



FORMATION

LA CONTINUITÉ DES AFFAIRES

Patrick Boucher

CISSP, CISA, CGEIT, ITIL et Auditeur ISO 27001



Gardien Virtuel
s é c u r i t é
i n f o r m a t i q u e

LE 5 MAI 2009

QUI SUIS-JE?



Patrick Boucher :

- Analyste principal chez Gardien Virtuel depuis 2003.
- Expérience en continuité des affaires pour plusieurs clients.
- Certifié CISSP, CISA, CGEIT, ITIL Mise en place/auditeur ISO 27001.



QUI EST GARDIEN VIRTUEL?



- ♦ Entreprise de services-conseils spécialisée dans la sécurité de l'information.
- ♦ Croissance constante depuis sa fondation en 2003.
- ♦ Première entreprise service-conseil certifié ISO27001.
- ♦ Bureau chef situé à Laval.
- ♦ 30 employés



NOTRE MISSION



- ♦ Augmenter la **Confidentialité**, l'**Intégrité** et la **Disponibilité** de vos systèmes d'informations.



OBJECTIFS DE LA PRÉSENTATION



- ♦ Fournir l'information nécessaire pour savoir comment mettre en place un plan de continuité des affaires (PCA).
- ♦ Passer en revue les stratégies de recouvrement.
- ♦ Présenter globalement la mise en place d'un PCA.
- ♦ ***Présentation personnalisée*** : Recherchez-vous quelque chose de particulier?

ORGANISATION DE LA PRÉSENTATION



- ♦ Vous pouvez me poser vos questions à tout moment. Je cherche surtout à échanger avec vous.
- ♦ Une pause est prévue, nous pouvons choisir le moment.
- ♦ SVP, fermez vos téléphones portables.



TABLE DES MATIÈRES



1) Introduction

2) Contexte de la sécurité

3) Phases de développement du PCA

Phase 1 : Politique et gestion du programme de PCA

Phase 2 : Comprendre l'organisation

Phase 3 : Sélectionner les stratégies du PCA

Phase 4 : Développer et mettre en place les mécanismes de réponse aux incidents

Phase 5 : Exercice, maintenance et réévaluation des plans

Phase 6 : Intégrer le PCA dans la culture de l'organisation

4) Pièges à éviter



DÉFINITIONS IMPORTANTES



- ♦ **SÉCURITÉ** : L'absence de risques inacceptables pour l'entreprise.
- ♦ **PCA** : Plan de Continuité des Affaires.
- ♦ **GCA** : Gestion de la Continuité des Affaires.
- ♦ **INTRUSION** : Accès non autorisé à un système d'information.
- ♦ **DÉSASTRE** : Destruction partielle ou complète d'un ensemble de système.
- ♦ **VULNÉRABILITÉ** : Faiblesse d'un système pouvant être exploitée.
- ♦ **CONTRÔLE** : Mesure prise pour diminuer une vulnérabilité.
- ♦ **INGÉNIERIE SOCIALE** : Obtenir de l'information confidentielle sans moyens techniques (ex : Facebook, MySpace etc.).



DÉFINITIONS IMPORTANTES (2/3)



BCP – « Business Continuity Planning » Représente une panne qui à un impact sur UN seul secteur d'activités (finance, distribution, opération, informatique)

DRP - « Disaster Recovery Planning » est le plan pour une reprise complète après une destruction majeure des équipements et infrastructure de l'entreprise.

Stratégie de recouvrement - Méthode choisie pour reconstruire ou continuer les opérations.

Sécurité normale – Redondance, copies de sauvegarde, formation, sensibilisation, coupe-feu

(Ce que nous avons tous n'est-ce pas? :-)



DÉFINITIONS IMPORTANTES (3/3)

Plan de continuité...de quoi ??

- Des affaires – chaque ligne d'affaire
- Des opérations – construction, traitement
- De service – livraison, prise de commande, finance
- De l'informatique – reprise des systèmes informatiques
- De l'entreprise – relève financière, de président etc.

INTRODUCTION

Avantage pour l'organisation

Plusieurs objectifs motive la mise en place d'un PCA:

- S'assurer que la réponse à une crise sera **coordonnée** et **organisée**.
- Répondre à une **exigence** réglementaire.
- Réviser les **processus d'affaires** et démontrer des faiblesses ou l'inefficacité de certains processus de l'organisation.
- Diminuer les **primes** d'assurances.
- Générer du matériel de **formation** pour les employés.
- Déterminer les actifs critiques et en assurer la **protection adéquate**.
- **Rentabiliser** et **orienter** le plus possible les efforts et les moyens déployés par une évaluation préalable des impacts.

INTRODUCTION

Avantage pour l'organisation – prise 2

Plusieurs objectifs motive la mise en place d'un PCA:

- ♦ Simplement documenter, peut-être pour la première fois les actifs de l'entreprise...
 - ♦ Avoir la liste, leur nom, emplacement
 - ♦ La valeur des actifs, qui les utilise...
 - ♦ Permet une bonne prise de décisions avec la bonne information.

QUELQUES CHIFFRES



Des raisons pour avoir un PCA corporatif solide :

- ♦ 2 entreprises sur 5 qui subissent un désastre devront fermer leurs portes. - *Gartner 2001*
- ♦ 50% des entreprises qui ont perdu leurs données ferment leurs portes, et 90% des restantes vont fermer dans les 2 ans suivant la perte. - *U. Texas centre pour la recherche des systèmes d'information.*
- ♦ 60% des moyennes et grandes entreprises vont faire l'expérience chaque année d'une panne imprévue d'une durée de 1 à 24 heures. - *Veritas/EMEA 2003*



ÉTAPES D'UN INCIDENT À HAUT NIVEAU



- 1) **Un désastre se produit** : Un désastre est une interruption qui affecte les opérations d'une organisation.
- 2) **Réponse d'urgence** : Assurer la sécurité des gens, prévenir de dommages supplémentaires et activer l'équipe de réponses aux incidents.
- 3) **Évaluation des dommages** : Dresser un portrait de la situation (ex: qui est affecté?) puis décider si oui ou non il y a activation du plan de continuité et dans quelle mesure.
- 4) **Recouvrement** : Reprise des activités au site de relève (en suivant les procédures de recouvrement) et remise en état du site primaire.
- 5) **Retour à la normale** : Déterminer si l'urgence (le désastre) est bien terminée, et retour des opérations au site principal.



CONTEXTE

Normes couvertes

- ♦ Normes présentées lors de cette formation
 - ♦ ISO 27002 (Bonnes pratiques)
 - ♦ BS 25999-1 (Grandes entreprises)
 - ♦ NIST 800-34 (Gouvernementale)

UN PLAN POUR NE PAS S'EN SERVIR



Aucune entreprise ne souhaite vivre un incident.

Très difficile de se préparer pour tous les scénarios

Par contre, grande probabilité qu'il pleuve!

Difficile pour les employés de créer un plan... dont l'objectif avoué, c'est d'être *tabletté*!

PIÈGES À ÉVITER



- ♦ Se fier SEULEMENT au plan;
- ♦ Mal définir les objectifs;
- ♦ Ne pas définir les priorités;
- ♦ Ne pas faire de mises à jour des plans;
- ♦ Ne pas impliquer tous les joueurs concernés;
- ♦ Faire compliqué!
- ♦ Ne pas utiliser ce qui existe;
- ♦ Oublier de communiquer les changements ou le plan en totalité;
- ♦ Ne pas avoir l'approbation de la haute direction!!!



LEÇONS APPRISES



- 1) **Différents désastres = Plans différents** : Il est donc important de faire une distinction entre les types de désastre (Ex. un feu versus une attaque informatique).
- 2) **Ne pas oublier de tester « à fond »** : Sans tests, impossible d'être certain que ça fonctionne. Par exemple, si un produit utilisé n'offrait pas le « hot-swap »?
- 3) **Reprendre des sauvegardes** : Ne pas juste les tester, mais les utiliser. Une personne a perdu un fichier, voilà une belle occasion de tester les copies de sauvegarde.
- 4) **Être préparé pour le pire** : Un rat qui ronge les câbles, des attaques terroristes, un refoulement d'égout, un toit enneigé, une grève, etc.



QUELQUES RÉFÉRENCES



- NIST Contingency plan - <http://csrc.nist.gov/publications/nistpubs/>
- MIT Business continuity plan - <http://web.mit.edu/security/www/pubplan.htm>
- Computer emergency Response team - <http://www.cert.org>
- Contingency Planning & management - <http://www.contingencyplanning.com>
- Federal Emergency Management Agency (FEMA) - <http://www.fema.gov>
- Disaster Recovery Journal - <http://www.drj.com>
- NFPA 1600 - <http://www.nfpa.org/Home/AboutNFPA/index.asp>





CONCLUSION – QUESTIONS?

Savez vous comment faire un plan de continuité maintenant?

C'est maintenant de faire la révision de la matière et de faire la lumière sur les zones grise que vous pouvez avoir!

Questions?



MERCI!



Gardien Virtuel

s é c u r i t é
i n f o r m a t i q u e

3185, rue Delaunay
Laval, Québec, H7L 5A4
Téléphone : (514) 907-5107
Télécopieur : (450) 680-1928
Sans frais : 1-888-377-7890
Courriel : info@gardienvirtuel.com

