

Prévention et gestion des crises en PME : apports de la veille et de l'intelligence économique

François Brouard
Professeur
Sprott School of Business,
Carleton University
1125 Colonel By Drive
Ottawa (Ontario) Canada K1S 5B6
(613) 520-2600, poste 2213
fax : 613.520.44.27
francois_brouard@carleton.ca

Sophie Larivet
Professeure
Ecole Supérieure du Commerce
Extérieur / CIRCEE / CEREGE
Pôle Universitaire Léonard de Vinci
92916 Paris La Défense Cedex France
33.01.41.16.74.53
sophie.larivet@esce.fr

Résumé :

En matière de crises, les PME sont plus vulnérables que les grandes entreprises en raison de leurs ressources limitées : elles ont peu de marge de manœuvre. Dans un environnement concurrentiel d'autant plus propice aux événements potentiellement dramatiques qu'il est complexe, la gestion des crises est une compétence stratégique que ne peuvent ignorer les PME. Notre communication aura pour but de montrer en quoi la veille et l'intelligence économique peuvent contribuer à la prévention et à la gestion des crises, particulièrement en PME. La détection des signaux faibles comme contribution de la veille à la prévention des crises est une première contribution. Mais nous défendons l'idée que le développement d'une culture de la sécurité et la modernisation de la conception du risque qu'engendre la pratique de la veille ou de l'intelligence économique contribuent aussi à développer la compétence des petites organisations en matière de gestion de crises.

Thèmes :

24 Autres – gestion de crise et PME
10 PME innovantes

1. Introduction

Imaginez les situations suivantes. Le personnel d'une petite et moyenne entreprise (PME) ne peut se rendre dans les locaux de l'entreprise car les voies de communication sont inondées suite à un ouragan et à une pluie abondante empêchant tout déplacement aux alentours. L'inventaire est perdu. Une autre PME ne peut répondre aux besoins de sa clientèle car il y a une panne majeure d'électricité dans la région suite à un verglas intense. Elle dure plusieurs jours et empêche tout travail dans l'entreprise. L'entreprise ne peut rendre des services à sa clientèle. Suite à un tsunami, les installations d'une troisième PME sont totalement balayées et plusieurs membres du personnel sont décédés. Une autre PME voit la majeure partie de son personnel absent pour cause de maladie contagieuse. L'entreprise ne peut opérer normalement. Enfin, une entreprise comptant 70 personnes perd 25% de son chiffre d'affaires suite au déclenchement d'une rumeur lors d'un salon professionnel. Elle mettra deux ans à convaincre ses donneurs d'ordre de lui faire à nouveau confiance, et devra faire appel à un consultant pour l'y aider.

Les exemples précédents présentent certaines crises qui peuvent affecter une PME. Il est possible de reconnaître l'ouragan Katrina qui a frappé la Nouvelle Orléans aux États-Unis en septembre 2005 (Runyan, 2006; Tarras, 2005), la crise du verglas en janvier 1998 au Québec et en Ontario au Canada (Lalonde, 2004; Scanlon, 1999), le tsunami de décembre 2004 qui a frappé l'Asie du Sud-est et la pandémie du Syndrome Respiratoire Aigu Sévère (SRAS) à Toronto et dans le monde au printemps 2003. Le dernier cas est celui d'une PME française ayant subi l'attaque d'un concurrent allemand lors d'une conférence à Chicago. Celui-ci a fait répandre une rumeur selon laquelle la PME aurait dérobé des découvertes à une autre société (Von Gastrow, 2007). D'autres exemples peuvent être mentionnés. Le 11 septembre 2001 présente certainement un autre bel exemple d'une crise majeure affectant toute la société et ayant des répercussions majeures (Alexander et Alexander, 2001; Brouard, 2004b).

Ces quelques exemples sont sans doute suffisants pour reconnaître l'importance grandissante que les crises provenant de désastres naturels ou faisant suite à des actions humaines peuvent avoir sur les organisations. Étant donné leur taille et les ressources dont elles disposent, les PME sont plus fragiles face aux conséquences de ces crises que les grandes entreprises (Drummond et Chell, 1994). Cette fragilité peut s'expliquer par un nombre restreint de produits et services, une possible dépendance économique face à un nombre plus limité de contrats, par une trésorerie plus limitée (Drummond et Chell, 1994). Les conséquences peuvent être dramatiques. Il y a peu de place à l'erreur. Les coûts liés aux crises sont également très importants, tant en termes de ressources financières qu'humaines (Coleman, 2004; Elsubbaugh, Fildes et Rose, 2004). Il en va de la survie des organisations.

Dans un environnement concurrentiel d'autant plus propice aux événements potentiellement dramatiques qu'il est complexe (Perrow, 1999), la gestion des crises est une compétence stratégique que ne peuvent ignorer les PME (Spillan et Hough, 2003). Le nombre grandissant de crises et leur caractère changeant amènent le besoin pour le développement d'une compétence en gestion de crises (Boin et Lagadec, 2000) : puisque le monde est en changement, les dirigeants d'entreprises doivent changer eux aussi (Grimaldi, 2002). Malheureusement, la gestion de crises est un sujet peu abordé dans la littérature sur les PME (Runyan, 2006) même s'il existe un besoin de recherche à ce niveau (Hart, Heyse et Boin, 2001).

L'objectif de la recherche vise à montrer en quoi la veille et l'intelligence économique peuvent contribuer à la prévention et à la gestion des crises, particulièrement en PME. Il s'agit essentiellement d'une communication conceptuelle permettant d'élaborer les différents éléments potentiellement intéressants pour les PME. La détection des signaux faibles ou forts comme contribution de la veille à la prévention des crises est une première contribution. Mais nous défendons aussi l'idée que le développement d'une culture de la sécurité, et la modernisation de la conception du risque qu'engendre la pratique de la veille ou de l'intelligence économique contribuent à améliorer la compétence des petites organisations en matière de gestion de crises.

La communication se divise en quatre grandes parties. Après l'introduction et la justification de l'importance du sujet dans la première partie, la deuxième partie présente la gestion de crises et un cadre conceptuel général. La troisième partie souligne les apports de la veille et de l'intelligence économique. La dernière partie présente une conclusion pour terminer le tout.

2. Gestion de crises

Pour mieux comprendre la gestion de crises auprès des PME, il est utile de se référer à des modèles conceptuels de la gestion de crises en général. Il ne s'agira pas pour nous de produire un nouvel apport sur ce thème, mais de rappeler les principes généraux de la gestion de crises utiles pour la suite de notre propos.

2.1. Les crises

Sans entrer dans le débat sur l'acceptation du terme, nous définirons une crise comme «une série de conditions qui requiert d'une organisation l'exécution de tâches qui excèdent ou qui sont proches d'excéder ses capacités à faire face sans recours à des ressources conséquentes (souvent externes)» (traduction de Smith, 2005, p.318). Une crise résulte notamment de la combinaison de vulnérabilité(s) et d'une capacité insuffisante de gestion du risque (Ahrens et Rudolph, 2006). Essentiellement, une crise implique de grandes conséquences, une probabilité faible, de l'ambiguïté et une pression dans le temps pour décider et agir (Runyan, 2006).

Même si les crises sont généralement associées à des effets négatifs, il peut aussi y avoir des effets positifs (Lalonde, 2004). Parmi les aspects négatifs, notons les perturbations, le désordre, l'inertie, la paralysie, la confusion, les conflits, la compétition, les tensions et le stress. Parmi les aspects positifs, citons la recherche d'occasions, le renouvellement du tissu social, l'arrivée de nouvelles actions et solutions plus efficaces, la coopération, les alliances, l'entraide, la prévention, la solidarité, l'expérimentation et l'apprentissage.

Gundel (2005) propose deux axes pour classer les crises, soit la dimension « prédictibilité » et la dimension « influence ». En combinant ces deux dimensions, quatre types de crises sont identifiés, soit : (1) les crises conventionnelles (prédiction facile et influence facile), (2) les crises inattendues (prédiction difficile et influence facile), (3) les crises insolubles (prédiction facile et influence difficile), (4) les crises fondamentales (prédiction difficile et influence difficile). Citons quelques exemples pour illustrer les différents types de crises. L'explosion d'une usine chimique comme Bhopal en 1984 représente un exemple de crise conventionnelle. Une crise inattendue peut être l'incendie d'un funiculaire dans un tunnel à

Kaprun en Autriche en 2000 ayant tué 151 personnes. L'explosion d'un réacteur nucléaire à Tchernobyl en Ukraine en 1986 illustre une crise insoluble. Les événements du 11 septembre 2001 aux États-Unis avec l'effondrement des deux tours du World Trade Center illustre une crise fondamentale.

Ces exemples, si on les rapproche de la vie d'une PME, semblent revêtir un caractère inéluctable ou du moins imprévisible. Or, le caractère d'imprévisibilité de la crise est discuté : certains considèrent que les crises font désormais partie de la norme de la vie des organisations et plusieurs recherches ont montré que les crises étaient précédées de signaux (Roux-Dufort et Métais, 1996; Quinn, 1996). Hwang et Lichtenthal (2000) préconisent ainsi une distinction entre le côté subit et le côté cumulatif des crises : les crises sont le plus souvent le résultat d'une accumulation de dysfonctionnements, qui constituent autant de signes avant-coureurs. Il est donc essentiel, notamment, d'avoir des mécanismes de détection de ces signaux (Hickman et Crandall, 1997; Salter, 1997).

Enfin, cette nécessité est renforcée par une certaine évolution des crises : les crises modernes semblent différentes des crises dites traditionnelles, en raison des caractéristiques du monde d'aujourd'hui (interconnexion des systèmes, changements rapides..., voir le tableau A). Cette évolution implique un besoin pour une plus grande, ou une meilleure vigilance.

Tableau A
Caractéristiques des crises

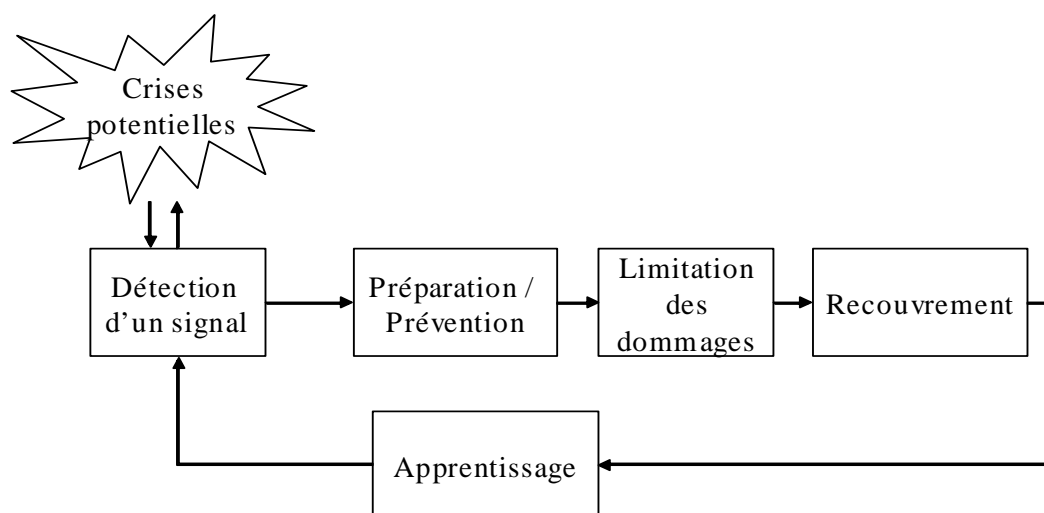
Crises plus traditionnelles	Crises plus modernes
<ul style="list-style-type: none"> - un événement connu, isolé - une situation perçue comme pouvant être gérée (techniquement, financièrement, socialement) - coûts relativement faciles à estimer - une durée limitée - procédures d'interventions codifiées et bien connues par des experts - un nombre limité d'intervenants - rôles, responsabilités et structure hiérarchique bien définis 	<ul style="list-style-type: none"> - impacts importants, population nombreuse affectée - coûts très élevés, dépassant les couvertures d'assurance - combinaison de problèmes sans précédent, touchant des ressources vitales - effet boule de neige ayant un écho d'une grande ampleur - systèmes d'urgence réagissant de la mauvaise manière : désuétude, non pertinence - incertitude extrême qui ne disparaît pas durant la période d'urgence - longue durée, se transformant dans le temps - convergence des intervenants - problèmes critiques de communication - enjeux majeurs de toutes sortes

Source : Boin et Lagadec (2000, p.186)

2.2. La gestion de crises

La gestion de crises peut se définir comme « un processus systématique engageant l'ensemble de l'organisation dans un effort pour éviter les crises pouvant toucher l'entreprise et gérer effectivement les crises qui surviennent » (traduction de Pearson, 2002, p.70). D'après les travaux de Elsubbaugh, Fildes et Rose (2004), Mitroff (1988) et Pearson et Mitroff (1993), le processus de gestion de crises peut se diviser en cinq phases : (1) détection des signaux, (2) préparation / prévention, (3) limitation des dommages, (4) recouvrement, (5) apprentissage. La figure A illustre la dynamique des cinq phases.

Figure A
Phases de la gestion de crise



Dans la section précédente le caractère rarement imprévisible des crises a été évoqué. La gestion de crise ne peut se faire que dans une entreprise qui accepte l'idée qu'une crise peut survenir. Alors elle cherchera à détecter les signes avant-coureurs d'une crise, et à l'éviter (prévention) ou du moins, si la crise est inéluctable, à s'y préparer et à en limiter les effets sur l'organisation. La phase de détection des signaux est donc fondamentale, car c'est son efficacité qui va, par la détection d'une crise potentielle, mettre en branle le processus de gestion de crises.

Les mécanismes de préparation / prévention permettent d'examiner les signes de faiblesses et de tester les réponses. L'importance de la préparation est reconnue comme un volet particulièrement important de la gestion de crise (King 2000). Il s'agit d'un sujet abondamment étudié (Runyan, 2006). L'idée est d'essayer de prévenir plutôt que de guérir. Par exemple, Gray (2002) mentionne les faiblesses dans la compatibilité des systèmes de communication des policiers et des pompiers pouvant avoir contribué au décès de pompiers de la ville de New York durant les événements du 11 septembre 2001.

Malgré toute la bonne volonté d'une organisation, il n'est pas possible d'éviter toutes les crises. Des mécanismes pour limiter les dommages permettent de prévenir la propagation des dommages et de limiter les effets de ceux-ci. Ces mécanismes permettent de se remettre sur pied le plus rapidement possible. La phase d'apprentissage offre une réflexion et un examen critique des événements et permet de tirer des leçons après la crise.

2.3. Gestion de crises et vulnérabilités des PME

Même s'il y a un intérêt certain pour la gestion de crises d'un côté et pour les PME de l'autre, il y a peu d'étude de la gestion de crises dans ces organisations (Drummond et Chell, 1994; Runyan, 2006). Cela s'explique sans doute par le peu de planification formelle dans les PME d'une manière générale et encore plus dans les situations de crises (Runyan, 2006; Smeltzer, Fann et Nikolaisen, 1988). Les dirigeants de PME doivent s'impliquer dans l'ensemble des phases de la gestion de crises (CICA, 2001). Pour qu'il y ait un intérêt pour la planification de crises, il faut que la PME ait déjà vécu elle-même une crise, ce qui n'implique pas la présence d'une équipe dédiée pour autant (Spillian et Hough, 2003).

À n'en pas douter, les PME ont des caractéristiques qui leur sont propres (GREPME, 1997). St-Pierre, Audet et Mathieu (2003) ont établis quatre types de PME, soit les PME globales, les PME innovantes, les PME exportatrices et les PME locales. Selon ces différents types de PME, il est possible que les PME soient exposées à des degrés divers aux crises. Par exemple, les PME globales ou PME exportatrices pourraient être plus sensibles à des crises internationales alors que les PME locales seraient moins affectées. Cela reste toutefois à démontrer par une étude empirique.

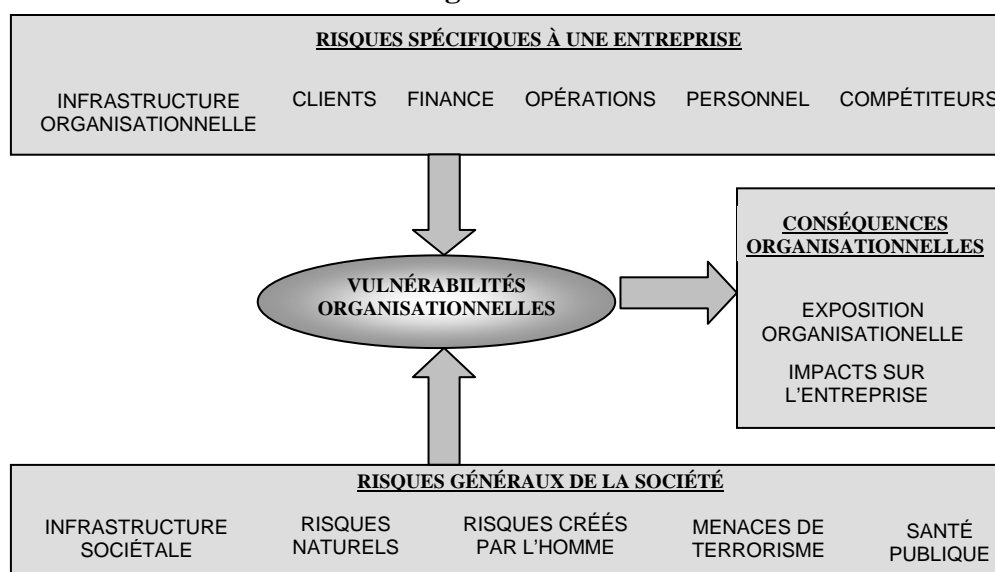
Une étude des entreprises australiennes confrontées à des crises permet de tirer certaines conclusions qui peuvent sans doute aussi s'appliquer aux PME (Coleman 2004). Aucun secteur d'activité n'est à l'abri des crises. Plus du quart (27%) des entreprises impliquées dans une crise n'a pas survécu. De plus, 10% des entreprises qui ont survécu sont aux prises avec une crise qui s'étire sur plusieurs années. Plus de la moitié des crises sont opérationnelles, lorsqu'une usine ou un processus connaît une défaillance et amène un incident ou un défaut dans les produits. Enfin, un peu moins de la moitié des crises implique des PME.

Afin de mieux cerner de manière pratique les défis que les PME doivent relever en termes de gestion de crise, il est essentiel d'identifier leurs vulnérabilités organisationnelles, possiblement par une étude diagnostique ou un audit (Besson et Possin, 1998; Hassid, Jacques-Gustave et Moinet, 1997). Haimès (2006) présente le concept de vulnérabilité comme une manifestation de l'état d'un système qui peut être exploité et ainsi causer des problèmes au système. Cependant, les vulnérabilités des PME ne sont pas liées qu'à des failles « exploitables » (par un concurrent par exemple), mais également à toutes sortes de risques pouvant se matérialiser sans qu'il y ait une intention malveillante. C'est le cas des risques naturels ou des défauts d'infrastructures. Nous emploierons donc le terme de vulnérabilités organisationnelles pour désigner l'ensemble des sources potentielles de crise pour une organisation donnée, que la menace soit intentionnelle ou accidentelle.

De nombreux auteurs ont proposé des listes afin de répertorier les différentes causes des crises (Ahrens et Rudolph, 2006; Boullé, Vrolijk et Palm, 1997; Coleman, 2004; Deloitte, 2007; Egan, 2007; Gorman, Schintler, Kulkarni et Stough, 2004; Haimès 2006; Mitroff et al., 1989a; Pearson and Clair, 1998; Salter 1997; Spillian et Hough, 2003). Nous en proposons un état synthétique et spécifique aux PME. La figure B illustre la structure proposée par les auteurs des vulnérabilités organisationnelles.

Dans la figure B, les composantes et conséquences des vulnérabilités organisationnelles sont représentées. Les composantes des vulnérabilités sont des risques liés soit à l'entreprise proprement dite, soit à la société en général. Un premier cadre regroupe les risques spécifiques à une entreprise, parmi lesquels figurent l'infrastructure de l'organisation, les clients, les finances, les opérations, le personnel et les compétiteurs. Un second cadre regroupe les risques généraux de la société : infrastructure sociétale, risques naturels, risques créés par l'homme, menaces terroristes et santé publique. Enfin, un dernier cadre regroupe les conséquences organisationnelles (exposition organisationnelle et impacts). Le tableau B regroupe des exemples illustrant chacune de ces dimensions.

Figure B
Vulnérabilités organisationnelles des PME



3. Contributions de la veille et de l'intelligence économique à la gestion de crise

La veille et l'intelligence économique sont des pratiques à présent bien connues des praticiens et des chercheurs. Nous nous bornerons à résumer ici leurs positionnements respectifs : l'intelligence économique est la combinaison de trois fonctions informationnelles (Clerc, 1995 ; Harbulot, 1995 ; Larivet, 2002 ; 2006) : la principale de ces fonctions est la veille stratégique, mais s'y ajoutent la gestion du risque informationnel et l'influence. Ces pratiques, et surtout la veille, sont assez développées en PME. Si l'on en croit les différentes études sur le sujet, on peut estimer grossièrement que 40 à 60% des PME font de la veille, de façon plus ou moins formalisée et/ou récurrente, et qu'environ 20% ont des pratiques, au moins parcellaires, d'intelligence économique (Larivet, 2002). Ce développement des pratiques informationnelles des PME nous invite à examiner en quoi elles sont susceptibles de contribuer à la gestion de crise.

3.1. Contribution à la phase de détection de signaux

La détection des signaux se situe au deuxième rang dans la préparation de la gestion de crise après la diffusion d'une culture favorable (Elsubbaugh, Fildes et Rose, 2004). Néanmoins, quand on réfléchit à la contribution de l'intelligence économique à la gestion de crise, c'est cette étape de détection des signaux qui apparaît comme étant directement dépendante d'une veille stratégique efficace.

La veille stratégique (parfois appelée renseignement ou renseignement économique) est un « processus informationnel par lequel une organisation se met à l'écoute de son environnement pour décider et agir dans la poursuite de ses objectifs » (Brouard, 2000, p.28). Elle est donc un système de détection de signaux, qui peuvent, le cas échéant, après analyse et diffusion, initier le cycle de la gestion de crise décrit dans la section précédente. Ce phénomène a déjà été décrit de façon générale par Brouard (2004a).

D'une façon plus spécifique aux PME, tout laisse à penser que le rôle de la veille stratégique sera d'autant plus important qu'il y existe rarement une équipe de gestion de crises dédiée. Dans une grande entreprise, où il peut exister, par exemple, une direction du risque, il faudrait étudier la façon dont le système de veille stratégique et celui de gestion de crise interagissent. Dans la plupart des PME, il faut envisager que c'est le processus de veille stratégique qui servira de système d'alerte et qui permettra, si une crise était détectée, de démarrer un processus de gestion de crises.

Tableau B
Facteurs contribuant à la vulnérabilité des PME et conséquences

RISQUES SPÉCIFIQUES À L'ORGANISATION	RISQUES GÉNÉRAUX DE LA SOCIÉTÉ
<p><i>Infrastructures organisationnelles</i> Actifs immobilisés (bâtiments, usines, terrain), actifs intangibles (brevets, droits d'auteurs, technologie de l'information)</p> <p><i>Clients</i> Satisfaction, prix, fraude, poursuites, plaintes, rappel de produits, boycottage de produits</p> <p><i>Finance</i> Financement, crédit, taux de change, taux d'intérêt, fiscalité, vol de documents</p> <p><i>Opérations</i> Recherche et développement, productivité, cycle du produit, fournisseur, qualité des produits, stratégie, mesure de performance, gouvernance, incident industriel, panne du système d'information, hacking, bris majeur d'équipement, enquête gouvernementale</p> <p><i>Personnel</i> Ressources humaines, santé et sécurité, poursuites, kidnapping, fraude et vol des cadres, fraude et vol des employés, décès d'un employé clé, violence au travail, harcèlement sexuel</p> <p><i>Compétiteurs et groupes de pression</i> Espionnage, extorsion, sabotage de produits, campagne de dénigrement, rumeurs, corruption, blanchiment d'argent, takeover hostile</p>	<p><i>Infrastructure sociétale</i> Transport (routes, ponts, autobus, trains, gare, avions, aéroport, hélicoptère), ressources (eau, énergie, électricité, gaz et pétrole) personnel d'urgence (police, pompiers, ambulances, services paramédicaux, hôpitaux), constructions (bâtiments, barrages, pipelines, collecte des égouts), télécommunications (TI, réseau internet, câbles de fibres optiques)</p> <p><i>Risques naturels</i> Tremblement de terre, inondation, feu, tornade, ouragan, tempête de neige, glissement de terrain, tsunami, volcans, avalanche, sécheresse</p> <p><i>Risques créés par l'homme</i> Guerre, crime, feu, émeute, déversement écologique</p> <p><i>Menaces de terrorisme</i> Biologique, chimique, explosif, incendiaire, nucléaire</p> <p><i>Santé publique</i> Pandémie, risques de santé publique</p>
↓	↓
CONSÉQUENCES ORGANISATIONNELLES	
<p align="center"><i>Exposition organisationnelle</i></p> <p>- Impact de l'exposition : habileté à opérer, habileté à survivre, coûts d'opérations, durée de l'interruption</p> <p>- Degré d'exposition : centralisation / décentralisation, activités critiques à la mission, opérations impliquées, interdépendance des tâches</p> <p align="center"><i>Impacts</i></p> <p>- Faillite, perte de clients, perte de contrats, réduction dans la part de marché, réduction de la rentabilité, réduction des ventes, réputation des ventes, perte de vie sur l'entreprise</p>	

Par ailleurs, même dans une PME qui se serait doté d'un système de gestion du risque prévoyant la mise en œuvre d'un processus de gestion de crises (si un risque majeur est avéré, il peut se transformer en crise), la veille stratégique aurait encore toute sa place dans le déclenchement de la gestion de crises. En effet, la gestion du risque s'appuie sur des risques calculés, évalués, cartographiés : ils sont répertoriés, leur occurrence et leur gravité estimées, un système d'alerte est mis en place. Lorsqu'une menace devient concrète, le risque qu'elle représente est traité (El Mabrouki, 2007). Ceci est supposé éviter la crise. Dans le cas d'un risque non cartographié, une PME risque tout simplement de ne pas voir arriver la menace, comme si elle avait des œillères. Il faut donc que l'entreprise puisse compter sur un système

qui ne se contente pas de collecter de l'information relative à des menaces déjà identifiées (signaux forts), mais également de recueillir, analyser et diffuser des signaux faibles, qui pourront se révéler précurseurs de crises.

Paturel (2002) a très bien décrit le cas de l'entreprise Markal, PME française qui a failli voir son produit phare (le boulgour) tomber en désuétude à cause d'une opération de lobbying communautaire menée par une entreprise américaine. Ce risque législatif ne faisait pas partie des risques imaginés par le dirigeant de la PME. Il n'a du qu'à un heureux hasard de s'apercevoir du danger et a pu intervenir juste à temps, avec l'aide du pouvoir politique. Ce cas illustre parfaitement l'intérêt de s'intéresser à tout l'environnement de la PME pour prévenir les crises, car elles peuvent survenir de n'importe quel élément de cet environnement, voir de l'entreprise elle-même. Le système de détection des signes avant-coureur de la crise ne doit exclure a priori aucune des vulnérabilités organisationnelles décrites dans la partie 2. Or, la veille stratégique permet justement de concevoir et de surveiller l'environnement de l'entreprise de façon très large.

En effet, la veille est souvent découpée en veille commerciale, concurrentielle, sociétale et technologique (Brouard, 2000). Certains auteurs (Brouard, 2004a ; Cristallini et Paturel, 1999) y ajoutent l'environnement « interne » de l'entreprise (procédures, management, culture, ressources humaines, actifs...). Typiquement, le risque successoral est une cause potentielle de crise en PME, et doit être détecté et traité pour éviter la crise. Ces différentes catégories de veille, généralement utilisées dans une optique offensive (détecter des opportunités) recouvrent l'ensemble des vulnérabilités organisationnelles des PME (voir tableau B). Elles peuvent donc également servir dans un but défensif : détecter les menaces et signaux de crises. Cette double orientation du système de recueil (ou cueillette) de la veille stratégique est représenté dans la figure C (Brouard, 2004). Le cycle du renseignement (cueillette) y est représenté à droite tandis que le cycle de la protection que nous aborderons dans la section suivante est à gauche.

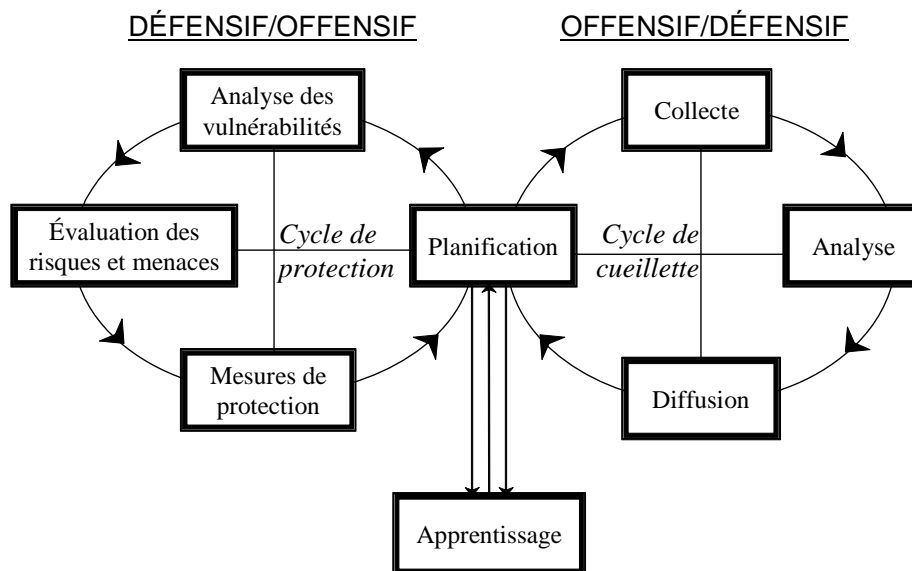
3.2. Protéger l'entreprise et moderniser sa culture de la protection

L'existence d'une culture favorable à la gestion de crises est primordiale (Elsabbagh, Fildes et Rose, 2004). C'est pourquoi les nouvelles approches de la veille stratégique et de l'intelligence économique, qui incluent un cycle de protection (voir figure C) sont d'excellents moyens de sensibiliser la direction comme le personnel d'une PME. La protection, encore appelée gestion du risque informationnel, regroupe les notions de sécurité et de sûreté de l'information, la contre-intelligence, la lutte contre les rumeurs, et la protection du patrimoine immatériel de l'entreprise (Larivet, 2002). Nous avons cité un exemple de crise vécue par une PME déclenchée par une rumeur en introduction. Un autre exemple est l'affaire, révélée en France, il y a quelques années, dans une affaire opposant deux grandes écoles de commerce. L'une avait utilisé un prestataire pour répandre une image négative de la formation de l'autre à travers des témoignages de faux clients (étudiants) sur des forums électroniques (Fauconnier, 2005).

Concrètement, la gestion du risque informationnel consiste à protéger l'entreprise des menaces accidentelles ou intentionnelles pesant sur ses ressources en informations, ses connaissances, ses compétences (on parle de patrimoine informationnel), ainsi qu'à contrôler les informations émises par l'entreprise et qui pourraient constituer une menace (révélation d'un secret de fabrication, par exemple). Elle suit le cycle représenté en figure C. Elle

contribue donc aux phases de préparation/prévention, de recouvrement et d'apprentissage du processus de gestion de crises, en ce qui concerne les menaces liées à l'information.

Figure C
Dimensions offensives et défensives de la veille stratégique



En dehors de cette contribution directe de l'intelligence économique ou de la veille stratégique au processus de gestion de crise, on peut envisager deux autres apports un peu moins concrets, mais essentiels.

Le premier de ces apports est la contribution à la culture de la protection. Sensibiliser une PME à la veille stratégique c'est lui faire entendre que l'inattendu la concerne, qu'il est probable qu'un jour ou l'autre, une crise survienne, et qu'elle peut et doit s'y préparer (Brouard, 2007). Certaines formations à l'intelligence économique incluent d'ailleurs des cours de gestion de crise (par exemple au CERAM à Nice). Les conférences de sensibilisation des PME françaises abordent systématiquement des exemples de crises qui auraient pu être minimisées ou évitées si un système de veille avait existé. Certains commentateurs notent même une très, voire trop grande présence de cet aspect sécuritaire dans la promotion de l'intelligence économique (Harbulot, 2007).

Le second apport, bien qu'il concerne également la culture de l'entreprise, est d'ordre plus « qualitatif » que « quantitatif ». Il consiste à une modernisation de la conception des crises. En effet, les crises de nature informationnelle sont de plus en plus fréquentes, mais restent méconnues. À ce titre, elles représentent un danger très important, le moindre retard dans la compréhension de la nature d'une crise pouvant engendrer des conséquences graves (à cause de l'effet « boule de neige » des crises modernes). C'est ce qui s'est passé dans le cas présenté en introduction : une rumeur mal traitée car non identifiée comme telle peut se répandre et provoquer une crise importante pour une PME. Même sans aller jusqu'à ce type de crise particulièrement complexe, la récente panne d'Internet en Inde montre que de nouveaux types de crises doivent être prises en considération par les PME. La veille stratégique et l'intelligence économique mettent l'accent sur ces nouvelles menaces et peuvent donc aider une petite entreprise à ouvrir son système de détection de signaux à des horizons plus variés.

3.3. Aider au recouvrement d'une crise

La dernière dimension de l'intelligence économique, la seule qui ne soit pas commune à la veille stratégique, est l'influence. Elle consiste à agir indirectement sur l'environnement (Baumard, 2000) par le truchement de dissémination d'informations dans celui-ci.

Il existe différentes techniques d'influence : par exemple, les pratiques de lobbying (qui peuvent prendre la forme de dossiers sur des problématiques sectorielles communiquées aux décideurs politiques) ou encore « l'undercover marketing » (type de communication d'influence) qui consiste à créer un « buzz » favorable grâce à des « taupes » sur les forums et autres lieux de discussions. Il existe ainsi de soi-disant internautes très calés qui répondent systématiquement aux attaques concernant les Airbus (Labbé et Recasens, 1998). C'est, entre autres, un moyen de contrebalancer les plaintes de clients mécontents.

Contrairement aux idées reçues, ces pratiques sont accessibles aux PME. Larivet (2002) a montré qu'environ 20% des PME pratiquaient l'influence, à un niveau plus ou moins modeste. C'est un moyen d'action parmi d'autres, pouvant aider au recouvrement des crises (à la limitation de leurs effets). Nous reprendrons ici l'exemple cité plus haut de l'entreprise Markal, qui a mis en place une opération de lobbying communautaire pour contrer celle de ses adversaires américains. On pourrait tout à fait imaginer, également, qu'une PME confrontée à une rumeur déploie un système comparable à celui d'Airbus (à plus petite échelle bien sûr).

Cette dernière contribution de l'intelligence économique mériterait d'être d'avantage étudiée, afin d'en préciser les modalités. Néanmoins, les exemples ci-dessus illustrent son existence et renforcent la thèse d'une contribution de la veille et de l'intelligence économique à la gestion des crises.

3.4. Aborder la gestion des crises en PME par la veille stratégique et l'IE

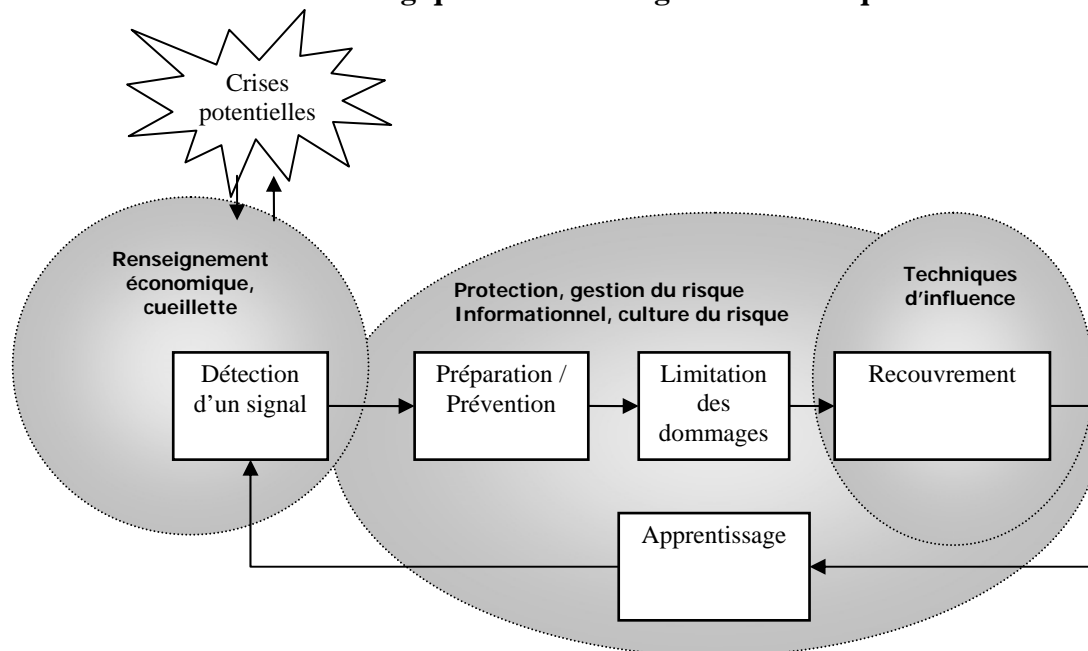
Comme nous l'avons vu dans les trois sous-sections précédentes, la veille stratégique et l'intelligence économiques peuvent représenter des apports à toutes les étapes de la gestion de crise, comme représenté dans la figure D. La cueillette d'information est susceptible de contribuer très fortement au système de détection des signaux, en mettant l'accent sur les signaux faibles et en permettant une surveillance de tous les éléments de vulnérabilité de l'entreprise. Le cycle de la protection et le développement d'une gestion du risque informationnel peuvent, par leurs processus et par la culture nouvelle du risque qu'ils proposent, contribuer aux phases suivantes du processus de gestion de crise. Enfin, pour les PME les plus avancées en matière d'intelligence économique, certaines techniques d'influence peuvent aider au recouvrement d'une crise.

Ces contributions, qu'on pourrait aussi envisager dans le cadre de grandes entreprises, sont toutefois particulièrement intéressantes à mettre en lumière pour la gestion des PME. En effet, un des moyens pour les petites entreprises de pallier leur manque de ressources est d'exploiter au maximum les synergies entre les processus de gestion qu'elles mettent en place. Une entreprise ayant des moyens financiers et humains limités peut ainsi tout à fait profiter de la mise en place ou du réexamen d'un système de veille stratégique pour penser et préparer sa gestion des crises. Par exemple, les personnes chargées de la veille concurrentielle pourront être sensibilisées aux crises que peuvent déclencher les rumeurs lancées par des concurrents. Elles pourront ainsi mettre en place de nouveaux indicateurs d'image ou de nouveaux sites internet à surveiller, et contribuer ainsi à une meilleure prévention des crises, sans que le

moyens déployés ne soient trop importants. Si une PME ne peut empêcher un tsunami ou un ouragan, son dirigeant, s'il prend conscience que le savoir-faire de son entreprise repose sur quelques rares techniciens spécialisés, pourra prendre quelques mesures simples pour éviter que toutes leurs connaissances ne disparaissent avec eux.

Nous suggérons ainsi que la veille stratégique et l'intelligence économique peuvent être un excellent point d'entrée dans la gestion de crise pour les PME, qui n'ont pas forcément les moyens de constituer un département spécialisé.

Figure D
Phases de la gestion de crise et apports de la veille stratégique et de l'intelligence économique



4. Conclusion

Dans cette communication conceptuelle, la gestion de crises est associée à la veille et à l'intelligence économique. L'objectif étant ici de présenter les différentes dimensions de la gestion de crises des PME. Dans un contexte de PME, la veille, qui est la plus évidente et la plus importante, et l'intelligence économique peuvent aider à prévenir les crises et améliorer leur gestion. De plus, le développement d'une culture de la sécurité, la modernisation de la conception du risque voire la connaissance de certaines techniques d'influence, qu'engendre la pratique de la veille ou de l'intelligence économique concourent aussi à améliorer la compétence des PME en matière de gestion de crises. La gestion de crises s'insère aussi dans l'implantation d'une stratégie organisationnelle pour anticiper l'avenir et dans un contexte général de gestion des connaissances.

Au plan pratique, les dirigeants de PME, manquant habituellement de ressources, doivent être davantage sensibilisés aux problèmes potentiels que peuvent engendrer les crises qui ne feraient pas l'objet d'une gestion attentive, et ce tant au plan de la détection initiale, de la prévention, de la limitation des dommages et du recouvrement. L'exploitation des synergies entre les différents processus étudiés pourraient leur permettre de développer un système de

prévention des crises en utilisant peu de moyens humains ou financiers. Nous avons suggéré quelques pistes de réflexion à des fins d'action, mais la dimension conceptuelle de notre travail ne nous a pas permis de faire plus de propositions concrètes. C'est cette limite qui nous conduit à terminer en proposant des pistes de recherche futures.

Au plan de la recherche, en effet, la communication amène un champ à explorer, en particulier dans le contexte de l'étude des PME. Par une série d'études empiriques auprès des PME, il serait possible de mieux cerner les types de crises que les PME doivent affronter, l'importance de ces crises, leur impact, le niveau de préparation, les meilleures pratiques et les obstacles pour implanter une bonne gestion de crise. Une autre possibilité serait d'étudier l'impact des crises pour différents types de PME. Ainsi, il serait possible de savoir si certaines PME seraient plus sensibles à des crises ou à certaines formes de crises.

Références

- Aguilar, F.J. (1967). *Scanning the Business Environment*. New York : Macmillan.
- Ahrens, J., Rudolph, P.M. (2006). The Importance of Governance in Risk Reduction and Disaster Management. *Journal of Contingencies and Crisis Management*. 14(4), 207-220.
- Alexander, D.C., Alexander, Y. (2002). *Terrorism and Business: The Impact of September 11, 2001*, Ardsley: Transnational Publishers inc., 265p.
- Baumard Ph. (2000). *Analyse stratégique, mouvements, signaux concurrentiels et interdépendance*, Paris : Dunod.
- Besson, B., Possin, J.-C. (1998). *L'audit d'intelligence économique*. Paris : Dunod.
- Boin, A., Lagadec, P. (2000). Preparing for the Future : Critical Challenges in Crisis Management. *Journal of Contingencies and Crisis Management*. 8(4), 185-191.
- Boullé, P., Vrolijk, L., Palm, E. (1997). Vulnerabilities Reduction for Sustainable Urban Development. *Journal of Contingencies and Crisis Management*. 5(3), 179-188.
- Brouard, F. (2000). Que la veille stratégique se lève : faisons le point sur la terminologie et le concept, Conférence conjointe de l'Association des sciences administratives du Canada (ASAC) / International Federation of Scholarly Associations of Management (IFSAM). Montréal, juillet, *stratégie* 21(6), 22-33.
- Brouard, F. (2004a). Développement d'un outil diagnostique des pratiques existantes de la veille stratégique auprès des PME. Thèse de doctorat, Université du Québec à Trois-Rivières.
- Brouard, F. (2004b). Business Intelligence for Canadian Corporations after September 11, *Journal of Competitive Intelligence and Management*. 2(1), 1-15.
- Brouard, F. (2007). Awareness and Assessment of Strategic Intelligence – A Diagnostic Tool, in M. Xu (Ed.) *Managing Strategic Intelligence: Techniques and Technologies*, Hershey, Information Science Reference, 122-140.
- CICA. (2001). *Crisis Management for Directors*, Toronto: Canadian Institute of Chartered Accountants, 11p.
- Clerc, P. (1995), Intelligence économique, *Encyclopædia Universalis*, 1995, http://www.universalis.fr/corpus2-encyclopedie/117/0/UN95029/encyclopedie/INTELLIGENCE_ECONOMIQUE.htm [consulté le 11.06.2008].
- Coleman, L. (2004). The Frequency and Cost of Corporate Crisis. *Journal of Contingencies and Crisis Management*. 12(1), 2-13.
- Cristallini V., Paturol R. (1999). Risques liés à un déficit de la fonction d'intelligence économique et à la polarisation sur l'environnement externe d'une entreprise, *Revue d'Intelligence Economique*, 5, 10-28.

- Daft, R.L., Weick, K.E. (1984). Toward a Model of Organizations as Interpretation Systems, *Academy of Management Review*, 9(2), p.284-295.
- Deloitte. (2007). *Crises et Menaces*. Montréal : Samson Blair / Deloitte & Touche.
- Drummond, H., Chell, E. (1994). Crisis Management in a Small Business : A Tale of Two Solicitors' Firms. *Management Decision*. 32(1), 37-40.
- Egan, M.J. (2007). Anticipating Future Vulnerability : Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Journal of Contingencies and Crisis Management*. 15(1), 4-17.
- El Mabrouki M.N. (2007). L'intelligence économique : quels apports à la gestion des risques ? 5ème colloque Veille Stratégique Scientifique et Technologique (VSST), Marrakech, octobre [CD-ROM].
- Elsaubaug, S., Fildes, R., Rose, M.B. (2004). Preparation for Crisis Management : A Proposed Model and Empirical Evidence. *Journal of Contingencies and Crisis Management*. 12(3), 112-127.
- Fauconnier P. (2005). Le scénario délirant de « l'opération volutes », *Le Nouvel Observateur*, 25/08/2005, 120-121.
- GAO. (2005). Homeland Security – Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention. United States Government Accountability Office, Report to Congressional Requesters GAO-05-170.
- Garg, V.K., Walters, B.A, Priem, R.L. (2003). Chief executive scanning emphases, environmental dynamism, and manufacturing firm performance, *Strategic Management Journal*, 24(8), p.725-744.
- Gorman, S.P., Schintler, L., Kulkarni, R., Stough, R. (2004). The Revenge of Distance : Vulnerability Analysis of Critical Information Infrastructure. *Journal of Contingencies and Crisis Management*. 12(2), 48-63.
- Gray, K. (2002). Ottawa could learn from Sept. 11, *The Ottawa Citizen*, July 25, p.D7.
- GREPME. (P.-A. Julien, dir.) (1997). *Les PME : bilan et perspectives*. GREPME (Groupe de recherche en économie et gestion des PME), 2^e édition. Cap Rouge : Presses inter universitaires/Economica.
- Gundel, S. (2005). Toward a New Typology of Crises. *Journal of Contingencies and Crisis Management*. 13(3), 106-115.
- Haines, Y.Y. (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. *Risk Analysis*. 26(2), 293-296.
- Harbulot C. (1995). *La machine de guerre économique*. Etats-Unis, Japon, Europe. Paris : Economica.
- Harbulot C. (2007). *La main invisible des puissances, les Européens face à la guerre économique*. Paris: Ellipses.
- Hart, P., Heyse, L., Boin, A. (2001). Guest Editorial Introduction New Trends in Crisis Management Practice and Crisis Management Research : Setting the Agenda. *Journal of Contingencies and Crisis Management*. 9(4), 181-188.
- Hassid, L., Jacques-Gustave, P., Moinet, N. (1997). *Les PME face au défi de l'intelligence économique*. Paris : Dunod.
- Hickman, J.R., Crandall, W. (1997). Before Disaster Hits : A Multifaceted Approach To Crisis Management. *Business Horizons*. 40(2), 75-79.
- Hwang, P., Lichtenthal, J.D. (2000). Anatomy of Organizational Crises. *Journal of Contingencies and Crisis Management*. 8(3), 129-140.
- King, D. (2000). You're on Your Own : Community Vulnerability and the Need for Awareness and Education for Predictable Natural Disasters. *Journal of Contingencies and Crisis Management*. 8(4), 223-228.
- Labbé et Recasens (1998). L'information sous influence, *Le Monde*, 18/01/1998.

- Lalonde, C. (2004). In Search of Archetypes in Crisis Management. *Journal of Contingencies and Crisis Management*. 12(2), 76-88.
- Larivet, S. (2002). Les réalités de l'intelligence économique en PME. Thèse de doctorat, Université de Toulon et du Var, Toulon.
- Larivet, S. (2006). L'intelligence économique : un concept managérial », *Revue Market Management - Marketing et Communication*, 3(3), 22-35.
- Paturel R. (2002). Markal- La pratique d'influence dans la petite entreprise, in *Les pratiques de l'Intelligence Economique, huit cas d'entreprises*, Levet J.-L., Paris : Economica, 83-100.
- Perrow, C. (1999). Organizing to Reduce the Vulnerabilities of Complexity. *Journal of Contingencies and Crisis Management*. 7(3), 150-155.
- Peteraf, M.A. (1993). The Cornerstones of Competitive Advantage: A Resource-Based View, *Strategic Management Journal*, 14(3), p.179-191.
- Quinn, J.F. (1996). Terrorism Comes to Tokyo: The Aum Shinri Ky Incident, *OPSEC Journal*, 3.
- Raymond, L., Julien, P.A., Ramangalahy, C. (2001). Technological Scanning by Small Canadian Manufacturers, *Journal of Small Business Management*, 39(2), p.123-138.
- Roux-Dufort C., Métais E. (1996). L'apprentissage organisationnel comme processus de développement des compétences centrales de l'entreprise : l'exemple de la gestion des crises à Electricité De France, 5ème Conférence de l'Association Internationale de Management Stratégique (AIMS), Lille, mai 1996, [<http://www.strategie-aims.com/lille/com6301.pdf>], 24p.
- Runyan, R.C. (2006). Small Business in the Face of Crisis: Identifying Barriers to Recovery from a Natural Disaster. *Journal of Contingencies and Crisis Management*. 14(1), 12-26.
- Salter, J. (1997). Risk Management in a Disaster Management Context. *Journal of Contingencies and Crisis Management*. 5(1), 60-65.
- Sarewitz, D., Pielke, R., Keykhah, M. (2003). Vulnerabilities and Risk : Some Thoughts from a Political and Policy Perspective. *Risk Analysis*. 23(4), 805-810.
- Scanlon, J. (1999). Emergent Groups in Established Frameworks : Ottawa Carleton's Response to the 1998 Ice Disaster. *Journal of Contingencies and Crisis Management*. 7(1), 30-37.
- Scanlon, J. (2005). Two Cities, Two Evacuations : Some Thoughts on Moving People Out. [version électronique] Saisie de <http://understandingkatrina.ssrc.org/Scanlon/pf/>
- Sheaffer, Z., Richardson, B., Rosenblatt, Z. (1998). Early-Warning-Signals Management : A Lesson from the Barings Crisis. *Journal of Contingencies and Crisis Management*. 6(1), 1-22.
- Smeltzer, L.R., Fann, G.L., Nikolaisen, V.N. (1988). Environmental Scanning Practices in Small Business. *Journal of Small Business Management*. 26(3), 55-62.
- Smith, D. (2005). Business (not) as usual : crisis management, service recovery and the vulnerability of organisations. *Journal of Services Marketing*. 19(5), 309-320.
- Spillan, J., Hough, M. (2003). Crisis Planning in Small Businesses : Importance, Impetus and Indifference. *European Management Journal*. 21(3), 398-407.
- St-Pierre, J., Audet, J., Mathieu, C. (2003). Les nouveaux modèles d'affaires des PME manufacturières : une étude exploratoire. Trois-Rivières: Laboratoire de Recherche sur la Performance des Entreprises, Institut de recherche sur les PME, Université du Québec à Trois-Rivières.
- Taras, R. (2005). After the Storm : pathologies of Decision-Making in New Orleans. *Options Politiques*. décembre, 60-65.
- Von Gastrow, J.-P. (2007). Rumeurs : la riposte des entreprises, *Le Monde*, 06/07/2007, 13.