle nécessaire au fonctionnement du système d'information.

Nous distinguerons :

- les bâtiments et locaux abritant les équipements informatiques et les servitudes diverses liées aux bâtiments et locaux,
- les équipements informatiques et leurs périphériques,
- la climatisation et les dispositifs annexes associés,
- l'alimentation en énergie, en particulier alimentation électrique, avec son câblage et les équipements associés, transformateurs, disjoncteurs, etc.,
- l'infrastructure des télécommunications, qui comprend les autocommutateurs, les têtes de lignes P.T.T., les répartiteurs et sous-répartiteurs, les armoires et boîtes de raccordement, les commutateurs et routeurs ainsi que les gardes-barrières, les modems et, enfin, les supports de transmissions, câbles et équipements.

Les supports de données ou de programmes

Les supports de données ou de programmes peuvent être des supports permanents, temporaires ou fugitifs. Nous distinguerons :

- les supports papier : listings, formulaires de saisie, correspondance, etc.,
- la documentation : documentation des logiciels, documentation d'exploitation, etc.,
- les supports amovibles : bandes magnétiques, disquettes, cartouches de streamer, disques amovibles, CD-ROM, disques optiques numériques, etc.,
- les micro-ordinateurs ou stations de travail dans lesquels ont été stockées des informations : ils seront ici considérés comme supports d'information et non comme moyens de traitement, notamment quand ils possèdent un disque dur fixe,
- les écrans de terminaux, micro-ordinateurs ou stations,
- les ondes électromagnétiques véhiculant de l'information : ces ondes peuvent être émises volontairement, c'est le cas des faisceaux hertziens, ou involontairement, c'est celui de la compromission par rayonnement ou par conduction.

Les processus et programmes

Sont considérés ici tous les processus de traitement de l'information, qu'ils soient automatisés ou non. Ils seront souvent des cibles primaires mises à contribution par des agresseurs humains dans le but d'attaquer une autre cible, en général des données. Ils comprennent :

- les logiciels de base : systèmes d'exploitation, utilitaires et bibliothèques-systèmes, etc., tant des systèmes centraux que des stations de travail,
- les logiciels associés aux équipements de télécommunication : logiciels des machines spécifiques assurant le routage des télécommunications, logiciels des autocommutateurs, logiciels des gardes-barrières, etc.,
- les logiciels et progiciels d'application, tant en phase de développement qu'en phase d'exploitation,
- les logiciels de sécurité des systèmes centraux et des stations de travail dont les fonctions sont l'authentification, la certification, le contrôle d'accès, l'administration des droits, etc.,
- les logiciels d'équipements spécifiques de sécurité : gestion des alarmes, etc.

Les données et les informations

Il peut être utile de faire la différence entre données et informations.

Une donnée est une représentation conventionnelle d'un fait, d'un objet, d'un état, etc.

Des exemples de données sont :

- les données techniques, sur les produits, sur les composants, etc.,
- les données industrielles, nombre de produits en stock, coûts, délais de production, main d'œuvre, etc.,
- les données commerciales, références des clients, tarifs, concessions, etc.,
- les données nominatives, à caractère personnel, social ou financier,

- les données opérationnelles concernant la planification de l'entreprise, tous secteurs confondus.

Les données sont le plus souvent représentées par des valeurs chiffrées.

Une information est l'interprétation d'une ou plusieurs données, en fonction de critères relatifs à un point de vue.

Des exemples d'informations concernant l'entreprise sont :

- les secrets d'entreprise concernant sa stratégie, de futures acquisitions, etc.,
- le savoir-faire scientifique, technique, industriel, commercial, éléments fondamentaux de la compétitivité de l'entreprise,
- l'analyse du marché, de la concurrence, etc.

Les informations sont le plus souvent représentées par du texte ou par une présentation particulière de chiffres manifestant l'association faite entre des valeurs de données et un objectif particulier.

Le personnel

Le personnel est, en soi, une ressource et, généralement, le système d'information ne peut se passer de sa disponibilité.

C'est la cible essentielle des mouvements sociaux et des grèves.

LA VALEUR DES RESSOURCES

Il doit être clair qu'à côté de la « *valeur intrinsèque* » d'une ressource, que l'on pourra estimer par son coût de remplacement, il y a une « *valeur d'usage* » dont la valeur prendra en compte les coûts engendrés par son indisponibilité ou son altération.

La valeur intrinsèque des ressources

La valeur intrinsèque d'une ressource pourra être estimée par sa valeur vénale ou par son coût de remplacement. On pourra ainsi évaluer la valeur d'une base de données par son coût de reconstitution si elle venait à être détruite ou par le prix auquel on pourrait la monnayer. Un fichier client, par exemple, a, dans certains secteurs, une valeur marchande connue.

La valeur d'usage

La valeur d'usage, a contrario, est définie par rapport à ce que subirait l'entreprise en cas d'altération d'une de ses qualités.

C'est donc une valeur définie « *par la négative* ».

Pour cela, trois critères seront pris en compte, la disponibilité de la ressource, son intégrité ou sa confidentialité. Ainsi la valeur d'usage d'une ressource pourra être définie par ce que coûterait à l'entreprise une atteinte à la disponibilité, à l'intégrité ou à la confidentialité de cette ressource.

III. LES MENACES ET LES AGRESSIONS

Nous appelons menace une agression potentielle qui ne s'est pas manifestée.

DÉFINITIONS

Menace : Toute action d'une personne ou tout événement susceptible de conduire à un changement non souhaité d'une ressource du système d'information, quel que soit son type.

Agression : Toute action effectivement entreprise par une personne ou tout événement réel, dont l'aboutissement, en l'absence de mesures de sécurité, sera un changement non souhaité d'une ressource du système d'information, quel que soit son type.

Nous appelons donc « *agression* » la phase du phénomène naturel, de l'accident, de l'erreur, de la faute ou de la malveillance, qui s'étend depuis son déclenchement jusqu'à son aboutissement sous la forme d'un sinistre. Par exemple, une agression peut être constituée d'un événement initial « *chute de la foudre* » qui entraîne un incendie se propageant au centre de calcul, le résultat étant la destruction par le feu des équipements informatiques. Un autre exemple d'agression pourrait être constitué d'un événement initial « *faute du compilateur* » (ou du programmeur, ou de l'unité logique de l'ordinateur) provoquant une erreur dans un programme, elle-même pouvant se propager jusqu'à la détérioration finale « *données faussées* ». On peut constater que de nombreuses agressions peuvent aboutir au même résultat, couramment appelé sinistre, c'est-à-dire aux mêmes détériorations.

L'agression peut elle-même comporter deux phases :

- une première phase où la source de l'agression, l'auteur, humain ou non, progresse jusqu'à la ressource sans dégradation, sans détérioration.

Il peut s'agir d'un intrus pénétrant dans l'entreprise ou dans les bâtiments où sont situées les ressources informatiques ou d'un pirate pénétrant le système d'information par les réseaux de télécommunication ou d'un virus implanté dans une station de travail mais qui n'a pas encore agi.

- une deuxième phase où il y a effectivement changement, détérioration, dans la constitution ou l'état d'une ressource du système d'information.

Les changements ou détériorations peuvent se poursuivre et s'étendre pendant cette deuxième phase qui s'arrête, soit naturellement, soit par une intervention extérieure.

Nous reviendrons très en détail là-dessus au chapitre 3 et dans la deuxième partie, mais disons déjà ici que les finalités défensives concernant ces deux phases sont nettement différentes : pendant la première phase d'agression, on cherchera à stopper l'agression ou à l'empêcher, à la prévenir, alors que, pendant la phase suivante qui correspond à des détériorations de ressources, l'on s'attachera à restreindre l'ampleur du sinistre, à en limiter les conséquences directes.

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

LES TYPES D'AGRESSION

Les agressions peuvent être de divers types, elles peuvent être physiques ou logiques, accidentelles ou malveillantes, et leur auteur peut être humain ou non humain. De manière

plus précise, nous distinguerons :

- l'environnement physique qui peut être source de deux types d'agressions, les agressions d'origine naturelle et celles d'origine industrielle,
- les accidents,
- les erreurs,
- les malveillances,
- enfin les agressions dues à l'environnement social et aux crises correspondantes.

Agressions physiques dues à des origines naturelles

Le sujet d'une telle agression est la nature, et peut appartenir à l'une des deux catégories suivantes :

- catastrophes et calamités à caractère exceptionnel typiques de zones géographiques et régions particulières : les agressions ou événements possibles sont les tremblements de terre, les cyclones et raz de marée, les grandes crues, les glissements de terrain, les avalanches et les feux de forêts.

Exemples typiques :

- la crue de la Saône dans la région lyonnaise en 1982,
- le tremblement de terre de San Francisco d'octobre 1989,
- événements à caractère météorologique tels les orages, la grêle, la neige et les vents : les événements ici sont la foudre, les précipitations, les débordements de rivières consécutives à des pluies, l'effondrement de toiture sous le poids de la neige, etc.

Exemple typique :

- région nîmoise, automne 1987 : orages et pluies diluviennes.

Agressions physiques dues à l'environnement industriel

L'implantation de systèmes informatiques dans une zone industrielle peut les exposer aux origines suivantes de sinistres :

- industries chimiques voisines : corrosion des circuits électroniques et des surfaces magnétiques, pollution, dépôt possible de particules grasses,
- travaux et chantiers, mines et carrières, voies à grande circulation à proximité : secousses, vibrations, câbles sectionnés, éléments mécaniques déréglés, pollution chimique, poussière, etc.,
- émissions radioélectriques parasites : voisinage de radars, faisceaux hertziens, antennes d'émetteurs de radio-télévision.

Agressions physiques d'origine accidentelle

Les sujets de tels accidents peuvent être humains ou non humains ; les accidents sont dus à un concours de circonstances ou au hasard, à des négligences, à une mauvaise conception, à une mauvaise réalisation ou à une mauvaise qualité des infrastructures ou des procédures. Ils peuvent aussi être dus à l'incompétence, à la fatigue, au stress. Quelques exemples typiques sont :

- un court-circuit,

- une fuite d'eau à un étage supérieur,
- une inattention lors de modifications de l'alimentation électrique, de la climatisation, des télécommunications,
- des perturbations électromagnétiques ou électrostatiques, au voisinage des équipements informatiques,
- des pannes des équipements informatiques ou auxiliaires.

Agressions logiques d'origines accidentelles

Il s'agit ici des erreurs au niveau de la conception, de la réalisation, de l'exploitation ou de l'utilisation de systèmes et applications informatiques. Des négligences, l'incompétence ou la méconnaissance des procédures sont susceptibles d'entraîner de tels événements, de même que la fatigue et le stress. Certains accidents physiques peuvent aussi être à l'origine de tels accidents, comme par exemple les pannes de la mémoire centrale ou les incidents sur les disques magnétiques, qui peuvent entraîner des altérations des programmes et des données.

Les malveillances

Les malveillances sont des actes volontaires, provoqués par des êtres humains qui peuvent ou non faire partie du personnel de l'entreprise.

On distingue :

- le sabotage matériel qui est l'endommagement ou la destruction d'une ressource physique, bien, équipement ou support de données,
- le sabotage immatériel qui est une agression perpétrée par voie logique dans le but de détruire ou d'altérer des données ou des programmes,
- les détournements de fonds par l'intermédiaire du système d'information, ces détournements pouvant découler de modifications de certaines données ou programmes ou résulter d'un chantage, après introduction d'un sabotage immatériel caché appelé bombe logique,
- les agressions physiques ou détournements de biens physiques rendus possibles ou facilités par l'altération de données ou de programmes,
- les détournements de logiciels, qui sont surtout importants dans les entreprises produisant des logiciels,
- les détournements d'information par vol ou copie,
- le vol de ressources physiques, essentiellement du petit matériel et en particulier vol des terminaux, PC, et maintenant ordinateurs portables et note-books,
- l'utilisation frauduleuse de ressources et en particulier utilisation frauduleuse des réseaux de télécommunication.

Crises ou conflits origines de sinistres

Il s'agit ici essentiellement des situations susceptibles de bloquer l'activité informationnelle, ou d'incapacité à assurer le travail, dues :

- à des grèves, en particulier au niveau du service informatique, à un lock-out, à des émeutes ou des mouvements populaires,
- au départ ou à l'absence, pour cause de maladie, accident ou démission, de personnels

- occupant des fonctions stratégiques, informaticiens ou utilisateurs d'applications critiques, par exemple,
- à des épidémies ou intoxications générales,
- à des interdictions de zone par la préfecture de police ou la protection civile.

LES VULNÉRABILITÉS

Une agression est donc caractérisée par un certain nombre de voies d'accès jusqu'à l'atteinte des ressources cibles de l'agression.

Chacune de ces voies d'accès possibles à une ressource, que celle-ci soit une cible intermédiaire ou finale de l'agression, constitue pour l'entreprise une « *vulnérabilité* », dont nous allons décrire les types principaux.

Les vulnérabilités qui peuvent être exploitées peuvent, pour plus de clarté, être regroupées en deux grandes catégories, les voies d'accès logiques et les voies d'accès physiques.

Les voies d'accès logiques

Les voies d'accès logiques et les vulnérabilités associées représentent toutes les manières d'accéder aux données ou aux informations par voie logique, c'est-à-dire par l'intermédiaire du système d'information sans avoir accès physiquement à un support d'information. Il s'agit donc d'accès empruntés par des personnes, de l'entreprise ou non. Ces vulnérabilités peuvent être décomposées en plusieurs sous-classes représentatives de la manière dont l'accès peut être obtenu :

- l'accès autorisé : c'est la vulnérabilité liée au fait que des individus autorisés à accéder à une information peuvent délibérément ou par erreur la divulguer, l'altérer, voire la détruire. Cette catégorie d'accès comporte deux sous-classes :
 - les accès autorisés légitimes, qui sont ceux réalisés par des personnes ayant réellement besoin d'avoir de tels droits d'accès dans le cadre de leur travail,
 - les accès autorisés illégitimes, qui sont ceux réalisés par des personnes n'ayant pas ou plus besoin de tels droits. Il s'agit généralement de droits attribués de manière laxiste ou non gérés dans le temps.
- l'usurpation de droits : il s'agit là de toutes les manières déguisées ou non prévues d'accéder à de l'information ou à une ressource. Cette catégorie comporte des sous-classes :
 - l'acquisition illicite de droits d'accès : il s'agit des cas où, pour obtenir des droits d'accès qu'il n'a pas, un « *pirate* » va agir de manière illicite, en forçant le système de gestion des droits, au niveau des tables système par exemple,
 - l'usurpation d'identité qui consiste à se présenter sous le nom d'une autre personne pour obtenir ses droits,
 - l'abus de droits : il s'agit de tous les cas où des voies dérobées, et non documentées en général, permettent d'obtenir, avec un niveau d'habilitation donné, plus de droits réels que prévus. Par exemple, certains ingénieurs de développement peuvent se prévoir des « *portes dérobées d'accès* » ou « *chevaux de Troie* » dans les logiciels pour intervenir plus facilement en phase d'exploitation, en cas de problème. Cette voie cachée constitue un abus de droits. Un autre exemple pourrait être l'abus d'utilitaires privilégiés par du personnel d'exploitation.

- le forçage de l'accès : il s'agit de la violation des systèmes de sécurité pour acquérir l'accès aux données ou aux programmes en l'absence de droits.

Les voies d'accès physiques

Les voies d'accès physiques sont toutes les manières d'accéder physiquement à une ressource du système d'information. Il s'agit donc soit de ressources physiques, soit de supports de données. Ces voies d'accès peuvent être empruntées aussi bien par des êtres humains que par des éléments naturels comme l'air, le feu ou l'eau. Parmi ces voies d'accès, qui sont autant de vulnérabilités, on distingue :

- les accès aux locaux qui peuvent se faire de différentes manières :
 - par les issues normales (portes et fenêtres) qui peuvent se situer à la périphérie du site, des bâtiments, ou du local,
 - par les faux planchers ou faux plafonds,
 - par les murs et les cloisons,
- les accès aux ressources situées dans les locaux de l'entreprise :
 - accès au contenu des supports de données,
 - accès aux stations de travail,
 - accès aux équipements, en particulier de télécommunication ou de servitudes comme la climatisation ou l'énergie,
- les accès aux ressources situées ou en transit hors des locaux de l'entreprise :
 - accès aux réseaux publics de télécommunication,
 - compromission électromagnétique
 - accès aux supports de données en transit hors de l'entreprise (bandes, disques, documents, etc.).

IV. LES DÉTÉRIORATIONS DE RESSOURCES

Les détériorations de ressources du système d'information sont provoquées pendant la deuxième phase de l'agression. Elles sont décrites du point de vue de l'entreprise et sont la conséquence de l'agression.

Elles peuvent être caractérisées par deux paramètres ou attributs : leur type et leur évolutivité.

LES TYPES DE DÉTÉRIORATIONS

Les types de détériorations sont représentatifs de ce qui peut advenir à une ressource, cible de l'agression. C'est une description de changement d'état au niveau de la ressource, sans l'analyse des conséquences au niveau de l'entreprise, qui sera prise en compte dans l'étude des « dysfonctionnements ».

Les détériorations peuvent porter sur la confidentialité des données, l'intégrité et la disponibilité des ressources ou la disponibilité du service.

Les détériorations seront classées et regroupées en trois catégories, chaque catégorie étant

elle-même composée de sous-classes spécifiques de niveaux de gravité différents :

- la compromission d'informations sensibles ou perte de confidentialité,
- l'altération d'informations sensibles ou vitales ou perte d'intégrité,
- la perte de disponibilité du service,

La compromission d'informations sensibles

Nous distinguerons trois sous-types de détériorations dans cette catégorie :

- la « *divulgaration* » d'informations confidentielles : une caractéristique de la divulgation est qu'elle porte sur des données singulières ou ponctuelles, qui cependant peuvent être très critiques, et non sur des ensembles d'informations structurés, complets. Une autre caractéristique est qu'elles sont souvent le fait de personnes internes à l'entreprise. Les cibles concernées sont aussi bien des données techniques, industrielles ou commerciales que des données nominatives ou des secrets d'entreprise. La divulgation peut se faire au profit de la presse, du fisc, du personnel de l'entreprise, des banques, des compagnies d'assurances, des créiteurs ou débiteurs, des concurrents, des clients ou fournisseurs. Il existe deux variantes : la divulgation de ce qui, en tout état de cause, ne doit pas être révélé, même à long terme, et la divulgation prématurée. La divulgation peut être due à l'ignorance, à une erreur, une négligence ou un accident, comme à la malveillance.
- le « *détournement* » d'informations sensibles : Ce que nous appelons détournement est très voisin de la divulgation, et pourrait d'ailleurs en être la conséquence ou une des conséquences. Il s'en distingue par la quantité d'informations détournées, un fichier complet par exemple, et par le fait qu'il est souvent réalisé au profit d'une organisation ou d'un bénéficiaire bien déterminés. Les cibles concernées sont, le plus souvent, les ressources onéreuses, les secrets d'entreprise ou le savoir-faire technique ou commercial. Le détournement est réalisé généralement au profit d'un concurrent ou d'un adversaire, quelquefois de la presse, et il est généralement malveillant.
- le « *détournement massif* » d'informations sensibles est le stade ultime de la compromission où tout un ensemble de fichiers sensibles est détourné. Ce peut être le résultat d'une action répétitive et de longue durée ou de la copie d'une grande quantité de supports de données sensibles, par exemple par un employé sur le point de quitter l'entreprise.

La distinction que nous faisons entre ces trois concepts est faite essentiellement sur la base de la quantité d'informations compromises, la gravité résultante pouvant être différente.

Informations altérées ou faussées

Il s'agit des données ayant subi une perte d'intégrité. Nous ferons les mêmes distinctions que ci-dessus selon la quantité d'informations altérées :

- l'« *altération ponctuelle* » de données qui portera le plus souvent sur un enregistrement d'un fichier. Ceci peut avoir été fait par erreur ou dans un but bien déterminé, par exemple pour frauder,
- la « *pollution d'un fichier* » qui portera soit sur de nombreuses altérations soit sur des ajouts ou des manques d'informations. C'est l'ensemble du fichier ou de la base de données qui est en cause et non seulement un de ses enregistrements.

- la « *pollution massive* » qui portera, comme précédemment, sur un ensemble complet de fichiers et peut-être sur leur globalité.

Perte de disponibilité du service

A l'origine, il peut s'agir de la perte de disponibilité des données, des programmes ou des équipements, et nous ne distinguerons pas ces différents cas car ils se traduisent tous par la perte de disponibilité du service attendu, et parce que c'est seulement au niveau de la perte de service que l'on peut apprécier la gravité potentielle de ce type de détérioration.

Nous qualifierons la perte de disponibilité par deux paramètres, le premier étant significatif de l'importance de l'impact et le second de sa durée.

Nous distinguerons ainsi, pour l'importance de l'impact :

- la « *dégradation du service* » : il peut s'agir d'une baisse de performances, de taux d'attente à la connexion, de taux d'erreurs important ralentissant les échanges, etc.,
- l' « *interruption d'une application* » spécifique : par exemple, indisponibilité de l'application prise de commandes ou de l'application paie ; cette indisponibilité est, le plus souvent, le résultat d'un sinistre ayant atteint un programme ou une base de données spécifique,
- l' « *interruption d'un service* » spécifique : par exemple indisponibilité du service transactionnel, ou interruption du service télétraitement ou réseau ; cette indisponibilité est, le plus souvent, le résultat d'un sinistre ayant atteint un programme-système ou alors une ressource très spécifique, telle qu'un frontal ou une ressource des télécommunications,
- l' « *interruption totale du système* » informatique : cette interruption totale du système est généralement le résultat d'un sinistre ayant atteint une ressource fondamentale du système d'information, ressource matérielle ou logicielle.

Quant à la durée de l'indisponibilité, nous distinguerons :

- l'interruption de courte durée, qui devra être qualifiée en fonction des impératifs de l'entreprise,
- l'interruption de moyenne durée,
- l'interruption de longue durée.

L'ÉVOLUTIVITÉ

Les mêmes types de détériorations peuvent être provoqués par divers types d'agression.

Selon les types d'agression, cependant, l'évolution des détériorations pourra être différente. On distingue ainsi les détériorations ponctuelles, les évolutives et les répétitives.

Les détériorations ponctuelles

Les détériorations ponctuelles sont celles qui résultent directement d'un acte unique et dont la manifestation est immédiate.

Des exemples de tels sinistres sont les vols de données ou de matériels ou des destructions de fichiers. La durée de la détérioration est tellement brève qu'on la considère comme ponctuelle.

Les détériorations évolutives

Les détériorations évolutives sont celles qui vont s'étendre naturellement ou progressivement. Des exemples sont une erreur dans un programme, qui va polluer de plus en plus de données si on ne la détecte pas, ou l'incendie qui évolue progressivement.

Beaucoup de sinistres provoquent des détériorations évolutives dans la mesure où l'absence de détection et le temps qui passe sont des facteurs d'aggravation.

Les détériorations répétitives

Les détériorations répétitives sont celles qui peuvent être liées à des occurrences internes ou externes dont chacune provoque une aggravation des dégâts. Les virus sont une illustration parfaite de tels sinistres : à chaque fois qu'un programme infecté s'exécute, un autre programme est infecté et, éventuellement, des données supplémentaires sont polluées.

V. LES DYSFONCTIONNEMENTS DE L'ENTREPRISE

Les dysfonctionnements de l'entreprise qui résultent des détériorations d'une ou plusieurs ressources du système d'information peuvent être analysés comme des perturbations ou des déviations des processus normaux mis en œuvre par l'entreprise pour exercer son activité.

Cette représentation par les processus sera d'ailleurs souvent une aide pour analyser les conséquences des détériorations.

La liste des dysfonctionnements potentiels causés à l'entreprise suite aux détériorations des ressources des systèmes d'information est longue, et varie d'une entreprise à l'autre, suivant sa taille, son secteur d'activité ou ses produits et compétences distinctives, et bien entendu, de son ampleur. On peut néanmoins distinguer deux types principaux.

TYPES DE DYSFONCTIONNEMENTS

Les dysfonctionnements opérationnels

Les dysfonctionnements opérationnels sont ceux qui vont perturber le fonctionnement quotidien de l'entreprise dans son cycle de travail. Les conséquences peuvent être de multiples natures, telles que :

- la prise de mauvaises décisions stratégiques,
- les ruptures ou perturbations du cycle de production,
- la détérioration de la qualité des biens et services rendus,
- l'incapacité à exploiter des opportunités commerciales,
- l'incapacité à remplir des obligations contractuelles ou statutaires,
- etc.

Les dysfonctionnements intangibles

Il s'agit là d'un type de dysfonctionnements dont les conséquences sont beaucoup plus difficiles à apprécier car n'ayant pas d'influence directe sur la vie quotidienne de l'entreprise. Ils comprennent :

- la perte de confiance des clients, fournisseurs, employés, actionnaires, du public,
- l'augmentation du risque de fraude ou d'erreur,
- la perte de productivité,
- la perte de compétitivité,
- l'affaiblissement de la capacité de négociation,
- l'affaiblissement de la capacité d'autofinancement.

VI. LES PERTES

La dernière phase du scénario de sinistre est celle où l'entreprise va d'une part, constater le sinistre et les dégâts correspondants, d'autre part, entreprendre des actions pour revenir à son état d'origine et retrouver un fonctionnement habituel.

Tout ceci va entraîner des pertes de différentes natures.

LES PERTES DIRECTES LIÉES AUX DÉTÉRIORATIONS

Il s'agit là des frais de toute nature que l'entreprise va devoir engager pour remédier aux détériorations subies par ses ressources.

Il s'agit donc de réparer ou de reconstruire les ressources matérielles, de reconstituer les bases de données, les fichiers de données ou les informations, ou de corriger les programmes.

On distinguera différents types de pertes :

- perte de fonds,
- perte de valeur liée à des valeurs immobilisées : bâtiments et locaux, matériels informatiques et péri-informatiques, armoires gaines et câbles, télécommunications, climatisation, énergie, stocks et autres immobilisations, y compris immatérielles,
- perte de valeur liée aux petits matériels, micros et équipements de bureau et fournitures diverses,
- perte de valeur liée aux supports et à leur contenu : bandes, disquettes, listings, etc.,

Pourront s'ajouter, le cas échéant, les frais suivants :

- frais de ressaisie ou reconstitution d'informations perdues, détruites ou dégradées,
- coûts directs de réparation, s'ils ne sont pas couverts par un contrat de maintenance,
- frais directs après sinistre : déblaiement, etc.,
- le cas échéant, pertes humaines.

LES PERTES INDIRECTES ENGENDRÉES PAR LES DYSFONCTIONNEMENTS

Les détériorations provoquées par un sinistre, au niveau du système d'information, entraînent en général, au niveau de l'entreprise, des dysfonctionnements, par exemple l'arrêt de l'activité, la perte d'efficacité commerciale, etc. Ils peuvent être immédiats ou différés, décalés dans le temps.

Les pertes dépendent de l'existence de mesures de secours ou de sauvegarde.

- pertes d'exploitation dues à des décalages de chiffres d'affaires ou de dépenses,
- pertes d'exploitation dues à des pertes d'affaires, de clientèle ou de parts de marché,
- pertes d'exploitation induites : paiement d'heures supplémentaires, de sous-traitance, d'intérimaires,
- frais supplémentaires liés à la poursuite de l'activité, occasionnés par le mode d'activité dégradée, ou le passage en fonctionnement de secours : paiement d'heures supplémentaires, de sous-traitance, d'intérimaires, de frais de transport et de convoyage, coûts d'usage d'autres matériels ou logiciels (secours),
- frais supplémentaires pour restaurer la situation antérieure ou une situation stable acceptable,
- coûts extraordinaires : location exceptionnelle de matériels, de locaux, frais d'expertise et de conseils juridiques, coûts d'acquisition ou de location de ressources complémentaires temporaires en télécommunications, logiciels et divers, coûts de recherche et de recrutement de personnel,
- préjudices, pertes ou surcoûts causés à des tiers du fait d'un sinistre dans l'entreprise, et susceptibles de faire l'objet d'un recours en responsabilité civile.

LES PERTES TOTALES

Il s'agit des pertes finales enregistrées, suite aux dysfonctionnements et aux restaurations entraînés par les détériorations consécutives à un sinistre.

S'agissant d'un bilan final, les pertes consécutives à un sinistre devraient pouvoir être ramenées à une valeur financière. Dans certains cas, cependant, cela est impossible. Si, par exemple, le résultat final est l'obligation de fermer une branche d'activité d'une société, on pourra bien sûr estimer les coûts directs de cette fermeture, mais on sera incapable d'estimer, sur le long terme, le véritable coût du préjudice subi.

Les pertes résiduelles

Avant de clore le bilan du sinistre, nous verrons qu'il y a encore quelque chose à faire pour minimiser le préjudice subi, c'est de récupérer une partie des pertes sur des tiers, en l'occurrence essentiellement sur l'assurance ou sur l'agresseur, s'il est humain, par action pénale.

Le bilan final que l'on pourra alors faire du sinistre donnera les pertes résiduelles.

En conclusion, nous avons passé en revue les différents éléments d'un scénario de sinistre. Ces éléments peuvent être considérés comme des étapes ou des phases d'une histoire qui peut arriver dans l'entreprise, mais ce sont surtout des concepts sur lesquels nous allons nous appuyer pour analyser les mesures possibles, c'est l'objet du prochain chapitre.

Chapitre 3

LES MESURES DE SÉCURITÉ

Après avoir établi un modèle pour l'analyse des scénarios de sinistres, nous allons maintenant aborder les mesures de sécurité.

On classe habituellement les mesures destinées à réduire les risques en trois domaines principaux : la sécurité physique, la sécurité organisationnelle et la sécurité logique. La sécurité des personnes, fondamentale, est assurée par une combinaison des trois.

La sécurité physique portera aussi bien sur le site et son périmètre, sur les bâtiments et locaux, tels que bureaux, salles informatiques, locaux techniques, sur les matériels de servitudes, alimentation électrique, chauffage, climatisation, aération, sur les communications et transmissions, sur les équipements informatiques, y compris les terminaux, micros, stations de travail situés chez les utilisateurs, enfin sur les supports informatiques tels que disques, disquettes et bandes magnétiques, sans oublier les listings et la documentation.

La sécurité organisationnelle traite de la gestion et de l'administration de la sécurité, des consignes et des procédures, et laisse souvent à désirer car son importance est sous-estimée. Elle est pourtant fondamentale, et les moyens techniques les plus sophistiqués risquent d'être illusoires s'ils ne sont accompagnés d'une organisation rigoureuse. Des exemples sont donnés par les procédures relatives à la gestion des mots de passe : imposition d'une longueur minimale, contrôle du rythme de renouvellement ou par les procédures d'exploitation, la maintenance, les secours et les sauvegardes, etc.

La sécurité logique est assurée au niveau des logiciels de base, des logiciels de réseau et des logiciels d'application, couplés, le cas échéant, avec des dispositifs matériels, tels les boîtiers de chiffrement ou les cartes à microprocesseurs, dites cartes à puce.

Cette décomposition classique, cependant, est insuffisante pour bien comprendre ce qu'il convient de faire à chaque phase du scénario de sinistre. C'est pourquoi, adaptée à ce scénario, nous allons proposer une autre approche des mesures de sécurité.

En considérant les concepts présentés au chapitre 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.

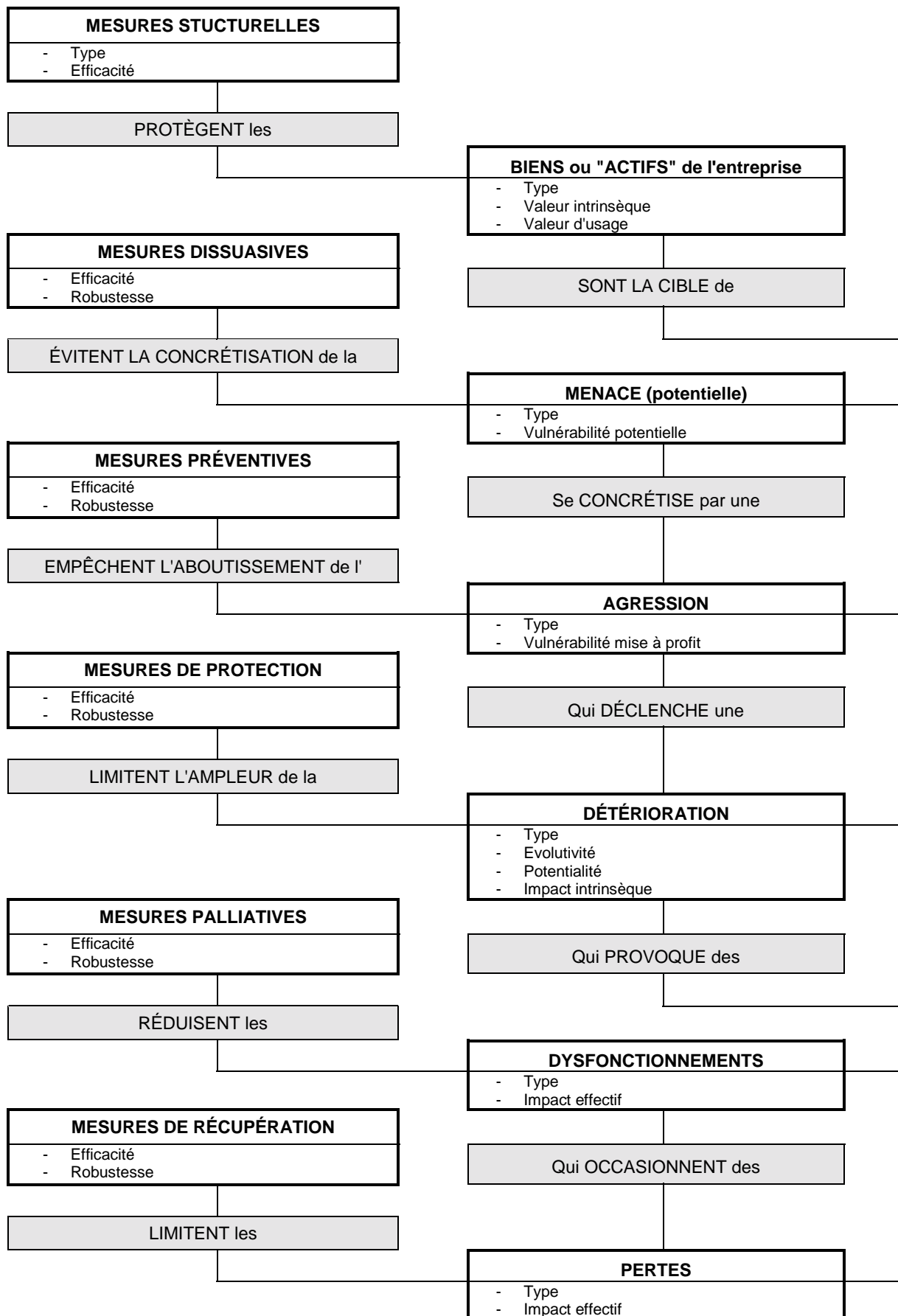


Figure 2

Aux niveaux du modèle relationnel de scénario de sinistre, on associe ainsi des classes de mesures de sécurité.

Ce découpage permet encore 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 potentialité,
- 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,
- les mesures « *préventives* » : celles qui permettent d'empêcher les détériorations ou d'éviter qu'une agression n'atteigne des ressources du système d'information,
- les mesures « *de protection* » qui, sans empêcher les détériorations, permettent tout au moins d'en limiter l'ampleur,
- les mesures « *palliatives* » qui, les détériorations étant ce qu'elles sont, permettent de réduire les dysfonctionnements induits au niveau de l'entreprise,
- les mesures de « *récupération* » qui visent à récupérer une partie du préjudice subi par transfert des pertes sur des tiers, assurances ou actions en justice dans le cas d'agresseurs humains.

Nous n'aborderons pas le problème du choix des mesures à mettre en œuvre qui ressort de méthodes de management de la sécurité. Nous resterons au niveau du modèle, c'est-à-dire à la présentation des concepts, à leur définition et à la mise en évidence des liens entre les types de mesures et les éléments du modèle de scénario de sinistre.

A chaque niveau, nous allons définir des types de mesures, représentant les classes de solutions à appliquer ; les types de mesures font eux-mêmes appel à des « *services* », qui peuvent, pour certains d'entre eux, faire appel à des sous-services plus basiques, s'appuyant sur des « *mécanismes* » variés et multiples, aussi bien du point de vue de leurs fonctions, que du point de vue de leur « *efficacité* » et de leur « *robustesse* », termes que nous définirons dans la deuxième partie.

I. LES MESURES STRUCTURELLES

Les mesures structurelles sont des mesures prises au niveau de la structure même du système d'information, de son architecture et qui vont modifier les conditions de l'agression par une diminution de l'enjeu pour l'agresseur ou par une diminution de l'exposition de l'entreprise à ce type de risque.

Ce qui différencie ces mesures des autres types est qu'elles sont prises au niveau des ressources du système d'information, indépendamment des scénarios d'agression.

On distingue la fragmentation de l'information, l'occultation des ressources, la réduction de la valeur des ressources et les mesures structurelles d'organisation.

La fragmentation de l'information

La « *fragmentation* » consiste à découper l'information en fragments, et faire en sorte qu'une agression n'atteigne que des fragments isolés.

L'intérêt de la fragmentation est que, pour un coût d'agression donné, le gain espéré par

l'agresseur est divisé par un certain facteur, ce qui est de nature à le dissuader.

Au niveau de la confidentialité, il faut faire en sorte que chaque fragment ne puisse fournir d'information ayant un intérêt en lui-même pour un agresseur. Par exemple, on peut découper un fichier confidentiel à transmettre d'un point à un autre en plusieurs fragments, longitudinalement, c'est-à-dire sans qu'un fragment ne puisse contenir de groupe d'informations autonome ou complet, et transmettre les divers fragments par des chemins différents du réseau de transmission.

L'occultation des ressources

L'« occultation » de la cible consiste à cacher jusqu'à l'existence même d'une cible potentielle ou d'un enjeu de quelque importance, par exemple ne pas faire de publicité autour de son informatique, ne pas révéler la nature des informations traitées, etc.

La réduction de la valeur des ressources

On diminue les dégâts en diminuant la valeur des ressources qui peuvent être la cible d'une agression, par exemple en décidant de ne pas traiter certaines données très sensibles (confidentielles, par exemple...) d'un fichier et de les traiter ailleurs, sur un système mieux sécurisé, ou même de les traiter manuellement ; ce dernier cas est assez fréquent, dans le cas des salaires des dirigeants d'entreprise, ou dans le cas d'informations très confidentielles.

Les mesures structurelles d'organisation

Les mesures structurelles d'organisation regroupent ce que l'on pourrait appeler les mesures positives de motivation.

Il n'est pas inutile de rappeler que la majorité des sinistres sont dus à des malveillances, pour beaucoup commises par du personnel de l'entreprise. Dans ces conditions, toute mesure prise pour éviter les mécontentements, pour sensibiliser et motiver le personnel est un facteur d'élimination de risque.

Il peut s'agir de :

- politiques de sensibilisation et de formation du personnel sérieuses et actualisées en permanence,
- conditions de travail ergonomiques et agréables, pour éviter la fatigue et le stress,
- politique du personnel active au niveau des plans de carrières et des salaires, de la reconnaissance des mérites et des résultats, en particulier en ce qui concerne les personnels critiques, informaticiens ou utilisateurs,
- la bonne adaptation de chaque salarié à son travail, aussi bien du point de vue de sa formation que du point de vue de ses goûts personnels,
- la sensibilisation du personnel aux problèmes de sécurité.

II. LES MESURES DISSUASIVES

Ces mesures ont pour objet d'empêcher le passage à l'acte d'un agresseur humain, d'empêcher la concrétisation de la menace, donc en amont du déclenchement de l'agression. C'est ce que nous appelons la dissuasion.

Il s'agit là de mesures prises au niveau de l'organisation même de l'entreprise et susceptibles d'éliminer ou de réduire les causes ou motivations qui sont à l'origine d'un accident, d'une erreur ou d'une agression dus à des êtres humains.

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 :

- 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,
- l'ampleur des sanctions encourues : risque de licenciement, appel aux services de police, dépôt de plainte et poursuites judiciaires.

Une remarque s'impose à ce niveau : qu'il s'agisse de diminuer l'attrait de l'agression ou d'autres formes de dissuasion, ces classes de mesures ne peuvent jouer leur rôle que si l'agresseur potentiel ne sous-estime pas leur ampleur. Ce qui va donc entrer en compte, est la perception que l'agresseur aura de ces mesures d'une part, et la crédibilité qu'il leur attachera d'autre part. Ainsi, si les responsables ne vont pas jusqu'au bout des investigations pour retrouver l'auteur d'une malveillance, par une analyse approfondie des éléments détectés et par l'ouverture d'une enquête sérieuse, ou si des sanctions ne sont, en fait, jamais prises, même si elles sont justifiées, la dissuasion attendue sera toute théorique. La politique en la matière doit donc être clairement affichée et rigoureusement appliquée.

III. LES MESURES PRÉVENTIVES

Ces mesures peuvent entrer en jeu quand on n'a pu dissuader ou empêcher la concrétisation de la menace.

Il s'agit alors d'empêcher l'agression d'aboutir à des détériorations soit par des mesures prises de manière permanente, soit par la détection de l'agression et intervention pour la stopper avant détérioration.

Chacune de ces mesures sera donc orientée principalement contre un type d'agression donné. On distingue les barrages, les contrôles d'accès, la détection-interception et le masquage de l'information.

Le barrage

Le « *barrage* » (ou imperméabilisation) consiste à barrer les voies d'accès aux ressources, sans distinction de personnes ni de circonstances, par exemple :

- dans le cas d'une agression physique, un mur de béton, l'absence de fenêtres ou des fenêtres blindées, un centre informatique enterré feront avorter une attaque à l'explosif,
- la surélévation d'un centre de calcul sera un barrage contre les inondations en provenance de l'extérieur du site,
- des câbles de transmissions blindés feront échouer un branchement parasite ayant pour but l'écoute du trafic-réseau,
- une cage de Faraday fera un barrage contre les perturbations électromagnétiques de l'environnement industriel ou contre la compromission électromagnétique,
- dans le cas d'une agression logique, la fermeture de tous les accès à un système en télétraitement, par coupure programmée du réseau de transmission lors de certains traitements très sensibles, est un barrage contre toute intrusion, c'est une pratique très courante dans le domaine militaire.

Les contrôles d'accès

Il s'agit des mesures permettant l'accès sélectif à une ressource à un nombre limité de personnes habilitées. Toute tentative d'accès est ainsi filtrée et celles non autorisées rejetées. Ces mesures sont aussi bien physiques que logiques, par exemple contrôle des accès physiques à une salle machine par badge ou contrôle des accès logiques à une application ou à un fichier réglementés par des droits d'accès nominatifs fixés dans des listes attachées à l'application ou au fichier.

Noter que les contrôles d'accès peuvent être cumulés, constituant ainsi autant de barrières de filtrage. On peut ainsi avoir un contrôle à l'entrée des bâtiments, un autre à l'entrée des salles-machines, un troisième au niveau des bandothèques, etc., ce cumul peut aussi se faire entre contrôles physiques et logiques.

Il faut remarquer encore que les contrôles d'accès ne peuvent rien contre les accidents ou les malveillances perpétrées par les personnes licitement autorisées. Ceci pose le problème des agressions dues au personnel de l'entreprise auquel on a accordé des droits, pour lesquelles seules les mesures dissuasives permettront d'éviter les détériorations.

Enfin, il faut signaler que ces contrôles exigent la conjonction de mesures de caractère technique pour le filtrage, et de mesures à caractère organisationnel, pour la définition et la gestion des populations habilitées et des conditions de mise en place et d'utilisation des moyens de contrôle.

La détection-interception

La détection-interception de l'agression réside dans sa détection directe avant qu'elle ne provoque un sinistre. L'agression de la ressource est en cours, mais il faut un certain temps pour qu'elle produise un début de détérioration et on profite de ce laps de temps pour intercepter la progression de l'agresseur, par exemple :

- une équipe de saboteurs est en train de forcer les contrôles d'accès et se dispose à

détruire des équipements informatiques, tant que les agresseurs n'ont pas commencé à attaquer le matériel, l'agression peut être interceptée, si des rondes sont effectuées ou si le contrôle d'accès était lui-même sous surveillance,

- un incendie peut être détecté avant qu'il n'atteigne les équipements informatiques et l'intervention des pompiers suffisamment rapide pour le circonscire avant toute détérioration de ressources du système d'information,
- une intrusion réussie au niveau de l'accès au système peut être bloquée, lors de la progression de l'intrusion, par déconnexion immédiate de l'intrus, ou, mieux, par son intoxication par des informations sans intérêt, le temps de l'identifier et le sanctionner.

Le masquage des informations

Le masquage de l'information est une technique utilisée pour assurer la confidentialité de données, soit lorsqu'elles sont stockées soit lors de leur transmission. Un exemple de masquage est le brouillage d'un message à l'émission par chiffrement. Le message, même intercepté, ne sera pas intelligible au pirate, seul le destinataire légitime pourra le déchiffrer, étant en possession de la clef du chiffre. Cette technique a pour résultat auxiliaire d'empêcher leur altération fine et intelligente, biaisage ou fraude par exemple, car l'agresseur ne pourra identifier avec précision la partie de la donnée qu'il souhaite modifier. Par contre, le masquage ne peut empêcher la destruction ou l'altération sauvage des données masquées.

IV. LES MESURES DE PROTECTION

Contrairement aux mesures de prévention qui sont orientées vers l'agression, les mesures de protection sont orientées vers les ressources pour limiter l'ampleur des détériorations.

Elles peuvent être considérées comme un prolongement des mesures préventives, mais en différent par le point d'application.

Par exemple, on détectera un incendie à l'extérieur d'un centre de traitement pour intervenir avant qu'il n'atteigne le centre, c'est une mesure préventive, on détectera aussi, en complément, les fumées à l'intérieur du centre pour éviter que l'incendie ne se propage et fasse des détériorations importantes, c'est une mesure de protection.

On distingue la détection-réaction, les mesures anti-propagation et la certification des données et programmes.

La détection-réaction

La chaîne détection-réaction peut jouer à des instants différents dans le déroulement de l'agression, avec, selon les cas, des caractéristiques particulières :

- la détection-réaction « *ponctuelle* », localisée dans le temps. Ce peut être le cas d'une agression évolutive dont on veut arrêter la progression, par exemple l'incendie, pour éviter qu'il ne détruise le centre de traitement ou la médiathèque, ou une erreur sur la valeur d'un stock d'un composant critique en long délai de réapprovisionnement, qui doit être découverte à temps pour éviter des erreurs de commande et, à terme, une rupture de stock. Ce peut, aussi, être le cas d'une agression à caractère continu ou répétitif : c'est donc la répétition que l'on veut enrayer, par exemple la fuite régulière et

organisée d'informations confidentielles. Le facteur temps de détection joue un rôle primordial dans tous ces problèmes.

- la détection-réaction « *continue* », dont la chaîne joue en permanence. Ce peut être :
 - la surveillance (monitoring) : comme la détection et la correction automatique d'erreurs de transmission, un « *watchdog* » de surveillance du fonctionnement du système,
 - des contrôles de cohérence : sans détecter la cause exacte ou les effets directs d'une agression, on est capable, par comparaison de données entre elles ou à des seuils, de bloquer le processus, par exemple vérification de tranche d'âge, surveillance d'un niveau minimum de stock ou d'une consommation.

Ce qu'il y a de commun à ces mesures de détection-réaction est l'adaptation nécessaire des services de détection à l'agression dont on veut enrayer la progression. On aura donc des détecteurs d'eau, d'incendie, d'agression physique, on effectuera une surveillance active de sessions de transactions utilisant certains programmes d'application ou initialisées depuis certains postes de travail, on surveillera particulièrement tel groupe de données critiques, etc.

Les mesures anti-propagation

Les mesures anti-propagation sont, soit des mesures absolues, soit des mesures de contrôle. Nous distinguerons :

- les barrières anti-propagation : il s'agit ici d'un cordon sanitaire permanent pour empêcher la propagation du sinistre. Il peut s'agir de portes coupe-feu ou de fermeture automatique des clapets de ventilation, dans le cas d'un incendie, ou du contrôle des données résultant d'un traitement avant leur réutilisation dans un autre traitement, ou avant leur diffusion, ou encore de la protection de fichiers contre toute écriture, pour éviter leur pollution.
- les contrôles d'accès anti-propagation : il s'agit de contrôles complémentaires, introduits tant au niveau physique qu'au niveau logique, permettant d'isoler certaines parties d'un système ou certaines données particulièrement sensibles.

La certification des données et programmes

On peut encore distinguer, à l'intérieur de cette classe, deux sous-classes :

- les redondances ponctuelles : on ajoute ponctuellement, en cours de traitement, des redondances à certaines informations jugées importantes, qui permettent de détecter des anomalies, ou même dans certains cas, de les reconstituer en cas de destruction ou d'altération,
- la certification des données ou programmes : elle permet de s'assurer de l'authenticité et de l'invariabilité de logiciels ou de données entre deux instants différents et permet éventuellement leur reconstitution malgré les dégâts éventuels subis. C'est une mesure contre l'altération, la suppression ou l'insertion parasite de données. Ainsi, si la certification est efficace, on peut faire en sorte que les dégâts se limitent à une perte de temps, qui peut, au plus, impacter la disponibilité de l'information.

V. LES MESURES PALLIATIVES

Les mesures palliatives agissent une fois que les détériorations ont été accomplies et visent d'une part à en minimiser les conséquences au niveau de l'entreprise, d'autre part à restaurer les ressources détériorées pour retrouver l'état initial.

LES MESURES ATTÉNUANT LES DYSFONCTIONNEMENTS

Elles ne sont plus spécifiques des ressources atteintes mais du système d'information dans son ensemble, voire des processus de l'entreprise.

Certaines de ces mesures que nous appelons palliatives, la plupart même, ont pu être prises à titre préventif. Il faut donc faire attention à ne pas les confondre avec les mesures préventives qui ont pour but de prévenir, au sens d'éviter, alors que les mesures palliatives ont été « *prévues* » avant les détériorations pour en réduire l'impact.

Le type général de ces mesures, qui est utilisé pour pallier la perte de disponibilité de ressources, est constitué par les mesures de reconfiguration.

La reconfiguration

La reconfiguration est une technique générique qui sera surtout utilisée dans les cas liés aux détérioration du type perte d'intégrité ou perte de disponibilité.

Les reconfigurations seront de trois types :

- la « *reconfiguration dynamique* » qui agit par les redondances intégrées en différents points du cycle de traitement : les redondances ici permettent la continuation du service, mais on ne peut affirmer à tous les coups qu'il sera totalement conforme, à cause des délais ou retards possibles induits par certains types de détériorations. Ces redondances peuvent être de deux types :
 - les redondances matérielles : il s'agit de la duplication des éléments de la configuration physique du système. Le service rendu pourra être dégradé par rapport à la normale : les redondances n'étant pas totalement gratuites sont souvent utilisées, en temps ordinaire, pour multiplier le volume des traitements ou pour améliorer les performances. Un exemple est donné par un ensemble de systèmes couplés, où la défaillance de l'un des deux entraîne la reconfiguration du système, avec intervention simple de l'opérateur, pour basculer dynamiquement les traitements prioritaires du système défaillant sur le système valide.

Noter que dans les redondances matérielles, nous incluons celles relatives aux servitudes : alimentation électrique de secours, climatisation, réseau de transmission.
 - les redondances logicielles qui, en particulier, permettent un redémarrage à chaud d'une application ou du système tout entier, après un délai faible, compatible avec le fonctionnement de l'exploitation.
- la reconfiguration semi-automatique : ce type de reconfiguration s'appuie sur des redondances non-intégrées. Les délais et retards ici sont plus conséquents, de par la

nécessaire élimination des résidus des détériorations (s'il y en a), et l'activation des redondances ; les délais induits peuvent être techniques ou organisationnels, et souvent les deux. Ces techniques de reconfiguration comprennent :

- les sauvegardes : on fait des copies de fichiers, de logiciels, de supports, pour le cas où les originaux seraient inutilisables. Dans ce dernier cas, on peut redémarrer les traitements après un certain délai, en utilisant les copies, dans la mesure où ces dernières reflètent bien la dernière version ou la dernière mise à jour ; le problème de la périodicité des copies est donc posé.
 - les points de reprise (check point) : les erreurs ou incidents ayant été détectés après un certain temps, on arrête le traitement et on reprend le traitement à partir d'un point antérieur stable et correct, le point de reprise, sans avoir à recommencer tout le travail. Ceci suppose l'existence de moyens de création de ces points stables, et des moyens pour revenir en arrière, du point où l'incident a eu lieu jusqu'au point de reprise, de manière synchrone, c'est à dire en réussissant à se remettre dans l'état exact où l'on se trouvait au moment de la création du point stable. Il faut donc conserver des informations relatives à des états antérieurs, dans des fichiers appelés « *journals-avant* ».
 - les redondances complémentaires : dans cette approche, on fait des copies non plus des supports ou des fichiers complets, mais simplement des évolutions et mises à jour. En effet, il est rare que tous les articles d'un fichier soient modifiés en même temps, le même jour, on prend alors une copie des seuls articles modifiés, ce qui minimise la charge du travail de recopie. Un exemple est donné par la journalisation des mises à jour dans des « *journals-après* ».
- la reconfiguration statique ou secours : dans ce cas, les dégâts ont rendu indisponibles tout ou partie des ressources. Si les dégâts sont partiels, on peut réaffecter les ressources restantes, pour favoriser les activités prioritaires, dans ce que nous avons appelé un « *fonctionnement dégradé* ». Si le système est inutilisable, ou si le mode dégradé est, en tout état de cause, insuffisant, on bascule alors en secours total ou partiel, sur un système externe de délestage (back-up). On s'appuie ainsi sur des redondances externes. Ce qui est primordial dans ces deux cas de figures, c'est le travail de préparation et de planification préalable nécessaire pour être prêt à toute éventualité, travail qui peut être considérable : c'est le « *plan de secours* » (contingency plan) qui doit être réglé dans ses moindres détails et être constamment à jour, si on veut être secouru correctement et surtout dans des délais raisonnables. On comprend, ainsi, l'importance des aspects organisationnels, qui sont plus délicats que les aspects purement techniques. Ces derniers s'appuient sur les redondances externes suivantes :
- centre de secours équipé,
 - copies de sauvegarde des logiciels et des fichiers de données,
 - copies de la documentation et des procédures opératoires,
 - secours des fournitures diverses : papier, bordereaux, formulaires, etc.

LES MESURES DE RESTAURATION DES RESSOURCES DÉTÉRIORÉES

C'est le retour à l'état normal, qui peut se dérouler parallèlement aux autres mesures palliatives. Nous distinguerons la *réparation*, la *correction* et la *reconstruction*.

La réparation

La réparation touche les éléments matériels. Cette opération peut être assez longue, surtout s'il s'agit d'un sinistre matériel important touchant les machines et les bâtiments. Peu d'entreprises peuvent se contenter de cette seule mesure pour survivre à de tels sinistres, compte tenu des délais. La réparation peut toutefois être accélérée par la disponibilité (en stock, par exemple) de pièces de rechange, de documentation et de personnels compétents. La réparation s'appuie sur des ressources externes et sur la maintenance corrective.

La correction

La correction touche essentiellement les éléments immatériels, données ou programmes. Après détection d'une erreur, par exemple, il s'agira de rétablir les données exactes, toute la difficulté résidant dans la propagation des erreurs. Après détection d'une altération de programme, il faudra rétablir la version d'origine.

Un problème typique de la réparation comme de la correction est celui de la disparition d'un fournisseur, ou l'arrêt de la production de tel matériel, l'arrêt de la maintenance de tel logiciel fourni par une société externe, le départ du développeur de telle application. Ces derniers cas peuvent être d'autant plus graves qu'en général les fournisseurs de logiciels ne donnent pas les « *sources* » des programmes.

La reconstruction

La reconstruction s'applique aussi bien aux ressources matérielles qu'aux bases de données ou aux programmes et consiste à rebâtir à nouveau ce qui a été détruit.

VI. LES MESURES DE RÉCUPÉRATION

Tous dysfonctionnements limités ou annulés, tous dégâts restaurés, il reste possible d'agir au niveau du préjudice final subi et des pertes induites. Il n'existe en pratique que deux moyens, le transfert du risque et les actions en justice avec dommages-intérêts.

Le transfert du risque sur des tiers

Il s'agit le plus souvent de transfert sur les assurances. On peut aujourd'hui s'assurer non seulement contre le vol et les dégâts physiques, mais aussi contre les pertes d'exploitation et autres pertes consécutives à certains sinistres, essentiellement matériels. Sous certaines conditions, on peut aussi s'assurer contre certains sinistres immatériels, tels que la fraude informatique. Dans ces derniers cas, il est en général exigé qu'il y ait dépôt de plainte, et parfois, ce qui est plus difficile, que l'on puisse faire la preuve du délit. L'assurance est indispensable, voire même obligatoire au niveau des dégâts matériels. En tout état de cause, elle s'imposera dans tous les cas de figures où les pertes potentielles risquent de dépasser la capacité, financière ou non, de l'entreprise ; encore faut-il, d'une part, être capable de déterminer de manière réaliste cette capacité, et, d'autre part, que le type de risque en question soit assurable. Par ailleurs, la notion de capacité financière n'a pas beaucoup de sens au niveau de certaines entreprises, où elle pourra se mesurer en dizaines de milliards de francs ou

même être considérée comme infinie, dans le cas de l'État et de ses administrations ; rappelons que pour ces dernières, l'État est son propre assureur.

L'action en justice

Pour ce type d'action, il faut avoir un dossier solide, des preuves, et souvent beaucoup de temps si on veut récupérer une partie de ses pertes. Nous ne discuterons pas ici de la nécessité de poursuivre en justice à des fins dissuasives, ce qui est une mesure qui relève de la phase d'agression. En tant que mesure susceptible de réduire les pertes par récupération sur l'agresseur, il faut retenir qu'une telle technique suppose des éléments de preuve extrêmement solides et que c'est le recueil de ces éléments qui constituera l'essentiel de la mesure.

*

* *

Nous avons, ainsi, vu qu'à chaque phase et qu'à chaque élément du modèle de scénario de sinistre correspondait une typologie de mesures s'appuyant sur des services spécifiques, bien que certains services soient utilisés par différentes mesures.

Le problème du choix des mesures suppose que l'on soit capable de définir l'influence d'une mesure donnée sur un risque que court l'entreprise, et donc que l'on définisse, sur ce modèle, une « *métrique* » du risque et de l'influence des mesures.

C'est ce que nous allons aborder dans la deuxième partie.

Deuxième partie

L'ÉVALUATION DU RISQUE

INTRODUCTION

Une préoccupation centrale dans la gestion de la sécurité d'une entreprise est d'établir une hiérarchie entre les problèmes auxquels il faudra apporter une solution, de définir un ordre de priorité entre les défauts auxquels il convient de porter remède.

Nous avons analysé, dans les chapitres précédents, les différentes parties du scénario de sinistre et les types de mesures qui peuvent être mises en œuvre. Le problème est donc maintenant d'avoir des critères pour opérer des choix entre ces mesures, afin d'aboutir à un plan de sécurité.

Nous regarderons, dans cette partie, comment caractériser un sinistre potentiel du point de vue du risque de l'entreprise, comment évaluer ce risque par une « *métrique* ».

La question posée est donc de mettre en évidence les paramètres caractéristiques des scénarios de sinistre qui vont nous permettre de les comparer entre eux, afin de pouvoir effectuer une sélection dans les solutions à apporter.

Parmi ces paramètres, 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. Nous distinguerons, en outre, l'« *impact intrinsèque* », en l'absence de toute mesure, et l'« *impact effectif* », en fonction des mesures mises en place.

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. En termes de mesures de sécurité, nous avons vu que celles qui agissent à ce niveau du scénario sont les mesures dissuasives et les mesures préventives.

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 du sinistre, et où les mesures à mettre en œuvre sont des mesures de protection, des mesures palliatives et des mesures de récupération.

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.

Chapitre 4

LA POTENTIALITÉ

I. INTRODUCTION

La question de la potentialité d'un scénario de sinistre est donc celle de savoir si les risques correspondants font réellement partie de l'environnement courant de l'entreprise, s'ils sont significatifs, et dans quelle mesure et avec quelle pondération ils doivent être pris en compte.

Toute la difficulté vient de la nécessité de séparer, c'est-à-dire de distinguer, les scénarios les plus invraisemblables de ceux dont on peut penser, qu'en l'absence de toute mesure spécifique, ils pourraient survenir dès le lendemain sans que quiconque trouve cela exceptionnel.

Certains risques sont en effet « *naturels* », d'autres exceptionnels et il est intuitif et sage d'accorder plus d'attention, une priorité plus grande, aux premiers qu'aux seconds.

Nous sommes tous assurés contre certains risques (circulation, responsabilité civile, incendie, dégâts des eaux, etc.), mais nous sommes très peu à avoir prévu un abri antiatomique, pour la seule raison que nous estimons ce risque comme éloigné, alors que l'abri est coûteux.

Il en est de même en ce qui concerne la sécurité informatique et il nous faut apprendre à reconnaître quels sont les risques proches et réels et quels sont ceux qui le sont moins.

C'est ce caractère de proximité que nous appelons « *potentialité* » pour marquer le côté plus ou moins possible, plausible, ou probable du risque considéré.

Il faut noter que le mot « *probable* » a été employé ici avec son sens le plus courant et qu'il faut éviter toute tentation de rapprochement avec une notion de probabilité qui a un sens mathématique précis et, en tout état de cause, une connotation de phénomène modélisable, ce qui ne nous semble pas approprié.

L'approche probabiliste consiste, en effet, à définir le caractère potentiel d'un sinistre comme sa probabilité d'occurrence. On peut alors calculer ce que les ingénieurs appellent une espérance mathématique du coût d'un dommage qui est le coût moyen probable si le dommage subi est exprimé en coût.

Deux remarques doivent être faites sur cette approche.

La première est que nous raisonnons, et c'est heureux quand on parle de sécurité, sur des événements rares, et que le coût moyen n'a pas de sens réel pour l'entreprise, pas plus qu'il n'en a pour l'individu qui subit un dommage précis, unique et qui ne sera pas réellement consolé de savoir que son cas est rare.

L'individu ne raisonne pas en termes de moyenne.

La personne qui joue à un jeu de hasard, loto ou loterie nationale par exemple, sait qu'en moyenne les individus sont perdants puisque la société organisatrice commence par prélever ses frais et son bénéfice avant de redistribuer le reste, mais cette personne trouve sa motivation dans l'espoir d'un gain susceptible de bouleverser sa vie pour un investissement faible.

De même, les primes d'assurance sont plus élevées que le coût moyen des sinistres, la différence étant les frais et les bénéfices des assureurs. Mais, pour un individu, le coût d'un sinistre peut être insupportable, et l'assurance la seule solution sage. La mutualisation des risques, c'est à dire le partage avec d'autres, est la seule solution pour atténuer les conséquences d'accidents que l'on ne sait éviter à coup sûr, et qui ont, à la fois, un coût élevé et une probabilité faible.

En termes de sécurité de l'entreprise, les risques majeurs seront donc, de toutes façons, exclus de l'analyse probabiliste.

La deuxième remarque est que, même pour les risques supportables, la grande majorité d'entre eux ne peuvent être décrits par une loi de probabilité qui puisse s'appliquer au contexte particulier rencontré dans une entreprise donnée.

Les risques matériels qui couvrent les accidents divers comme l'incendie, le dégât des eaux, la foudre, etc., sont dépendants des conditions géographiques régionales, pour lesquelles on pourra vraisemblablement trouver des éléments statistiques, mais également des conditions locales, voire de voisinage immédiat, pour lesquelles on ne pourra trouver, ni même établir, de base statistique.

Les pannes et dysfonctionnements de matériels et logiciels de base sont dépendants, pour une entreprise donnée, de multiples facteurs tels que les procédures de choix et de validation techniques, les politiques d'achat qui peuvent tenir plus ou moins compte de la qualité du fournisseur et de sa réputation ou au contraire ne s'attacher qu'au coût des produits, de la politique et des contrats de maintenance, de la qualification des produits avant mise en service, etc. Une statistique générale, établie pour un ensemble d'entreprises n'aura ainsi qu'un lointain rapport avec le contexte local.

Les erreurs, qu'il s'agisse d'erreurs de saisie, d'erreurs d'exploitation ou d'erreurs de conception et de réalisation, dépendent, elles aussi, d'un ensemble de paramètres techniques et des mesures qui ont été prises pour les enrayer ou pour éviter leur propagation, mais également d'un ensemble de paramètres psychologiques ou sociologiques guère probabilisables, comme le climat régnant dans l'entreprise, la motivation du personnel, les conditions de travail.

Enfin, toutes les catégories de dommages faisant appel à des actions humaines volontaires, vol, sabotage, fraude, détournement d'informations, grève ou départ de personnel, ne peuvent, bien sûr, être modélisées par une loi de probabilité.

Notre approche sera donc de remplacer cette probabilité, impropre à l'analyse de la sécurité de l'entreprise, par une notion de potentialité exprimant le caractère plus ou moins plausible d'une menace donnée. Nous analyserons ce concept en détail.

La potentialité d'un risque sera, au contraire, vue comme une caractéristique non mathématique et intuitive 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.

II. LES NIVEAUX DE POTENTIALITÉ

Nous avons vu qu'il y a de solides raisons pour ne pas retenir une approche probabiliste. Il faut, néanmoins définir des niveaux de potentialité.

Nous sommes, pour notre part, d'avis qu'un nombre limité de niveaux suffit à décrire la potentialité des scénarios, et nous avons retenu quatre niveaux : forte, moyenne, faible et insignifiante.

Il appartient à chaque entreprise de définir les scénarios qui lui semblent revêtir des caractères de forte potentialité, ou simplement moyenne, faible ou insignifiante, et c'est la raison pour laquelle il nous faudra analyser les facteurs qui interviennent dans cette potentialité, afin de guider l'utilisateur. C'est ce qui sera fait plus loin dans ce chapitre.

Les définitions ci-dessous sont générales et sont suivies d'exemples qui sont le plus souvent applicables dans un univers industriel concurrentiel normal. Les entreprises qui vivent dans un univers de concurrence exceptionnellement vive, dans des environnements particulièrement conflictuels, ou dans des zones géographiques à risque élevé doivent adapter les exemples à leur contexte propre.

Potentialité forte

Les scénarios à forte potentialité sont ceux dont on dira qu'ils font partie de la vie courante de l'entreprise, qu'en l'état actuel des mesures on ne peut être surpris s'ils se réalisent.

A titre d'exemple, la catégorie des scénarios à forte potentialité pourra comprendre ceux qui sont dus à l'action humaine motivée, voulue par intérêt et décidée, tant que les facteurs de dissuasion mis en place sont faibles ou inexistants.

Il peut en être ainsi, en particulier, de phénomènes de vol d'information à des fins de concurrence, voire de perturbations volontairement causées pour nuire à un concurrent et pour en tirer un profit.

Nous entrerons plus en détail dans la manière de prendre en compte les différents aspects de cette motivation et les freins que l'on peut susciter.

Disons simplement, à ce stade de la présentation, que nous considérerons souvent comme à forte potentialité les scénarios de concurrence déloyale (vol, détournement d'information), ou de malveillances (destruction de ressources, informations, matériel, ou logiciel) qu'un concurrent ou qu'une personne interne à l'entreprise peut mettre en œuvre sans grande difficulté et sans subir de préjudice, ou qu'il peut être tenté de mettre en œuvre en pensant pouvoir le faire en toute impunité.

Peuvent être considérés aussi comme à forte potentialité des scénarios qui sont complètement déterminés par une action humaine involontaire, comme une erreur commise par un employé dans le cadre de son travail, ou ceux qui résultent d'un geste de mauvaise humeur non prémédité.

Seront également inclus dans les scénarios à forte potentialité, ceux qui sont issus de jeux, tant qu'ils ne nécessitent pas de chance particulière, c'est à dire tant que le seul fait d'essayer procure une chance non négligeable d'aboutir.

Ainsi, en l'absence de mesures, l'activité de pirates, tentant de pénétrer un ordinateur via les réseaux de télécommunications, sera considérée comme à forte potentialité.

On trouvera également souvent, dans la catégorie des scénarios à forte potentialité, tels que nous les avons définis, des accidents ou phénomènes naturels prenant naissance à

l'intérieur de l'entreprise ou à proximité, tant qu'ils ne demandent pas, pour se manifester, de concours de circonstances particuliers.

Potentialité moyenne

Les scénarios à potentialité moyenne sont ceux dont on peut dire qu'ils ne font pas partie de la vie courante de l'entreprise, qu'éventuellement on n'a jamais connu de sinistre de ce type dans l'histoire de la société, mais dont on peut raisonnablement penser qu'il est néanmoins possible qu'un tel scénario se réalise dans un avenir, proche ou non.

Nous mettons souvent dans cette catégorie les accidents, événements naturels ou les erreurs qui demandent des « *concours de circonstances* », certes peu probables, mais réalistes.

Un contrôle indépendant, par exemple, peut laisser passer une erreur, c'est peut-être rare mais tout à fait possible.

Seront aussi souvent considérés comme des scénarios à potentialité « *moyenne* », sans cependant atteindre le niveau supérieur, les actes humains qui demandent à leur auteur d'entrer franchement dans l'illégalité et donc de prendre des risques, tels que celui de perdre leur emploi ou d'être poursuivi en justice, ou de devoir investir de manière significative en ressources personnelles, temps ou argent.

Notons seulement ici que la potentialité est réduite par la nécessité pour l'agresseur de « *payer* » soit par le temps qu'il va passer à déclencher le scénario, soit par l'investissement financier qu'il devra consentir, soit encore par la crainte à surmonter d'être découvert, et d'en subir des conséquences pénalisantes.

Nous considérerons enfin, dans cette catégorie, les scénarios de jeux mettant en œuvre une part de hasard telle que leur réussite nécessite un grand facteur chance.

Potentialité faible

Les scénarios à potentialité faible sont ceux que l'on considérerait comme exceptionnels mais qui demeurent possibles.

On mettra souvent dans cette catégorie les événements qui ne peuvent être réalisés que grâce à des concours de circonstances exceptionnels.

De grandes catastrophes avaient ainsi une potentialité faible, mais une somme de conditions se sont trouvées réunies pour faire que l'accident arrive néanmoins effectivement.

Les actes malveillants entreront souvent dans cette catégorie dès lors que le temps à passer ou le prix à payer sont sans commune mesure avec l'enjeu, ou dès lors que le risque, par exemple la sanction en cas de découverte n'est plus en rapport avec le gain espéré de l'action, et donc que tout individu raisonnable et averti éviterait même d'essayer de déclencher le scénario. La seule réserve rendant la potentialité non nulle est le caractère non raisonnable de certaines motivations qui font qu'en dépit de toute logique des hommes se lancent dans des actions qui seront dommageables tant pour eux que pour l'entreprise.

Potentialité insignifiante

Les scénarios à potentialité insignifiante sont ceux qui sont à la limite du possible, mais cependant « *imaginables* ».

Nous considérerons souvent qu'un scénario n'a qu'une potentialité insignifiante quand, outre ce qui a été dit pour la potentialité faible, les chances de réussite sont infinitésimales.

Il en serait ainsi, par exemple de vouloir rechercher et de trouver, par hasard, un mot de passe de douze caractères, changé dynamiquement et sans signification.

Nous assimilons une potentialité nulle à une potentialité insignifiante, ce qui veut dire que nous considérons qu'une potentialité n'est jamais totalement nulle.

III. LA POTENTIALITÉ ET LES FACTEURS DE RISQUE

Plusieurs facteurs sont susceptibles d'augmenter ou de diminuer, pour une entreprise donnée, la potentialité de certains scénarios.

Nous appelons ces facteurs des *facteurs de risque*.

On peut mettre en évidence ces facteurs, en analysant le processus de prise de décision d'action chez un agresseur humain, puis en élargissant les concepts aux cas d'erreurs ou d'accidents et, enfin, aux phénomènes naturels.

Si l'on reprend la partie haute du schéma relationnel que nous avons déjà présenté (fig. 1) en analysant de plus près les relations entre entités, on obtient le schéma de la figure ci-après.

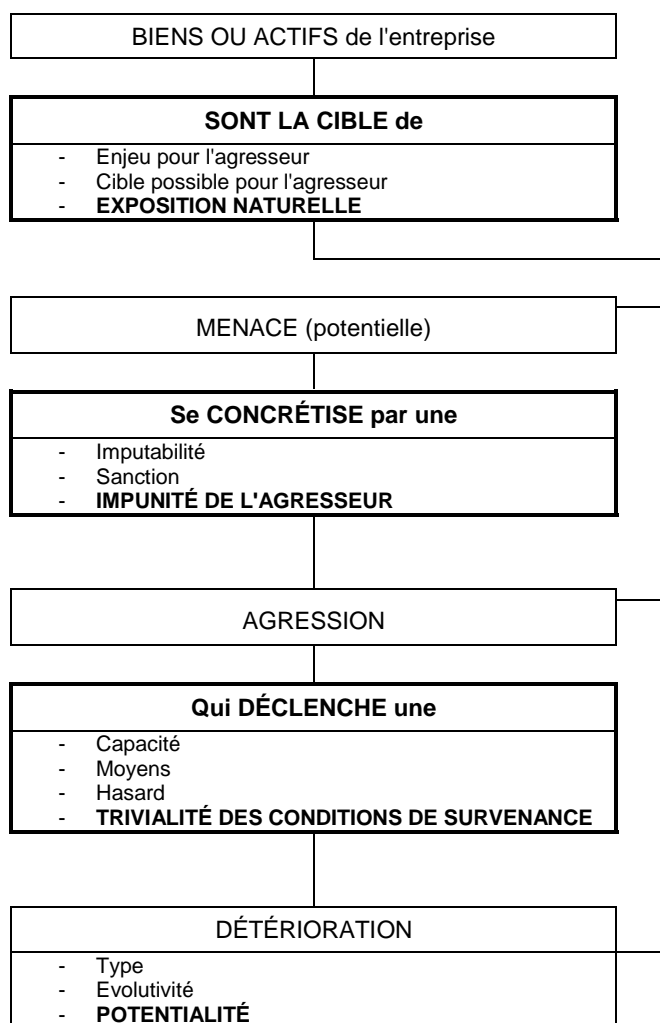


Figure 3

La première étape d'une agression volontaire correspond à la naissance de l'idée même de l'agression. Elle correspond, pour les actes ayant une volonté humaine à l'origine, à une certaine envie donc à un enjeu. Elle correspond aussi au choix de la cible, en l'occurrence l'entreprise.

La relation « *est la cible de* » qui associe une ressource de l'entreprise à une menace peut ainsi être caractérisée par différents facteurs dont l'un qualifie l'ampleur, le niveau, de cette relation et que nous appelons « *exposition naturelle* ».

Ce facteur vise à mettre en évidence 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.

Pour les agressions volontaires, la deuxième étape à prendre en compte correspond à l'analyse 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.

Nous caractériserons ce paramètre par un facteur de risque appelé « *impunité de l'agresseur* ». Ce facteur caractérise la relation qui fait se transformer une menace en une agression.

Le stade ultérieur, 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 les 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.

Plusieurs facteurs caractérisent la relation « *qui déclenche une* » associant l'agression à une détérioration. L'ensemble de ces facteurs que nous étudierons en détail est regroupé en un facteur de risque appelé « *trivialité des conditions de survenance* ».

En effet, notre approche sera la suivante : quels que soient les contrôles d'accès effectués et les mesures préventives mises en place, il existe toujours un moyen de les contourner ou un ensemble de phénomènes naturels ou de circonstances capable de rendre inefficaces les moyens de prévention. Il existe toujours des conditions, de niveau, de hasard, de compétence ou de moyens qui rendent possibles un scénario de risque.

Cependant plus ces conditions seront triviales, banales, plus potentiel sera le risque, alors que plus le niveau technique de la prévention s'élève et moins potentiel devient le scénario de sinistre. Tel est le sens de ce facteur qui reflète la trivialité des conditions à remplir pour que des détériorations soient la conséquence du scénario 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. Ce peut être par exemple un climat hostile rendant plus plausible un taux d'erreur élevé, une installation vétuste pouvant être à la source de courts-circuits électriques, etc.

Il n'y a pas pour les phénomènes purement naturels d'analyse ni de facteur de risque

correspondant à l'impunité de l'agresseur. Cependant, pour les erreurs humaines ou les accidents mettant en cause, soit directement une action humaine, soit indirectement une responsabilité humaine, l'entretien ou la surveillance par exemple, on peut considérer une impunité d'agresseur liée au risque de se voir imputer une négligence ou un laxisme.

La trivialité des conditions de survenance est, pour ces types d'agression, un facteur caractérisant une ampleur du phénomène, par exemple ampleur d'un incendie, ampleur d'une crue ou d'une inondation, taux d'erreur, etc.

Le schéma de la figure 3 est ainsi applicable à l'ensemble des agressions ayant pour origine des êtres humains, alors que pour des événements purement naturels il devient le schéma de la figure 4, ci-après.

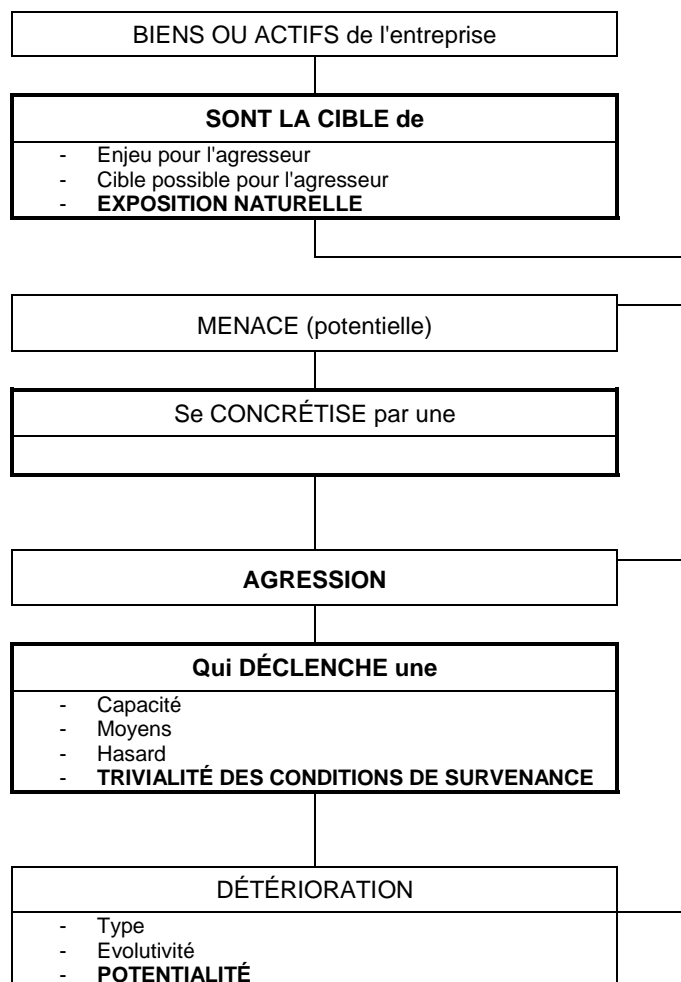


Figure 4

Nous allons maintenant revenir plus en détail sur ces trois facteurs de risque ayant une influence sur la potentialité.

L'EXPOSITION NATURELLE

Nous avons vu apparaître, lors de la description des niveaux de potentialité et dans l'introduction ci-dessus, une distinction entre des facteurs renforçant la potentialité, tel que l'intérêt d'une agression pour celui qui la commet, et des facteurs venant limiter cette potentialité, tel que le risque de se faire découvrir.

Nous appellerons « *exposition naturelle* » tout ce qui fait que l'entreprise est plus ou moins exposée à la naissance même de l'événement qui sera à l'origine du risque considéré.

S'il y a à l'origine de la menace un être humain, il s'agira effectivement de l'attrait que représente l'attaque de l'entreprise pour l'agresseur, du bénéfice qu'il en attend, indépendamment des difficultés qu'il pourra rencontrer dans la réalisation de la menace.

S'il s'agit d'un phénomène non volontaire, on exprimera par là tout ce qui fait que ce phénomène atteint cette entreprise plutôt qu'une autre, ou tout ce qui fait que l'événement initial, erreur, accident ou phénomène purement naturel, peut survenir naturellement dans l'entreprise.

Il s'agit donc des facteurs qui vont déterminer le début de l'action, son déclenchement.

Deux paramètres doivent être pris en compte pour analyser ce facteur de risque.

L'enjeu

On considérera comme plus potentiels des scénarios qui, toutes choses égales par ailleurs, sont susceptibles d'apporter un avantage à leur auteur. Ainsi à chaque fois qu'il y a un enjeu, de quelque ordre que ce soit, il y a un renforcement de la potentialité.

L'enjeu peut être financier, comme dans les détournements de fonds, il peut être psychologique, c'est le cas des virus développés et diffusés par jeu ou des malveillances faites par vengeance envers un collègue ou la société, il peut être concurrentiel et c'est tout le domaine du détournement d'information, technique, commerciale ou autre, ou celui du sabotage, commandité ou non.

Le ciblage

Pour analyser l'importance de l'exposition naturelle, il ne suffit pas de regarder l'enjeu que peut représenter, pour l'agresseur, l'aboutissement du scénario envisagé, il faut tenir compte du choix qu'a l'agresseur quant à la cible.

L'entreprise peut représenter une cible privilégiée, voire unique, et la motivation d'attaquer cette entreprise sera forte, si l'enjeu lui-même est important. Si, au contraire, l'entreprise ne représente qu'une cible parmi les autres, la motivation d'attaquer cette entreprise particulièrement ne sera peut-être que moyenne, voire faible.

En ce qui concerne les événements et phénomènes naturels, où l'on ne peut parler d'enjeu, le ciblage représentera la plus ou moins grande exposition de l'entreprise à ces risques.

On pourra ainsi, par exemple, consulter les statistiques météorologiques pour estimer si telle entreprise est située dans une région où il y a fréquemment des tornades violentes, auquel cas on attribuera, par l'intermédiaire du paramètre « *ciblage* », un facteur d'exposition naturelle fort pour les scénarios de dégâts dus à de telles conditions atmosphériques.

On pourra, de même, vérifier s'il n'existe pas de conditions aggravantes qui feraient

considérer que l'entreprise est plus exposée que la moyenne à tel type de risque, ou, au contraire, de conditions favorables diminuant son exposition au risque considéré.

Le facteur que nous considérons là est donc destiné à refléter combien l'entreprise, le site ou une partie de ce site, sont naturellement exposés au scénario de risque considéré, et dans quelle mesure ils représentent une cible particulière pour le type d'agression, que l'origine en soit un être humain ou qu'il s'agisse de phénomènes naturels.

NIVEAUX D'EXPOSITION NATURELLE

Exposition naturelle forte

Une exposition naturelle forte sera souvent associée à des contextes difficiles.

Ainsi, l'entreprise peut avoir une forte exposition naturelle aux malveillances internes, en fonction du climat social.

L'enjeu est, le plus souvent, de nature psychologique, et peut être considéré comme moyen, en général, mais peut varier dans le temps. En période de conflit social l'enjeu peut devenir très fort. Le ciblage, lui, est toujours très fort : c'est l'entreprise parce que c'est là que l'auteur travaille, et parce que l'auteur utilise, en général, les outils mis à sa disposition par l'entreprise dans le cadre normal de travail.

L'entreprise peut également être fortement exposée à des dégradations et à des actes de sabotage, si ses locaux sont situés dans une zone où il y a fréquemment des dégradations causées par des voyous, même si ces dégradations ne sont pas ciblées.

On pourra également attribuer une forte exposition naturelle à certains sinistres volontairement perpétrés par des personnes peu au courant du fonctionnement interne de l'entreprise, s'il apparaît que celle-ci a des raisons de penser qu'elle peut être spécialement visée, par exemple parce qu'elle occupe une place de leader dans un secteur particulièrement concurrentiel. C'est tout le domaine de l'espionnage industriel et les entreprises qui possèdent des avantages concurrentiels notables ou des positions privilégiées, dont la teneur est contenue dans des informations, sont, bien sûr, très exposées à ce que des concurrents cherchent à les obtenir par des moyens illicites.

On peut également attribuer un niveau de forte exposition naturelle quand il s'agit d'actions menées par des anciens collaborateurs de l'entreprise, qui en connaissent parfaitement les rouages et qui savent où trouver l'information.

Enfin, on considérera les sinistres dus à certaines catastrophes naturelles, si l'entreprise y est « *naturellement* » exposée. Cela sera particulièrement le cas dans des situations de carence d'entretien, d'organisation ou, plus généralement, à chaque fois que le contexte ou l'environnement du site favorise la naissance de l'événement à l'origine du sinistre.

Exposition naturelle moyenne

On considérera tout d'abord les erreurs ou les accidents involontaires causés par le personnel de l'entreprise, dans un contexte normal. L'exposition naturelle est en effet réduite par rapport au cas précédent par le manque d'enjeu, sauf climat ou environnement spécialement défavorables.

Une exposition naturelle moyenne sera également attribuée à des sinistres dont les auteurs sont extérieurs à l'entreprise et qui n'ont pas de raisons particulières de choisir l'entreprise comme cible.

Il peut s'agir de la concurrence, en particulier pour tous les sinistres mettant en cause la confidentialité, mais aussi de sabotages ou d'agressions faits par des voyous ne faisant pas partie du voisinage immédiat de l'entreprise. Le terrorisme sera généralement exclu de ce niveau.

On considérera le plus souvent comme étant de niveau d'exposition naturelle moyen la plupart des catastrophes naturelles ou accidents divers non directement causés par des personnes de l'entreprise.

Certains sinistres, enfin, sont décrits comme des failles d'organisation. Nous considérerons souvent que le niveau d'exposition naturelle est moyen quand on pourra penser que ce genre de dysfonctionnement peut exister dans l'entreprise et que le scénario n'est pas susceptible d'apporter à son auteur un avantage particulier.

Exposition naturelle faible

On classera à ce niveau, soit des catastrophes naturelles hautement improbables telles que glissement de terrains, ou secousses sismiques (sauf en certaines régions), soit des scénarios réclamant des concours de circonstances tout à fait exceptionnels, soit les actes malveillants nécessitant un fort degré de professionnalisme comme le terrorisme, l'espionnage par des espions de puissance étrangère, etc.

Les accidents ou erreurs ne seront qu'exceptionnellement classés à ce niveau, dans les cas où on pourra considérer qu'il existe sur le site examiné un très haut degré de professionnalisme et de motivation.

Exposition naturelle très faible ou réduite

On classera à ce niveau des situations pour lesquelles l'entreprise a mis en œuvre des mesures spécifiques, comme, par exemple, la fragmentation des informations, la recherche de l'anonymat, la non publication de résultats positifs, la mise en place de plans de motivation, de plans de carrières ou de contrats de travail contenant des clauses particulières, etc.

L'IMPUNITÉ DE L'AGRESSEUR

Le deuxième facteur venant jouer sur la potentialité est un facteur lié à l'existence ou non de moyens de dissuasion capable de venir freiner l'envie qu'un agresseur peut avoir de mettre à exécution une menace.

A chaque fois que l'auteur du scénario est un être humain, le risque encouru est un facteur de diminution de la potentialité. Le sentiment d'impunité est, au contraire, un facteur de risque augmentant la potentialité.

Il faut remarquer que les contrôles d'accès ne pouvant, à l'évidence, qu'empêcher les accès non autorisés, la seule manière de freiner une action malveillante d'une personne autorisée à accéder à l'information est de faire que cette action représente un risque suffisamment dissuasif.

Le plus souvent, il s'agit du risque d'être découvert et reconnu comme l'auteur d'une malveillance, avec des conséquences qui vont de la honte d'une réprobation publique, au licenciement, voire aux actions pénales.

Les auteurs de scénarios de menace sont, en effet, souvent des personnes fort respectables dans la vie civile qui n'ont pas véritablement basculé dans l'illégalité et que le risque d'être

découverts fera beaucoup réfléchir.

On fera attention, dans l'estimation de la potentialité, au fait que, quand on parle de l'impunité de l'agresseur, on parle de la perception qu'il en a et non de ce qui lui arriverait dans la réalité. Ainsi avons nous vu et rencontré des employés qui avaient détruit intentionnellement des fichiers en ignorant les sanctions qu'ils risquaient et qui ne l'auraient pas fait en connaissance de cause.

Nous parlerons par la suite de l'impunité de l'agresseur, sans distinguer le risque réel du risque perçu par l'agresseur, laissant au responsable de l'évaluation la responsabilité de corriger l'estimation faite, s'il estime qu'entre la réalité et ce qui est ressenti, il y a un écart notable.

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, et par les conséquences qui peuvent en découler pour l'auteur lui-même.

L'imputabilité de l'action à son auteur

L'imputabilité de l'action à son auteur demande que soient réalisées plusieurs conditions.

La première est qu'il y ait effectivement moyen d'identifier l'auteur par des moyens généralement constitués de traces et d'enregistrements : enregistrement du passage physique par une porte équipée d'un lecteur de badge, enregistrement du login dans un système, etc.

La deuxième condition est que cette identification soit sûre. En effet, la possibilité de se retourner contre l'agresseur, de le punir, sera nulle s'il peut démontrer que n'importe qui a pu usurper son identité. Ce sera le cas, par exemple, si l'authentification ne repose que sur un mot de passe et si celui-ci peut être très court ou si les locaux sont des open spaces dans lesquels la discrétion de la frappe du mot de passe ne peut être assurée.

Les sanctions et conséquences de la découverte de l'action

Il n'y aura risque pour l'agresseur que s'il y a effectivement des sanctions prises à son égard s'il est découvert.

Ce facteur est important car il met en évidence qu'un pirate individuel agissant de l'extérieur n'encourt en pratique qu'un risque faible. En effet, l'entreprise attaquée n'aura guère de moyens d'action : elle refusera souvent de porter plainte pour ne pas faire de publicité à un état de vulnérabilité qui peut être critique et elle n'a pas grand chose à attendre en réparation d'un préjudice qu'elle aura d'ailleurs du mal à évaluer, et encore plus à justifier.

NIVEAUX D'IMPUNITÉ DE L'AGRESSEUR

On peut classer l'impunité de l'agresseur en quatre niveaux, en se posant la question suivante: quelles sont les conséquences pour l'agresseur si son action est détectée ?

Impunité très forte (ou risque insignifiant)

A ce niveau les conséquences directes ou indirectes pour l'agresseur, en cas de découverte de l'action, sont nulles ou insignifiantes.

Ceci veut dire, soit que l'action est complètement anonyme, soit que les possibilités de remonter jusqu'à l'auteur sont extrêmement faibles.

Cela sera, en particulier, le cas pour toutes les tentatives d'intrusion dans un système informatique à partir du réseau téléphonique standard ou via Internet, en notant que c'est aussi le cas des points d'accès vidéotex au réseau Transpac (PAVI), qui étaient effectivement les moyens les plus utilisés, avant Internet, car les plus « *discrets* ».

Il en sera de même, à l'intérieur de l'entreprise, pour les accès via les réseaux locaux, s'il n'y a aucune procédure de « *trace* » permettant de remonter à l'auteur d'une connexion et de garder une trace de son activité, par la journalisation de son identification ou de celle de son poste de travail et d'un résumé de ses sessions.

Le risque sera également insignifiant s'il n'y pas de moyen d'authentification crédible ou si l'authentification ne concerne que le poste de travail et non la personne qui est derrière.

Impunité moyenne (ou risque moyen)

On peut caractériser une impunité moyenne par une probabilité faible, mais non nulle, d'être découvert et par l'existence de conséquences faibles ou passagères pour l'auteur de l'action s'il est découvert.

Ceci veut dire qu'il y a un moyen de remonter à l'auteur, mais que cela n'est pas certain et qu'il peut espérer y échapper et que, s'il est découvert malgré tout, les conséquences de cette découverte ne vont pas modifier profondément sa vie professionnelle ou familiale.

Le risque d'être découvert concerne, par exemple, le fait de rentrer dans un bureau ouvert et d'y dérober quelque chose ou d'y effectuer une action rapide comme de faire une copie d'un fichier sur une disquette. Il y a risque car présence physique et donc possibilité que le propriétaire du bureau survienne et demande des explications, mais en choisissant une heure tardive ou très matinale, le risque peut être considéré comme faible.

Quant aux conséquences, s'il s'agit d'un salarié de l'entreprise, le risque ne sera que moyen s'il persiste un doute ou si une explication peut être avancée : même si personne n'y croit, il ne restera que de la suspicion sans véritable risque de sanction immédiate.

Impunité faible (ou risque fort)

On peut caractériser une impunité faible par comparaison avec une impunité moyenne en notant que ce qui différencie l'impunité faible est que l'un des facteurs a changé : soit le risque d'être découvert est faible et les conséquences graves mais supportables, soit le risque d'être découvert est fort mais les conséquences faibles.

Dans le cas évoqué de la pénétration dans un bureau, le risque sera fort si l'action demande en outre un acte non équivoque comme le forçage d'une serrure. L'action sera qualifiée comme délictueuse et les sanctions pourront être graves.

Dans le cas d'une action faite après avoir pénétré un système sous sa propre identité, avec une probabilité forte que des traces aient été enregistrées, le risque ne sera que fort si les conséquences peuvent être faibles, si la cause est plaidable. Par exemple, le jeu peut être invoqué comme circonstances atténuantes ou le défi, ou la simple curiosité, sans intention de nuire à la société. Sauf récidive les conséquences seront très souvent limitées à une réprimande ou à un avertissement sans conséquence immédiate grave.

Il en va de même pour un attaquant extérieur, tant que les moyens mis en œuvre restent compatibles avec la plaidoirie du jeu, et en l'état actuel de la législation et de la jurisprudence.

Il faut d'ailleurs remarquer que la législation et la jurisprudence, qu'il s'agisse de celles de l'État ou du règlement intérieur de l'entreprise, influent très directement sur ce facteur de risque.

Impunité insignifiante (risque très fort)

L'impunité sera considérée comme insignifiante quand la probabilité que l'agresseur soit découvert est très forte et que les conséquences qui en découleraient sont durables, de sorte qu'il faille véritablement être inconscient pour tenter l'action.

Outre donc la quasi certitude que l'action sera découverte et imputée à son auteur, il y aura un niveau de risque très fort pour l'agresseur et aucune impunité à espérer si les conséquences peuvent être une condamnation pénale, ou la perte d'emploi avec licenciement pour faute grave.

Si c'est une entreprise qui est l'auteur d'une agression, le risque sera généralement très fort de se voir condamner, s'il y a possibilité de remonter jusqu'à elle, ce qui est généralement le cas si elle a mandaté ou financé quelqu'un pour faire l'action.

LA TRIVIALITÉ DES CONDITIONS DE SURVENANCE

Par opposition à l'exposition naturelle, sur laquelle l'entreprise agit davantage par des mesures d'organisation, il existe de nombreux facteurs techniques visant à empêcher l'agression de provoquer des détériorations.

Cependant, ces moyens n'étant pas parfaits, ils ne pourront que réduire la potentialité du risque considéré pour l'entreprise, sans l'annuler complètement.

Ceci étant, ce qui va jouer sur la vulnérabilité de l'entreprise, et en particulier sur la potentialité du risque, c'est la possibilité, pour une agression d'un type donné, d'outrepasser les contrôles d'accès ou les moyens de prévention installés. Cette possibilité dépend du niveau des mesures de prévention. Plus ce dernier est augmenté et plus il faudra de conditions pour que l'agression, ou l'agresseur, puisse aboutir. Les mesures de prévention sont ainsi des mesures destinées à augmenter le niveau des conditions nécessaires pour qu'une agression puisse déclencher des détériorations.

Il est clair que, pour certains types d'agressions, en particulier celles dont les auteurs sont des sujets autorisés, personnes ou processus, il est impossible de jouer sur ce facteur et que le seul facteur sur lequel l'entreprise puisse agir est l'impunité de l'agresseur.

Ce sont donc les possibilités d'atteintes non autorisées ou non prévues des ressources qu'il faut analyser à ce niveau.

Ces possibilités vont dépendre de trois paramètres.

La capacité (requis)

La capacité qualifie le fait que l'agresseur doit être « *capable* » de mener à bien le scénario d'agression.

Pour des agresseurs humains, il s'agira le plus souvent de compétences, c'est-à-dire de savoir-faire technique, et de connaissances du site ou du système d'information.

Pour pouvoir pénétrer un système d'information par les réseaux de télécommunications, il faut à la fois des compétences informatiques, en réseaux et sur le système d'exploitation à pirater, et un minimum de connaissances sur le site visé, par exemple une adresse IP. Ceci étant, plus des mesures de sécurité préventives seront prises, plus il faudra être spécialiste, voire expert, pour réussir.

On place ainsi sous cette rubrique, pour les agresseurs humains, aussi bien le niveau requis de connaissance théorique, et donc de compétence, que de connaissance pratique de l'entreprise.

Pour les événements naturels, la capacité requise représente un niveau dans la hauteur des obstacles que l'agression est capable de franchir.

Ainsi, un incendie débutant, de faible capacité, ne sera pas capable de franchir une zone antifeu de dix mètres, alors qu'un feu de forêt bien démarré a cette capacité.

On place ainsi sous cette rubrique, pour les événements naturels, tout ce qui peut ressembler à une capacité de nuisance, en commençant par l'énergie emmagasinée ou disponible sous une forme quelconque, chaleur, masse, énergie cinétique, énergie électromagnétique, etc.

Les moyens (à mettre en œuvre)

Les moyens à mettre en œuvre 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.

Une autre manière de voir les moyens requis est d'en exprimer le coût. Moins le coût sera élevé et plus triviales seront les conditions requises et donc plus forte sera la potentialité. Cependant, les coûts ne sont relatifs qu'à des auteurs humains et pour les actes volontaires alors que la notion de moyens est plus générale car applicable aussi bien aux erreurs et aux accidents.

Pour les erreurs, en effet, les moyens sont ceux mis à la disposition du personnel pour l'exercice normal de son métier.

Pour les accidents, les moyens représentent tout ce qui est dans l'entreprise et qui va permettre à l'incident initial de se développer, depuis son déclenchement jusqu'au début des détériorations. Ainsi, pour un incendie, les moyens sont-ils toutes les matières combustibles qui permettent à un court-circuit, par exemple, de devenir un foyer d'incendie puis de se propager jusqu'à une ressource. Pour les dégâts des eaux, les moyens sont la gravité, les plans inclinés, les dénivelés, les joints d'étanchéité défectueux, etc.

Pour les malveillances, les moyens sont les droits d'accès accordés aux utilisateurs autorisés ou les moyens d'obtenir ces droits pour les personnes non autorisées.

Les moyens sont toutes les ressources qui doivent être disponibles pour que le scénario d'agression puisse être développé en entier.

Ce paramètre vise donc à mettre en évidence que plus triviaux seront les moyens requis, plus forte sera la potentialité.

Le hasard

Certains scénarios mettent en cause un facteur « *chance* ».

Il en est ainsi, par exemple, quand la réussite d'une tentative d'accès à un ordinateur dépend de la découverte d'un élément secret, un mot de passe, ou de l'occurrence d'événements gouvernés par le seul hasard.

Plus triviaux seront les mots de passe, plus forte sera la potentialité.

NIVEAUX DE TRIVIALITÉ DES CONDITIONS DE SURVENANCE

Les niveaux de trivialité des conditions de survenance dépendent directement des capacités et moyens nécessaires à l'accomplissement de l'agression à l'origine du sinistre.

Nous définissons les « *niveaux de trivialité* » par le niveau de capacités et de moyens nécessaires pour accéder à l'information ou à la ressource considérée, pour la dérober, la copier, la modifier ou la détruire.

On notera que parler de conditions de survenance revient à parler de catégories d'agresseurs, certaines catégories ayant la possibilité, c'est à dire les capacités et les moyens, d'accéder à la ressource ou à l'information, d'autres catégories n'ayant pas cette possibilité. Nous reviendrons plus en détail sur ces catégories d'agresseurs, et nous nous contenterons ici de décrire brièvement les niveaux de trivialité de conditions d survenance.

Forte trivialité des conditions de survenance (ou conditions de survenance standard)

Un fort niveau de trivialité correspond à des conditions de survenance standard et signifie qu'il est possible d'accéder à la cible du scénario de sinistre sans moyens spécifiques ni capacités particulières.

C'est le cas général pour les utilisateurs autorisés, qui peuvent accéder aux informations pour lesquelles ils ont l'habilitation, sans compétences autres que celles nécessaires à l'accomplissement de leur travail, ni moyens autres que ceux mis à leur disposition par l'entreprise.

Pour les personnes non autorisées, ce niveau de conditions autorise le déroulement du scénario si l'accès est possible avec très peu de moyens, à condition de le vouloir. C'est le cas si les contrôles d'accès sont absents, ineffectifs ou faciles à violer ou s'il suffit d'être un « *initié* » pour le contourner. Ainsi, une authentification simple par mot de passe dans un open space ne résistera pas à celui qui prend soin de regarder une personne autorisée se connecter et de mémoriser son mot de passe.

On placera également à ce niveau les capacités de propagation d'une catastrophe naturelle comme un incendie ou un dégât des eaux, en l'absence de toute barrière à la propagation de tels accidents.

Trivialité moyenne des conditions de survenance (ou conditions de survenance non standard)

Ce niveau de conditions de survenance est caractérisé par des capacités au dessus du niveau standard, et par des moyens facilement disponibles, mais qui ne sont pas d'un usage généralisé.

A ce niveau, l'accès non autorisé ou imprévu peut provenir de personnes averties, connaissant l'entreprise et ayant une certaine technicité, disons celle d'un bon professionnel. Cependant, ces conditions peuvent encore être remplies par un grand nombre de personnes, internes ou non à l'entreprise.

Certains utilisateurs, connaissant à fond les applications auxquelles ils ont accès atteignent ce niveau de force. Ils seront donc à même de trouver des failles éventuelles leur permettant d'accéder à des informations pour lesquelles ils ne sont pas habilités, c'est ce que nous appelons l'abus de droits.

Au niveau des catastrophes naturelles, il existe des moyens de protection standard, qui peuvent, dans certaines circonstances, ne pas suffire à empêcher le sinistre. Un incendie de force moyenne ne sera pas circonscrit par un simple extincteur mais le sera par une lance de pompier.

Faible trivialité des conditions de survenance (ou conditions de survenance rares)

Les moyens de prévention, à ce niveau, sont sérieusement établis et contrôlés, avec un bon niveau de professionnalisme. Par exemple, l'accès aux systèmes d'information est protégé par des mots de passe qui ne sont pas triviaux et qui ont une longueur suffisante. Cependant il reste des failles, que les meilleurs spécialistes de la branche d'activité connaissent, et qui permettent l'intrusion. Ce niveau de capacité est donc caractérisé par des compétences très sérieuses et spécialisées, qui dépassent le niveau d'un professionnel courant. Des compétences multiples sont nécessaires à ce niveau.

Ce niveau est également requis si la réussite de l'agression demande des moyens spéciaux dont ne disposent pas habituellement des professionnels ou des moyens très onéreux.

Dans le domaine des catastrophes naturelles, les événements ont atteint une telle ampleur que des moyens exceptionnels peuvent être nécessaires pour stopper l'évolution de l'agression avant les détériorations.

On attribuera aussi ce niveau trivialité à des agressions nécessitant des circonstances exceptionnelles pour aboutir.

Très faible trivialité des conditions de survenance (ou conditions de survenance exceptionnelles)

Ce niveau est nécessaire quand tout ce qui est possible, dans le contexte industriel, a été fait, quand le meilleur niveau de protection qui ne soit pas réservé aux autorités gouvernementales est implanté.

Mais, dans le domaine de la sécurité logique, cette force peut être atteinte par les meilleurs experts mondiaux qui connaissent quelques failles non encore dévoilées.

Au niveau des moyens, on est là au plus haut niveau de sophistication, donc à un niveau où les seuls agresseurs possibles sont financés par des groupes industriels extrêmement puissants ou par des puissances étrangères.

Dans le domaine de la sécurité physique, des moyens existent encore de forcer les barrages installés, par exemple en faisant appel à des artificiers et en usant d'explosifs.

IV. LA POTENTIALITÉ ET LES PROFILS D'AGRESSEURS

On a été amené à distinguer, dans les paragraphes précédents, les malveillances et actes volontaires effectués, d'une part par des personnes autorisées, et d'autre part par des personnes non autorisées, les erreurs ou accidents et les phénomènes naturels.

Les malveillances sont faites par des auteurs humains en fonction de l'enjeu que cette malveillance représente pour eux, en dépit des risques, parce qu'ils ont choisi l'entreprise comme cible, parce qu'ils ont les capacités pour le faire et qu'ils y ont mis les moyens.

Les erreurs ou accidents sont à la base d'un scénario de menace parce qu'ils sont faits par

des êtres humains, parce que l'enjeu de qualité n'était pas suffisant ou que le risque personnel lié à l'erreur était insuffisant ou mal ressenti et parce qu'ils en avaient la capacité.

Les phénomènes naturels ne mettent en cause ni enjeu ni risque, puisqu'il n'y a pas d'individu, mais atteignent l'entreprise parce qu'elle était particulièrement exposée, se développent en profitant des moyens offerts par le site et en fonction de leur capacité naturelle.

En résumé, on a vu ainsi apparaître :

- des facteurs de risque préexistants sur le site ou dans l'entreprise, que nous regroupons sous l'appellation de : « *exposition naturelle* »,
- un facteur de risque lié à l' « *impunité de l'agresseur* » sur lequel nous verrons que l'entreprise peut jouer, par des mesures dissuasives, contre des sinistres déclenchés par des personnes,
- des facteurs de risque liés aux conditions de capacité, de moyens ou de chance nécessaires pour accéder aux ressources que nous regroupons sous l'appellation « *trivialité des conditions de survenance* », et sur lesquels l'entreprise peut agir, par des mesures préventives, pour diminuer la potentialité des détériorations.

La potentialité du scénario de sinistre, que nous cherchons à évaluer, est donc l'expression de la potentialité qu'une agression, d'origine humaine ou non, rassemble les conditions requises pour accéder à la cible du sinistre, que l'agresseur en prenne le risque s'il s'agit d'un être humain, tout ceci compte tenu de l'exposition naturelle de l'entreprise à ce sinistre.

Ceci fait donc apparaître une notion fondamentale de niveau d'agresseur. Nous reviendrons au chapitre 7 sur les profils d'agresseurs, mais on doit tout de suite remarquer que la potentialité est essentiellement une potentialité d'un type d'agresseur qui est caractérisé par le penchant naturel qui va le pousser à attaquer l'entreprise, par le niveau de capacité et de moyens qu'il va être capable de mettre en œuvre afin d'outrepasser le filtrage des accès, et par le niveau de risque qu'il va accepter d'assumer.

V. ÉVALUATION DE LA POTENTIALITÉ

L'analyse des facteurs de risque, en se référant aux définitions des différents niveaux de chaque facteur, est une première étape de l'évaluation de la potentialité.

Cette analyse permet, dans un premier temps, de se faire une idée des conditions de réalisation du risque.

On pourrait, à ce stade, évaluer globalement la potentialité, de manière intuitive mais raisonnée, en fonction des facteurs de risque.

On obtient, en pratique, une bien meilleure reproductibilité du raisonnement en construisant des grilles d'analyse qui permettent de passer des facteurs de risque à une évaluation de la potentialité.

Ces grilles dépendent des types d'agresseurs et on en construira donc plusieurs selon qu'il s'agit de malveillances, d'erreurs, d'accidents ou d'événements naturels.

Chapitre 5

L'IMPACT

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 tels qu'ils ont été définis au chapitre 2.

I. L'IMPACT DES DÉTÉRIORATIONS ET DES DYSFONCTIONNEMENTS

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.

Évaluer l'impact des détériorations revient à estimer le coût des restaurations.

Évaluer l'impact des dysfonctionnements de l'entreprise, revient à déterminer la gravité de l'ensemble des conséquences d'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'une des ressources constituant le système d'information.

Nous allons donner un certain nombre d'indications permettant de faire cette évaluation dans de bonnes conditions et mettre en évidence, de même que pour la potentialité, des facteurs de risque caractéristiques et déterminants.

QUELQUES NOTIONS INSTINCTIVES

Nous pouvons faire une comparaison avec le monde de la santé où il est courant de parler de gravité pour qualifier une maladie ou un accident.

Parler de maladie très grave veut le plus souvent dire que les chances de survie sont faibles, voire nulles. Une maladie grave sera assimilée à une atteinte mettant les jours en danger avec des chances réelles de s'en sortir, une maladie bénigne n'inquiète personne, bien que les complications soient toujours possibles mais peu probables.

Les divers scénarios que nous avons en tête, par référence à nos souvenirs, sont des

scénarios ayant une issue fatale, ou ayant conduit à une hospitalisation de longue durée, ou plus bénins, etc.

Dans le domaine des accidents, la brutalité de l'événement conduit à des qualificatifs légèrement différents.

L'accident mortel sera qualifié comme tel. L'accident très grave signifie souvent que les séquelles seront définitives et d'une certaine importance.

Dans ces deux exemples, on se réfère à une notion de performance, en l'occurrence la santé tant physique qu'intellectuelle. C'est la performance résiduelle du corps humain, après guérison qui détermine l'échelle de gravité.

On pourra aussi, au sein de l'entreprise, se référer à sa performance, celle-ci dépendant d'un système de valeurs qui lui est propre.

On pourra ainsi parler de performance commerciale, technique, financière, etc.

Ce qui compte, c'est de trouver l'échelle de performance la plus représentative du scénario de sinistre, et d'évaluer ensuite l'impact du sinistre sur l'entreprise, en fonction de cette échelle.

Un autre aspect, tout aussi instinctifs est qu'il existe, dans l'entreprise comme dans le monde de la santé, des facteurs de risque et que plus ces facteurs de risque sont importants, plus le risque doit être considéré comme important. Certains de ces facteurs sont liés à la potentialité du risque et ont été abordés dans le chapitre correspondant. D'autres, au contraire, sont liés aux conséquences du risque et à son impact. Nous reviendrons dessus dans ce chapitre.

UN NOMBRE LIMITÉ DE NIVEAUX DE GRAVITÉ

Il ne faut pas attribuer à la notion de gravité une valeur scientifique, mais prendre conscience qu'il ne s'agit que de la valeur relative des choses et d'ordre de grandeur.

Partant, le nombre de niveaux de gravité doit être limité et il suffit de distinguer ce que l'on considère comme extrêmement grave, très grave, moyennement grave et peu grave, soit quatre niveaux :

extrêmement grave

très grave

moyennement grave

peu grave

Ceci étant, la détermination de l'impact d'un ensemble de scénarios revient à une suite de comparaisons entre des « accidents » qui, pris deux à deux, peuvent être comparés et pour lesquels la question que l'on souhaite poser est : « A tout prendre, lequel préférerais-je encore ? ».

On peut alors supposer que l'accident le plus redouté peut être considéré comme plus grave et réciproquement et qu'en comparant deux à deux tous les accidents possibles, on arrivera à les ordonner, donc à déterminer une échelle de gravité des conséquences de chaque scénario de menace.

LA RELATIVITÉ DE L'ÉVALUATION DE L'IMPACT

Que la cotation, ou que la détermination de la gravité de l'impact soit faite par un individu ou par un groupe d'individus (commission d'évaluation), il faut admettre la relativité de cette action.

Ce que nous appelons relativité est le fait que ce ne soit pas une échelle absolue qui est recherchée mais une échelle qui reflète la personnalité de l'entreprise.

Il s'agit bien de refléter l'entreprise et tout un travail de préparation ou de discussion pourra être nécessaire pour atteindre un véritable consensus, s'il s'agit d'un groupe d'individus, sur les valeurs essentielles de l'entreprise. Ceci ne veut pas dire que la cotation ne dépende pas, pour une faible part, des individus qui la font.

Non seulement il faut l'admettre mais il convient de reconnaître la valeur de cette relativité.

Cela veut dire que, comme nous le disions plus haut, les échelles de performance sont nombreuses et se réfèrent, plus ou moins explicitement, à des échelles de valeur de l'individu ou de l'entreprise.

Pour certains la perte d'argent sera négligeable devant une perte d'honneur, pour d'autres ce sera l'inverse, mais il appartient bien à chacun de déterminer quelles valeurs sont essentielles, primordiales.

De même, l'entreprise se doit de déterminer son échelle de valeur qui se traduira en échelles de gravité de sinistre pour les menaces considérées.

Ainsi, certaines entreprises pourront considérer qu'un mécontentement durable du personnel, suite à l'occurrence d'un sinistre, serait très grave alors que d'autres considéreront cela comme peu grave, voire sans importance.

Ceci étant, il faudra, pour ces valeurs, déterminer les atteintes que l'on considère comme extrêmement graves, très graves, moyennement graves ou peu graves, c'est-à-dire déterminer les seuils correspondants.

Là encore, on retrouvera le principe de relativité et il ne faudra pas rechercher des valeurs absolues mais des ordres de grandeur et s'appuyer sur des objectifs définis par la Direction Générale.

II. NIVEAUX D'IMPACT

Les définitions évoquées précédemment en termes de gravité peuvent ne pas être suffisantes pour exprimer clairement la relation entre un type de conséquence et un niveau de gravité et pour que cette relation soit comprise de manière unique dans l'entreprise.

Il faut donc donner quelques indications complémentaires pour aider à établir cette relation.

Les indications ci-dessous sont données à titre d'exemple, voire de recommandations, étant entendu que ces précisions doivent faire l'objet d'un accord formel au sein de l'entreprise et que des seuils de gravité d'impact chiffrés sont une aide supplémentaire à ne pas négliger.

Impact extrêmement grave

On réserve habituellement ce niveau à des sinistres tels que l'avenir de la société puisse être remis en cause, ou du moins celui d'une de ses parties essentielles, telle qu'une division, une filiale, etc.

Si un seuil de pertes financières doit être fixé, ce qui est souhaitable, il correspond généralement à un niveau de pertes tel que l'indépendance de l'entreprise puisse être menacée, en particulier par une baisse notable du cours de l'action, pour une société cotée, autorisant une OPA hostile ou tel que les actionnaires puissent exiger une évolution notable de la stratégie de l'entreprise.

Ce niveau de conséquences est toujours synonyme d'un impact se faisant ressentir sur le long terme, c'est-à-dire sur plusieurs années.

Il est extrêmement rare de trouver des systèmes d'informations à ce niveau, tant en ce qui concerne la confidentialité que l'intégrité. Ce peut être le cas pour certaines bases de données dont la disponibilité est absolument impérative pour la survie de l'entreprise. C'est souvent le cas pour la disponibilité des centres de calcul et les sinistres majeurs de salles-machines, pour lesquelles il n'avait pas été prévu de back-up, ont effectivement souvent conduit à des dépôts de bilan.

Impact très grave

Il s'agit là des sinistres ayant un impact très sérieux sur le fonctionnement de la compagnie, sans toutefois que son avenir soit menacé.

En termes financiers, cela peut aller jusqu'à l'annulation du résultat de l'exercice, voire à un déficit modéré.

En termes d'image, on considérera souvent à ce niveau une perte d'image dommageable qu'il faudra plusieurs mois à remonter, même si l'impact financier ne peut être évalué avec précision.

On évaluera aussi, souvent, à ce niveau, des sinistres conduisant à une désorganisation notable de l'entreprise pendant une durée de plusieurs mois.

Impact moyennement grave

Ce troisième niveau d'impact relève de tous les sinistres ayant des conséquences certaines sur l'entreprise, notables au plan de ses résultats, de son climat social, ou de son image mais non durables.

Ce sera le cas, par exemple, si un service ou un groupe de personnes limité doit, en conséquence du sinistre, accepter une surcharge importante durant quelques semaines, sans que les performances du reste de l'entreprise en soit fortement perturbées ou si l'ensemble de l'entreprise devait être perturbé pendant une courte durée.

Impact peu grave

La meilleure définition de ce niveau d'impact se réfère au nombre de personnes touchées par le sinistre et la durée de cette perturbation : peu de personnes et pendant une période courte, disons de quelques jours.

III. IMPACT INTRINSÈQUE ET IMPACT EFFECTIF D'UN SCÉNARIO DE SINISTRE

Une erreur méthodologique que nous avons souvent rencontrée, est de limiter l'impact attribué à un sinistre, pour la raison que des moyens existent rendant cette menace improbable ou en atténuant les conséquences.

Il s'agit d'une confusion entre impact et risque.

En effet, la facilité avec laquelle telle menace peut se réaliser n'a rien à voir avec la gravité de ses conséquences.

Restant très proche de notre réaction dans la vie quotidienne, la surveillance étroite d'un patrimoine, si elle dissuade un agresseur éventuel, ne change en rien le préjudice subi en cas de vol ou de destruction.

L'impact d'un sinistre doit être jugé en l'absence de tout moyen de prévention.

La mise en place de moyens de protection et de mesures palliatives pose un problème d'une autre nature.

Il s'agit en effet, non d'empêcher, de prévenir, un événement, mais d'en limiter les conséquences, c'est à dire l'ampleur du sinistre, donc l'impact.

Nous étudierons un peu plus loin la manière de prendre en compte ces moyens dans notre modèle et nous ne ferons ici que rappeler ce que nous avons vu dans le modèle de base du scénario de sinistre, à savoir que des moyens existent de limiter la gravité d'un sinistre.

La question est alors : « *de quoi tenir compte pour déterminer l'impact d'un sinistre ?* ».

Nous définissons deux natures d'impact : « *l'impact intrinsèque* » et « *l'impact effectif* ».

Avant toute mesure, nous définissons ainsi un impact, que nous appellerons « *intrinsèque* ».

L'impact intrinsèque est l'impact d'un sinistre défini en fonction des principes que nous avons vus plus haut et sans tenir compte ni des moyens de dissuasion ou de prévention, ni des moyens de protection, palliatifs ou de récupération.

On définit ainsi un impact maximal au sens où l'on cherche à évaluer le pire si les moyens de dissuasion et de prévention, visant à empêcher le début de réalisation de la menace et des détériorations, étaient, soit inefficaces, soit volontairement court-circuités ou si les moyens de protection ou palliatifs étaient inhibés ou indisponibles.

On peut éventuellement conserver cependant les limitations qui sont, soit naturelles, soit structurelles et absolument incontournables ; certaines mesures structurelles seront donc prises en compte, si elles ne sont pas susceptibles d'être annihilées.

Le maximum absolu serait atteint bien entendu si l'on n'en tenait pas compte non plus. Il apparaît cependant que dans la majorité des cas, et en particulier quand la fragmentation est réellement difficile à contourner (atteinte simultanée de plusieurs cibles) ou quand le transfert de risques a été solidement établi, cette limitation correspond bien à la notion de gravité intrinsèque.

L'impact intrinsèque est donc déterminé sans tenir compte ni des mesures de dissuasion ou de prévention ni des mesures de protection, ni des mesures palliatives. C'est ce niveau d'impact, sa gravité, qui doit servir de base à la classification des informations et des ressources de l'entreprise.

Par opposition, l'« *impact effectif* » est défini en partant de l'impact intrinsèque, mais en tenant compte des mesures de protection, palliatives et de récupération qui vont le réduire.

IV. L'IMPACT EFFECTIF ET LES FACTEURS DE RISQUE

De même que pour la potentialité, plusieurs facteurs sont susceptibles d'augmenter ou de diminuer, pour une entreprise donnée, l'impact de certains scénarios de risque.

Il s'agit, là aussi, de facteurs de risque, que nous allons décrire.

On peut mettre en évidence ces facteurs en analysant la partie basse du schéma relationnel présenté figure 1. En analysant de plus près les relations entre entités, on obtient le schéma de la figure 5 ci-après.

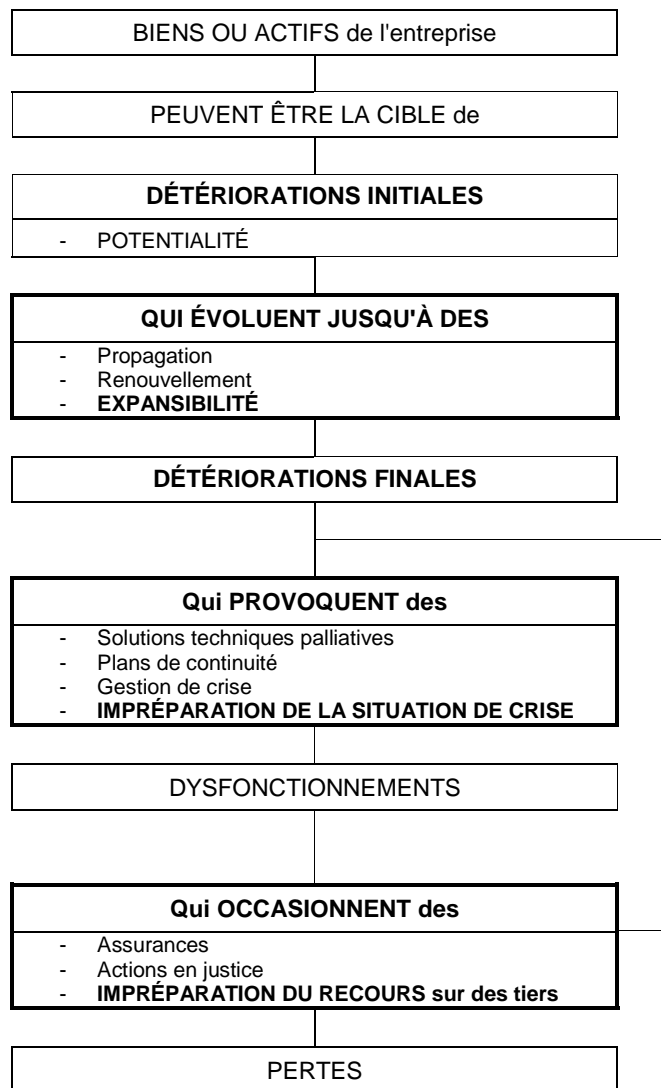


Figure 5

Le premier résultat d'une agression est un premier niveau de détériorations initiales. Cependant, ces détériorations peuvent évoluer ou se répéter, donc s'étendre jusqu'à l'arrêt complet de l'agression, le plus souvent par une action volontariste. La relation qui décrit cette évolution peut être caractérisée par un facteur de risque que nous appelons « *Expansibilité* » du scénario concerné.

Ce facteur vise donc à mettre en évidence que les détériorations seront d'autant plus importantes et donc l'impact plus sévère que rien n'aura été fait pour freiner l'expansion, dans l'espace ou le temps, des détériorations initiales.

Le deuxième type de conséquence et donc d'impact se situe au niveau des dysfonctionnements de l'entreprise provoqués par les détériorations de ressources du système d'information.

Cette relation « *qui provoquent* » peut être également caractérisée par un facteur de risque qui représente le degré d'improvisation que l'entreprise devra mettre en œuvre pour faire face à la situation créée par le sinistre.

Nous considérons, en effet, que plus cette improvisation sera grande et plus graves seront les dysfonctionnements.

Nous appelons ce facteur de risque : « *Impréparation de la situation de crise* ».

Les détériorations et les dysfonctionnements vont occasionner des pertes pour l'entreprise.

La relation « *qui occasionnent* » peut être également caractérisée par un facteur de risque qui représente le degré d'incapacité de l'entreprise à transférer une partie des pertes sur des tiers par manque de préparation préalable.

Nous appelons ce facteur de risque : « *Impréparation du recours sur des tiers* ».

Nous allons revenir en détail sur ces facteurs de risque.

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.

Deux paramètres doivent être pris en compte pour analyser ce facteur de risque.

La propagation du sinistre à d'autres ressources

Il peut s'agir de propagation dans l'espace.

C'est souvent le cas des sinistres dus à des événements naturels comme l'incendie ou un dégât des eaux. En l'absence de confinement ou de mesures spécifiques de détection et de réaction, les détériorations initiales atteindront, de proche en proche, d'autres ressources et s'étendront progressivement.

Il peut également s'agir de propagations d'erreurs au sein de fichiers ou de bases de données. L'expansibilité caractérisera le fait qu'une erreur sera susceptible de se propager à d'autres fichiers ou bases de données et donc de se multiplier rapidement. On parlera alors de pollution progressive.

Le renouvellement ou la répétition des détériorations

Cet autre élément est à prendre en compte pour des actions humaines volontaires, comme des actes de piratage ou d'intrusion dans les systèmes d'information.

Il s'agit donc d'une expansion non pas naturelle mais réfléchie. Cet élément vise à mettre

en évidence que si un acte délictueux a été tenté et réussi et qu'aucune réaction ne l'est manifestée, il sera renouvelé par son auteur, pour obtenir plus d'avantages, pour parfaire éventuellement ce qu'il n'aura pas eu le temps de finir la première fois, etc.

Globalement l'expansibilité des détériorations caractérise l'absence ou la lenteur des réactions de l'entreprise à un début de sinistre.

NIVEAUX D'EXPANSIBILITÉ

Expansibilité forte

Une expansibilité forte est généralement associée à des contextes ou à des scénarios pour lesquels il n'existe pratiquement aucun système de détection.

Le sinistre débutant ne sera pas détecté et il faudra qu'il ait atteint un stade très avancé ou commencé à provoquer des dysfonctionnements notables pour que l'entreprise réagisse.

Ce sera le cas d'installations sans systèmes de détection d'incendie ou de dégâts des eaux.

Ce sera également le cas de réseaux dénués de surveillance active ou d'applications n'ayant prévu aucune détection d'erreur. A ce niveau et dans ce type de cas, lors de la découverte du sinistre, il pourra même être difficile d'en cerner l'ampleur et le périmètre.

On attribuera également une forte expansibilité à des scénarios pour lesquels on peut craindre que, malgré une détection précoce du sinistre, on peut s'attendre à une absence de réaction. Ce pourrait être le cas, par exemple, s'il n'y avait, dans l'entreprise ou à la disposition de l'entreprise, aucune équipe ayant la technicité nécessaire pour une intervention donnée.

Expansibilité moyenne

Une expansibilité moyenne est généralement associée à des contextes ou à des scénarios pour lesquels il existe des systèmes de détection peu performants mais permettant néanmoins de contrôler l'étendue des dégâts, ainsi que des capacités de réaction.

Le sinistre débutant ne sera pas détecté immédiatement mais il finira par l'être, à un stade déjà avancé, mais contrôlable

Ce sera le cas d'installations sans systèmes de détection d'incendie ou de dégâts des eaux, mais faisant néanmoins l'objet de contrôles visuels renforcés, par exemple par des rondes de gardiens.

Ce sera également le cas de systèmes ou d'applications faisant l'objet d'audits réguliers ou d'analyse périodique des traces, hebdomadaire par exemple, ou d'applications ayant prévu une détection d'erreur avec des seuils relativement larges permettant une détection tardive.

On attribuera également une expansibilité moyenne à des scénarios pour lesquels on peut craindre que, malgré une détection précoce du sinistre, les conditions d'une réaction rapide ne sont pas remplies. Ce pourrait être le cas, par exemple, s'il n'y avait aucune garantie de disponibilité de l'équipe ayant la technicité nécessaire pour une intervention donnée.

Expansibilité faible

Une expansibilité faible est généralement associée à des contextes ou à des scénarios pour lesquels il existe des systèmes de détection et de réaction performants permettant de circonscrire rapidement les détériorations.

Ce sera le cas d'installations ou de systèmes équipés de systèmes de détection d'incidents automatiques.

Ce sera également le cas de systèmes ou d'applications faisant l'objet de systèmes de surveillance dynamique permanente ou d'applications ayant prévu une détection d'erreur avec des seuils relativement étroits permettant une détection rapide.

Expansibilité insignifiante

Une expansibilité insignifiante est généralement associée à des situations pour lesquelles il existe des systèmes temps réel de détection d'incidents performants associés à des systèmes de blocage ou d'arrêt automatiques, de sorte que les détériorations soient extrêmement limitées.

Il peut s'agir, par exemple de système de déconnexion ou d'arrêt automatique empêchant dès la détection d'un incident, qu'il n'entraîne des conséquences en cascade (sur détection de virus, par exemple).

Il restera, bien sûr, toujours à réparer l'erreur, la défaillance ou la panne initiale.

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.

Deux paramètres devront donc être pris en compte pour analyser ce facteur de risque.

La capacité de restauration des ressources

Ce paramètre regroupe, en fait, plusieurs significations selon le type de ressource concernée.

Pour les équipements matériels, il correspond aux capacités de *réparation* et de *remplacement* des ressources. Par capacité, dans ce contexte, on entend les délais et les garanties de délais, ainsi que les conditions de coût.

Pour les logiciels, il s'agit des capacités de *correction* des erreurs détectées, c'est-à-dire du support immédiatement disponible, de la réactivité de l'entreprise au du service ayant fourni le logiciel et des moyens dont on peut être sûr de disposer pour obtenir une correction provisoire satisfaisante (patch).

Pour les données, il s'agit des capacités de *correction* des erreurs, donc des ressources mobilisables pour effectuer ces corrections et du délai nécessaire pour les mobiliser.

Il peut aussi s'agir, pour les données, des capacités de *reconstruction* des données, à partir des éléments ayant servi initialement à leur constitution.

Ces différentes capacités de restauration sont habituellement décrites dans des Plans de Reprise d'Activité (PRA). L'absence de PRA, même si les capacités de restauration existent naturellement, est en soi un facteur de risque important.

La capacité de reconfiguration

Ce paramètre décrit, globalement, la capacité de l'entreprise à faire face à la situation de crise, née des détériorations de ressources, pour minimiser les dysfonctionnements.

Il comprend les moyens de remplacement qui peuvent être mis en action, que ces moyens s'appuient sur une reconfiguration statique ou dynamique, et toutes les procédures permettant aux divers services de l'entreprise de fonctionner au mieux, d'abord en l'absence temporaire de toute ressource de remplacement, puis avec les ressources de remplacement qui peuvent ne pas offrir le même niveau de service que les ressources qui ont été détériorées.

La mise en place des ressources de remplacement est généralement décrite dans des Plans de Reprise d'Activité (PRA) et les procédures de fonctionnement des utilisateurs en période de crise dans des Plans de Continuité Utilisateurs (PCU).

L'absence de PRA et de PCU est, en soi, un facteur de risque important qui dénote l'impréparation de l'entreprise à ce type de situation.

NIVEAUX D'IMPRÉPARATION DE LA SITUATION DE CRISE

Impréparation forte

Une impréparation forte est généralement associée à des contextes ou à des scénarios pour lesquels il n'existe pratiquement aucun plan préétabli de gestion de la crise.

Ce sera donc l'improvisation devant la situation.

Il s'agit souvent d'entreprises qui comptent sur leurs capacités de réaction et sur la cohésion de son personnel pour faire face à une difficulté.

Sans négliger ce facteur positif, nous considérons qu'une entreprise non préparée devra faire face à des impondérables et à des difficultés de détail qui, mises bout à bout, la conduiront à des restaurations plus difficiles et plus longues et à des dysfonctionnements plus profonds et plus durables.

A ce niveau d'impréparation, la solution générale à une crise donnée n'a même pas été envisagée, ou, sinon, les éléments essentiels nécessaires, sauvegardes ou éléments de dossiers, n'ont même pas fait l'objet d'une procédure quelconque permettant de garantir qu'ils pourront être récupérés.

En fonction du scénario envisagé, il peut s'agir d'une absence de contrat de maintenance ou d'entretien, d'absence de sauvegardes, de plans de continuité inexistant, etc.

Impréparation moyenne

Une impréparation moyenne est généralement associée à des situations pour lesquelles il a bien été prévu des mesures de restauration ou de reconfiguration, mais à un niveau global et sans plans formalisés ni, a fortiori, testés.

On a effectivement prévu, par exemple, de secourir un système par un autre, mais des tests de reconfiguration ou de basculement n'ont pas été effectués. Les difficultés, qui sont la règle en ce domaine, devront donc être résolues à chaud, en période de crise (ce qui ne facilitera pas leur résolution).

Il existe bien des sauvegardes, mais leur synchronisme et leur aptitude à restaurer un

système complet n'a pas été vérifiée.

Il peut y avoir, à ce niveau, des scénarios ayant fait l'objet de plans de secours en bonne et due forme (PRA et PCU), mais qui n'ont pas été remis à jour depuis longtemps.

Pour des restaurations de matériels, il a bien été prévu un contrat de maintenance, mais aucune garantie de délai n'a été négociée.

Impréparation faible

Une impréparation faible est généralement associée à des situations pour lesquelles il existe des plans complets, détaillés, mis à jour et testés régulièrement.

En ce qui concerne les restaurations, il existe des contrats, ou des ressources internes associées à des contrats de service, où sont détaillées toutes les exigences de nature à réduire les délais de restauration à un minimum acceptable.

Impréparation insignifiante

Une impréparation insignifiante est généralement associée à des systèmes de reconfiguration automatiques, de sorte que les conséquences, en termes de dysfonctionnements, seront nulles.

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.

Le recours sur des tiers peut prendre deux aspects : le transfert de risque par le biais de l'assurance et les actions en justice.

Les assurances

Ce ne sont, bien sûr, que des pis-aller mais cela peut aider à réduire les pertes finales.

Notons bien que le principe de l'assurance est de couvrir, par une mutualisation, des risques que l'entreprise ne peut supporter à elle seule.

Ceci étant, certains sinistres peuvent parfaitement être partiellement couverts par une assurance et ce sera, en cas de sinistre, autant de charges financières en moins pour l'entreprise.

A l'inverse, l'absence d'assurances correctement souscrites est un facteur de risque supplémentaire.

Les actions en justice

Les actions en justice sont une autre forme de transfert sur un tiers, quand il y a malveillance.

Il faut, pour que cela soit possible après un sinistre, que des précautions aient été prises auparavant : prélèvement et enregistrement de traces licites et conformes à la législation, éléments de preuve, etc.

A l'inverse, l'absence de plan établi pour se donner de telles possibilités est un facteur de risque supplémentaire.

NIVEAUX D'IMPRÉPARATION DU RECOURS SUR DES TIERS

Impréparation forte

Une impréparation forte est généralement associée à des contextes pour lesquels il n'existe pratiquement aucune assurance spécifique au risque informatique et où rien n'a été prévu pour pouvoir recueillir des éléments de preuve contre un acteur malveillant.

Aucun transfert de risque ne sera donc possible.

Il peut aussi s'agir de scénarios pour lesquels aucune action de recours ne pourrait s'avérer efficace.

Impréparation moyenne

Une impréparation moyenne est généralement associée à des situations pour lesquelles il a bien été prévu des mesures de recours, mais dont l'intérêt ne sera que minime par rapport aux enjeux du scénario de risque.

Il y aura éventuellement transfert sur un tiers, mais d'une partie très faible eu égard au risque.

Il peut également s'agir d'assurances correctement établies en leur temps, mais dont les clauses n'ont pas été revues et qui se trouvent décalées par rapport aux enjeux. Il peut aussi se faire qu'il y ait des traces prélevées des transactions les plus sensibles, mais que ces éléments n'aient pas été analysés avec un avocat et qu'ils puissent s'avérer irrecevables par un magistrat.

Impréparation faible

Une impréparation faible est généralement associée à des situations pour lesquelles il existe des assurances revues annuellement et des éléments de traces pertinents analysés avec un avocat.

Impréparation insignifiante

Une impréparation insignifiante est généralement associée à des situations totalement cernées pour lesquelles une couverture d'assurance assure que les risques resteront à un niveau aisément supportable.

Il ne peut s'agir, à ce niveau, d'actions en justice dont le résultat ne peut jamais être garanti.

V. IMPACT ET CLASSIFICATION DES INFORMATIONS

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.

En effet, si les méthodes d'analyse de risques sont des instruments puissants, elles ne peuvent être employées par l'ensemble du personnel pendant les actions courantes.

Or la protection des informations nécessite, pour l'action quotidienne, des réflexes, ce qui suppose que l'on sache attacher à chaque information une « *étiquette* » représentative de sa valeur ou de sa criticité, et que l'on ait défini des normes permettant de savoir immédiatement la conduite à tenir pour protéger une information, au seul vu de son étiquette.

Le contenu de cette étiquette est la « *classification de l'information* ».

L'analyse de l'impact des scénarios de sinistre peut servir de base à l'établissement d'une telle classification.

Il faut noter alors que la classification est le reflet direct des pires cas d'impact intrinsèque et ne doit jamais tenir compte des mesures de sécurité donc d'une atténuation des facteurs de risques

C'est une retombée d'une méthode de modélisation et d'évaluation des risques que de fournir cette classification ou de fournir une révision des classifications précédemment effectuées.

V. ÉVALUATION DE L'IMPACT

L'analyse des facteurs de risque, en se référant aux définitions des différents niveaux de chaque facteur, est une première étape de l'évaluation de la potentialité.

Cette analyse permet, dans un premier temps, de se faire une idée des conséquences de la réalisation du risque.

Cependant, l'évaluation globale de l'impact effectif d'un scénario de risque doit tenir compte à la fois :

- De l'impact intrinsèque, donc de la classification de la sensibilité de la ressource, si cette classification existe.
- Des facteurs de risque qui peuvent venir atténuer cette évaluation intrinsèque, par définition pessimiste.

On pourrait, à ce stade, évaluer globalement l'impact effectif, de manière intuitive mais raisonnée, en fonction des facteurs de risque et de l'impact intrinsèque.

On obtient, en pratique, une bien meilleure reproductibilité du raisonnement en construisant des grilles d'analyse qui permettent de passer des facteurs de risque à une évaluation de la « *réduction d'impact* », puis une grille de passage de l'impact intrinsèque et de la réduction d'impact à l'impact effectif.

Ces grilles dépendent des types d'agresseurs et on en construira donc plusieurs selon qu'il s'agit de malveillances, d'erreurs, d'accidents ou d'événements naturels.

Chapitre 6

EFFETS DES MESURES DE SÉCURITÉ

Il y a un parallèle évident entre les facteurs de risques évoqués au chapitre précédent et la typologie des mesures de sécurité présentée au chapitre 3 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.

Nous allons maintenant mettre en évidence la manière de quantifier leur influence sur ces facteurs que nous venons d'étudier et qui sont représentatifs des risques de l'entreprise.

I. EFFICACITÉ DES MESURES DE SÉCURITÉ

Le premier paramètre permettant de mesurer l'effet d'une mesure est son efficacité.

L'efficacité vise à mesurer l'ampleur de l'effet d'un type de mesure sur un facteur de risque d'un scénario de sinistre.

Un même type de mesure peut être très efficace contre un type de menace donné et avoir des effets atténuateurs très différents contre un autre type de menace ou dans une autre entreprise.

La détection d'une erreur dans un fichier, si elle est détectée de manière très précoce, peut faire passer l'impact de ce sinistre de « *très grave* » à « *insignifiant* », alors que la détection, aussi précoce, de la fuite d'une information commerciale peut ne faire passer l'impact de ce sinistre que de « *très grave* » à « *grave* », voire ne changer que de manière insignifiante le niveau d'impact.

Nous dirons que l'« *efficacité* » de la détection est différente dans ces deux cas.

L'exemple pris était relatif à des mesures de détection mais nous allons passer en revue les différents types de mesures et décrire ce que l'on appelle leur efficacité, en séparant, pour plus de clarté, et bien que le concept d'efficacité soit le même dans les deux cas, les mesures

structurelles, dissuasives et préventives, jouant sur la potentialité, des mesures de protection, palliatives et de récupération, jouant sur l'impact.

EFFICACITÉ DES MESURES DISSUASIVES OU PRÉVENTIVES

Les mesures structurelles, les mesures dissuasives et les mesures préventives ont donc une influence sur la potentialité.

Si on analyse le mode d'action de ces mesures, on remarque que c'est avant tout par un « *changement de niveau* » d'un des paramètres de la potentialité.

Ainsi, si des efforts d'organisation visent à amoindrir une exposition naturelle, qu'une absence de maintenance préventive, par exemple, rendait initialement forte, le résultat sera une exposition naturelle moyenne. Mais si l'exposition naturelle était au départ moyenne, le résultat de la même mesure d'organisation ne conduira pas forcément à une exposition naturelle faible.

De même, le niveau de risque personnel que va devoir prendre l'agresseur, après mise en place de mesures dissuasives, ne dépend-il que de mesures qui vont déterminer la possibilité de remonter jusqu'à l'auteur de l'agression et des conséquences qu'il devra supporter alors. Pour un même facteur, il n'y a donc pas d'effet progressif et cumulatif, avec une efficacité finale résultant de l'ensemble des mesures, mais une efficacité fixée par la seule mesure la plus efficace.

On pourrait envisager le cas où un cumul de mesures permettrait d'atteindre pour le même facteur, par complémentarité, un niveau de risque qui ne soit pas directement lié à une seule des mesures. Mais, dans ce cas, il convient de regarder le cumul de mesures comme une seule mesure qui impose son niveau de risque.

La notion de niveau est encore plus nette pour les mesures de prévention qui agissent sur les conditions requises et leur trivialité. Une mesure, dans ce cas, ne sera efficace que si elle permet d'élever le niveau de ces conditions, et la mesure de son efficacité sera directement le niveau atteint, indépendamment du niveau initial.

Ainsi, pour ces mesures, l'efficacité n'est-elle pas une amélioration du niveau initial, mais, le cas échéant, un changement de niveau. L'efficacité d'une mesure d'organisation générale visant à réduire l'exposition naturelle est définie par le niveau atteint si cette mesure est appliquée. De même, l'efficacité d'une mesure dissuasive est le niveau d'impunité de l'agresseur atteint après mise en œuvre de la mesure. Enfin l'efficacité d'une mesure technique de contrôle d'accès est le niveau de trivialité des conditions de survenance qu'elle impose.

On voit que, dans ces trois cas, l'efficacité d'une mesure ne dépend pas du type de sinistre, elle dépend par contre de l'origine de l'agression et en particulier du type d'agresseur. En effet, la perception du risque sera différente selon les agresseurs et, concernant les contrôles d'accès par exemple, une mesure peut être efficace contre un type d'agresseur et inefficace pour un autre. Un contrôle d'accès par serrure de sûreté est efficace contre un visiteur, il l'est moyennement contre un employé interne qui pourra peut-être emprunter la clé, et ne l'est plus du tout contre un cambrioleur professionnel.

L'efficacité d'une mesure structurelle, dissuasive ou préventive se définit par le niveau auquel elle positionne le facteur de risque auquel elle s'adresse. Cette efficacité dépend essentiellement du type d'agresseur.

On a vu que la potentialité d'un scénario de sinistre était celle qu'une agression rassemble les conditions de survenance nécessaires, que l'agresseur, s'il est humain, en ait la volonté malgré les risques encourus, et ceci en fonction de l'attrait naturel que représente la cible.

Les mesures réduisent cette potentialité en exigeant davantage de l'agresseur, soit en réduisant l'intérêt qu'il peut en retirer, soit en augmentant les risques qu'il devra prendre, soit en augmentant les moyens et les capacités minima qu'il devra mettre en œuvre.

EFFICACITÉ DES MESURES DE PROTECTION, PALLIATIVES OU DE RÉCUPÉRATION

Pour les trois types de mesures ayant un effet sur l'impact du sinistre, c'est-à-dire les mesures de protection, les mesures palliatives et les mesures de récupération, leur efficacité sera, de la même manière, le niveau d'impact atteint si la mesure est mise en œuvre.

L'effet de ces types de mesures sera, cependant, légèrement différent.

Les mesures de protection agissent sur l'ampleur des détériorations. Ces mesures ont donc un effet direct sur le facteur de risque correspondant qui est l'expansibilité des détériorations.

Les mesures palliatives n'ont d'effet que sur les dysfonctionnements et non sur les détériorations. Elles ont un effet sur un autre facteur de risque qui est l'impréparation de la situation de crise.

Les mesures de récupération permettent d'atténuer les pertes finales, en valeur monétaire. Elles agissent donc sur l'impréparation du recours sur des tiers.

L'efficacité d'une mesure sera, dans ces trois cas, définie comme le niveau auquel elle permet de limiter le facteur de risque correspondant.

Pour évaluer l'efficacité d'une mesure, cependant, il faut bien distinguer en fonction du type de détérioration ou de dysfonctionnement auquel a conduit le scénario de sinistre : nature de la ressource atteinte pour les mesures de protection ou nature du sinistre ayant conduit au dysfonctionnement, perte de confidentialité, d'intégrité, de disponibilité de service pour les mesures palliatives ou nature du sinistre (assuré) pour les mesures de récupération.

En effet, une mesure d'un type donné, la reconfiguration par exemple, n'a pas du tout la même efficacité s'il s'agit de s'attaquer à l'impact d'une divulgation d'information ou à celui de sa destruction.

Non seulement, donc, l'efficacité d'une mesure de protection, palliative ou de récupération dépend du type de sinistre, mais si le sinistre a plusieurs effets comme c'est souvent le cas, perte de confidentialité et perte de disponibilité dans le cas d'un vol par exemple, on évaluera une efficacité de mesure par type d'effet.

L'efficacité d'une mesure de protection, palliative ou de récupération mesure le niveau auquel elle positionne le facteur de risque auquel elle s'adresse. Elle dépend du type de sinistre.

On remarquera, par opposition à l'efficacité des mesures dissuasives ou préventives, que l'efficacité de ces mesures ne dépend pas du type d'agresseur.

II. ROBUSTESSE DES MESURES

La robustesse de la mesure vise à définir dans quelle mesure la mesure peut résister à une attaque directe.

Pour prendre un exemple, la sauvegarde sur disquettes des données et programmes est,

indiscutablement, un moyen très « efficace » de protection de ces données et programmes contre une perte de disponibilité. Si ces sauvegardes sont rangées à côté du micro, ce moyen est efficace contre une panne ou un crash du disque dur, mais son efficacité peut être mise en défaut s'il s'agit de se protéger contre un effacement malveillant d'une personne de passage, qui pourra aussi bien effacer les sauvegardes ou les emporter.

Nous dirons, dans le deuxième cas, que la mesure n'a pas résisté à l'agresseur, que sa robustesse était insuffisante pour garantir son efficacité.

Pour prendre un autre exemple dans le domaine de la protection contre l'altération des données, un contrôle des données entrées, par une double saisie par le même opérateur, est une mesure efficace contre les erreurs, mais ne résiste pas à la malveillance.

Un contrôle par une deuxième personne résiste à une malveillance simple mais ne résiste pas à la collusion de deux personnes.

Pour prendre un dernier exemple, une trace des transactions et actions menées dans un système informatique peut être une mesure efficace de dissuasion, et diminuer l'impunité de l'agresseur. Si les traces ne sont pas elles-mêmes suffisamment protégées, un agresseur pourra les effacer. On dira, dans ce cas, que la mesure n'était pas assez robuste pour résister à l'agression.

L'analyse de la robustesse d'une mesure consiste donc à déterminer les catégories d'agressions auxquelles cette mesure résiste.

On notera bien qu'il ne s'agit pas d'attribuer une note de qualité aux mécanismes de sécurité mis en œuvre par la mesure, mais de garantir le maintien de son efficacité en cas d'attaque par des agresseurs d'un type donné.

La seule question à laquelle il faut répondre est de savoir si la mesure choisie peut être inhibée ou contournée par l'agresseur ou rendue inefficace par l'agression elle-même.

Il n'y a donc pas d'effet proportionnel de la robustesse sur la potentialité ou sur l'impact, mais application ou non, succès de la mesure ou non. Ainsi, la mesure dissuasive joue son rôle ou non, le contrôle d'accès fonctionne ou non, la détection a lieu ou non, le message est indécryptable par l'agresseur ou non, le centre de secours peut jouer son rôle ou non.

Or la réponse est fonction de ce que peut faire l'agresseur, humain ou non.

L'efficacité d'une mesure définit le niveau auquel elle positionne le facteur de risque auquel elle s'adresse. La robustesse de la mesure définit le niveau de capacité d'agresseur à partir duquel la mesure doit être considérée comme non efficace.

Bien plus, cette robustesse devrait pouvoir être garantie, c'est-à-dire que l'assurance de l'impossibilité de contournement ou d'inhibition, par tels types d'agresseurs, des mesures dissuasives, préventives, de protection, palliatives ou de récupération, devrait être fournie par des experts, et ne peut être laissée à l'interprétation des responsables de l'entreprise.

La robustesse d'une mesure est donc, en fait, le niveau d'agresseur auquel la mesure résiste. Ce niveau doit être garanti par un ou des experts.

Il nous faut donc définir les niveaux d'agresseurs, c'est ce que nous ferons au chapitre suivant.

III. EFFETS DES SERVICES DE SÉCURITÉ

La plupart des services de sécurité ont des effets multiples.

Ainsi, un gardien surveillant l'entrée dans une salle machine est à la fois une mesure de contrôle des accès, donc préventive, une mesure dissuasive car le gardien peut reconnaître une personne autorisée et se souvenir de son passage, et une mesure de protection par la détection en cas d'incendie, de sabotage ou autre sinistre mettant en cause la disponibilité des machines.

On sera donc amené à définir, pour une même solution de sécurité, pour un même service de sécurité, plusieurs domaines d'action.

Un service de sécurité, qui est une solution concrète qu'une entreprise peut mettre en œuvre, correspond généralement à plusieurs types de mesures, chacune ayant son efficacité vis-à-vis d'un facteur de risque déterminé. Par contre, la robustesse du service est unique, c'est celle du niveau d'agresseur nécessaire pour l'inhiber, la contourner ou l'empêcher d'agir.

Par ailleurs, nous l'avons vu avec l'exemple du gardiennage, un service de sécurité peut avoir une influence, donc une certaine efficacité, pour plusieurs types de scénarios, correspondant à des types d'agressions différents et ayant des types de conséquences différents.

On définira donc, pour un même service de sécurité :

- en fonction de chaque type d'agression auquel elle s'adresse, et donc de chaque profil d'agresseur :
 - l'efficacité d'organisation, contre le facteur de risque *exposition naturelle*, caractérisée par le niveau d'exposition naturelle résultant,
 - l'efficacité dissuasive, contre le facteur de risque *impunité de l'agresseur*, caractérisée par le niveau d'impunité résultant,
 - l'efficacité préventive, contre le facteur de risque *trivialité des conditions de survenance*, caractérisée par le niveau de trivialité résultant,
- en fonction de chaque type de sinistre, atteinte à la disponibilité du service, à l'intégrité, à la confidentialité ou au patrimoine :
 - l'efficacité de la protection, contre le facteur de risque *expansibilité des détériorations*, caractérisée par le niveau d'expansibilité résultant,
 - l'efficacité palliative, contre le facteur de risque *impréparation de la situation de crise*, caractérisée par le niveau d'impréparation de la crise résultant,
 - l'efficacité de récupération, contre le facteur de risque *impréparation du recours contre des tiers*, caractérisée par le niveau d'impréparation du recours résultant,
- en fonction de chaque profil d'agresseur :
 - la robustesse de la mesure.

IV. EFFETS DU CUMUL DE SERVICES

Dans la pratique, plusieurs services de sécurité vont se combiner, ou se compléter, en général pour s'attaquer à des facteurs de risque différents.

On installera ainsi, par exemple, des contrôles d'accès pour n'autoriser que les personnes ayant besoin d'en connaître, des traces comme mesures de dissuasion, et des moyens de secours. Il y a donc cumul des effets de ces différents services.

L'approche par niveaux que nous avons présentée permet une réponse simple au problème de cumul.

Pour un niveau d'agresseur donné et pour chaque facteur de risque, on retiendra le niveau de facteur de risque minimum obtenu après mise en place des services qui ont été sélectionnés et dont la robustesse est supérieure au niveau d'agresseur possible.

Ainsi, quand plusieurs services ont été sélectionnés, on peut déterminer, tout d'abord, le niveau d'agression imposé par le niveau de trivialité des conditions de survenance, en fonction de la mesure la plus efficace de ce point de vue. Ceci permet de déterminer le profil d'agresseur minimum possible et donc d'éliminer, en termes d'efficacité, toutes les mesures dont la robustesse est inférieure au niveau de l'agresseur. On peut alors déterminer le minimum atteint de chaque facteur de risque. On a alors tous les paramètres nécessaires à l'estimation du risque.

Chapitre 7

LES CATÉGORIES D'AGRESSEURS

Le scénario de sinistre, qui nous a servi de modèle de base, décrit des types d'agression.

Il s'agit, par exemple, d'un phénomène naturel comme un incendie prenant naissance à la suite d'un court-circuit dans le faux plancher d'une salle informatique, d'un pirate accédant par les réseaux à un système, d'un visiteur sabotant un matériel, d'un personnel de nettoyage endommageant l'autocommutateur, d'un employé dérobant en bandothèque une bande sensible, etc.

Ce que nous avons appelé filière d'agresseur comprend donc des notions multiples qui sont le caractère humain ou non de l'agresseur, le mode de pénétration, logique ou physique, dans l'entreprise, les moyens dont il dispose, etc.

La capacité de l'agresseur, que nous avons défini en termes de niveaux, et dont nous avons vu apparaître le rôle essentiel, tant pour l'expression de la potentialité que pour analyser la robustesse des mesures, se définit donc à l'intérieur d'une filière d'agresseur. La capacité d'un pirate agissant depuis un Minitel n'a rien de comparable avec celle d'un terroriste manipulant des explosifs.

Le scénario de risque doit définir la filière de l'agresseur, et l'analyse doit déterminer quelle est la capacité minimum que doit avoir un agresseur de ce profil pour pouvoir accéder à une ressource.

Nous allons donc commencer par décrire les différentes filières d'agresseurs, qui diffèrent par les liens qu'ils ont avec l'entreprise et par les modes d'accès qu'ils sont susceptibles d'employer.

I. LES FILIÈRES D'AGRESSEURS

LE PERSONNEL ET LES PERSONNES ASSIMILÉES

Il s'agit là tant du personnel propre de l'entreprise que des partenaires et sous-traitants qui ont un lien contractuel avec l'entreprise.

On trouvera donc, outre l'ensemble du personnel, tous ceux qui ont une occasion régulière et organisée par contrat, de pénétrer dans l'entreprise, comme le personnel de nettoyage, le personnel de gardiennage, les divers personnels de maintenance de tous les équipements présents dans l'entreprise, les coursiers et postiers, etc.

Ces personnels ont deux caractéristiques :

Qu'ils soient autorisés ou non à accéder à une information ou à une ressource sensible, ils sont proches de l'entreprise et connaissent bien ses modes de fonctionnement. Ils ont, en tout cas, accès à des ressources de l'entreprise, dans le cadre normal de leur travail.

Ils ont, en contrepartie, un risque particulier qui est la rupture du lien contractuel les unissant à leur entreprise, par licenciement direct s'il s'agit du personnel de l'entreprise, ou par licenciement provoqué, s'il s'agit de sous-traitants ou de partenaires, la société qui les emploie pouvant les licencier à la demande de la société au profit de qui ils travaillent.

Ces personnels, qu'il s'agisse des employés de l'entreprise, ou des partenaires ou sous-traitants, sont certainement dans l'ensemble très honnêtes et consciencieux, mais tout peut arriver, et il ne s'agit pas, en considérant cette filière, de jeter un doute sur la probité des employés, mais d'imaginer un certain nombre de scénarios tout à fait plausibles, voire de constater la réalité.

Un employé qui s'apprête à quitter sa société aura-t-il la même éthique et la même droiture d'esprit qu'il a montrées dans le passé, si, en outre, les informations auxquelles il a accès peuvent être intéressantes dans sa nouvelle situation, et si le climat dans lequel son départ se produit n'est pas le meilleur ? L'expérience nous fait répondre non.

Un autre cas doit être examiné avec sang froid. Si l'enjeu de la cible est suffisamment important pour une personne externe, elle peut tenter de soudoyer du personnel de l'entreprise autorisé à accéder à l'information visée. La question n'est pas de savoir si un utilisateur résistera à cette demande, mais à quel montant il acceptera de trahir. Dans le même état d'esprit, le chantage est un moyen de pression également efficace, et certains services de renseignements étrangers ne se sont pas privés d'employer ce moyen d'acquisition d'informations confidentielles.

Les utilisateurs accrédités

Les utilisateurs accrédités sont tous ceux à qui on a accordé des droits d'accéder à de l'information.

Il s'agit, en tout premier, lieu des utilisateurs du système d'information, mais aussi de certaines catégories de personnel d'exploitation et de maintenance des systèmes informatiques, voire des ingénieurs de développement des applications informatiques, à qui

on a pu accorder des droits d'accès à de l'information sensible.

Pour toutes ces personnes, les mesures préventives basées sur le filtrage des accès ne s'appliquent pas, du moins pour les informations auxquelles ils ont accès.

Les utilisateurs accrédités représentent donc un profil particulier, d'autant que les moyens d'accéder à l'information leur sont donnés par l'entreprise.

Leur capacité jouera soit pour abuser de leurs droits, c'est-à-dire pour accéder à des informations pour lesquelles ils ne sont pas habilités, soit pour déjouer les autres mesures, traces, moyens de protection ou mesures palliatives.

Les opérateurs accrédités

Les opérateurs accrédités sont tous ceux à qui on a accordé des droits d'accéder à des ressources sensibles.

Il s'agit, en tout premier lieu de tout le personnel d'exploitation et de maintenance de l'informatique, mais aussi des personnels chargés de gérer et de maintenir des équipements sensibles comme les autocommutateurs et les ressources en énergie ou en fluides, du personnel de gardiennage qui a accès à tous les équipements et à tous les terminaux.

Les accès physiques aux ressources étant autorisés, les contrôles d'accès à ces ressources ne joueront pas davantage, et comme pour les utilisateurs accrédités, la capacité de ces personnes sera vue comme celle qu'elles pourront mettre en œuvre pour court-circuiter les autres mesures.

Les non accrédités

Il s'agit de tout le personnel qui n'a pas de droit particulier pour accéder à de l'information ou à une ressource, mais qui côtoie au quotidien des personnes qui ont accès au système d'information et qui jouit ainsi d'une connaissance particulière.

Les contrôles d'accès peuvent avoir une efficacité, mais il reste à démontrer que cette efficacité est réelle, la connaissance ou l'observation d'un mot de passe, par exemple, étant parfois tout à fait possible pour un collègue de bureau.

LES AGRESSEURS EXTERNES

Les agresseurs externes sont des personnes qui n'entretiennent aucun lien de nature contractuelle avec l'entreprise. Leur motif d'attaquer cette société plutôt qu'une autre sera parfois la concurrence, souvent le fait qu'ils la connaissent ou qu'ils en connaissent les failles, quelquefois le hasard.

Les concurrents peuvent être tentés de se procurer des informations de nature à leur donner des avantages concurrentiels. Si, de plus, parmi ces concurrents, il y a d'anciens collaborateurs, alors ils allieront l'envie à la connaissance de l'entreprise, de ses modes de fonctionnement, et éventuellement de ses faiblesses, s'ils n'ont pas conservé des droits d'accès.

Les pirates et jeunes hackers agissent le plus souvent par jeu ou par défi. L'entreprise pourrait donc considérer qu'elle n'a pas de raison d'être spécialement visée. Si elle possède des faiblesses, et si des moyens de pénétrer ses systèmes d'information ont été découverts, alors les pirates échangeront vraisemblablement cette information (des messageries spécialisées de pirates existent) et le nombre de tentatives et de pénétrations réussies ira grandissant.

Enfin, les agressions physiques existent, qu'il s'agisse de jeunes voyous, de bandes organisées, de sabotage délibéré, voire de terrorisme.

Nous distinguerons donc trois catégories de profils, selon que la caractéristique principale de la voie de pénétration est une voie logique ou une voie physique et selon les moyens employés.

Les pirates

Les pirates que nous considérons là sont donc étrangers à l'entreprise et agissent par voie logique pour dérober, altérer ou détruire de l'information. Il s'agit donc d'informaticiens dont les buts peuvent tout aussi bien être le jeu que l'intérêt, et en particulier la fraude, et dont les possibilités varient avec le niveau.

Il n'est pas exclu qu'ils aient pénétré physiquement dans l'entreprise en fraude ou avec l'intention de fraude, par exemple en se faisant passer pour un visiteur, mais c'est l'agression finale par voie logique, et leur capacité à pénétrer les systèmes par voie logique, qui en fait des « pirates » et non des « malfaiteurs » ou des « espions ».

Les malfaiteurs

Les malfaiteurs, par opposition à la catégorie des pirates, agissent par voie physique pour accéder à une ressource pour la détruire ou pour la dérober.

Nous classons dans cette catégorie tous les auteurs de sabotage, de vol avec ou sans effraction, d'agression physique directe.

Leurs capacités seront donc liées à leur faculté de déjouer les contrôles d'accès physiques, et aux moyens mis en œuvre pour détruire, voler ou endommager des installations concrètes.

Les espions

Les espions, par opposition à la catégorie des malfaiteurs, visent l'information, essentiellement pour la dérober ou la copier, mais éventuellement pour l'altérer, et agissent par voie physique.

Nous mettons dans cette catégorie toutes les formes d'écoutes, de vol de document, de piégeages divers qui demandent une intervention physique.

LES PHÉNOMÈNES NATURELS

La dernière catégorie est celle des phénomènes naturels, qu'ils prennent naissance dans l'entreprise ou qu'ils se propagent jusqu'à elle.

Certaines catastrophes naturelles ne sont que des accidents ou des erreurs, voire des malveillances, qui ont pris naissance en dehors de l'entreprise. Nous les considérerons comme des phénomènes naturels tant que leur déclenchement n'était pas dirigé contre l'entreprise.

Cette catégorie comprend donc les incendies, les dégâts des eaux, la pollution due au voisinage, les dégâts de tous ordres causés par les orages, tornades ou autres cataclysmes, les glissements de terrain, les avalanches, les chutes d'objet, etc.

Nous avons donc une double classification des agresseurs, selon leur filière et selon leur niveau, que nous allons maintenant aborder en adoptant une description par niveau.

II. LES NIVEAUX D'AGRESSEURS

NIVEAU STANDARD

Ce niveau est caractérisé par des compétences techniques non spécialisées, par l'absence de connaissances précises sur les systèmes de protection et de sécurisation des ressources sensibles de l'entreprise et par l'absence de moyens techniques ou financiers.

Ce niveau est bien sûr suffisant, pour les *utilisateurs accrédités* et les *opérateurs accrédités*, pour accéder respectivement aux informations ou aux ressources pour lesquelles ils ont été autorisés.

Concernant la filière *non accrédités*, c'est le niveau général atteint sans aucun privilège ou droit particulier, comme l'accès aux serveurs d'un grand groupe, l'annuaire téléphonique, etc.

Ce niveau n'est suffisant, pour une personne non autorisée, que si l'entreprise ne dispose que de protections faibles contre le sinistre envisagé. Dans ce cas, comme nous l'avons déjà dit, l'entourage direct ou proche de personnes autorisées, donc dans la filière *non accrédités*, peut mettre à profit la connaissance du contexte ou l'observation pour accéder à l'information de manière non autorisée.

La population des « *initiés* », qui est nombreuse, atteint donc ce niveau standard.

On mettra aussi, souvent, dans cette catégorie tous les partenaires ou sous-traitants, si l'agression ou l'action ne demande pas d'autres moyens ou connaissances spécifiques, et s'il suffit d'être dans l'enceinte de l'entreprise.

Concernant la filière *pirates*, il peut s'agir de tout concurrent sans qu'il ait besoin de chercher des informations confidentielles comme des numéros d'accès spécifiques ou des procédures particulières de communication.

Pour la filière *malfaiteurs*, il s'agit des actions physiques non ciblées et donc de ce qu'est capable de faire un voyou ou une bande de jeunes délinquants. Un exemple typique d'agression ne demandant aucune compétence ni aucun moyen serait le vandalisme contre un centre de calcul situé au rez-de-chaussée ou au premier étage, avec des fenêtres donnant sur la voie publique, fenêtres ouvertes ou sans précaution particulière. N'importe quels voyous ou bande de jeunes casseurs peuvent être à l'origine d'un sinistre de ce type.

Pour la filière *espions*, il peut s'agir d'un visiteur occasionnel de l'entreprise ou d'une personne présente sur un stand lors d'un salon ou d'une foire professionnelle, donc sans lien particulier avec l'entreprise, qui peut avoir l'occasion de dérober une information sensible.

En ce qui concerne les *phénomènes naturels*, il s'agit là du niveau le plus courant auquel tout le monde est exposé, tel que la fuite d'une canalisation d'eau à un étage supérieur, un incendie voisin amenant les pompiers à intervenir avec des lances et pouvant provoquer des dégâts des eaux importants, etc.

NIVEAU MOYEN

Ce niveau est caractérisé par une compétence technique certaine, mais que possède normalement un bon professionnel de la filière, par des connaissances de l'entreprise ou de son système d'information accessibles par une recherche sérieuse, par des moyens techniques professionnels existant dans le commerce, et par des moyens financiers limités.

En interne, en y incluant les sous-traitants, il s'agit de professionnels, soit du logiciel, soit du matériel.

Parmi les *utilisateurs accrédités*, il s'agira des ingénieurs-système, des ingénieurs de développement ou des ingénieurs de maintenance, qui ont la compétence et les outils pour être à ce niveau sans moyens financiers supplémentaires, ou de certains utilisateurs qui ont ce niveau.

Pour les *opérateurs accrédités*, il s'agit davantage du personnel de maintenance, qui a accès physique au matériel, et qui peut, à ce niveau de capacité, effectuer des actions et des modifications sur le matériel pouvant passer inaperçues, telles que des inhibitions de fonctions de sécurité, branchements parasites d'écoutes ou de dérivations, etc.

Pour les *pirates* extérieurs, il s'agira de personnes pratiquant ce type d'activité de manière régulière et qui, s'ils ne connaissent pas l'entreprise et ses numéros d'accès, auront accès à ces informations par les messageries spécialisées et sauront utiliser ensuite des logiciels spécialisés de « *crackage* » de systèmes.

Des agressions qui ne réclament que ce niveau de compétence ou de moyens sont, par exemple, les accès au système d'information par les réseaux et la recherche de mots de passe par automatisme programmé sur micro ou par utilisation de listes de mots de passe classiquement utilisés.

Pour la filière *espions*, ce peut être des personnes entraînées, pouvant essayer de rentrer dans l'entreprise sous un prétexte quelconque pour y dérober des informations confidentielles qu'ils savent où chercher, avec effraction légère, en fracturant une serrure de tiroir de bureau par exemple.

En ce qui concerne la filière *malfaiteurs*, il s'agit de cambrioleurs pouvant tenter de pénétrer dans l'entreprise pour y dérober du matériel.

Sont classés à ce niveau moyen, les *phénomènes naturels* rares ou qui ne se propagent que par des concours de circonstances rares.

NIVEAU IMPORTANT

On considère, à ce niveau, une compétence technique de spécialiste, généralement associée à des moyens techniques matériels ou logiciels sophistiqués, commercialisés ou développés spécialement, ou à des moyens financiers relativement importants.

En interne, en y incluant les sous-traitants, il s'agit de bons spécialistes, soit du logiciel, soit du matériel, qui en connaissent tous les moindres détails.

En externe, il s'agit de spécialistes qui mettent en œuvre des moyens techniques et/ou financiers importants, financés éventuellement par leurs sponsors.

S'il s'agit de *pirates*, ce sont d'excellents spécialistes des réseaux, des protocoles de communication, et des systèmes d'exploitation. Ils en connaissent les faiblesses et les failles

possibles, sont à l'écoute permanente des techniques d'intrusion et savent exploiter la moindre opportunité.

Pour un *espion*, c'est le niveau de compétence nécessaire pour crocheter une serrure de sûreté sans laisser de traces et visiter à plusieurs reprises l'entreprise pour rechercher une information sans que personne ne remarque quoi que ce soit, pour écouter à distance une conversation grâce à des appareils très spécialisés ou pour monter une opération de chantage sur un membre du personnel.

A ce niveau, un *malfaiteur* n'hésitera pas à intervenir par une agression à main armée.

Les *événements naturels* qui atteignent ce niveau sont des cataclysmes exceptionnels ou des catastrophes de grande ampleur tels que des cyclones, tremblements de terre, glissements de terrain, etc.

NIVEAU TRÈS IMPORTANT

On considère à ce niveau une compétence d'expert et des moyens techniques extrêmement sophistiqués, ce qui implique des moyens financiers très importants, à la hauteur de ce que pourrait consentir un groupe international.

Ce niveau est souvent celui qui est mis en œuvre par de l'espionnage industriel de grande envergure ou par des organisations recherchant des gains financiers importants par détournement de fonds.

S'il s'agit du *personnel* de l'entreprise, il peut s'agir d'ingénieurs informaticiens de développement, capables d'introduire dans leurs logiciels des bombes logiques ou des « *chevaux de Troie* » indécélables sans procédures très strictes de test et de qualification.

S'il s'agit de *pirates*, c'est le niveau nécessaire pour décrypter un message chiffré avec un algorithme commercial de bonne tenue, comme un DES avec une clé de 112 bits, ou pour intercepter et reconstituer les signaux électromagnétiques émis par les équipements informatiques, et en particulier par les écrans des terminaux, que ce soit par rayonnement ou par conduction.

S'il s'agit d'un *espion*, des techniques très sophistiquées d'écoute des rayonnements émis par les équipements informatiques peuvent être un exemple. Le matériel nécessaire est déjà onéreux et ne peut être manipulé que par des experts.

S'il s'agit de *malfaiteurs*, c'est le niveau requis pour un sabotage avec des explosifs. On a donc atteint le niveau de la grande criminalité.

III. NIVEAUX D'AGRESSEURS ET TRIVIALITÉ DES CONDITIONS DE SURVENANCE

Il y a un parallélisme évident entre les niveaux d'agresseurs et la trivialité des conditions de survenance.

Il importe de bien comprendre le rôle du niveau d'agresseur dans l'évaluation du risque.

La trivialité des conditions de survenance indique le niveau minimum que doit avoir l'agression pour aboutir. Ce facteur de risque ne joue que sur la potentialité.

Le niveau d'agresseur, déterminé par les conditions de survenance nécessaires, aura une

influence sur la robustesse des mesures et donc sur l'ensemble des facteurs du risque et, en particulier sur l'impact.

En effet, nous considérons que les mesures dont la robustesse est inférieure au niveau de l'agresseur ont une efficacité nulle pour ce scénario.

Une bonne compréhension du rôle central joué par le niveau de l'agresseur évitera de mettre en place des mesures inutiles car insuffisamment robustes vis-à-vis de l'agresseur redouté.

Chapitre 8

LE MODÈLE DE RISQUE

Ayant abordé et décrit les différents facteurs ayant une influence sur le risque lié aux systèmes d'information, nous allons aborder la manière de caractériser de façon globale le risque dû aux divers scénarios de sinistre.

Il s'agit, en effet, dans un premier temps, de comparer les risques de l'entreprise face à divers scénarios, pour déterminer quels sont les plus critiques, quels sont ceux dont il convient de s'occuper en priorité.

Dans un deuxième temps, on choisira des mesures de sécurité et il faudra alors évaluer leurs effets, c'est-à-dire voir en quoi et comment elles ont fait évoluer les comparaisons faites précédemment.

I. ÉVALUATION DU RISQUE

Nous avons, à ce stade, reconnu deux composantes essentielles de la vulnérabilité de l'entreprise et appris à les évaluer, la question est donc maintenant de savoir comment évaluer un risque, en fonction de ces deux paramètres.

Nous ferons, tout d'abord, deux remarques sur les rôles respectifs de ces deux paramètres.

DISSYMMÉTRIE DES ESTIMATIONS

La première remarque concerne la dissymétrie des estimations de l'impact et de la potentialité.

En effet, autant l'impact peut être analysé de manière objective, autant la potentialité comporte une forte part de subjectivité.

Des analyses précises des pertes encourues après un sinistre peuvent être entreprises et le seul caractère de subjectivité, qui demeure néanmoins, réside dans l'estimation des seuils entre les niveaux de gravité d'impact. Il y a, certes, une part de subjectivité, mais qui consiste à estimer ce qui est plus ou moins grave pour nous-mêmes.

Par opposition, l'estimation de l'exposition naturelle et celle de l'impunité de l'agresseur ont un caractère plus subjectif car ce sont des évaluations de perceptions, l'enjeu ou le risque, ressenties par d'autres que nous.

Il faut donc être prudent et, éventuellement, affecter des coefficients d'incertitude différents à l'impact et à la potentialité.

DISSYMMÉTRIE DES POIDS DES FACTEURS

Les facteurs d'impact et de potentialité n'ont, à l'évidence, pas le même poids.

Nous entendons par là que peu d'entreprises considéreront comme équivalents un scénario de risque à impact extrêmement grave et potentialité faible et un scénario à impact peu grave et à potentialité forte.

Les facteurs ne sont pas multiplicatifs.

Ce raisonnement est presque universel ; il est à la base de l'assurance : nous préférons déboursier une faible somme, certaine dans ce cas, à une forte somme, même très hypothétique.

Si l'on veut parler du risque, il faut donc considérer qu'il est caractérisé par deux paramètres et ne pas tenter de les réduire à un.

Par contre, il est possible de définir autre chose, qui permet de comparer les risques entre eux, c'est l'aversion au risque.

II. L'AVERSION AU RISQUE

Rappelons, tout d'abord, que l'objectif de tout ce travail est fondamentalement d'être sélectif dans le choix de mesures de sécurité, c'est-à-dire d'exprimer un ordre de priorité entre les différentes solutions.

Alors l'étape finale qui consiste à établir ces priorités en fonction de la potentialité et de l'impact est un acte d'une dimension stratégique qui peut être préparé par des responsables de sécurité, mais qui demande une décision qui revient, en dernier chef, à la Direction de l'entreprise.

Pour ce faire, on peut préparer un cadre servant de support à la prise de décision, en demandant de remplir un tableau qui indique le niveau d' « *aversion au risque* » que l'on a pour chaque type de scénario de sinistre caractérisé par sa potentialité et son impact effectif.

Les stratégies que l'on peut exprimer à partir d'un tel tableau sont très diverses.

Dans le tableau donné en exemple, figure 6 ci-dessous, où l'aversion est notée de zéro à quatre, on a exprimé une priorité absolue au traitement des sinistres potentiels en fonction de la gravité de leur impact en indiquant une aversion au risque directement fonction de l'impact.

Ceci conduit à traiter en priorité les plus graves, parmi lesquels on pourra choisir en priorité les plus potentiels, et ainsi de suite. On peut constater que, dans une telle stratégie, on considère comme plus important, et donc comme une aversion au risque plus forte, un scénario de sinistre extrêmement grave mais de potentialité insignifiante qu'un scénario très grave et de forte potentialité.

Les méthodes qui ne tiennent pas compte de la potentialité ne font qu'admettre

implicitement une telle stratégie.

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

Figure 6

Une méthode qui retiendrait comme équivalents les paramètres de gravité et de potentialité reviendrait à remplir le tableau diagonale par diagonale.

Ce qui découle de ces exemples est que la seule solution sensée est de remplir ce tableau sans a priori, en se disant que l'on est en train de fixer sa stratégie, et que, surtout, il n'y a pas de vérité absolue dans ce domaine.

L'important est de déterminer son mode de conduite, avec un mode de réflexion et en s'appuyant sur des paramètres de base significatifs, afin que les parties prenantes dans la décision soient conscientes des choix qui ont été faits, et sachent que ces choix sont, en fait, des compromis et donc des « *impasses* ».

Pour finir, nous donnons figure 7, à titre d'exemple, un tableau 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.

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

Figure 7

