LIVRE BLANC

LEXSI
INNOVATIVE SECURITY

Plan de Continuité d'Activité : le chemin de la maturité

BENCHMARKING DES ENTREPRISES ET INSTITUTIONS FRANÇAISES / PAR MATTHIEU BENNASAR ET LEONARD KEAT

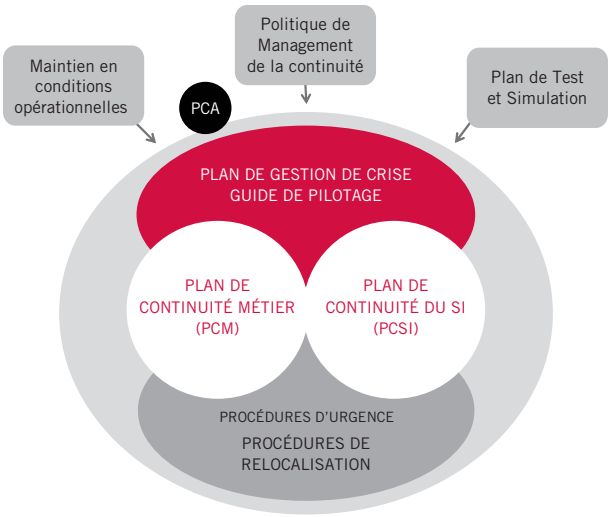
Plan de Continuité d'Activité : le chemin de la maturité

par Matthieu Bennasar & Léonard Keat

La plupart des enquêtes et publications sur la maturité des entreprises sur les Plans de Continuité d'Activité (PCA) se concentrent sur les grands comptes, voire les très grands comptes de plus d'1 milliard d'euros de chiffre d'affaires et de plus de dix mille salariés. Si la maturité des entreprises sondées est jugée satisfaisante dans les enquêtes, la nature du panel occulte souvent un pan entier des entreprises : les PME. LEXSI propose une étude des entreprises de toute taille, implantées en France, sur la base du retour d'expérience de ses consultants spécialisés en résilience et continuité d'activité.
Si les résultats de ce benchmarking paraissent sévères à certains égards, il faudra se rappeler que la méthodologie d'enquête n'est pas auto déclarative et que les réponses des sondés sont vues par le prisme sans complaisance d'experts du domaine. De plus, aucun niveau de maturité n'est garanti dans la durée : les meilleurs d'hier ne sont ceux d'aujourd'hui qu'au prix d'efforts conséquents de maintien en conditions opérationnelles.

LE CŒUR DU PCA A DEUX VENTRICULES : LE PCM ET LE PCSI

Un rappel tout d'abord : un Plan de Continuité d'Activité (PCA) est "l'ensemble des 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" (CRBF 2004-02)[1].
Un PCA n'est donc pas un outil garantissant le maintien du niveau de service courant des activités. Au vu de son coût d'activation, ce plan n'est à activer qu'en cas de sinistre majeur. Ce n'est pas non plus une solution unique et universelle permettant de faire face à toutes les situations de sinistres imaginables. Il est évident que l'entreprise n'utilise pas les mêmes moyens face à un sinistre de bâtiment que face à une vague pandémique. Enfin, et surtout, ce n'est pas une simple solution technique (informatique ou industrielle) à une problématique d'entreprise : une organisation et des moyens humains sont indispensables pour assurer notamment la gestion de la crise et les fonctionnements dégradés des métiers.



Plus complexe qu'il n'y paraît, un PCA est à l'image d'un cœur humain. Il a besoin de 2 "ventricules" pour fonctionner : un Plan de Continuité Métier (PCM), et un Plan de Continuité du Système d'Information (PCSI).
Le PCA est complété par des procédures transverses (procédures d'urgence, procédures de relocalisation des utilisateurs,...) d'un processus et d'une organisation de gestion de crise (logistique de crise, guide de pilotage d'activation des plans de continuité...) et de documents de gestion du PCA (maintenance, test et management du plan).
Le Plan de Continuité Métier (PCM) traite de l'ensemble des procédures, moyens et stratégies capables de garantir la continuité des activités

Le PCA n'est pas une solution unique et universelle permettant de faire face à toutes les situations de sinistres imaginables !

1. Comité de la Réglementation Bancaire et Financière

métier essentielles face à un sinistre touchant une ou plusieurs ressources essentielles (destruction de bâtiment, pandémie, fournisseur vital défaillant,…). Les stratégies souvent évoquées sont celles de repli utilisateurs vers un site de secours, d'accord de réciprocité avec un partenaire ou de secours mutuel des équipes et des services.

Le Plan de Continuité du Système d'Information (PCSI) décrit les moyens techniques, l'organisation et les stratégies pour faire face à un sinistre informatique de grande ampleur (destruction de la salle informatique, rupture de lien télécom,…). De nombreuses solutions sont envisageables allant de la simple externalisation des sauvegardes à une infrastructure de haute disponibilité géographiquement répartie et éloignée.

Les résultats de notre étude présentent la maturité d'une centaine d'entreprises françaises sur ces deux notions : PCSI et PCM.

VOLET 1 – PCSI : UNE MATURITÉ DES TECHNOLOGIES, UNE ORGANISATION À RENFORCER

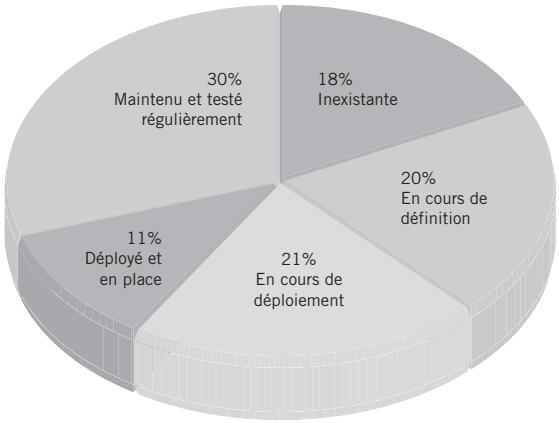
Il est attendu que la maturité des plans de secours informatiques soit avérée, puisque la problématique de disponibilité des applications est prise en compte depuis très longtemps au sein des Directions des Systèmes d'Information.

A peine 41% de notre échantillon d'entreprises disposent d'un PCSI en place et/ ou maintenu et testé régulièrement. Parmi elles, près de 60% ont un chiffre d'affaires supérieur à 1 milliard d'euros. Mais nous constatons quand même une plus grande maturité des entreprises françaises dans la mesure où 82% d'entre elles ont un projet PCSI en cours ou finalisée. Sans surprise, les PME sont moins matures que les Grands Comptes, à secteur égal. Deux raisons peuvent être avancées :

1. La première réside dans la perception que les budgets nécessaires pour faire face à un sinistre de salle informatique sont rédhibitoires. Les PME privilégient ainsi les mesures de prévention pour limiter les impacts et la probabilité d'occurrence d'un sinistre de grande ampleur.
2. La seconde est plus inquiétante : les PME ne mesurent pas les risques et les acceptent en refoulant le sentiment inconscient de la nécessité de s'en protéger.

La maturité des entreprises françaises est meilleure que ce que montraient les précédentes enquêtes.

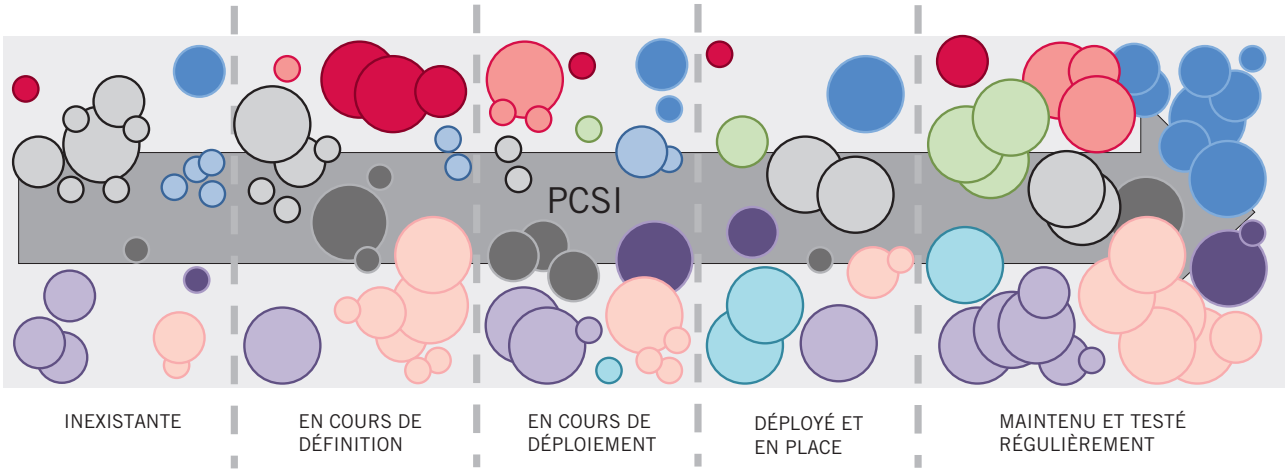
MATURITÉ PCSI

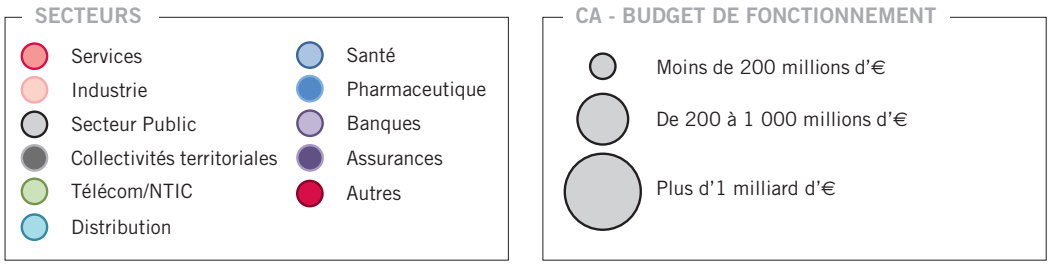


Lorsque nous regardons par secteur d'activités[1] :

- Le secteur des Banques & Assurances et le secteur pharmaceutique sont globalement en avance. Poussés par les contraintes réglementaires (CRBF, SOX, FDA, Bâle II, Solvency II…)[2], ces deux secteurs font souvent figure de modèle du secours informatique. Sur le chemin critique de toute l'économie, le secteur bancaire a des contraintes de disponibilité très fortes, avec peu de solutions de contournement satisfaisantes, même en mode dégradé.
- Les entreprises de l'Industrie ont des niveaux de maturité hétérogènes avec, sans surprise, une avance pour

1. Traditionnellement, le secteur Banque et Assurances a beaucoup formalisé (parfois un peu "scolairement") pour répondre à la pression réglementaire tandis que l'Industrie a des solutions pragmatiques en place mais manque cruellement de formalisation.
2. SOX : Sarbanes-Oxley Act ; FDA : Food and Drug Administration.





les grands groupes. Nous soulignons un niveau de maturité bien meilleur que par le passé, avec une informatique dite "de gestion" bien mieux prise en compte.

■ Le secteur public, les collectivités territoriales et le secteur de la santé sont en retrait, mais la situation s'améliore, plus rapidement pour les grandes institutions publiques et de santé. Cette augmentation de la maturité témoigne que les Directions SI et les Directions Générales sont de plus en plus conscientes du caractère vital du Système d'Information dans la continuité des activités essentielles de l'entreprise ou de l'institution.

Disposer d'un véritable plan global PCSI qui "orchestre" l'ensemble des procédures techniques de reprise.

Deux points ressortent comme lacunaires dans notre retour d'expérience :

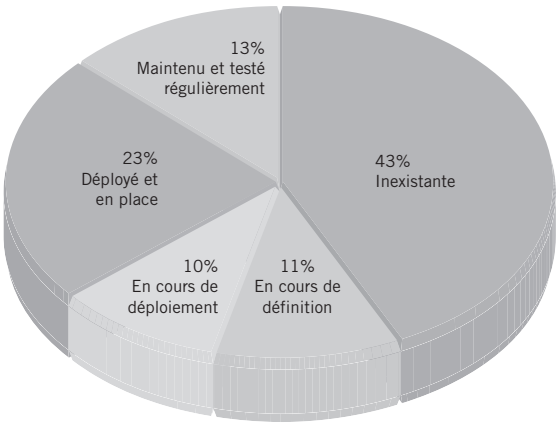
1. Il manque un plan global PCSI qui "orchestre" l'ensemble des procédures techniques de continuité du SI, selon des scénarii de sinistre établis. L'ordonnancement et l'organisation autour du plan sont à formaliser pour éviter de les faire porter exclusivement par la Cellule de Crise Informatique, peu efficace sinon.

2. Les tests de PCSI sont trop souvent incomplets et ne mettent pas en scène les scénarii prévus par le Plan, faute de budget ou de disponibilité des équipes informatiques. Cela est d'autant plus dommage que nous constatons que c'est souvent dû à un Bilan d'Impact sur l'Activité insuffisamment travaillé : un trop grand nombre d'applications y ressortent comme critiques, ce qui complique notablement les tests. Un audit des PCSI permet dans ce cas de savoir si le périmètre des tests est correctement défini.

VOLET 2 – PCM : DES PROJETS À RÉACTION PLUTÔT QUE PROACTIFS

NOTE : pour des raisons de représentativité, nos statistiques relatives aux PCM ne prennent pas en compte les organisations dont les seules mesures de continuité sont un plan "pandémie" mis en place autour de la menace du virus H1N1. Plus de 80% des organisations l'ont mis en place, notamment dans le secteur public sous l'impulsion des ministères et du gouvernement. Nous constatons néanmoins un démantèlement massif des équipes projet et des moyens permettant le maintien à jour de ces plans suite à ce qu'il convient d'appeler un sinistre manqué.

MATURITÉ PCM



Le constat est plus sévère pour ce deuxième volet (PCM) : 43% des entreprises du panel n'ont aucun projet PCM en cours ou en place. Parmi elles, 60% ont un CA inférieur à 200 millions d'€. Près de 52% ayant un PCM en place et/ou maintenu et testé régulièrement ont un CA supérieur à 1 milliard d'€. Les Plans de Continuité Métier sont vus comme des projets coûteux et difficiles à mettre en œuvre. La priorité n'est pas dans ce type de projet parce que, logiquement, la prévention est toujours privilégiée, surtout pour les PME.

Nous retrouvons, dans l'analyse par secteur d'activités, les profils du volet 1 (cf schéma page 6):

- Le secteur des Banques & Assurances et le secteur pharmaceutique sont au-dessus du lot : toujours poussés par les contraintes réglementaires, les plans et les procédures sont formalisés, parfois "scolairement". Le contrôle de leur efficience est difficile car très coûteux et consommateur en ressources humaines.
- Le secteur de l'Industrie n'a généralement pas de PCM formel en place, bien que la résilience soit souvent intrinsèque dans ce secteur : la rupture de sa chaine de production met sans doute plus vite un industriel en émoi qu'une société de services. Il suffit souvent alors de formaliser l'organisation, les procédures et les mesures de secours en place pour que le PCM prenne vie.
- Le secteur public et les collectivités territoriales sont encore en retrait. Et quand les procédures existent, celles de gestion de crise et de secours des activités critiques ne sont pas toujours mises en œuvre lors d'un sinistre, parfois en raison de la pression hiérarchique.

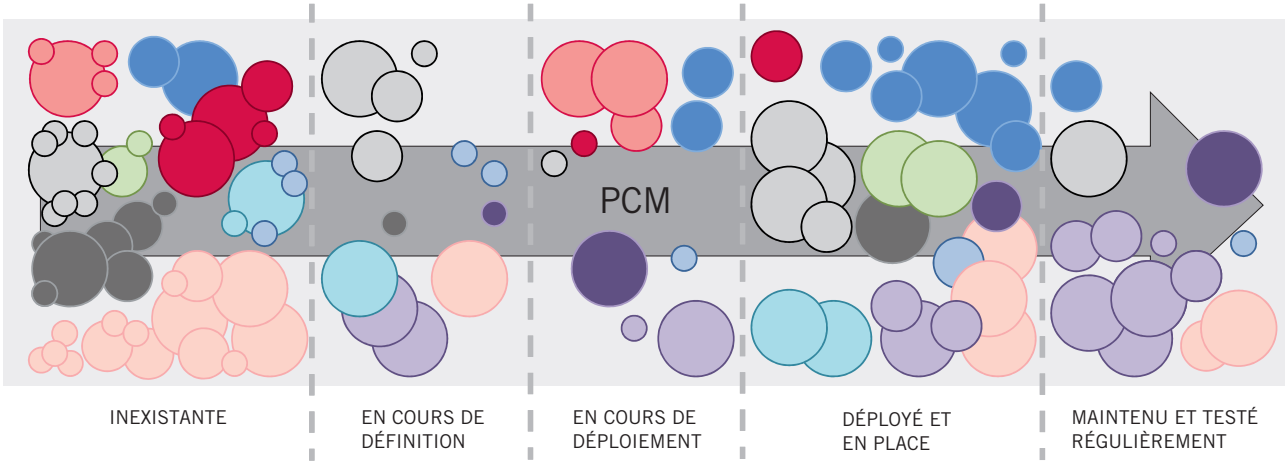
Si elle reste largement insuffisante, la maturité des PCM a fait un pas en avant. Les PME restent les parents pauvres de la démarche alors qu'elles sont les plus vulnérables à un sinistre majeur.

DES FREINS AUX PROJETS PCA À LEVER

Les freins au lancement d'un projet PCA trouvent leurs sources dans les idées véhiculées au sein des comités et entités de décision. Or, pour la plupart, ces idées reçues sont tout bonnement fausses.

Un PCA coûte les yeux de la tête ?

Même s'il est vrai qu'un projet PCA nécessite un budget et des charges à réserver pour le mener à bien, sa mise en place est une nécessité que



l'on rend accessible en ajustant la démarche aux enjeux de l'entreprise, avec beaucoup de pragmatisme et le souci de la maîtrise de l'investissement : en fonction des risques considérés et des sinistres envisagés, l'entreprise met en place tous les moyens, toutes les procédures et les organisations adaptés à son contexte.

Une PME peut moins se permettre de laisser un sinistre décider de son avenir qu'un concurrent de type Grand Compte.

Il faut donc envisager de :
– continuer à privilégier la prévention, afin d'éliminer durablement des scénarii de sinistres ;
– externaliser son secours, si l'entreprise souhaite se concentrer sur son cœur de métier ;
– investir dans des solutions techniques de secours dont les coûts ont beaucoup baissé et/ou mutualiser les infrastructures de secours ;
– profiter d'un projet PCA pour répondre à la problématique de disponibilité "au quotidien".

La mise en œuvre d'un plan PCA est donc proche de la signature d'un contrat d'assurance, qui vous couvre en cas de sinistres majeurs. La question à se poser alors n'est pas : "Avons-nous besoin d'un PCA ?" mais plutôt : "Jusqu'à quel point avons-nous besoin de définir des mesures de continuité d'activité ?". Une telle approche privilégie donc l'adéquation des mesures aux enjeux de l'entreprise et doit garantir un retour sur investissement "par construction", c'est-à-dire dont les bénéfices attendus s'ajustent aux risques encourus et considérés.

Les PME ont moins besoin des PCA ?

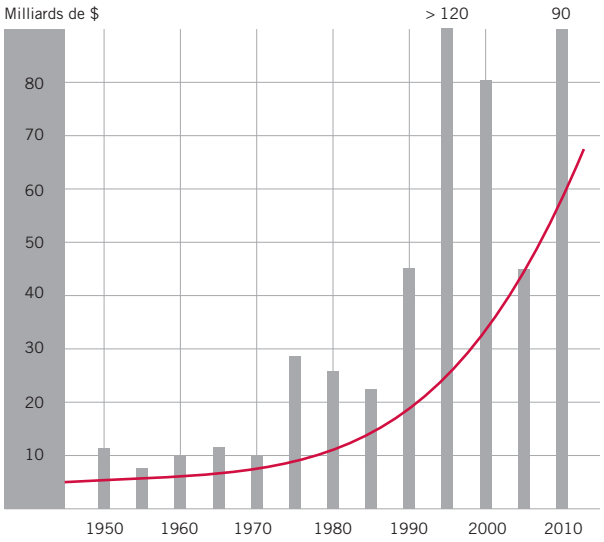
Notre étude met en relief le manque de maturité des PME concernant les PCA. Nous devons rappeler qu'elles sont plus sensibles aux chocs extrêmes :

– leurs ressources et activités vitales sont souvent regroupées sur un site unique ;
– leur bassin commercial est souvent régional ;
– leur assise financière est plus fragile ;
– leurs fonctions et compétences clés sont souvent uniques.
Une PME peut moins se permettre de laisser un sinistre décider de son avenir qu'un concurrent de type Grand Compte, assis sur plusieurs continents et adossé à des investisseurs puissants. L'organisation de crise et le dispositif PCA doivent être aussi souples et agiles que les PME, sans négliger la phase de formalisation du Plan.

Un sinistre, cela n'arrive qu'aux autres ?

Il est désormais admis que le nombre de catastrophes naturelles est en constante augmentation, à la fois en fréquence et en gravité, même dans les pays au climat tempéré. En France, il suffit pour cela de se souvenir de quelques catastrophes récentes :
– les tempêtes de décembre 1999 (Lothar & Martin) ;
– les inondations du Gard en 2002 ;
– la canicule de 2003 ;
– les inondations du nord de la France en 2006 ;
– la tempête Klaus en janvier 2009 ;
– la tempête Xynthia de février 2010 ;
– les inondations du Var en février et juin 2010.

A cela s'ajoutent les catastrophes issues d'incidents d'origine humaine ou non : l'explosion de l'usine AZF en 2001, les émeutes en région parisienne et en province de 2005, la coupure massive d'électricité dans le nord-est de la France, la grève générale des transports publics en 2007 et le nuage de cendres du volcan islandais en 2010. Au lendemain de ces catastrophes, de nombreuses entreprises, notamment les PME, n'ont pas survécu et ont aujourd'hui disparu. Les pertes financières de ces crises se chiffrent à plusieurs centaines de millions d'euros.



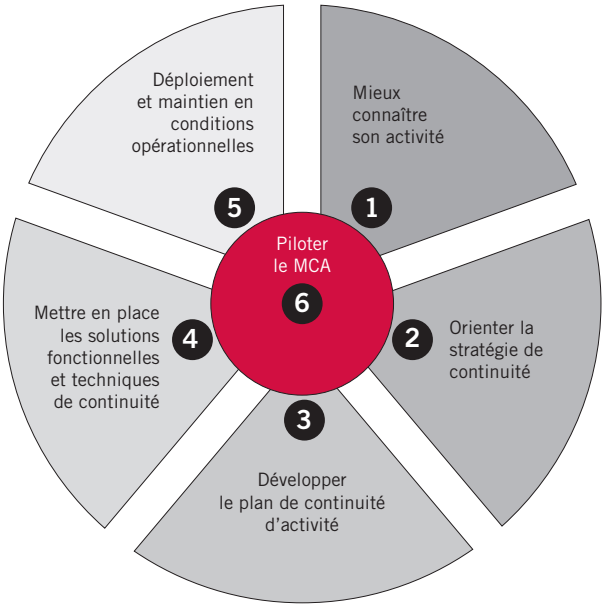
Evolution des pertes économiques dues aux catastrophes naturelles de la période 1950-2009 (d'après Munich Re)

SE LANCER DANS UN PROJET PCA : LA MÉTHODOLOGIE E=MCA

Si vous vous décidez à vous lancer dans un projet PCA, ou l'une de ces composantes (PCM, PCSI), LEXSI vous invite à suivre la méthodologie propriétaire appelée E=MCA (Etapes vers le Management de la Continuité d'Activité). Cette méthodologie a été validée par le *Business Continuity Institute* et s'appuie sur un cycle projet perpétuel garantissant la réussite dans la mise en place et le maintien en conditions opérationnelles d'un Plan de Continuité d'Activité.

Le PCA doit être efficace dans la durée afin de ne pas perdre tous les bénéfices et les investissements consentis à sa mise en place.

Cette méthodologie de projet en forme de cycle prend en compte un aspect important d'un PCA : tout niveau de maturité atteint par un projet PCA doit être maintenu dans le temps. Le sinistre peut en effet survenir dans 1, 5 ou 10 ans. Le PCA doit être efficace dans la durée afin de ne pas perdre tous les bénéfices acquis et les investissements consentis à sa mise en place.



Description de notre panel d'analyse

Notre enquête s'appuie sur nos références clients et prospections. L'analyse a été réalisée par nos consultants experts dans le domaine. Ce n'est donc pas à partir de questionnaires auto-renseignés par les Responsables PCA ou les Responsables Sécurité que les résultats ont été obtenus. Le portrait ainsi dressé se veut réaliste.

Notre panel d'analyse se caractérise par une répartition homogène en termes de secteurs d'activité et de chiffre d'affaires ou budget de fonctionnement. Notre panel prend en compte des entreprises à quelques centaines de milliers d'euros de chiffre d'affaires.

METHODOLOGIE E=MCA

1A - Cartographie et scénarii de sinistres
1B - Bilan d'impacts sur l'Activité
1C - Analyse des risques

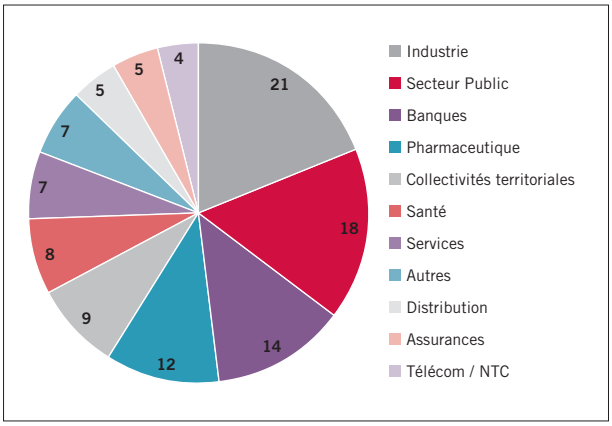
2A - Stratégie globale de continuité
2B - Stratégie locale de continuiuté
2C - Choix des solutions techniques de continuité

3A - Plan de Gestion de Crise
3B - Plans transverses (PJ, GP, PR)
3C - Plan de Continuité Métier (PCM) et Plan de Continuité du SI (PCSI)

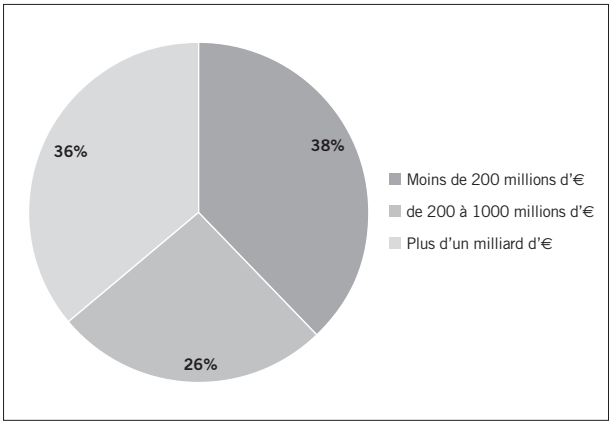
4A - Mise en places des infrastructures de continuité
4B - Procédures Fonctionnelles de Continuité (PFC)
4C - Procédures Informatiques de Continuité (PIC)
4D - Tests des dispositifs fonctionnels et techniques de continuité

5A - Sensibilisation, formation et communication
5B - Maintien en condition opérationnelle
5C - Exercices, tests ou simulations PCA
5D - Contrôle du PCA

REPARTITION PAR SECTEUR



REPARTITION PAR CHIFFRE D'AFFAIRES



QUELQUES MOTS SUR LE GROUPE

Le groupe LEXSI est un cabinet indépendant de protection du patrimoine informationnel.
Axant sa stratégie sur l'innovation depuis 1999, le groupe LEXSI est aujourd'hui le premier cabinet indépendant en sécurité de l'information et en gestion des risques. Sa singularité réside dans une alliance unique de technologies, de méthodes et de talents, pour protéger les intérêts de ses clients.
Le groupe LEXSI est actif à l'international à travers ses filiales de Montréal et Singapour. Il a pour mission d'aider les entreprises à renforcer leur sécurité et à gérer leurs risques, à travers 4 grands métiers :

– Audit des systèmes d'information
– Conseil en sécurité de l'information et en management des risques
– Veille technologique & lutte contre la cybercriminalité
– Formation ciblée SSI & Management des risques

LEXSI dispose d'un pôle de compétence Résilience & Continuité d'Activité de 20 consultants certifiés (MBCI, CBCP, E=MCA…) présents à Paris et Lyon. Il compte plus d'une centaine de missions et de projets PCA dans tous les secteurs d'activité, de l'étude d'opportunité au test de bout-en-bout du PCA.

LES AUTEURS

Léonard KEAT est consultant en sécurité de l'information et en continuité d'activités depuis 2002. Il compte plus d'une dizaine de missions en continuité d'activité et en secours informatique dans des secteurs comme les assurances, les banques, l'énergie, la distribution et les services. Il est membre et animateur du pôle de compétence Résilience & Continuité d'Activité du groupe LEXSI. Il est certifié Lead Auditor ISO 27001 et E=MCA.

Matthieu BENNASAR dirige le Pôle Conseil de LEXSI Régions et le Pôle de Compétences Résilience & Continuité d'Activité de LEXSI. Consultant expert depuis 12 ans, il est l'auteur de deux ouvrages de référence : *Plan de Continuité d'Activité et Système d'Information*, dans lequel est décrite la méthodologie E=MCA, et *Manager la Sécurité du SI* tous deux publiés chez Dunod. Il est membre du BCI (MBCI) et certifié CISM.

Matthieu BENNASAR
+33 (0)6 13 33 19 01
mbennasar@lexsi.com

Léonard KEAT
+33 (0)6 34 47 32 79
lkeat@lexsi.com

www.lexsi.com

SIEGE SOCIAL :
Tours Mercuriales Ponant
40 rue Jean Jaurès
93170 Bagnolet

Tél. (+33) 01 55 86 88 88
Fax. (+33) 01 55 86 88 89