Résumé de l'article : « The Role of Business Impact Analysis and Testing in Disaster Recovery Planning by Health Maintenance Organizations »

Abstract : Cet article se penche sur la problématique des disaster recovery planning dans les HMO (Health Maintenance Oraganizations). L'auteur défini deux étapes cruciales pour le succès de la mise en oeuvre d'un DRP (disaster recovery plan). Ces étapes sont les suivantes :

- élaborer un « business impact analysis » (BIA) afin de connaître les effets d'une rupture du système informatique sur les activités commerciales.
- Tester le plan (DRP) qui découlera du BIA.

Disaster recovery planning.

Définition 1 (selon Andrews) : « Un DRP = les processus du développement et du maintient d'un plan effectif écrit sur comment les organisations vont continuer à fonctionner dans le cas d'une interruption des fonctions business. »

Définition 2 (selon Epich & Persson) : « DRP = un plan d'action écrit qui permet à une compagnie de répondre rapidement à un désastre.»

Le DRP doit inclure les informations suivantes :

- Une liste des personnes à appeler en cas d'urgence ainsi que leur assignation.
- Un guide pas à pas de ce qui doit être fait (actions et process) dans chaque phase de recovery.
- Les spécifications du minimum d'équipement requis.
- Les noms de nos contacts chez les sous-traitants et les fournisseurs.
- Provision pour garantir un niveau de télécommunication adéquat.
- Les procédures pour tourner sur les backup.
- …

Les raisons pour mettre en place un DRP sont les suivantes :

- pour de simples raisons commerciales, il paraît évident de mettre en place un plan qui protège l'entreprise contre des désastres éventuels.
- Le DRP permet de diminuer la pression qui s'exerce sur les épaules des managers et des employés. (on sait se qu'on doit faire ➔ on est rassuré)
- Certaines entreprises le font pour se protéger contre des pertes dues à un désastre naturel.
- D'autres entreprises le font pour diminuer les risques au niveau légal et juridique.

A noter que les risques de désastres sont autant externes (catastrophe naturelles,…) qu'interne (fautes humaines, problèmes techniques avec les machines, attaques d'employés mal intentionnés,…)

Business Impact Analysis.

Le BIA est une procédure qui permet d'étudier les effets qu'une indisponibilité du SI pourrait avoir sur les différentes fonctions business.

Le BIA se compose des parties suivantes :

1. **le SI downtime :** déterminer la période à partir de laquelle la perte complète du SI deviendrait critique pour l'organisation (dans notre cas le HMO).
2. **Les fonctions critiques :** déterminer quels process sont essentiels pour la continuité du business et qui doivent être rétablit immédiatement.
3. **Les vulnérabilités aux désastres :** identifier les fonctions qui sont vulnérables aux désastres et introduire des mesures de sécurité afin de protéger les composants vitaux.
4. **La liste des priorités :** toutes les fonctions ne nécessitent pas d'être protégées au même niveau. Il faut donc faire une liste des fonctions qui doivent être rétablies après le désastre afin de garantir un retour à un niveau acceptable d'opérabilité.
5. **Principales pertes du business :** identifier les pertes principales dues au désastre telles que le manque à gagner, la perte de clients, la perte de part de marché, l'exposition à des risques légaux,…
6. **Les coûts :** faire une analyse du trade-off coûts-bénéfices afin de déterminer pour chaque activité, lesquelles valent la peine d'être protégées par le DRP.
7. **Les conséquences légales :** déterminer comment une interruption peut résulter en des obligations légales pour l'organisation concernée.
8. **Les « Disasters recovery strategies » :** déterminer les mesures préventives qui doivent être entreprises afin de garantir la protection des assets vitaux pour l'entreprise tels que les softwares, le hardware, les données, les moyens de communication. Les stratégies s'appuient principalement sur la duplication des systèmes, les internal hot sites, cold sites, commercial hot sites, warm sites, mobile cold sites ou encore le « manual processing ». A noter que les trois stratégies les plus souvent utilisées chez les HMO sont les commercial hot sites, le manual processing et la duplication des systèmes.

Testing the DRP

Une fois le BIA mis en place, on va donc définir un DRP qu'il faudra par la suite tester. Tester le DRP veut dire, en réalité, exercer le plan. Ceci permet de garantir la robustesse ainsi que la fiabilité du DRP. Cet exercice doit être effectué au moins une fois par an. De plus le DRP doit être adapté en fonction des besoins, comme par exemple, lors de changements majeurs dans certaines fonctions de l'organisation. Il est accepté par tous qu'un DRP qui n'a pas été testé ne peut pas être considéré comme fiable. En effet, un plan qui n'a pas été testé et mis à jour ne pourra pas protéger l'organisation contre les désastres éventuels. Les tests permettent également de rappeler les procédures aux employés et donc de les rafraîchir. C'est pourquoi, la probabilité d'une bonne mise en œuvre du plan lors d'incidents sera plus grande si le plan a été testé et mise à jour régulièrement.