La conception d'un Plan de Continuité d'Activité (noté PCA) n'est pas sans difficultés. Ici, nous nous intéresserons à synthétiser la démarche de conception d'un plan de continuité d'activité, à identifier les écueils à éviter pour chaque étape et à souligner les facteurs clés de succès.

Les enjeux de la continuité d'activité pour les entreprises

Aujourd'hui plus que jamais, les entreprises sont exposées à des risques majeurs d'origines diverses (climatiques, pandémies, accidents, malveillances, conflits sociaux, défaillances techniques, erreurs, terrorisme, …). Ces risques peuvent entrainer de véritables sinistres pouvant avoir des conséquences gravissimes, voire définitives sur leurs activités et leurs missions.

Elles sont donc amenées à gérer des situations imprévues pouvant entraîner des chocs extrêmes ayant pour conséquence une incapacité à redémarrer les activités et de fournir les services attendus par les clients ou usagers. L'impact est alors extrêmement grave, perte financière lourde, perte de confiance des clients, des partenaires, sanction civile ou pénale, …). Selon le Disaster Recovery Institute International, au Canada, 43% des entreprises ferment après un sinistre et 29% de celles qui survivent périclitent dans les deux ans qui suivent.

Afin de faire face à ces statistiques préoccupantes, la réglementation et la normalisation se sont fortement précisées. Les exemples ci-dessous n'ont pas pour objectif de formaliser une liste exhaustive, mais bien d'illustrer l'avancement des exigences juridiques et l'évolution des outils normatifs.

Les obligations réglementaires et légales se généralisent

Les réglementations internationales et nationales telles que par exemple :

- le Sarbannes Oxley Act de 2002, pour les entreprises ou leurs maisons mères cotées sur le marché américain,
- en environnement bancaire et les accords Bâle II, puis suite à la crise de 2010 les accords de Bâle III obligent les organismes bancaires à maîtriser non seulement les risques classiques liés au crédit mais aussi les risques opérationnels résultant de procédures internes inadéquates ou défaillantes conduisant à une incapacité à continuer leurs activités,
- dans le monde de l'assurance, le « dispositif de contrôle interne » de la règlementation Solvency 2 explicite les exigences de la continuité de l'activité et le maintien des données et des fonctions essentielles de l'organisme,
- la loi sur la sécurité financière 2003-706 du premier août 2003 définit des exigences de continuité d'activités pouvant être auditées par la Commission bancaire,
- le Code du commerce dans l'article 123-20 alinéa 2,
- …

Les normes et standards se précisent

- la norme ISO / TS16949 formalise des exigences de disponibilité et de continuité d'activités pour le secteur de l'automobile,
- la norme TL 9000 structure un système de mesure de la qualité pour l'industrie des télécommunications et définit le management de la conduite d'activité,
- le chapitre 17 de la norme ISO 27002 version 2013, repris notamment dans l'objectif 33 de la Politique des Systèmes d'information de l'État français,
- la norme ISO 27001 formalisant le système de management de la sécurité de l'information permet de suivre la continuité d'activités puis la norme ISO 22301 de système de management pour la continuité d'activité qui peut être utilisée par des organisations de toutes tailles et de tous types. Une fois leur système de continuité d'activités en place, les organisations ont la possibilité de solliciter une certification accréditée de conformité à la norme pour prouver leur respect des bonnes pratiques de continuité d'activités aux instances réglementaires, aux clients potentiels et à d'autres parties intéressées.
- une norme d'orientation plus complète (ISO 22313) fournissant plus de détails pour chaque exigence d'ISO 22301 est en préparation.

Ainsi le PCA, (en anglais le Business Continuity Plan) peut être défini conformément à la proposition du CRBF (Comité de Réglementation Bancaire et Financière), comme étant un ensemble de 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.

La modélisation globale du PCA conduit donc à formaliser les mesures, les procédures, les moyens humains et matériels aux niveaux des équipes métiers et techniques pour organiser un cadre de référence de résilience pour faire face à ces chocs extrêmes. Il sera donc nécessaire d'identifier et d'évaluer l'exposition de l'entreprise à ces chocs extrêmes et les conséquences associées, puis de définir une organisation de gestion de crise permettant de mobiliser les équipes métiers et techniques permettant une reprise normale des activités.

La démarche, et les principaux acteurs, vision globale synthétique

Afin d'être synthétique, et conforme à la norme ISO 22301, la démarche de conception d'un PCA peut être structurée en 5 étapes :

1. la définition des besoins métiers,
2. la définition de la stratégie,
3. la définition des plans de continuité, d'hébergement, de communication et de gestion de crise,
4. la formation des personnes concernées,
5. la maintenance du PCA.

Ces étapes doivent être organisées, suivies et contrôlées par une organisation chargée de la bonne gouvernance du PCA.

La direction générale de l'entreprise doit donc nommer une personne responsable de la conception et de la coordination du PCA.

Il est important de souligner que ceci suppose une délégation de responsabilité a minima pour la définition et la mise en œuvre du plan de continuité. Cette fonction doit faire l'objet d'une fiche de poste bien documentée précisant son autorité.

Ce Responsable pour la Conduite de l'Activité doit rédiger et proposer la Politique Générale du Plan de Continuité d'Activité et ses évolutions à la direction générale pour validation. Il doit s'assurer que la Politique couvre les risques majeurs et extrêmes. Il veille à son application et doit être chargé de la diffusion de la Politique auprès de toutes les entités concernées.

Il s'assure de sa mise en œuvre. Ces plans d'actions sont constitués avec les métiers et les activités de support, (maîtrise d'œuvre informatique, ressources humaines, communication, logistiques, …).

Il doit ainsi assurer le reporting sur l'avancement des plans d'actions.

Le premier piège classique concerne les entités à maturité naissante ou moyenne en termes de sécurité. En effet il est courant pour ce profil d'entité de vouloir charger le Responsable Sécurité des Systèmes d'Information (noté RSSI) de la conception et du suivi du PCA. Dans ce profil d'entité à maturité naissante ou moyenne, le RSSI à profil technique est classiquement nommé au sein de la DSI. Il est chargé de la sécurité opérationnelle et de la mise en œuvre des bonnes pratiques de sécurité informatique, appelées par l'Agence Nationale de Sécurité des Systèmes d'Information, « les règles d'hygiène informatique ». Ces règles sont identifiées comme « allant de soi » et deviennent auto justifiées par la compétence des informaticiens. Ne pas les appliquer, serait considéré comme une faute. Il faut noter le paradoxe : le RSSI est ici un profil technique ne maîtrisant ni les obligations légales spécifiques à une activité, ni les besoins spécifiques des métiers alors qu'il serait chargé de répondre aux chocs extrêmes aux impacts métiers.

Il serait sans aucun doute plus judicieux de charger le secrétaire général (entreprises, académies, …) ou le directeur général des services pour les collectivités de faire concevoir le PCA. En effet, ici cette fonction à haute responsabilité sera plus à même d'assurer un support aux directions afin qu'elles puissent assumer leurs responsabilités.

Le Responsable du PCA devra constituer un Comité pour le PCA regroupant des représentants des équipes métiers, des maitrises d'œuvre, (DSI, logistique, …), des équipes de contrôle et d'audit, des supports (DRH, formation, …) et bien évidemment de la direction générale. Ce comité devra donc se réunir a minima une fois par trimestre ou au mieux une fois par mois.

Le deuxième piège classique est de sous-estimer la nécessité d'organiser ce comité.

En effet dans les entités à maturité naissante ou moyenne en sécurité, la multiplication des comités fait peur aux instances dirigeantes. Les comités de pilotage, arbitrage et suivi de la sécurité, s'ajoutant pour les autorités administratives aux Comités d'homologation des télé-services devant valider les risques résiduels, les comités de projet pour la validation et le contrôle de conformité des systèmes d'information semblent souvent pour les directions

générales superflus ou redondants. Ceci constitue un vrai piège. Les périmètres, les enjeux et les acteurs sont réellement différents. Constituer un seul comité pour l'ensemble des sujets et acteurs finira par troubler les messages et l'efficacité des différents plans.

Les entreprises plus matures n'hésiteront pas à bien séparer les comités puisque leurs objectifs sont bien différents. Elles n'hésiteront pas, pour les plus avancées, à non seulement constituer un Comité pour le Plan de Continuité d'Activité chargé de la conception, du suivi et de la coordination, à organiser une cellule de crise décisionnelle (CCD) complétée d'une ou plusieurs cellules de crise opérationnelles chainées entre elles et positionnées à différents niveaux dans l'organisation.

La cellule de crise décisionnelle est ainsi composée des responsables de chaque direction métier concernée par le PCA. Elle comprend également des membres de la direction générale, de la direction des services généraux, de la direction des ressources humaines, de la direction de la communication, de la direction informatique et des responsables PCA.

Son rôle est de se réunir en cas d'incident grave pour décider de déclencher ou non le PCA. Ses membres doivent être assujettis à des astreintes (service de garde) ou au moins être disponible à tout moment et en tout lieu. Leurs coordonnées doivent être consignées dans un annuaire de gestion crise.

Le troisième piège classique pour les entités à maturité naissante ou moyenne est de ne pas se donner les moyens nécessaires pour la conduite et le suivi du PCA, notamment en termes de budget, puis de ressources humaines disponibles par exemple en phase de conception, de sous-estimer la formalisation de la répartition des rôles des directions et ou filiales de l'entreprise, les outils de gestion documentaire et de suivi du PCA lui-même.

Le quatrième piège classique des entités à maturité naissante ou moyenne est de sous-estimer le besoin de formalisation d'un référentiel documentaire pour la continuité d'activité.

En effet ce référentiel doit être absolument être constitué autour d'une Politique Générale pour la Continuité de l'Activité complétée de différents Plans : le Plan de Continuité des Opérations (PCO), le Plan de Gestion de Crise (PGC), le Plan de Communication de Crise (PGC, le Plan de Secours Informatique (PSI), le Plan de Repli Utilisateur (PRU) et le Plan de Repli Utilisateur (PRU). L'inflation de documents à concevoir fait souvent peur aux instances dirigeantes et renvoient trop souvent cette responsabilité au RSSI chargé alors de définir des règles de continuité d'activité dans la Politique de Sécurité des Systèmes d'information. Il y a donc ici confusion entre la continuité des activités métier et la disponibilité du système d'information. Encore une fois, dans ce cas les messages liés aux exigences de la continuité perdront de leurs efficacités

Après avoir identifié les principaux écueils liés à l'organisation de la démarche globale nous soulignerons les difficultés liées à chaque étape.

L’étape 1 : la définition des besoins métiers

L’objectif est de définir le périmètre fonctionnel et/ou géographique pour lequel le PCA devra être fonctionnel. Les questions à traiter sont : quels sont les métiers concernés, quels sont les sites et les bâtiments à prendre en compte, quelles sont les interactions avec les autres projets tels que la qualité et/ou la sécurité ? Le périmètre devra donc être validé par la direction générale lors de l’organisation du Comité pour la Continuité d’Activité.

Une fois le périmètre défini le RPCA (Responsable du Plan de Continuité d’Activité) devra assister les directions métiers à lister les processus critiques qui devront être prioritairement poursuivis et/ou redémarrés en cas de crise majeure. Ces processus devront être ensuite classifiés par leur ordre d’importance pour l’entreprise et ce, en cohérence avec les systèmes de classification des risques opérationnels et de la Politique de Sécurité des Systèmes d’Information.

Il est fondamental de bien identifier les pièges classiques et nombreux de la classification.

Le premier est de se tromper d’interlocuteur et de faire classifier par le RPCA, le RSSI voire par le DSI. Or il devrait être clair que seules les directions métiers ont une légitimité, voire les compétences pour classifier les processus, les informations, les documents et les données traitées pour réaliser les missions de l’entreprise.

Le deuxième piège est de ne pas former correctement les directions métiers au travail de classification, conduisant à la définition des BIA (Bilan d’Impact sur l’Activité). Les conséquences seront réellement dommageables pour l’expression des besoins de continuité d’activité. Les erreurs types sont nombreuses et classiques :

- classifier en fonction, non pas de l’impact mais en fonction de la probabilité,
- « sur classifier » par réflexe de « survalorisation » de sa mission ;
- classifier en fonction de règles ou de solutions déjà mises en place ;
- classifier en fonction des règles jugées comme admissibles ;
- classifier en fonction des budgets jugés opportuns.

Aussi il est important d’aider les directions métier à formaliser l’importance des processus métiers pour la conduite des activités. Non seulement, il s’agira de se référer à une échelle d’impact structurée sur 3 à 5 niveaux, classiquement 4, mais aussi et surtout aux valeurs essentielles de l’entreprise facilement compréhensibles et donc mobilisatrices pour les directions métiers.

Ces valeurs essentielles formalisées par la direction générale devraient être classiquement :

- la garantie de disponibilité et de qualité du service aux clients ou usages,
- la confiance des clients ou des usagers dans leurs échanges avec l’entité,

- la protection des investissements de l'entité,
- l'engagement de l'entité et de tous les acteurs concernés par la mission de l'entité à respecter les obligations légales et contractuelles,
- la protection des personnes et des biens,
- l'entretien de relations sociales de qualité,
- le respect des intérêts légitimes et justifiés des partenaires et fournisseurs,
- le respect de la culture et de la souveraineté des pays dans lesquels l'entité est présente,
- la préservation de l'environnement,
- la protection et la valorisation de l'image de l'entité,
- la protection du patrimoine historique et culturel de l'entité,
- …

L'analyse d'impact devra tenir tient compte des principaux paramètres suivants :

- l'emplacement des installations critiques de l'établissement et leur sensibilité aux évènements de risques majeurs,
- les facteurs géographiques (par exemple, la concentration des établissements dans les zones d'activité de grandes villes),
- la nature et la complexité des activités de l'établissement,
- la taille et l'extension géographique du réseau de l'établissement,
- les fonctions essentielles ou processus critiques (externalisés, centralisés ou décentralisés),
- les contraintes résultantes de divers types de dépendance, y compris celles vis-à-vis des fournisseurs, des clients et d'autres établissements.

Cette analyse d'impact devra aussi prendre en considération les contraintes éventuelles (calendaires, réglementaires et/ou contractuelles) qui pourraient avoir une influence sur les choix stratégiques et les solutions à retenir.

Le troisième piège pour cette étape est de raisonner uniquement en termes d'impact métier sur la disponibilité du processus, des données et des informations. Or la perte de confidentialité, d'intégrité, voire de preuve peut être tout aussi catastrophique pour l'entreprise.

Il est important de souligner l'importance de la formalisation de fiches de renseignement de ces processus par les directions métiers afin d'obtenir une cohérence dans les expressions de besoins de continuité par les métiers.

Dans ces fiches de renseignement des processus métiers, les directions concernées devront définir des besoins en DMIA (Délai Maximal Indisponibilité Admissible) et PDMA (Perte de Données Maximale Admissible). Ces besoins gradués consolidés par l'évaluation des scénarios de risques permettront d'orienter une stratégie de continuité.

Une fois la classification des processus métiers réalisée avec les directions concernées, il est alors nécessaire de procéder à une évaluation des risques pouvant provoquer des dysfonctionnements ou un arrêt prolongé des activités.

Les entreprises à maturité naissante ou moyenne chercheront le pragmatisme en évaluant la vraisemblance du risque. Par contre, les entreprises plus avancées et plus matures chercheront

à évaluer par des méthodes (ISO 27005, EBIOS, MEHARI, ISACA, OCTAVE,…), les menaces pouvant exploiter les vulnérabilités de l'entreprise pouvant conduire à des interruptions d'activités.

L'identification des risques permettra donc à la direction générale de retenir les scénarios de crise à prendre en compte.

Le quatrième piège de cette étape est consécutif à une tentation intellectuelle classique de vouloir formaliser un seul plan de continuité d'activité « générique » multi sinistres.

Il faut donc souligner l'importance de la formalisation de la vraisemblance des risques par les menaces exploitant des vulnérabilités pour bien mettre en évidence les différentes causes de sinistres et les solutions pour les limiter et/ou les surmonter. Par exemple une solution de site de repli ne pourra permettre de gérer une crise liée aux ressources humaines consécutive à une pandémie ou un conflit social.

L'étape 2 : la définition de la stratégie

L'objectif est de définir les scénarios de sinistres à prendre en compte. Les critères de sélection sont classiquement les suivants :

- le niveau d'exposition au risque et la probabilité de survenance,
- la situation géographique / environnementale de l'entreprise (exposition aux risques naturels, aux risques malveillants),
- l'environnement social interne de l'entreprise et le climat de confiance,
- la situation financière de l'entreprise,
- la capacité de l'entreprise à reporter des risques financiers sur des contrats d'assurance.
- …

Après cette définition, la direction générale devra donc décider d'assumer ces risques, de transférer les risques aux assurances ou de les traiter dans le cadre d'un ou de plusieurs PCA.

La stratégie de traitement des sinistres est classiquement structurée pour prendre en compte trois grands types de scénarios :

- les scénarios nécessitant la définition d'un PCA complet, par exemple l'indisponibilité des établissements, du système d'information et des ressources humaines,
- les scénarios à traiter uniquement dans le cadre d'une gestion de crise,
- les scénarios à ne pas traiter dans le cas d'un PCA, mais dans le cadre de la gestion d'incidents.

La stratégie de contournement des sinistres engendrés par les risques devra permettre de définir les orientations et les solutions qui pourront être obtenus pour poursuivre les activités de l'entreprise y compris en mode dégradé. A ce sujet et afin d'éviter les mauvaises surprises lors

de la mise en œuvre effective du ou des PCA, il est primordial de bien communiquer avec le métier sur le niveau du mode dégradé.

Cette stratégie permettra de formaliser des objectifs de reprise activité. Le piège classique est de définir des valeurs égales aux DMIA et PDMA en oubliant les délais supplémentaires de reprise induits par la remontée d'incidents, l'évaluation du niveau de l'incidents, la décision d'activation de la cellule de crise et / ou du Plan de Continuité.

Encore une fois, les entreprises (plutôt matures en termes de sécurité) ont tendance à retenir trois types de stratégies de contournement, une pour gérer le scénario de destruction du site principal, une deuxième pour gérer le scénario d'indisponibilité du système d'information, par exemple par destruction de la salle hébergeant le « Data Center » et une troisième pour gérer le scénario de destruction des bureaux utilisateurs.

Les solutions de contournement seront basées autour de solution d'hébergement, de travail à domicile.

Le piège classique concernant les solutions d'hébergement des ressources système d'information ou des ressources humaines est de ne pas s'attacher à la formalisation de clauses sécurité telles que celles constituées dans les Plans d'Assurance Sécurité obligatoires pour les externalisations et les hébergements.

Ces clauses conformément aux recommandations de l'ANSSI doivent définir :

- le respect d'un référentiel de sécurité sous la forme d'un Plan d'Assurance Sécurité (PAS) validé par la fonction SSI sécurité,
- l'application des obligations légales,
- l'auditabilité,
- la réversibilité du contrat,
- le maintien de la propriété du client,
- la protection contre les actions en contrefaçon,
- la formation à la sécurité du personnel du prestataire et aux règles de l'entreprise cliente,
- la confidentialité du contrat et de ses annexes,
- le suivi du contrat de service avec des indicateurs précis,
- l'obligation de conseil.

La formalisation des types de solutions devra prendre en compte les besoins en ressources humaines, les moyens logistiques, (mobiliers, superficie, …), les moyens systèmes d'information, (ordinateurs imprimantes, applications réseaux, VPN de télé accès, téléphonie, internet, …), les matériels de bureau, (photocopie, machine à affranchir, …) et les budgets associés.

Le RPCA est alors confronté à la réalisation d'un équilibre entre les niveaux de performance attendus et les moyens raisonnables qu'il est susceptible d'obtenir.

L’étape 3 : la définition des plans de continuité, d’hébergement, de communication et de gestion de crise.

Cette étape a pour objectifs de définir les procédures métiers en mode dégradé, la gestion de crise, le plan éventuel de relocalisation, le plan de communication et le plan de secours informatique.

Les procédures fonctionnelles dégradées doivent être structurées dans le cadre d’un Plan de Continuité des Opérations pour chaque processus métier identifié comme critique et devant faire l’objet d’un PCA.

Ces procédures doivent définir les modes opératoires à mettre en place en cas de sinistre dans l’attente d’un retour normal.

Cette étape présente des difficultés classiques quel que soit le niveau de maturité de l’entreprise en sécurité. Les directions métiers n’ont pas conscience que c’est à elles d’écrire ces procédures et ce n’est pas au RPCA de les concevoir. Le RPCA peut les aider, les conseiller, mais ne peut aucun cas se substituer à elles.

Lors de cette étape il n’est pas rare de rencontrer de véritables écueils. Certaines applications ont été installées ou conçues par la DSI, certaines données ne sont pas stockées ou sauvegardées sur les serveurs gérés par la DSI. Ceci montre bien encore une fois la nécessité incontournable de mettre en place un Comité pour la continuité d’activités regroupant les différents acteurs techniques, support et métiers pour la formalisation de la mise en œuvre du ou des PCA.

Cette étape devra aussi organiser et définir le ou les Plans de gestion de crise. L’objectif est de définir les rôles, les responsabilités et les procédures du traitement d’une crise de la phase de déclenchement jusqu’à la phase de sortie de crise.

La gestion de crise doit recouvrir l’ensemble des modes d’organisation, des techniques et des moyens qui permettent à l’organisation de se préparer et de faire face à la survenance d’une crise, puis de tirer les enseignements de l’évènement pour améliorer les procédures et les structures dans une vision prospective.

Les éléments incontournables à définir sont :

- le mode de remontée d’alerte,
- les acteurs du processus d’analyse et de décision, leurs rôles et responsabilités
- les critères d’évaluation des sinistres,
- les étapes, les responsabilités et autorité du processus de décision d’activation du PCA,
- les modes de communication et d’interaction avec les services publics de crise,
- les actions de communication interne et externe au voisinage immédiat de la crise,
- l’évaluation, la validation et la communication du schéma de déclenchement du PCA.

Comme évoqué plus haut la gestion de crise devrait conduire à une structuration à deux niveaux : d'une part, la cellule de crise décisionnelle qui déciderait de l'activation ou non du PCA, qui prendrait toutes les décisions d'ordre stratégique et d'autre part, la cellule de crise opérationnelle qui activerait les solutions adaptées à la situation et notamment les plans de secours.

Lors de cette troisième étape, l'éventuel plan de repli des utilisateurs doit aussi être formalisé afin d'élaborer les chronologies de mesures et des solutions de repli des utilisateurs. Il est important de ne pas oublier les soutiens psychologiques complémentaires à apporter aux utilisateurs qui doivent se replier dans le cadre d'un sinistre majeur.

Cette étape doit se conclure par la définition des plans de communication internes et externes.

Lorsqu'une crise éclate, les employés sont souvent les premiers concernés par l'événement. Mais on oublie pourtant très souvent de les informer. Les employés sont alors tentés de communiquer sur leur connaissance de l'évènement vers l'extérieur de l'entreprise. Le risque de perte de la maitrise des informations communiquées devient alors extrêmement important. Il est nécessaire que l'entreprise adopte une information interne claire et extrêmement précoce pour rassurer, mobiliser et obtenir de la part des internes, adhésion et soutien.

Pour une communication externe cohérente et efficace, il faut aider les communicants présents dans la cellule de crise à :

- informer les autorités, ANSSI, CNIL, Ministère de tutelle, maison mère, …
- informer les clients,
- informer les partenaires locaux et les fournisseurs,
- rédiger les communiqués de presse,
- rédiger les premiers documents de défense,
- entraîner le porte-parole de l'entreprise,
- suivre et synthétiser les commentaires des médias à propos de la crise.

Face à la presse, le piège le plus courant est d'oublier une règle essentielle de la communication en situation sensible : une interview ne s'improvise pas ! Il faut être préparé à un entretien avec un journaliste pour :

- communiquer les bons messages,
- ne pas être emmené par le journaliste sur des sujets que l'on ne maîtrise pas,
- rester maître de sa communication vis à vis des médias,
- comprendre le fonctionnement des médias,
- savoir présenter son point de vue.

Lorsque la crise le nécessite, il convient de ne pas oublier bien évidemment, son expérience et sa connaissance en matière de gestion des victimes et de leur entourage.

C’est lors de l’étape 3 que devra être défini aussi le Plan de Secours Informatique. L’objectif est de garantir la reprise des systèmes et des données désignés comme critiques dans le temps minimum fixé.

Les solutions sont nombreuses et souvent bien comprises des DSI et bien sur beaucoup moins par les directions métiers. Elles sont basées à partir :

- de salles de secours blanches, (non équipées, mais pouvant recevoir les équipements),
- oranges (partiellement équipées),
- rouges (équipées mais sans l’installation des applications),
- miroir totalement redondantes, voire mobiles.

Les critères de choix retenus par la majorité des entreprises sont les délais de reprise, le degré de fraicheur des données, le niveau de couverture, la vraisemblance de la solution à valider par des tests, la souplesse de la mise en œuvre, l’évolutivité de la solution et bien sur les coûts.

Le piège classique est de ne prendre en compte uniquement ce dernier critère.

L’étape 4 : la formation des personnes concernées :

La formation doit permettre à l‘ensemble des acteurs de l’entreprise de connaître les procédures et les démarches à adopter, notamment en cas de crise majeure et lors de la survenance d’un sinistre moins important.

Un plan de formation doit être défini pour l’ensemble des acteurs. Malheureusement c’est l’un des points faibles classiques des PCA rencontrés dans les entreprises. Ceci est bien révélateur de l’oubli de la prise en compte du facteur humain dans la gestion des risques liés à l’utilisation des données et des systèmes d’information. Un certain nombre de profils types devraient pourtant être identifiés : les membres de la cellule de crise décisionnelle, les membres de la cellule de crise opérationnelle, les utilisateurs « clés » dans les métiers, les acteurs de la DSI, le responsable de la sécurité physique, la direction des ressources humaines, etc.

La plus classique des difficultés de cette étape est de trouver « le bon formateur » sachant communiquer avec tous les profils identifiés. Or il n’est pas certain que le RPCA recouvre toutes les compétences du pédagogue. Cette difficulté tés courante est souvent rencontrée dans le domaine de la responsabilisation au respect des bonnes pratiques de manipulation de l’information et d’utilisation des ressources associées.

L’étape 5 : la maintenance du PCA.

L’objectif est de simuler des situations crises dans le but de tester les procédures et les moyens définis pour la reprise d’activité afin d’identifier les erreurs ou les failles des dispositifs prévus.

Trois catégories de test sont classiquement prévues:

- les tests techniques unitaires pour valider les éléments de secours, les configurations, les délais, la documentation…,
- les tests d'intégration pour vérifier la compatibilité entre les éléments de secours et la synchronisation des opérations techniques…,
- les tests en vraie grandeur pour simuler un cas et éprouver la combinaison adoptée.

Les difficultés classiques rencontrées par l'ensemble des entreprises est la formalisation des protocoles de tests et de fiches de suivi.

De plus il n'est pas rare de rencontrer une situation paradoxale où une direction métier à formaliser des besoins élevés en continuité mais « répugne » à organiser des tests réels de Plans de Continuité sous « prétexte » de contraintes opérationnelles, de temps et d'exigences de continuité !

La réalisation et le suivi de ces tests permettra de évoluer les plans et les procédures définis dans le cadre du ou des PCA.

La maintenance du plan de continuité prendra en compte les éléments suivants :

- les résultats des tests du plan de continuité,
- toute modification organisationnelle ou stratégique qui peut avoir un impact sur les procédures existantes
- tout élément technique (notamment informatique) qui peut avoir un impact sur le bon déroulement d'une procédure en mode dégradée.

Les facteurs clés de succès d'un PCA

Pour conclure et synthétiser comment surmonter toutes les difficultés identifiées, il est incontournable d'impliquer ou plutôt de responsabiliser la direction générale et tous les acteurs de l'entreprise (utilisateurs, DSI, logistique, etc.). La sensibilisation formation doit donner les éléments nécessaires à la mise en œuvre d'une organisation de conduite de projet (Chef de projet RPCA, Comité PCA, etc.). Elle doit souligner que l'objectif du PCA n'est pas de vouloir couvrir 100 % des risques et surtout de bien mettre en avant, qu'il ne faut pas raisonner uniquement en termes de solution technique (informatique) et de ne pas confondre Qualité de Service et PCA. Les acteurs du PCA devront bien prendre conscience que le bon fonctionnement d'un PCA nécessite la mise en œuvre d'un processus d'amélioration continue et enfin de tester régulièrement les procédures et les plans.

Denis VIROLE

Gérant de VIROLE CONSEIL FORMATION Groupe Ageris

Directeur des services d'Ageris GROUP