PLAN DE CONTINUITÉ D'ACTIVITÉ, PARANGON DE LA REPRISE APRÈS SINISTRE ?

Par Lionel Mourer, Fondateur de MANIKA

Face à l'informatisation croissante et à l'augmentation continue du nombre de menaces, les organisations comprennent de plus en plus aujourd'hui l'importance de mettre en place un plan de continuité d'activité (PCA). Mais, avant de se lancer « bille en tête » dans la définition et la mise en œuvre de son PCA, il est nécessaire de prendre un peu de hauteur, de se poser les bonnes questions et de s'assurer que les conditions essentielles à son fonctionnement ont bel et bien été prises en compte.

Reprenons les basiques : un PCA, quel intérêt ?

Les organisations connaissent une informatisation croissante accompagnée d'un développement rapide des échanges avec leurs clients et partenaires, au travers de l'augmentation des flux externes, du développement des réseaux, et de l'attention accrue au service rendu à la clientèle ou aux usagers.
Ce mouvement rend nécessaire, a minima, de mettre en place un dispositif de protection permettant d'assurer la continuité des missions essentielles de l'organisation. Les menaces pesant sur les Systèmes d'Information des entreprises sont nombreuses. Citons pour exemple les risques naturels (incendie, inondation, foudre, pandémie, etc.), les risques techniques (pollution logique, problème d'énergie, explosion, etc.), et les facteurs humains (erreur, malveillance, piratage, attentat, etc.).

De fait, mettre en place un plan de continuité d'activité dans son entreprise permet de contrer les risques majeurs. Son objectif est de réduire les risques d'indisponibilité de ressources (humaines, IT, etc.) et de discontinuité de service, par la mise en œuvre de moyens humains, techniques et organisationnels. Pour ce faire, il faut :

- Évaluer les risques majeurs d'indisponibilité : des locaux, des équipements, des moyens de communication, des personnes ;
- Définir une stratégie et un plan d'action face à ces risques : politique de prévention, organisation de la sécurité et mécanismes de continuité d'activité.

Mais, avant de se lancer « bille en tête » dans la définition d'un plan de continuité d'activité, il est nécessaire de prendre un peu de hauteur et de vérifier que plusieurs conditions essentielles sont prises en compte :

- L'objectif du PCA doit être affirmé : par exemple, garantir la résilience des services critiques en cas de crise majeure (reste à définir ce qu'est une crise majeure dans le contexte de sa propre organisation) et/ou répondre à des attentes réglementaires, légales ou contractuelles ;
- L'adhésion par tous les acteurs doit être validée : le PCA a comme finalité, pour une entreprise, de survivre à une crise majeure, et ainsi d'assurer la pérennité de l'organisation (et de l'emploi de ses salariés…) à l'ensemble de ses collaborateurs. Pour autant, cette évidence doit être partagée par tous afin de permettre, le jour venu, une mise en œuvre opérationnelle réelle… ;
- Les bons moyens pourront être mis à disposition : la majorité des ressources déployées pour un PCA sont classiquement identifiées comme « non-productives »… C'est pourquoi, il est nécessaire de s'assurer de la capacité de l'organisation à soutenir les investissements nécessaires permettant au PCA d'être raisonnablement dimensionné, maintenu à jour et, si besoin…, activé à tout moment avec les solutions initialement définies.

Ces conditions sont particulièrement à prendre en compte par la Direction générale de l'entreprise, afin d'assurer au porteur du PCA (appelons-le « RPCA » pour Responsable du PCA) le support nécessaire dans le déploiement de ce projet structurant et

ambitieux ! Sans ce soutien, il sera difficile au RPCA de mettre en œuvre le « bon PCA » pour l'organisation.

Et il reste encore du travail… comme le montre la dernière étude « Menaces informatiques et pratiques de sécurité en France » (MIPS 2018 [1]) du CLUSIF, où 21% des sondés [2] avouent n'avoir mis aucun mécanisme de continuité en place et 25% ne disposent pas d'une gestion de crise formalisée…

Alors, comment on s'y prend… ?

A titre d'illustration, la Figure 1 ci-dessous reprend un exemple classique d'organisation d'un plan de continuité d'activité. Il est à noter que cette décomposition complète et précise doit être adaptée en fonction des enjeux, des attentes et/ou des moyens techniques et organisationnels de chaque entité.

BCP

Business continuity plan: essential for disaster recovery?

By Lionel Mourer, Founder of MANIKA

Organisations today are coping with ever-more ubiquitous computerisation and faced with a relentless growth in the number of threats. It follows that they are also more acutely aware than ever of the importance of implementing a Business Continuity Plan (BCP)). But before embarking on the planning and implementation of your BCP, it is worthwhile taking a step back, look at the broader picture, ask the proper questions and make sure that the essential conditions for implementation have been taken into account.

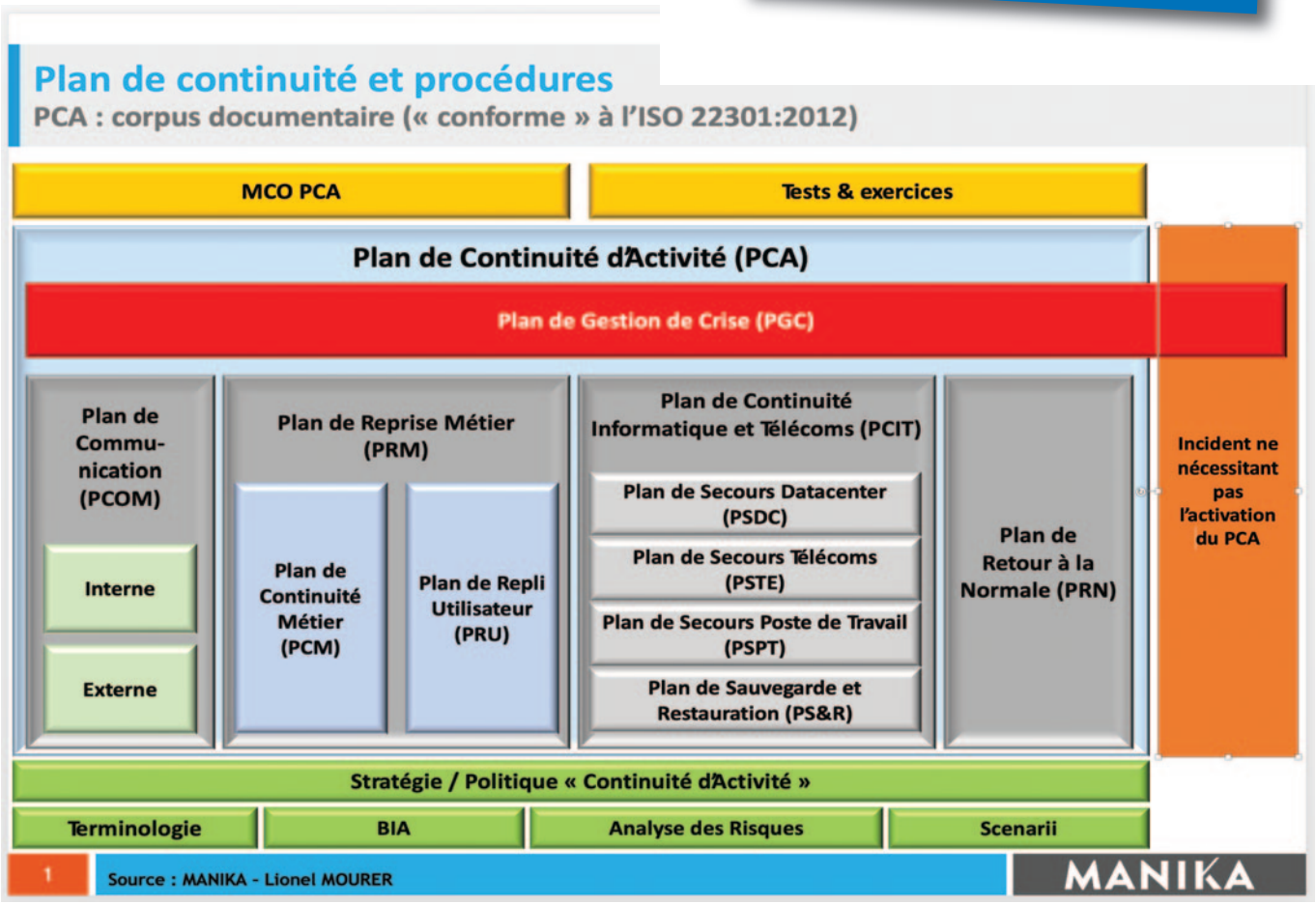

Figure 1 – Exemple de contenu d'un PCA

Nous ne nous attarderons pas sur le détail de chaque partie (cela prendrait un livre entier…), mais les jalons critiques à retenir sont les suivants :

- Formaliser la stratégie de continuité d'activité ;
- Identifier et déployer les mécanismes de continuité (technique, humain, etc.) à mettre en œuvre ;
- Formaliser les procédures utiles à l'activation de tout ou partie du PCA ;
- Maintenir le PCA en condition opérationnelle ;
- Préparer les acteurs du PCA au travers de tests et d'exercices.

Par ailleurs, et pour ceux qui ne savent pas par où commencer, la littérature sur le sujet est relativement importante et de nombreux documents permettent de démarrer un PCA selon une bonne méthodologie. Citons pour exemple (liste non exhaustive) :

- La norme ISO 22301:2019 décrivant les exigences d'un Système de management de la continuité d'activité (SMCA) et permettant de certifier une organisation en matière de continuité d'activité, sur un périmètre donné [3] ;
- Le document « Cellules de crises et SI », publié par le CLUSIF en janvier 2017 ayant pour vocation de mettre à disposition du lecteur une série de repères, établis suivant l'état de l'art, pour l'aider à

organiser la gestion d'une crise sur son SI [4] ;
- Le « Guide pour réaliser un plan de continuité d'activité », publié par le SGDSN, proposant une démarche méthodologique permettant l'élaboration concrète d'un plan de continuité d'activité [5].

Formaliser la stratégie de continuité d'activité

Pour ce faire, il faut :
- Se mettre d'accord sur la terminologie employée et les définitions qui en découlent : en continuité d'activité (comme ailleurs), de nombreux acronymes sont utilisés et lorsque l'on demande à plusieurs personnes la définition de ces acronymes, il est fréquent que ces dernières soient différentes… ;
- Identifier le périmètre et les scenarii que l'on souhaite couvrir ;
- Identifier les risques pesant sur l'organisation (sur le périmètre retenu) ;
- Identifier les critères de reprise (au travers du BIA – *Business Impact Analysis*) et en particulier :
  - le RTO (*Recovery Time Objective*) identifiant les délais sous lesquels devraient redémarrer les applications (des + au – critiques),
  - le RPO (*Recovery Point Objective*) identifiant l'acceptation de perte de données,
  - la montée en charge des utilisateurs identifiant combien de personnes sont attendues à un instant t pour assurer la reprise d'activité.

Identifier et déployer les mécanismes de continuité

La continuité d'activité s'appuie sur des ressources identifiées lors de l'étape précédente. Ces ressources peuvent être :
- Humaines : cœur de métier, métier support (dont l'informatique) ;
- Techniques : informatique centrale, PC utilisateurs, locaux, matériels spécifiques, etc.

Du côté « humain », il s'agira principalement d'identifier les personnes qui interviendront le jour du sinistre et leur *timing* d'arrivée, à la fois côté SI et côté utilisateur, mais aussi celles qui seront à l'écart de la reprise.
Côté « technique », l'objectif sera notamment d'identifier les technologies à mettre en place (sauvegarde, réplication asynchrone ou synchrone, cluster, connexion à distance via un VPN, etc.), et de déployer celles qui sont nécessaires (préparation d'un site de secours, de PC utilisateurs, etc.).

Ce chantier est souvent le plus coûteux – lorsque rien (ou presque) n'existe déjà au sein de l'organisation – puisqu'il nécessite des investissements importants (en propre ou via un prestataire spécialisé).

Formaliser les procédures utiles à l'activation de tout ou partie du PCA

Cette phase est particulièrement importante, pourtant dans les organisations ayant déjà déployé des mécanismes de reprise technique, elle est (assez) souvent oubliée… Il s'agit ici de formaliser les procédures qui permettront le jour du sinistre de ne pas se poser de mauvaises questions : « Où est le n° de téléphone de… ? », « J'interviens sur le PCA, mais je ne sais pas où je dois me rendre, ni qui appeler… », « Comment puis-je restaurer le système de base de données, d'annuaire, etc. ? »…
Bien entendu, les procédures ne répondent pas à tout et ne croyez pas ceux qui vous vendent un « PCA clé-en-main tout prêt sur étagère » : ils vous feraient prendre des vessies pour des lanternes… Les procédures de continuité d'activité ne s'improvisent pas ; pour être adaptées à l'organisation, elles demandent une expertise rigoureuse, du temps et des moyens !
Alors, ces procédures permettront de « robotiser » un certain nombre de tâches et de fiabiliser les données utiles à la reprise d'activités. De fait, elles sont indispensables et doivent être formalisées avec soin en prenant en compte les spécificités de l'organisation.
Ces procédures s'appliquent à l'ensemble des différents plans identifiés en Figure 1 : Plan de Gestion de Crise (PGC), Plan de Communication (PCOM), Plan de Reprise Métier (PRM, y compris le repli des utilisateurs), Plan de Continuité Informatique et Télécoms (PCIT) et Plan de Retour à la Normale (PRN).
Les écarts (qui ne manqueront pas d'arriver !) avec les plans formalisés et la réalité de la crise seront quant à eux traités en direct par la Cellule de crise.

Maintenir le PCA en condition opérationnelle

Bien entendu, le Système d'Information de l'organisation vit et évolue au fil du temps. De ce fait, le PCA doit également évoluer. Ainsi, il est nécessaire de formaliser le cycle de vie des documents liés au PCA, en identifiant :
- La politique de révision des BIA (fréquence, périmètre) ;
- La prise en compte de nouveaux scenarii ;
- Les entrées/sorties des personnes impliquées dans le PCA (gestion des annuaires liés au PCA) ;
- Les évolutions (mineures et majeures) du Système d'Information (gestion de l'obsolescence des procédures techniques) ;
- Les évolutions de l'organisation (acquisition, cession, organigramme), les changements de sites, de locaux ;
- Etc.

Préparer les acteurs du PCA au travers de tests et d'exercices

Enfin, après avoir passé beaucoup de temps à la mise en place des mécanismes de continuité d'activité, il est temps de vérifier que tout cela fonctionne ! Pour ce faire, rien de tel que des tests et exercices, permettant de valider que les hommes et les femmes, ainsi que la technique sont opérationnels et prêts à réagir en temps de crise… et d'activation de tout ou partie du PCA.
Parmi les alternatives existantes, il est possible d'organiser des exercices de simulation de crise permettant de valider les réactions de la cellule de crise de l'organisation, des tests de bascules techniques (tout ou partie du PCIT), des exercices de repli utilisateurs, ou des exercices combinant 2 ou 3 de ces items.

Et la cybercrise, dans tout cela…

Comme exprimé précédemment, le PCA a vocation à répondre à tout sinistre majeur qui toucherait directement ou indirectement l'organisation qui le déploie. Historiquement, ces sinistres étaient particulièrement vus sous l'angle « sécurité physique – sûreté » (incendie, crue, grève, pandémie, etc.).
Toutefois et depuis quelques années maintenant, un nouveau type de sinistre est pris en compte par les RPCA (en connexion forte avec les RSSI) : la cyberattaque ! En effet, celle-ci est à même de bloquer très largement le SI, suite à la destruction massive des données ou, plus couramment, à l'installation de cryptovirus, chiffrant toutes les données auxquelles ils accèdent, rendant ainsi le SI totalement indisponible…
Les exemples récents (et publics), tels que Saint Gobain [6], Altran [7], M6 [8], CHU de Rouen [9], et bien d'autres, montrent à quel point il est important de se préparer à ce type de sinistre.

Alors, quelles sont les spécificités d'une cybercrise ? Elles sont multiples et comprennent :

- Une visibilité très faible (en première intention…) par rapport aux sinistres « sécurité physique – sûreté » ;
- Une difficulté à évaluer :
  - la durée de l'attaque : depuis combien de temps le pirate est-il en place au sein de votre SI ?,
  - son étendue : sur quel périmètre l'attaque est-elle étendue ?,
  - la réalité de l'attaque : parle-t-on « seulement » de chiffrement ou y a-t-il également eu vol des données ? Pour mémoire, en informatique, il est possible de voler des données tout en les laissant à leur place… cela s'appelle une copie et l'identification du vol peut alors prendre beaucoup plus de temps… ;
- Le besoin substantiel de compétences « informatiques » rares (donc chères) et dans un délai très court (les pirates attaquent rarement à 15h en semaine…). Peu d'organisations disposent de ce type de compétences, mobilisables 24/7, et il faut alors identifier quels sont les acteurs externes qui pourront/devront vous aider ? Etc. ;
- La potentielle diminution de la capacité de réponse !!! Effectivement : « mon SI est attaqué », alors comment mon SI peut-il m'aider ? Est-il encore fiable ? Ne vais-je pas aggraver la situation ? Les processus de continuité d'activité « classiques » répondent-ils au besoin (la belle affaire de basculer les utilisateurs sur le site de repli, s'il n'y a plus du tout d'informatique…) ?

Le tableau semble bien sombre et personne ne peut aujourd'hui jurer qu'il est à l'abri d'un tel scénario. Alors pour répondre au mieux à une cyberattaque de grande ampleur, il faut :

- Se préparer (la crise arrive, n'en doutez pas…) : identifier son patrimoine informationnel (typologie des données, sensibilité, attractivité, localisation, circulation), mettre en place des mesures de prévention/protection, contracter une assurance « cyber risques » [10] ;
- Détecter (tiens, serait-ce une crise, par hasard ?) : au travers de mécanismes techniques (SOC/SIEM – 24/7), souvent efficaces mais chers… ; suite à l'appel des attaquants : dommage ! ; suite à la publication dans la presse : re-dommage ! ;
- Réagir (la crise est là : on fait quoi ??!!…) : identifier le « scénario » d'attaque, dérouler les protocoles préétablis, prévenir les autorités [11], aller chercher de l'aide (assureurs, prestataires de réponse aux incidents de sécurité qualifiés - PRIS), porter plainte.

Et n'oubliez pas, pour « mieux réagir », il est essentiel de s'entraîner en réalisant régulièrement des exercices de simulation de cybercrise. ■■■

[1] https://clusif.fr/publications/menaces-informatiques-pratiques-de-securite-france-edition-2018-rapport/ (cf. figures 43 et 44, page 48 du rapport)
[2] Cible : entreprises privées de +100 salariés
[3] https://norminfo.afnor.org/norme/NF%20EN%20ISO%2022301/securite-et-resilience-systemes-de-management-de-la-continuite-dactivite-exigences/123980
[4] https://clusif.fr/publications/cellules-de-crises/
[5] http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf
[6] 27 juin 2017 : https://www.saint-gobain.com/fr/point-sur-la-cyberattaque
[7] 24 janvier 2019 : https://www.altran.com/fr/fr/news_press_release/information-sur-une-cyberattaque/
[8] 12 octobre 2019 : https://www.lemonde.fr/actualite-medias/article/2019/10/14/le-groupe-m6-victime-d-une-cyberattaque_6015369_3236.html
[9] 15 novembre 2019 : https://www.lemonde.fr/pixels/article/2019/11/18/frappe-par-une-cyberattaque-massive-le-chu-de-rouen-force-de-tourner-sansordinateurs_6019650_4408996.html
[10] https://www.cyber-cover.fr/
[11] https://www.ssi.gouv.fr/en-cas-dincident/, https://www.cybermalveillance.gouv.fr/diagnostic, https://clusif.fr/cyber-victimes/