PLAN DE CONTINUITÉ D'ACTIVITÉ ET SYSTÈME D'INFORMATION

Vers l'entreprise résiliente

Matthieu Bennasar

MBCI et CISM

Préface de Paul Théron

DUNOD

Toutes les marques citées dans cet ouvrage sont des marques déposées par leurs propriétaires respectifs.

Illustration de couverture :
Landscape Arch-Arches National Park, Utah, États-Unis.
© Matthieu Bennasar

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.
Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.
Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).

DANGER
LE PHOTOCOPILLAGE TUE LE LIVRE

© Dunod, Paris, 2010
ISBN 978-2-10-054830-9

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).
Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Préface

Ce qui frappe une Direction Générale lorsque survient une crise, c'est souvent le sentiment du manque de préparation pour y faire face.

Pour Gilbert (in GEM 2002[1]), les crises sont des « *situations où, en raison de la disproportion existant entre les problèmes apparaissant et les moyens de les traiter, les organisations en charge des activités à risques se trouvent de fait "dépossédées" de ces problèmes par de nombreux et divers acteurs intervenant et voient leur compétence et leur légitimité remises en question (du fait, notamment, de l'intervention de la justice, etc.)* ». Pour le European Center of Technological Safety (in GEM 2002), la crise est définie ainsi : « *Derived from the Greek "krisis", meaning a crucial turning point in the course of anything, an unstable condition in which an abrupt or decisive change is impending. A major, unpredictable event that has potentially negative results. The event and its aftermath may significantly dammage an organization and its employees, products, services, financial condition, and reputation. A crisis, like an accident, is a disruption that physically affects a system as a whole and also threatens the priority goals of an organization and challenges the traditional behaviors and values shared in a organization* ».

Interruption du business = Dommage subi

C'est dans cette équation du risque que le *Business Continuity Management* (BCM, ou MCA pour Management de la continuité d'activité en français) intervient. Avec ses démarches et ses réponses fédératrices propres.

La notion de « continuité » doit être bien comprise. Il ne s'agit pas simplement de faire en sorte que les chaînes de production ou les serveurs et réseaux informatiques continuent de fonctionner malgré les phénomènes pouvant les affecter. Il s'agit de poursuivre les activités d'une organisation dans des conditions aussi nominales que possible malgré ce qui les perturbe. Ce disant, on comprend alors qu'une crise d'image est potentiellement aussi dommageable que l'arrêt d'un centre informatique ou que la destruction d'une ligne de fabrication, et que le MCA a pour but d'organiser

1. Groupement des Écoles des Mines, 2002. *Terminologie en Science du Risque. Recueil de définitions*. Documents recueillis et présentés par Chloé GRIOT et Pierre-Alain AYRAL. GEM, juin 2002.

l'entreprise pour faire face sereinement à tout ce qui peut la mettre en situation de rupture du « cours stratégique » qu'elle a choisi.

Cette deuxième édition du livre de Matthieu BENNASAR, dans ce cadre – qui a évolué depuis la première édition –, est un outil précieux.

Dans les organisations les plus avancées en la matière, le MCA est largement sorti du strict périmètre informatique.

Deuxièmement, la problématique de la continuité de la *Supply-Chain* a émergé dans les grands groupes mondialisés.

Troisièmement, la notion d'infrastructure critique (vitale dans le vocabulaire français) a désormais pris sens et vigueur.

Enfin, et pour limiter ce propos préliminaire, disons que les réglementations les plus variées (gouvernance, finance, assurance…) et le cheminement vers une normalisation mondiale de la pratique du MCA, étape ultime avant la mise en place de la certification MCA des organisations, contribuent activement à faire progresser les mentalités. Et continueront à le faire.

Cette deuxième édition, comme la première, est concrète et pleine de recommandations pratiques. Mais, à la différence de la première édition, celle-ci ouvre la voie d'une réflexion plus managériale sur le MCA. Et c'est tant mieux puisqu'il s'agit avant tout d'un aspect fondamental de la direction d'entreprise désormais.

Lorsque, avec l'appui bienveillant du sénateur Paul Girod, président du Haut comité français pour la Défense civile, et l'aide de son secrétaire permanent, Christian Sommade, j'ai fondé le Conseil national de la continuité d'activité, les réunions de travail et colloques que nous avons organisés ont clairement montré que la continuité de la vie économique et sociale de la Nation passait par plusieurs axes d'effort déterminants.

Une coopération active entre services de l'État, collectivités territoriales et entreprises. La coordination des diverses gestions de risque au sein des entreprises. Et une préparation active et collaborative des acteurs susceptibles d'être impliqués dans la conduite des plans de continuité.

Aujourd'hui, toutes les directions d'entreprise, grandes et moyennes, de production, de service ou de commerce, et les services publics ne sont pas sur un même pied d'égalité. Les études de marché auxquelles Matthieu fait allusion témoignent de l'avance du secteur financier, réglementé depuis le milieu des années 1990, tandis que les autres secteurs ne se sont mis au MCA que très tardivement, et encore peu d'entre elles. Les chiffres, réels, montrent en effet qu'en Occident, et selon les secteurs, ce ne sont qu'entre 10 et 50 % des entreprises qui ont élaboré des plans de continuité d'activité. Et ces mêmes chiffres tendent à montrer que seulement 10 à 15 % des grands groupes globalisés ont une politique active de management de la continuité de leur *Supply-Chain*.

Deux profils d'organisation se dessinent aujourd'hui, qui ont des besoins très différents, tout en étant pris dans le même maillage d'obligations.

Les grands groupes, plus matures, doivent désormais relever le défi de la continuité de la *Supply-Chain*, et de ce fait reconsidérer d'une part leurs politiques de réduction des coûts dont l'expérience montre qu'elle nuit à leur résilience, d'autre part repenser leur politique de sous-traitance pour mieux en maîtriser la continuité.

Les PME, et toutes les organisations qui ont moins investi jusqu'alors sur le MCA, doivent se hâter de progresser. Elles sont ces maillons de la *Supply-Chain* des grands groupes qui subiront une pression de plus en plus grande de leurs donneurs d'ordres en ce sens. Le contexte économique étant difficile, et une interruption significative du business peut avoir des effets dramatiques.

La vie de nos territoires dépend de plus en plus de la survie de nos entreprises. Le MCA doit donc faire partie des préoccupations du conseil d'administration et de la direction générale. Et les autorités, locales et nationales, doivent intégrer cette réflexion à la leur, et penser le territoire et les services de façon à faciliter la continuité de l'activité.

Mais revenons au livre… qui intéressera surtout ceux qui sont tentés de s'y mettre.

Inspirée du *Good Practice Guidelines*[1] du Business Continuity Institute (BCI), cette deuxième édition est toujours aussi précieuse à qui veut découvrir, de manière illustrée et concrète, ce qu'est le MCA.

Le lecteur devra prendre le temps de méditer les nombreux cas réels rapportés par Matthieu. Pour avoir été sur le terrain si longtemps, je le confirme : ces exemples reflètent exactement la réalité du risque pris par les organisations qui n'ont pas pris la peine de se préparer à affronter les situations délicates ainsi décrites.

Le deuxième intérêt de ce livre est de présenter une démarche méthodologique pratique (Matthieu l'a baptisée E = MCA, et cela lui confère le lustre particulier d'une familiarité tentante).

Là aussi, le lecteur souhaitant découvrir le MCA et se demandant comment ajouter cette corde managériale à son arc trouvera dans cette deuxième édition toutes les clés d'accès indispensables à une première approche du sujet.

Le manager d'entreprise devra s'appuyer sur des compétences, que Matthieu nomme méthodologiques, pour mettre en place un système de management de la continuité, définir des plans et des stratégies pratiques de continuité, et préparer les équipes et le management à les mettre en œuvre dans un champ d'aléas toujours extraordinaire. Ces compétences, et les techniques qu'elles mettront en branle, sont bien décrites dans l'ouvrage.

Et si l'auteur attire maintes fois l'attention du lecteur sur le fait qu'un plan de continuité doit à la fois être régulièrement revu en fonction de l'évolution du business et être adapté aux circonstances particulières de son activation, cela doit encourager le responsable MCA à faire deux choses.

Dialoguer très régulièrement avec tous les acteurs de l'entreprise, responsables des lignes métiers d'une part, gestionnaires de risques d'autre part, direction générale enfin.

1. Version 2008. Version anglaise sur www.thebci.org.

Cela lui permettra de maintenir l'édifice en phase avec les nécessités et les dangers de l'activité.

Entraîner les équipes et le management. Former et exercer sont les deux piliers de cet entraînement. Avoir un plan, c'est nécessaire. Le tester, c'est mieux. Cette formule pourrait résumer l'essence du management de la continuité d'activité. Sans vouloir empiéter sur ce qu'indique l'ouvrage, disons que, lorsqu'on parle de la continuité des métiers, par opposition à la continuité des systèmes techniques (informatiques en particulier), les plans de continuité sont en soi des guides généraux dont la mise en application sera invariablement rendue difficile par les circonstances réelles. Matthieu n'a pas manqué de le souligner, savoir décider est fondamental. Pouvoir s'appuyer sur des plans facilite la décision sous stress. Et l'entraînement a pour intérêt de familiariser les équipes et le management avec les aléas des situations de « crise » et de leur faire toucher du doigt les difficultés auxquelles ils devront faire face le jour où une interruption de l'activité se produira réellement.

Pour autant, malgré son orientation plus délibérément business, cette seconde édition n'oublie pas l'angle d'attaque de la première : le management de la continuité des systèmes d'information. Et c'est tant mieux car c'est effectivement une composante importante des organisations contemporaines.

Je m'associe donc aujourd'hui, tout autant que lors de la première édition, aux propos de Matthieu Bennasar, sans oublier celui de ma défunte grand-mère : « *quand c'est trop tard, c'est trop tard* ».

Cette deuxième édition est aussi, et enfin, le vivant témoignage de l'évolution de la discipline.

Les quelques années à venir verront la tendance si bien rapportée ici se confirmer.

Ce livre est une porte ouverte sur le devenir de nos organisations

Le reste, c'est-à-dire l'essentiel, la stratégie de continuité et sa mise en œuvre, appartient toujours au lecteur. Cela ne changera jamais.

Paul Théron, MBCI
Représentant en France du Business Continuity Institute
Fondateur du Conseil national de la continuité d'activité
Expert en Management et Ingénierie de la résilience du Groupe Thales

Le Business Continuity Institute (BCI) a été fondé en 1994 pour permettre à ses adhérents de bénéficier de l'expérience de toute la communauté professionnelle des spécialistes de la continuité des opérations. Son schéma de certification professionnelle, organisé par niveaux de qualification, reconnaît internationalement à ses membres le statut de professionnel de la continuité des opérations. Les adhérents du BCI sont plus de 5 000 aujourd'hui et se répartissent dans plus de 80 pays. Le BCI mène une action de fond au sein de la communauté professionnelle et normative en faveur de la promotion de standards méthodologiques et éthiques de haut niveau. Il est représenté en France et en Europe francophone. Son site internet fournit tous renseignements utiles : www.thebci.org.

Table des matières

Préface V

Avant-propos XVII

Première partie – Manager la continuité d'activité

Chapitre 1 – La problématique et les acteurs de la continuité d'activité 3

1.1 Quelques faits et chiffres 3

1.1.1 Le risque majeur face aux sinistres de notre temps 3

1.1.2 Le coût et la criticité des interruptions de SI 4

1.1.3 La situation des entreprises françaises, comparées au reste du monde 4

1.1.4 Un benchmarking français sur la maturité des entreprises en termes de PCA . . . 5

1.1.5 Quelques exemples frappants 5

1.1.6 Bilan 7

1.2 Se préparer au pire : une vision pessimiste du monde ? 7

1.3 Contours et domaines de la continuité d'activité 10

1.3.1 Une approche holistique du management 11

1.3.2 Gouvernement d'entreprise, management des risques et continuité d'activité . . . 12

1.3.3 Le plan de continuité d'activité : une définition 13

1.3.4 De l'incident au sinistre majeur 14

1.3.5 Ce qui n'est pas du ressort de la continuité d'activité 15

1.4 La réglementation et quelques normes 15
1.4.1 La réglementation 15
1.4.2 Les normes et standards 19
1.4.3 Autres réglementations et normes 24
1.4.4 Synthèse 26
1.5 PCA, PRA, PCO, PCM, PSI, PGC, etc. : qu'en est-il ? 27
1.5.1 Une terminologie en quête de normalisation 27
1.5.2 Proposition de définitions 27
1.5.3 Tableau comparatif 29
1.6 Les acteurs 29
1.6.1 La direction générale 29
1.6.2 Le risk manager 29
1.6.3 Les directions métier 31
1.6.4 Le Responsable du PCA (RPCA) 31
1.6.5 Le Responsable de la sécurité du système d'information (RSSI) 32
1.6.6 Responsabilités et niveau hiérarchique 32

Chapitre 2 – Décider la mise en place de la continuité d'activité 35
2.1 Un projet d'entreprise 35
2.1.1 Mandat et sponsor 35
2.1.2 Pilotage de la démarche 36
2.1.3 Conduite du changement 36
2.1.4 Régime établi 37
2.1.5 Se faire aider ou pas ? 37
2.1.6 Quelques écueils courants 38
2.2 Décider de mettre en place un PCA 44
2.2.1 Les bonnes raisons de mettre en place un MCA 44
2.2.2 Quelques préalables 47
2.2.3 Les quatre principaux composants d'un PCA 47
2.2.4 Le ROI par construction 48
2.2.5 Le « ROI » inquantifiable 51
2.2.6 Quelques conseils aux décideurs 54

Deuxième partie – Méthodes et outils de la continuité d'activité

Chapitre 3 – Mettre en place la continuité d'activité : méthodologie commentée . 63

3.1 Démarche générale 63

3.1.1 De l'« expertise » en continuité d'activité 63

3.1.2 Les principaux composants d'un dispositif de continuité d'activité 64

3.1.3 La démarche E = MCA en six phases 65

3.1.4 Notes sur le formalisme utilisé pour décrire la méthodologie 66

3.2 Phase 1 – Mieux connaître son activité : l'étape décisive 67

3.2.1 Étape 1.A : cartographie et scénarios de sinistres 67

3.2.2 Étape 1.B : Bilan d'Impact sur l'Activité (BIA) 69

3.2.3 Étape 1.C : Analyse des Risques (AR) 72

3.2.4 Première étape facultative de la phase 1 : analyse de couverture des contrats d'assurances 74

3.2.5 Deuxième étape facultative de la phase 1 : diagnostic de prévention 75

3.3 Phase 2 – Orienter la stratégie de continuité d'activité 77

3.3.1 Étape 2.A : stratégie globale de continuité 77

3.3.2 Étape 2.B : stratégie locale de continuité 78

3.3.3 Étape 2.C : choix des solutions techniques de continuité 80

3.4 Phase 3 – Développer le Plan de continuité d'activité (PCA) 82

3.4.1 Étape 3.A : Plan de Gestion de Crise (PGC) 82

3.4.2 Étape 3.B : plans transverses (PU, GP, PR) 86

3.4.3 Étape 3.C-1 : Plan de Continuité Métier (PCM) 87

3.4.4 Étape 3.C-2 : Plan de Continuité du SI (PCSI) 88

3.5 Phase 4 – Mettre en place les solutions fonctionnelles et techniques de continuité 90

3.5.1 Étape 4.A : mise en place des infrastructures de continuité 90

3.5.2 Étape 4.B : Procédures Fonctionnelles de Continuité (PFC) 92

3.5.3 Étape 4.C : Procédures Informatiques de Continuité (PIC) 93

3.5.4 Étape 4.D : test des dispositifs techniques de continuité 94

3.6 Phase 5 – Déployer et maintenir en conditions opérationnelles 96

3.6.1 Étape 5.A : sensibilisation, formation et communication 97

3.6.2 Étape 5.B : maintien en conditions opérationnelles du PCA 99

3.6.3 Étape 5.C : test du PCA 100

3.6.4 Étape 5.D : contrôle du PCA 102

3.7 Phase 6 – Piloter le management de la continuité d'activité 104

3.7.1 Étape 6.A : pilotage du projet PCA 104

3.7.2 Étape 6.B : pilotage du MCA 105

3.8 Synoptiques récapitulatifs de la méthodologie E = MCA 107

3.9 Quelques cas particuliers 116

3.9.1 Le secteur banques et finance 116

3.9.2 Le secteur PME/PMI 116

3.9.3 Le secteur public 117

3.9.4 Le SI infogéré 118

Chapitre 4 – Panorama des solutions techniques de secours 119

4.1 Les solutions de secours des moyens informatiques 119

4.1.1 Solutions de secours du SI 120

4.1.2 Typologie des moyens de secours (SI) : avantages et limites 120

4.1.3 De la bonne distance du site de secours (SI) 123

4.1.4 Disponibilité des solutions : conséquences sur les principaux composants de la chaîne SI 124

4.1.5 Mener l'analyse coûts/bénéfices et avantages/inconvénients sur les solutions de secours (SI) 124

4.1.6 Le marché et les principaux fournisseurs de services et solutions de secours (SI) 126

4.1.7 Un mot sur l'aspect contractuel du secours informatique 128

4.2 Les solutions de secours des moyens de production 130

4.2.1 Une problématique bien différente de celle du SI ! 130

4.2.2 Axes de réflexion et retours d'expérience 131

4.3 Les solutions de secours des locaux et équipements 132

4.3.1 Sauvetage des locaux et équipements 132

4.3.2 Secours des locaux et équipements 132

4.4 Le secours des ressources humaines 133

4.5 Les systèmes d'information du MCA(SIMCA) 134

4.5.1 Où l'on définit un SIMCA 134

4.5.2 Les fonctionnalités d'un SIMCA 135

4.5.3 Quelques raisons pour mettre en place un SIMCA 135

4.5.4 Critères de succès pour la mise en œuvre d'un SIMCA 136

4.5.5 *Quelques outils* ... 136
4.5.6 *Le coût d'un SIMCA intégré* ... 137
4.6 La question des coûts du secours ... 138
4.6.1 *Aspects financiers liés à la mise en place de la partie fonctionnelle d'un plan de continuité d'activité* ... 138
4.6.2 *Ordres de grandeur financiers pour la solution technique de secours (SI)* ... 141

Chapitre 5 – Considérations techniques sur les solutions de secours ... 145
5.1 Sauvegarde, restauration et disponibilité des données ... 145
5.1.1 *Méthodes de sauvegarde* ... 147
5.1.2 *Cas particuliers de sauvegarde* ... 148
5.1.3 *Technologies de sauvegarde et architecture de haute disponibilité des données* ... 149
5.1.4 *Critères de choix des solutions de sauvegarde* ... 156
5.2 Considérations techniques sur les composants critiques du SI : stratégies de secours ... 157
5.2.1 *Serveurs* ... 158
5.2.2 *Réseau local* ... 159
5.2.3 *Réseau WAN* ... 160
5.2.4 *Sites web* ... 161
5.3 Considérations techniques sur les outils et moyens périphériques ... 162
5.3.1 *Postes et stations de travail* ... 162
5.3.2 *Téléphonie* ... 164
5.3.3 *Impression* ... 164
5.3.4 *Internet* ... 165

Chapitre 6 – Études de cas ... 167
6.1 Cas n° 1 – Mise en place d'un plan de continuité informatique local ... 167
6.1.1 *L'énoncé du problème* ... 168
6.1.2 *L'approche proposée et la démarche mise en œuvre* ... 169
6.1.3 *Étape 1 – Mieux connaître l'activité* ... 169
6.1.4 *Étape 2 – Orienter la stratégie de continuité* ... 171
6.1.5 *Étape 3 – Mettre en place la solution technique de continuité* ... 171
6.1.6 *Conclusion* ... 172
6.2 Cas n° 2 – Audit d'un plan de continuité informatique et définition du PCA ... 172
6.2.1 *L'énoncé du problème* ... 173

6.2.2 *L'approche proposée et la démarche mise en œuvre* 174
6.2.3 *Les livrables et les résultats* 176
6.2.4 *Conclusion* 178
6.3 Cas n° 3 – Mise en place d'un plan de continuité métier (PCM) 179
6.3.1 *L'énoncé du problème* 180
6.3.2 *L'approche proposée et la démarche mise en œuvre* 181
6.3.3 *Étape 1 – Mieux connaître l'activité* 182
6.3.4 *Étape 3 : Développer le plan de continuité d'activité* 191
6.3.5 *Étape 5 – Assurer la conduite du changement, le déploiement du PCM et son maintien en conditions opérationnelles* 196
6.3.6 *Conclusion* 201
6.4 Cas n° 4 – Retour d'expérience pour une crise majeure : les attentats de Londres 201

Troisième partie – Perspectives

Chapitre 7 – Vers un système de management de la continuité d'activité et une entreprise résiliente ? 205
7.1 Les principaux systèmes de management de l'entreprise 206
7.1.1 *Qualité (ISO 9001)* 206
7.1.2 *Sécurité et santé au travail (OHSAS 18001)* 206
7.1.3 *Environnement (ISO 14001)* 206
7.1.4 *Sécurité de l'information (ISO 27002 et ISO 27001)* 207
7.1.5 *Éthique et responsabilité sociale(SA 8000)* 207
7.1.6 *Systèmes propres à l'entreprise* 207
7.2 L'intégration des divers systèmes de management : vers un SMI 208
7.2.1 *Les concepts intégrateurs* 208
7.2.2 *La construction du tronc commun* 212
7.2.3 *Les avantages* 212
7.3 Proposition d'un Système de management de la continuité d'activité (SMCA) 214
7.3.1 *Un système de management de la continuité d'activité* 214
7.3.2 *Vers le management unifié ?* 214
7.4 Vers la résilience 216
7.4.1 *Vous avez dit résilience ?* 216
7.4.2 *Construire la résilience* 217

7.5 Conclusion 219

Conclusion 221

Annexes

Annexe A – Sigles et abréviations 227

Annexe B – Quelques illustrations documentaires de la méthodologie 229

Annexe C – Les démarches connexes et les méthodes associées 275

Références bibliographiques 291

Index 299

Avant-propos

La continuité d'activité en question

Le 7 janvier 2009, les Marseillais se réveillent dans un paysage irréel : le sol est recouvert d'une couche d'une dizaine de centimètres de neige ! Si la situation fait le bonheur des enfants, elle paralyse purement et simplement l'essentiel de l'activité de la ville pendant plusieurs jours. À tel point, que le Premier ministre, François Fillon s'exclame : « *Quand il y a des milliers de gens bloqués pendant des heures et des heures, quand des aéroports dans un pays moderne ne fonctionnent plus parce qu'il y a de la neige, c'est qu'il y a des déficiences.* » La panique n'est pas loin et le temps de préparer ses mesures de continuité d'activité est clairement passé : on en est à les mettre en œuvre ! La crise permet d'identifier rapidement les entreprises qui sont effectivement prêtes à faire face à un sinistre majeur. La neige est un juge de paix sévère. Certaines des entreprises qui exigent des mesures de continuité d'activité de leurs fournisseurs sont ainsi incapables de mettre en œuvre leur propre plan !

Deux semaines plus tard, le 24 janvier 2009, la tempête KLAUS, d'une violence inouïe, s'abat sur le sud-ouest de la France : des vents de 175 km/h déracinent les arbres, arrachent les toitures et causent des dégâts matériels considérables. Douze personnes meurent en France et trente-et-une en Espagne. À 16 h 30, 1,7 million de foyers sont privés d'électricité. EDF est pointé du doigt : la dépendance des foyers à l'électricité en cette période hivernale est grande. Combien de temps leur faudra-t-il tenir ? La pression médiatique est intense. D'après les experts, ce genre de tempête sévit tous les 40 ans. De mémoire de Girondins, on ne se souvient pas de tels ravages. À moins que…

Il y a « à peine » 10 ans, à la même époque, une tempête d'une violence comparable provoquait le même genre de dégâts, privant un nombre comparable de foyer d'électricité. Mais la réponse n'est cette fois pas la même : l'organisation des secours d'EDF avec le soutien de l'armée permettra cette fois de diviser par deux le temps de rétablissement du réseau électrique. Ce que les mots ont du mal à enseigner, l'expérience l'apporte. On finit par apprendre…

Ce type de sinistre reste exceptionnel. Mais s'il est évident que les chances qu'un sinistre donné frappe une entreprise définie à un moment précis sont infimes, la probabilité que certaines entreprises soient victimes d'un sinistre majeur au cours de leur histoire n'est pas négligeable. Les journaux nous abreuvent presque quotidiennement de nouvelles de catastrophes naturelles, technologiques ou humaines. Le recours à une stratégie défensive basée exclusivement sur l'assurance est de nature à limiter les pertes, mais cette approche ne couvre pas toujours la baisse de productivité, rarement la perte de clients, les dégâts sur l'image et les pénalités réglementaires pour non-respect de ses obligations. En fait, il est estimé que, « *lorsqu'elles n'y sont pas préparées, 43 % des entreprises ferment au moment d'un sinistre majeur, et 29 % de celles qui survivent, périclitent dans les deux ans qui suivent*[1] ».

On ne reprochera pas à une entreprise d'être victime d'un sinistre majeur. Mais c'est un risque en soi que de faire des affaires, en toute connaissance de cause, avec une entreprise qui n'a pas prévu une gestion des situations de crise dans un monde où l'impact négatif des seules catastrophes naturelles croît selon une courbe quasi exponentielle depuis 50 ans. À juste titre, l'adjonction d'un critère relatif à la continuité des opérations dans les éléments de choix lors d'appels d'offres et de consultations devient de plus en plus systématique : la mise en place d'une solution de secours efficace devient ainsi un élément différenciant. En France, être « prestataire essentiel » d'un établissement financier place une entreprise dans l'obligation de prévoir un Plan de continuité d'activité (PCA) aligné sur les objectifs de son client. Mais au-delà de la réglementation, de plus en plus de cahiers des charges imposent de faire la preuve de son efficacité face à l'imprévu grave.

La continuité d'activité est une discipline nouvelle qui plonge ses racines dans la sécurité des systèmes d'information mais dont les branches ont aujourd'hui poussé jusqu'à la gestion de crise et jusqu'aux démarches processus. Selon la définition du CRBF[2], le plan de continuité d'activité est l'« *ensemble de[s] mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités* »[3]. C'est de la définition et de la mise en œuvre de telles mesures qu'il est question dans ce livre.

Pourquoi un livre ?

Le mieux français !

Quand j'écrivais la première édition de ce livre fin 2005, en France, le sujet de la continuité d'activité avait inspiré plusieurs livres blancs, quelques articles généralistes dans la presse spécialisée et un ouvrage du Clusif[4] qui traitait du plan de secours informatique[5] mais qui abordait peu la problématique plus large de la continuité

1. Disaster Recovery Institute International, Canada, 2001.
2. Comité de la réglementation bancaire et financière.
3. CRBF 2004-02.
4. Club de la sécurité des systèmes d'information français.
5. Intitulé *Plan de Continuité d'Activité : stratégie et solution de secours du SI*, septembre 2003.