DISASTER RECOVERY: ΜΕΘΟΔΟΙ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΓΙΑ ΑΝΑΚΑΜΨΗ ΑΠΟ ΚΑΤΑΣΤΡΟΦΗ

METHODS &TECHNOLOGIES USED IN DISASTER RECOVERY PLANNING

Όνομα: Δερμεντζή Ελένη

ΑΜ:7/11

Ιανουάριος 2012

Πανεπιστήμιο Μακεδονίας **University of Macedonia**

ΔΠΜΣ Πληροφοριακά Συστήματα **Master Information Systems**

Δίκτυα Υπολογιστών **Computer Networks**

Καθηγητής: Α.Α. Οικονομίδης **Professor: A.A. Economides**

Abstract

Disasters, either natural or man-made, may cause pause of business' processes or even the shutdown of a business. This paper examines the methods and the technologies that are used in order to reassure that a company is able to survive from potential disasters and return to normal operation as soon as possible. The first part of the paper presents a bibliographic review of Disaster Recovery's methodology and the second, the technologies that could be used in order to make Disaster Recovery Planning more effective. As a conclusion, it is deduced that with the utilization of new technologies, such as virtualization and cloud computing, a business can be prepared against a disaster, even with low cost.

Περίληψη

Οι καταστροφές, είτε οφείλονται σε φυσικά φαινόμενα, είτε σε ανθρώπινες ενέργειες, μπορούν να προκαλέσουν την προσωρινή αναστολή των λειτουργιών μιας επιχείρησης, ακόμα και την οριστική διακοπή της λειτουργίας της. Στην παρούσα εργασία, εξετάζονται οι μέθοδοι και οι τεχνολογίες που χρησιμοποιούνται ώστε να μπορέσει η επιχείρηση να αντιμετωπίσει πιθανές καταστροφές και να ανακάμψει το συντομότερο δυνατό. Αρχικά, παρουσιάζεται η σχετική μεθοδολογία που συναντάται στη βιβλιογραφία και στη συνέχεια γίνεται αναφορά στις τεχνολογίες που μπορούν να χρησιμοποιηθούν, ώστε ο σχεδιασμός της ανάκαμψης από καταστροφή (Disaster Recovery Planning) να γίνει αποδοτικότερος. Το συμπέρασμα της εργασίας είναι ότι με την αξιοποίηση των σύγχρονων τεχνολογιών (virtualization, cloud computing), μια επιχείρηση μπορεί να θωρακισθεί από τις δυσάρεστες συνέπειες μιας καταστροφής, ακόμα και με χαμηλό κόστος.

Εισαγωγή- Παρουσίαση Θέματος

Η ανάπτυξη σχεδίου επανάκαμψης των λειτουργιών μιας επιχείρησης μετά από καταστροφή, είναι απαραίτητη για κάθε οργανισμό. Καταστροφές μπορούν να συμβούν ανά πάσα στιγμή και συνήθως χωρίς καμία προειδοποίηση. Ως καταστροφή ορίζεται οποιοδήποτε γεγονός προκαλεί διακοπή κάποιας υπηρεσίας ή αδυναμία συνεχούς λειτουργίας κάποιου τμήματος, ζωτικής σημασίας για τον οργανισμό, για απροσδιόριστο χρονικό διάστημα (Al-Khabbaz et al., 2011). Οι καταστροφές διακρίνονται σε αυτές που προκαλούνται από ανθρώπινη παρεμβολή (είτε πρόκειται για λάθη, είτε για κακόβουλες ενέργειες), όπως είναι οι βλάβες στον εξοπλισμό από λανθασμένη χρήση, βλάβες στις τηλεπικοινωνίες, πυρκαγιές, τρομοκρατικές ενέργειες κτλ, και σε φυσικές καταστροφές (για παράδειγμα, πλημμύρες, σεισμοί, τυφώνες κ.α.) (EC-Council, 2011a).

Σχετικά με τις επιπτώσεις που μπορούν να έχουν αυτές οι καταστροφές στην επιχείρηση ή στον οργανισμό, τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα, τα στοιχεία είναι ξεκάθαρα. Σύμφωνα με έρευνα του «London Chamber of Commerce», το 90% των επιχειρήσεων που έχασε δεδομένα εξαιτίας κάποιας καταστροφής, αναγκάστηκε να κλείσει μέσα στα επόμενα 2 χρόνια, ενώ το 43% των οργανισμών που αντιμετώπισε κάποια καταστροφή δεν κατάφερε να επανακάμψει ποτέ («Business Continuity- is it expensive and hard?», 2006). Παρόμοια είναι τα αποτελέσματα άλλης έρευνας, σύμφωνα με την οποία το 40% των επιχειρήσεων που επηρεάστηκε από κάποια μεγάλη καταστροφή, δεν επαναλειτούργησε ποτέ, ενώ 6 στις 10 επιχειρήσεις θα αποτύχουν αν παραμείνουν κλειστές για 2 χρόνια (Duncan, Yeager, Rucks, Ginter, 2011).

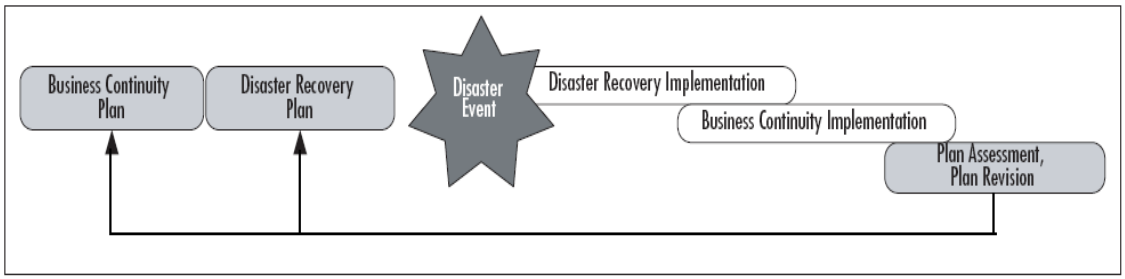
Σε απάντηση των παραπάνω, αναπτύχθηκαν οι διάφορες τεχνικές που ανήκουν στη Διαχείριση Επιχειρησιακής Συνέχειας (Business Continuity Management – BCM), η οποία αποτελεί εξέλιξη του Σχεδιασμού Επιχειρησιακής Συνέχειας (Business Continuity Planning) και του Σχεδιασμού Ανάκαμψης από Καταστροφές (Disaster Recovery Planning), που εμφανίστηκε πρώτη φορά στα μέσα της δεκαετίας του ’70 (Herbane, 2010). Στη βιβλιογραφία, οι έννοιες «Disaster Recovery» και «Business Continuity» πολλές φορές συνθέτουν από κοινού τον όρο «Business Resiliency Planning», ο οποίος θεωρείται συνώνυμος του όρου «Business Continuity Management» (Peterson, 2009). Σύμφωνα με μία άλλη άποψη, ο όρος «Disaster Recovery» συνήθως αναφέρεται σε συστήματα IT (Information Technology) και πρόκειται για τη διαδικασία που λαμβάνει χώρα **κατά τη διάρκεια** και **μετά** την καταστροφή, ενώ ο όρος του «Business Continuity Planning» χρησιμοποιείται για να περιγράψει τη διαδικασία που έχει ως στόχο να διασφαλίσει ότι ο οργανισμός θα επιβιώσει μετά από μια καταστροφή και λαμβάνει χώρα **πριν** συμβεί η καταστροφή (Stanton, 2005; Cervone, 2006). Το σίγουρο είναι ότι οι δύο όροι παρουσιάζουν πολλές ομοιότητες και περιέχουν ενέργειες και έννοιες που συναντώνται και στις δύο περιπτώσεις ή αλληλοσυμπληρώνονται.

Βασικοί ορισμοί και έννοιες

Πριν δοθεί ο ορισμός του όρου «Disaster Recovery», κρίνεται σκόπιμο να οριστεί η έννοια του Σχεδιασμού Επιχειρησιακής Συνέχειας, αφού όπως ειπώθηκε οι δύο έννοιες είναι αλληλένδετες.

Ο Σχεδιασμός Επιχειρησιακής Συνέχειας (Business Continuity Planning – BCP) είναι η μεθοδολογία που χρησιμοποιείται για τη δημιουργία ενός σχεδίου για τη διατήρηση της συνέχειας των λειτουργιών της επιχείρησης, πριν, κατά τη διάρκεια και μετά από μια καταστροφή.

Η Ανάκαμψη από Καταστροφή (Disaster Recovery) είναι υποσύνολο της Επιχειρησιακής Συνέχειας και έχει ως στόχο την άμεση αντιμετώπιση ενός γεγονότος. Περιλαμβάνει την προσπάθεια εξάλειψης των αρνητικών συνεπειών μιας καταστροφής το συντομότερο δυνατό και τη διερεύνηση του άμεσου αντίκτυπου που έχει αυτή στον οργανισμό (Snedaker, 2007, p 4). Όπως φαίνεται στο παρακάτω σχήμα, από ένα σημείο και μετά οι διαδικασίες του «Disaster Recovery» και του «Business Continuity Planning» αλληλεπικαλύπτονται:



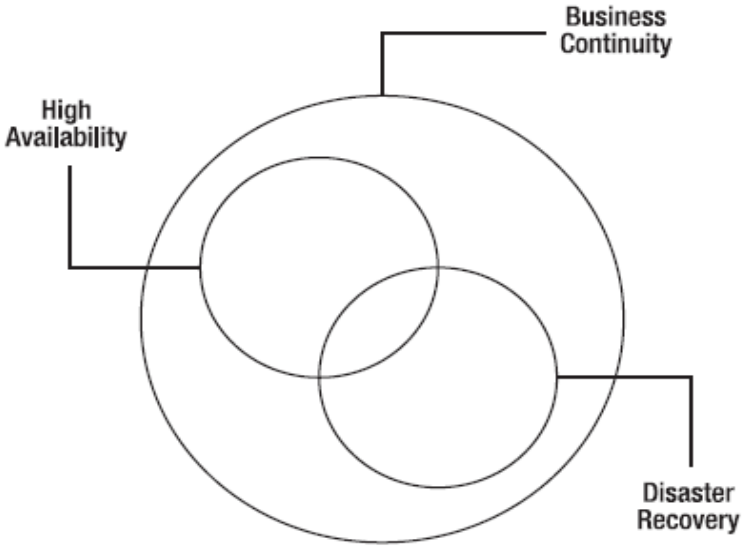
Σχήμα 1:Business Continuity and Disaster Recovery Planning, Implementation, and Revision Cycle(Snedaker, 2007, p5).

Μία άλλη έννοια που συναντάται στη βιβλιογραφία, είναι αυτή της Υψηλής/Συνεχούς Διαθεσιμότητας (High Availability/ Continuous Availability). Θεωρείται επίσης υποσύνολο της Επιχειρησιακής Συνέχειας (Business Continuity) και πρόκειται για τη διαδικασία που διασφαλίζει ότι οι πόροι της Πληροφοριακής Τεχνολογίας (Information Technology) παραμένουν διαθέσιμοι για όσο μεγαλύτερο χρονικό διάστημα γίνεται, ανεξάρτητα από την αιτία της διακοπής της λειτουργίας τους (Luetkehoelter, 2008, p 3; Rittinghouse &Ransome, 2005, p2).

Η σχέση των τριών παραπάνω εννοιών φαίνεται στο Σχήμα 2.

Τα βασικά βήματα του Σχεδιασμού Ανάκαμψης από Καταστροφή/ Επιχειρησιακής Συνέχειας

Παρ' όλο που παρουσιάζονται διάφορες παραλλαγές της λίστας με τα βήματα του «Disaster Recovery Planning» και «Business Continuity Planning», τα παρακάτω



Σχήμα 2: «The relationship between business continuity, high availability, and disaster recovery» (Luetkehoelter,2008, p3).

σημεία είναι κοινά και μπορούν να θεωρηθούν ως βασικά βήματα ενός τέτοιου σχεδιασμού (EC-Council, 2011a; Snedaker, 2007; Cousins, 2007):

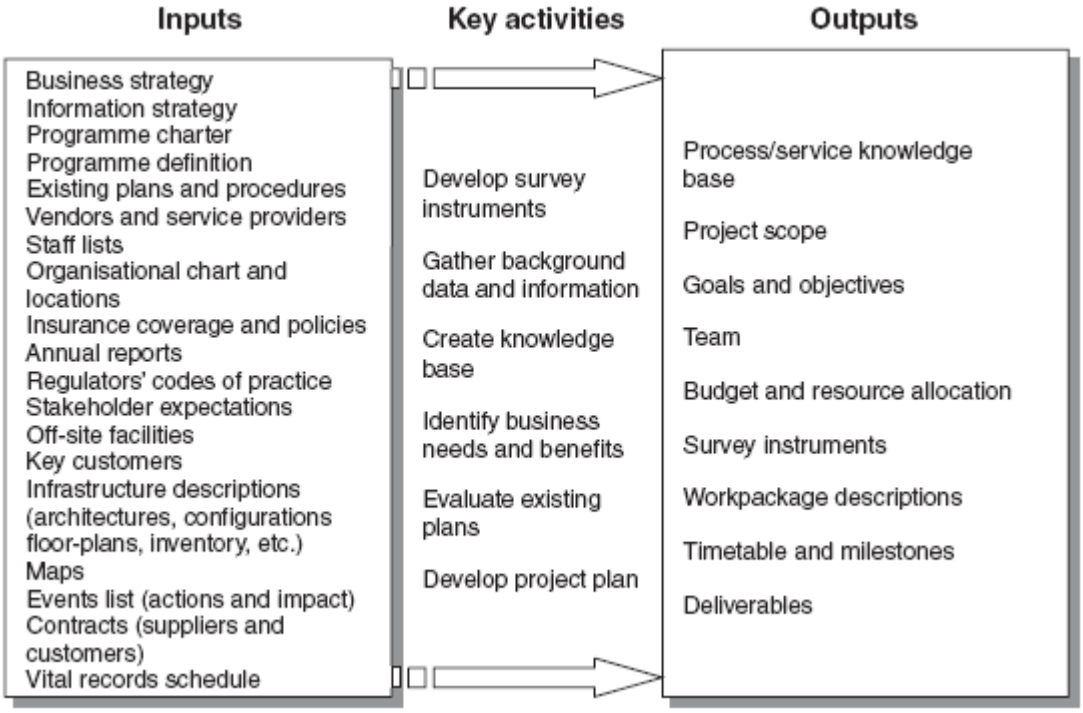
- Έναρξη του project/ καθορισμός των στόχων και του περιεχομένου.
- Αξιολόγηση του κινδύνου (Risk assessment).
- «Ανάλυση BIA» (Business Impact Analysis).
- Ανάπτυξη Στρατηγικών/Λύσεων και Διαχείριση Κινδύνου.
- Ανάπτυξη του σχεδίου.
- Εκπαίδευση, δοκιμή, έλεγχος του σχεδίου.
- Ενημέρωση/ διατήρηση του σχεδίου.

Κατά την έναρξη του project, αναπτύσσονται εργαλεία έρευνας και συλλέγονται δεδομένα και πληροφορίες της επιχείρησης που θα χρησιμοποιηθούν για τον καθορισμό των στόχων του project (Σχήμα 3).

Στο στάδιο της αξιολόγησης του κινδύνου, εντοπίζονται οι πόροι, οι αδυναμίες του οργανισμού, καθώς και οι απειλές και οι κίνδυνοι που αντιμετωπίζει (Σχήμα 4), ενώ ακολουθεί η «Ανάλυση BIA» (Business Impact Analysis), η οποία είναι η διαδικασία αναγνώρισης των κρίσιμων λειτουργιών της επιχείρησης, όπως επίσης και των επιπτώσεων που θα υπάρξουν αν αυτές δεν είναι διαθέσιμες.

Παρ' όλο που τα δύο παραπάνω βήματα μπορεί να μοιάζουν πανομοιότυπα, δεν θα πρέπει να συγχέονται. Η Αξιολόγηση του Κινδύνου (Risk assessment) αφορά τον προσδιορισμό των πιθανών ζημιών που μπορεί να προκαλέσει μια απειλή σε σύγκριση με το κόστος των προληπτικών μέτρων που μπορούν να παρθούν για την αντιμετώπισή της. Πρόκειται ουσιαστικά για τον προσδιορισμό του ποσού που πρέπει να επενδυθεί για πρόληψη και προστασία. Η «Ανάλυση BIA» από την άλλη, εκφράζει τις ανάγκες του οργανισμού και διερευνά τον αντίκτυπο που θα είχε στην επιχείρηση, η μη

ανάκαμψη των κρίσιμων λειτουργιών της, σε εύλογο χρονικό διάστημα (Rittinghouse & Ransome, 2005, p 70).

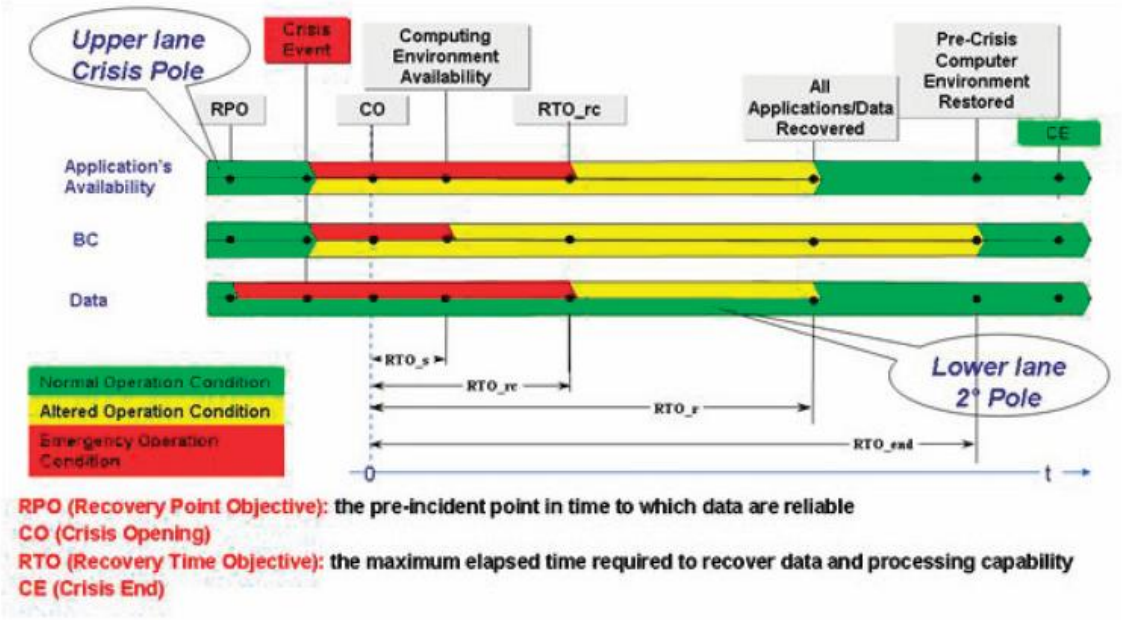


Σχήμα 3: «Project initiation» (Gibb & Buchanan, 2006, p 131).

Σχήμα 4: «Key elements in a risk assessment» (Lingeswara Tammineedi, 2010, p 41).

Τα αποτελέσματα μιας «Ανάλυσης BIA» παρέχουν μεταξύ άλλων (McDonald, 2008):

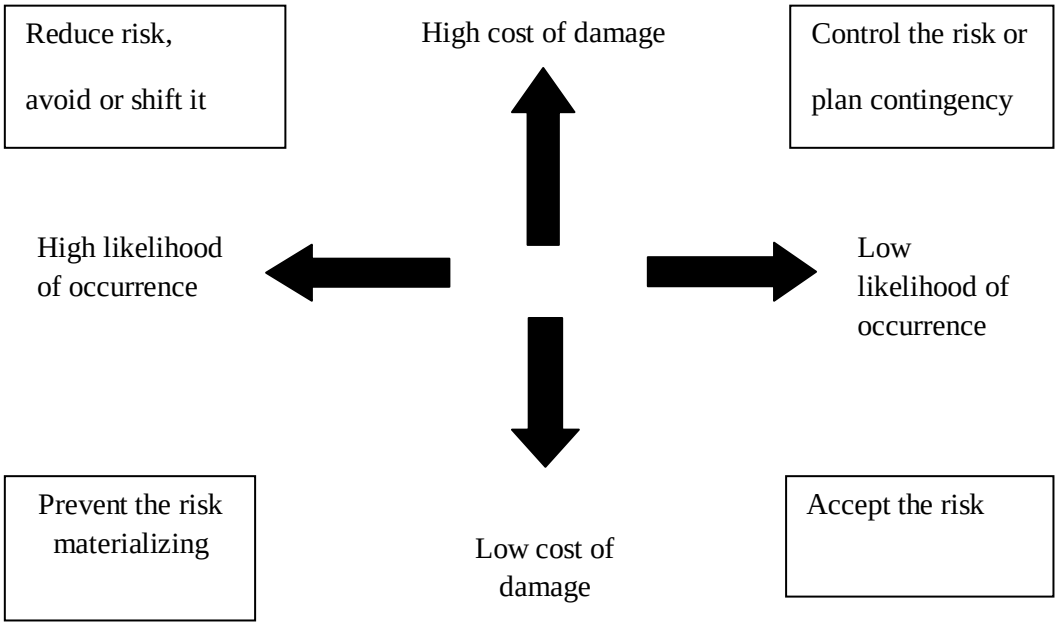
- Δεδομένα για την ταξινόμηση των λειτουργιών του οργανισμού ως προς την κρισιμότητά τους.
- Δεδομένα που μπορούν να χρησιμοποιηθούν στη διαμόρφωση στρατηγικών ανάκαμψης.
- Δεδομένα που μπορούν να χρησιμοποιηθούν στον Σχεδιασμό Διαχείρισης Κινδύνου (Risk Management Planning).
- Δεδομένα για τη διαμόρφωση RTO (Recovery Time Objectives) και RPO (Recovery Point Objectives).



Σχήμα 5: «RPO &RTO» (Arduini& Morabito, 2010, p 124).

RTO (Recovery Time Objectives) (Σχήμα 5) ονομάζονται οι μετρήσιμοι στόχοι που βάζει ο οργανισμός όσον αφορά το χρονικό διάστημα που μεσολαβεί ανάμεσα στη διακοπή και στην επαναφορά μιας λειτουργίας. Ορίζονται σε ώρες και λεπτά και είναι διαφορετικοί για κάθε λειτουργία.

RPO (Recovery Point Objectives) είναι επίσης στόχοι που μετρούνται σε μονάδες χρόνου, αλλά αναφέρονται στο πόσο πρόσφατα πρέπει να είναι τα δεδομένα που απαιτούνται για την επαναφορά μιας λειτουργίας μετά από μια διακοπή. Για παράδειγμα, για έναν οργανισμό μπορεί να είναι αναγκαίο να δημιουργούνται αντίγραφα ασφαλείας κάθε 24 ώρες και να είναι ανεκτή η απώλεια κάποιων δεδομένων, ενώ για κάποιον άλλο, όπου RPO=0, να απαιτείται η συνεχής ενημέρωση των back-up αρχείων (Liotine, 2003, p32).



Σχήμα 6: «Risk Management»(Dey, 2011, p 231).

Μετά το πέρας της «Ανάλυσης BIA», ακολουθεί η Διαχείριση του Κινδύνου (Risk Management) των πιθανών απειλών (Σχήμα 6), όπου συνυπολογίζονται τόσο η πιθανότητα να πραγματοποιηθεί η απειλή, όσο και ο αντίκτυπος που μπορεί να έχει στην επιχείρηση καθώς και τα σχετικά κόστη που συνεπάγονται. Στην περίπτωση που ο αντίκτυπος είναι μικρός και η πιθανότητα να πραγματοποιηθεί η απειλή είναι μικρή, ο οργανισμός μπορεί να δεχτεί την παρούσα κατάσταση και να μην λάβει περαιτέρω μέτρα (accept the risk). Από την άλλη, αν το κόστος που μπορεί να επιφέρει ένας επικείμενος κίνδυνος είναι υψηλό, χρησιμοποιούνται επιπλέον μέσα ελέγχου σε συνδυασμό με τα σχέδια Επιχειρησιακής Συνέχειας (control the risk/risk limitation). Υψηλό κόστος και μεγάλη πιθανότητα εμφάνισης του κινδύνου, οδηγούν σε στρατηγικές μείωσης ή μεταφοράς του (mitigation strategies). Αποτέλεσμα μιας τέτοιας στρατηγικής αποτελεί η ασφαλιστική κάλυψη της επιχείρησης. Τέλος, αν είναι σχεδόν σίγουρο ότι πρόκειται να συμβεί η απειλή και ο αντίκτυπος θα είναι σχετικά μικρός, μπορούν να παρθούν τα απαραίτητα προληπτικά μέτρα για να αποφευχθεί εντελώς ο κίνδυνος (prevent the risk/risk avoidance) (Rittinghouse& Ransome, 2005; Dey, 2011; Oberg et al., 2011).

Επόμενο βήμα είναι η Ανάπτυξη του Σχεδίου, κατά την οποία τα αποτελέσματα όλων των παραπάνω βημάτων χρησιμοποιούνται για τη σύνταξη του εγγράφου, όπου αναφέρονται ποιες ενέργειες θα πραγματοποιηθούν την ώρα και το χρονικό διάστημα που έπεται της καταστροφής, ποιες είναι οι αρμοδιότητες του κάθε εμπλεκόμενου και πως θα διεξάγεται η επικοινωνία μεταξύ αυτών (Peterson,2009; Lingeswara Tammineedi, 2010).

Σημαντικός είναι και ο έλεγχος του σχεδίου καθώς και η ενημέρωσή του μετά από κάποιο χρονικό διάστημα ώστε να είναι σίγουρο ότι το σχέδιο συμπεριλαμβάνει τις

αλλαγές που μπορεί να έχουν επέλθει στον οργανισμό και ότι εξακολουθεί να είναι εφαρμόσιμο. Η αναθεώρηση του σχεδίου θα πρέπει να γίνεται τουλάχιστον μία φορά το χρόνο (Peterson,2009; Gibb &Buchanan, 2006).

Συστήματα για back up και ανάκαμψη από καταστροφές.

Alternate sites

Η δημιουργία αντιγράφων ασφαλείας είναι απαραίτητη ενέργεια προκειμένου να είναι εφικτή η ανάκαμψη του οργανισμού μετά από μια καταστροφή. Χρήσιμο είναι αυτά τα αντίγραφα να φυλάσσονται σε διαφορετική τοποθεσία από αυτή του οργανισμού. Για την επιλογή της κατάλληλης τοποθεσίας θα πρέπει να ληφθούν υπόψη (Fulmer, 2005; EC-Council, 2011a, p4-13):

- Η γεωγραφική περιοχή (θα πρέπει να είναι σε ασφαλή απόσταση από τις εγκαταστάσεις του οργανισμού, ώστε σε περίπτωση καταστροφής να είναι ασφαλή τα δεδομένα).
- Προσβασιμότητα (πόσο γρήγορα μπορούν να ανακτηθούν τα δεδομένα από την απομακρυσμένη περιοχή).
- Ασφάλεια
- Συνθήκες του περιβάλλοντος (θερμοκρασία, υγρασία, ανιχνευτές πυρκαγιάς κτλ)
- Κόστος

Επιπλέον, η επιχείρηση θα χρειαστεί προσωρινές εγκαταστάσεις μέχρι να μπορέσει να ανακάμψει πλήρως από την καταστροφή. Οι «εναλλακτικές» αυτές τοποθεσίες (alternate sites) διακρίνονται σε (Liotine, 2003, p 360-363; Rittinghouse &Ransome, 2005, p 91-92):

- Hot sites- Πρόκειται για εγκαταστάσεις στις οποίες μπορεί να εργαστεί το προσωπικό της επιχείρησης αμέσως μετά την καταστροφή, χωρίς καθυστέρηση και είναι πλήρως εξοπλισμένες με όλα τα απαραίτητα μέσα για την ανάκαμψη της επιχείρησης.
- Cold sites – Είναι εγκαταστάσεις που είναι κατάλληλες για να μεταφερθούν προσωρινά οι λειτουργίες της επιχείρησης, αλλά δεν είναι εξοπλισμένες. Είναι εφοδιασμένες με τηλεφωνική σύνδεση, παροχή ρεύματος κτλ και είναι έτοιμες για να μεταφερθεί ο εξοπλισμός της επιχείρησης. Μπορούν να γίνουν πλήρως λειτουργικές σε σχετικά μικρό χρονικό διάστημα.
- Warm sites – Είναι μερικώς εξοπλισμένα Hot sites.
- Mobile sites- Είναι κινητές εγκαταστάσεις, που μπορούν να τοποθετηθούν κοντά στις εγκαταστάσεις της επιχείρησης ώστε να εξοικονομηθεί χρόνος μεταφοράς του προσωπικού.

- Mirrored sites – Πρόκειται για πανομοιότυπες εγκαταστάσεις- κλώνους των βασικών εγκαταστάσεων της επιχείρησης (ουσιαστικά πλεονάζουσες εγκαταστάσεις της επιχείρησης), και προφανώς είναι η επιλογή που κοστίζει πιο ακριβά.

Επιλογές αποθήκευσης

Raid (redundant array of independent disks).

«Raid» ονομάζεται ένας τύπος εικονικού (virtual) σκληρού δίσκου που αποτελείται από 2 ή περισσότερους σκληρούς δίσκους. Η βασική ιδέα είναι ότι με το να συνδυαστούν πολλοί μικροί δίσκοι χαμηλού κόστους μπορεί να επιτευχθούν καλύτερες επιδόσεις από ότι αν χρησιμοποιούνταν ένας μοναδικός δίσκος υψηλού κόστους (EC-Council, 2011a, p 123; Rittinghouse &Ransome, 2005 p138).

Electronic Vaulting

«Electronic vaulting» ονομάζεται η διαδικασία με την οποία μεταδίδονται μέσω δικτύου τα αντίγραφα ασφαλείας των δεδομένων σε μία απομακρυσμένη τοποθεσία. Με αυτόν τον τρόπο τα δεδομένα μεταφέρονται και ανακτώνται πολύ πιο γρήγορα απ' ότι με το φυσικό τρόπο (Snedaker, 2007, p 285).

NAS (Network Attached Storage)

Πρόκειται για ευφυείς συσκευές αποθήκευσης οι οποίες συνδέονται με δίκτυα και παρέχουν πρόσβαση σε αρχεία, είτε σε υπολογιστές είτε σε διακομιστές βάσεων δεδομένων (database servers) (Σχήμα 7). Χρησιμοποιούν πρωτόκολλα πρόσβασης αρχείων (file access protocols), όπως είναι τα πρωτόκολλα CIFS και NFS (Barker& Massiglia, 2002, p18).

SAN (Storage Area Network)

Με τον όρο «SAN» (Σχήμα 8) νοείται οποιοδήποτε δίκτυο υψηλών επιδόσεων έχει ως βασικό στόχο να καταστήσει δυνατή την επικοινωνία των συσκευών αποθήκευσης με συστήματα υπολογιστών και μεταξύ τους (Barker& Massiglia, 2002, p34). Ένα δίκτυο αυτού του είδους υποστηρίζει αποθήκευση και ανάκτηση δεδομένων για επιχειρησιακά δίκτυα μέσω διακομιστών, πολλαπλών RAID, και τεχνολογίας διασύνδεσης καναλιού οπτικών ινών (Fibre Channel).

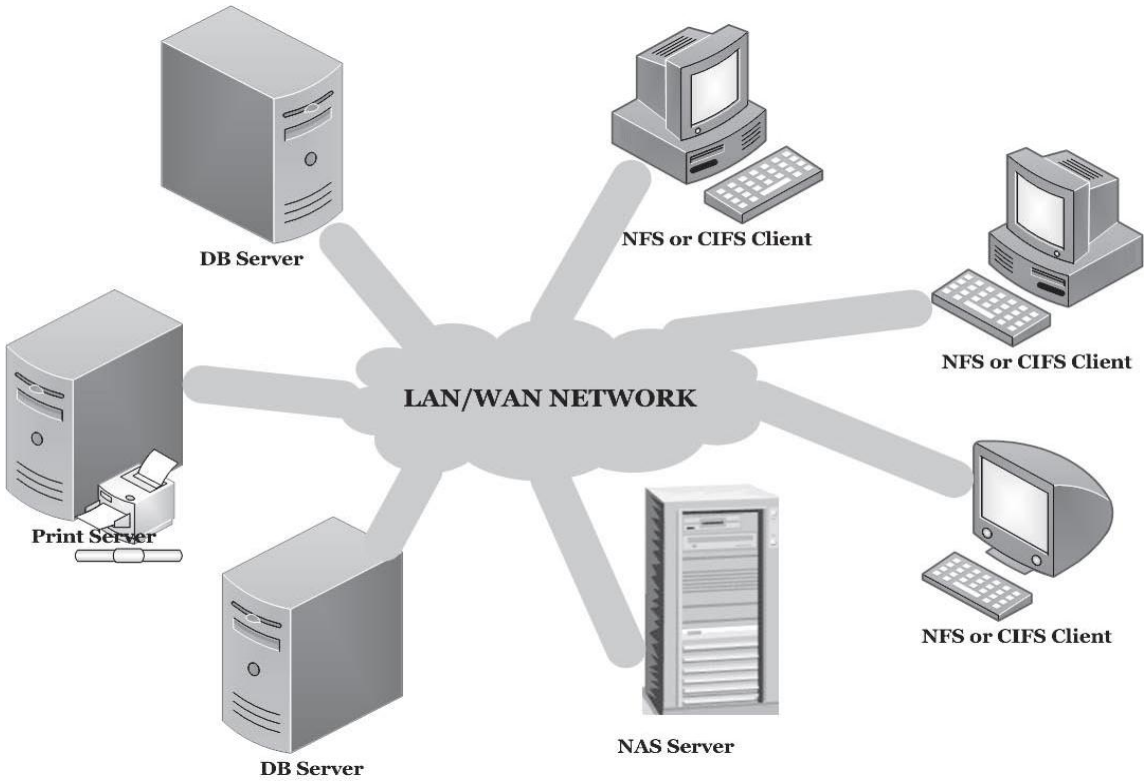
Τα πλεονεκτήματα και μειονεκτήματα της χρήσης ενός δικτύου SAN είναι (EC-Council, 2011a, p202):

Πλεονεκτήματα

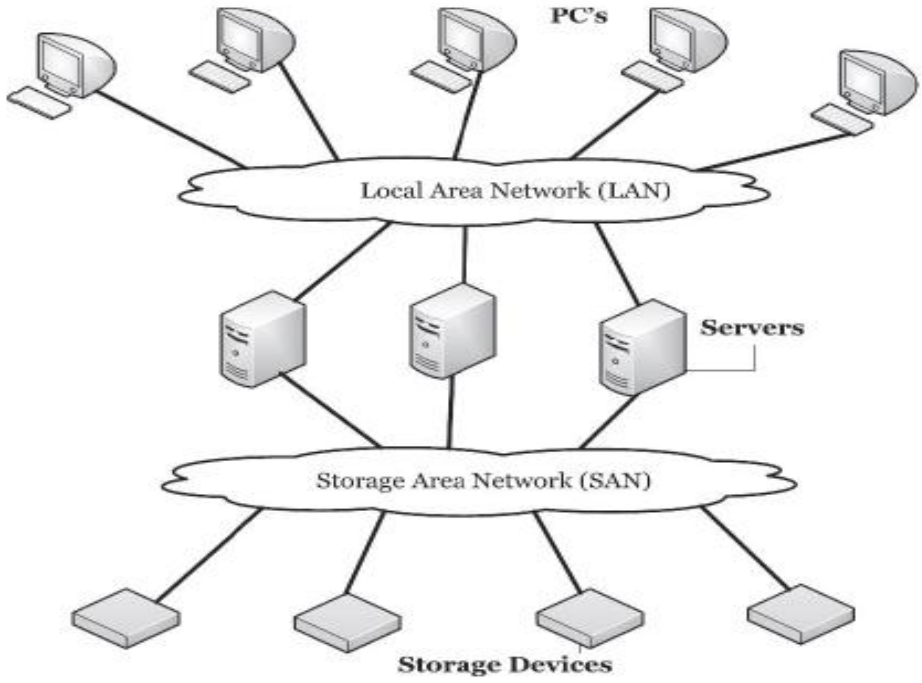
- Αποδοτικότερη χρήση των δίσκων (disk utilization).
- Γρήγορη και εκτενής ανάκαμψη από την καταστροφή.
- Αύξηση της διαθεσιμότητας των εφαρμογών.
- Η δημιουργία αντιγράφων μεγάλης ποσότητας δεδομένων γίνεται πιο γρήγορα.

Μειονεκτήματα

- Η εγκατάσταση ενός δικτύου SAN είναι ακριβή.



Σχήμα 7: «All of these clients can access the NAS server» (EC-Council, 2011a, p 184).



Σχήμα 8: «A Storage area network (SAN) links storage devices to other parts of the network» (EC-Council, 2011a, p196).

- Το κόστος διαχείρισης αυξάνεται.
- Δεν είναι πρακτική λύση αν χρησιμοποιείται για μία μόνο εφαρμογή.
- Απαιτείται γρήγορη WAN σύνδεση, η οποία μπορεί να είναι ακριβή.

Οι διαφορές μεταξύ NAS και SAN είναι (Liotine,2003, p 269):

- Στην περίπτωση του συστήματος NAS, η συσκευή αποθήκευσης είναι προσβάσιμη μέσω του δικτύου LAN. Αντίθετα στην περίπτωση του SAN, χρησιμοποιείται ένα δίκτυο αφιερωμένο αποκλειστικά για την επικοινωνία μεταξύ των διακομιστών και των συσκευών αποθήκευσης (Σχήματα 7& 8).
- Σε ένα σύστημα NAS, τα δεδομένα μεταφέρονται σε πακέτα με τις ταχύτητες που ισχύουν σε ένα δίκτυο LAN, ενώ σε ένα SAN τα δεδομένα μεταφέρονται σε μπλοκ με τις ταχύτητες ενός καναλιού οπτικών ινών (Fibre Channel).
- Ένα NAS παρέχει υψηλών επιδόσεων διαμοιραζόμενη πρόσβαση σε ένα σύστημα αρχείων, από έναν αριθμό διαφορετικών πελατών (clients) περιορισμένων δυνατοτήτων ως προς το όγκο των δεδομένων που μπορούν να διαχειριστούν. Τα δίκτυα SAN από την άλλη, είναι σχεδιασμένα για εφαρμογές που απαιτούν την μεταφορά μεγάλων ποσοτήτων δεδομένων, όπως είναι η δημιουργία αντιγράφων ασφαλείας (back up), η ανάκτηση μεγάλης ποσότητας δεδομένων κτλ.
- Τα SAN χρησιμοποιούν κανάλια οπτικών ινών (Fibre Channel) και προσφέρουν τουλάχιστον τρεις φορές μεγαλύτερη απόδοση από τα NAS. Επιπλέον, το «data throughput» μένει ανεπηρέαστο από την συμφόρηση του δικτύου (LAN), κάτι το οποίο δεν ισχύει για τα NAS.

Τάσεις και σύγχρονες τεχνολογίες

Virtualization

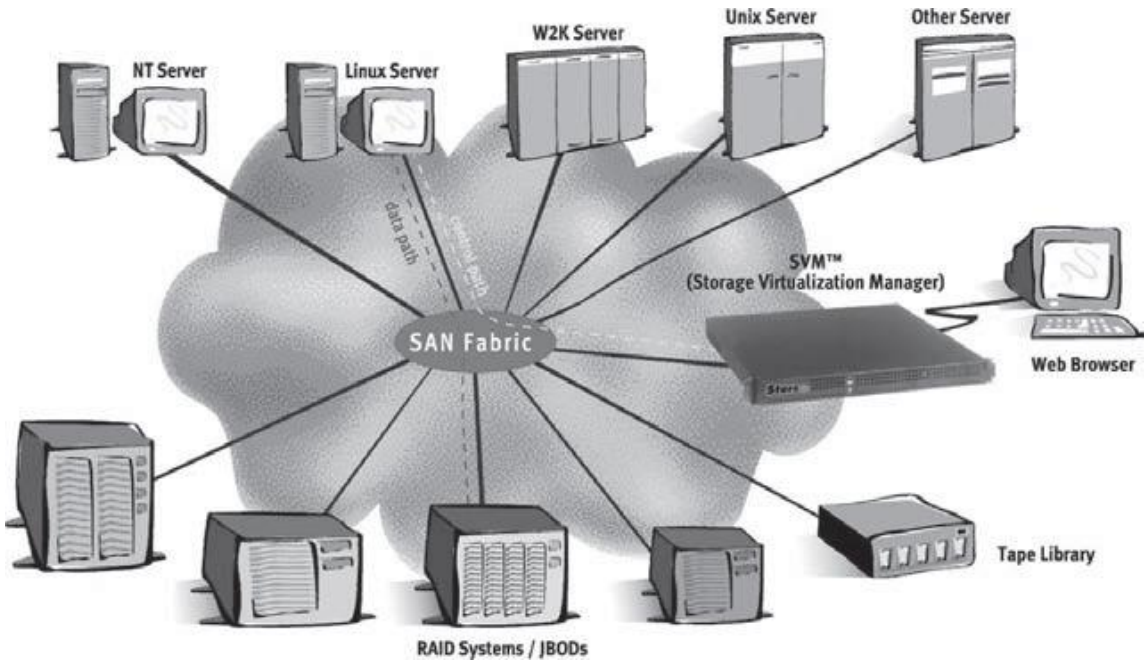
«Εικονοποίηση» (virtualization) είναι ένας ευρύς όρος της πληροφορικής, ο οποίος χρησιμοποιείται για να περιγράψει τον μηχανισμό αφαίρεσης (abstraction) που επιτρέπει την ανάπτυξη ενός διαμοιραζόμενου περιβάλλοντος, όπου διάφορες εφαρμογές χρησιμοποιούν από κοινού υπολογιστικούς, δικτυακούς και αποθηκευτικούς πόρους. Η αφαίρεση αυτή αναγκάζει έναν πόρο να συμπεριφέρεται είτε ως πλειάδα πόρων, είτε πολλαπλούς πόρους να συμπεριφέρονται ως ένας (Mikkilineni & Kankanhalli,2010).

Η εικονοποίηση επέτρεψε στο υλικό των υπολογιστών (hardware) να είναι ανεξάρτητο από εφαρμογές και λειτουργικά συστήματα (EC-Council, 2011b, p 17). Θεωρείται ιδανική λύση για το σχεδιασμό ανάκαμψης από καταστροφές (DRP) αφού ελαχιστοποιεί

το κόστος αγοράς του επιπλέον εξοπλισμού που χρειάζεται να έχει η επιχείρηση για έκτακτη ανάγκη (Hoopes, 2009, p34).

Τα είδη της εικονοποίησης είναι (Mikkilineni &Kankanhalli, 2010; EC-Council, 2011b, p20; Hoopes, 2009, p32):

- Desktop virtualization: Χρησιμοποιεί εικονικές συσκευές για να δώσει τη δυνατότητα σε πολλούς χρήστες ενός δικτύου να διατηρούν εξατομικευμένα λειτουργικά συστήματα σε έναν μοναδικό υπολογιστή.
- Server virtualization: Πρόκειται για την απόκρυψη των πόρων του server, όπως και του αριθμού και της ταυτότητας των μεμονωμένων φυσικών διακομιστών, επεξεργαστών και λειτουργικών συστημάτων, από τους χρήστες του διακομιστή. Προσφέρει εξοικονόμηση ενέργειας, ευκολία στη διαχείριση και διευκολύνει τη διαδικασία ανάκαμψης μετά από καταστροφή.
- Storage virtualization: Είναι ο συνδυασμός πολλαπλών δικτυακών συσκευών αποθήκευσης σε μία εικονική συσκευή αποθήκευσης που ελέγχεται μέσω μίας κεντρικής κονσόλας. Αυτό το είδος εικονοποίησης χρησιμοποιείται συχνά στα δίκτυα SAN που αναφέρθηκαν παραπάνω (Σχήμα 9).
- Network virtualization: Η εικονοποίηση ενός δικτύου προστατεύει τις εφαρμογές από την ετερογένεια τόσο των δικτυακών όσο και των αποθηκευτικών πόρων και επιτρέπει τη δυναμική ανακατανομή τους στις εφαρμογές.
- Application virtualization: Είναι η διαδικασία της εκτέλεσης μιας εφαρμογής από έναν απομακρυσμένο διακομιστή (remote server).

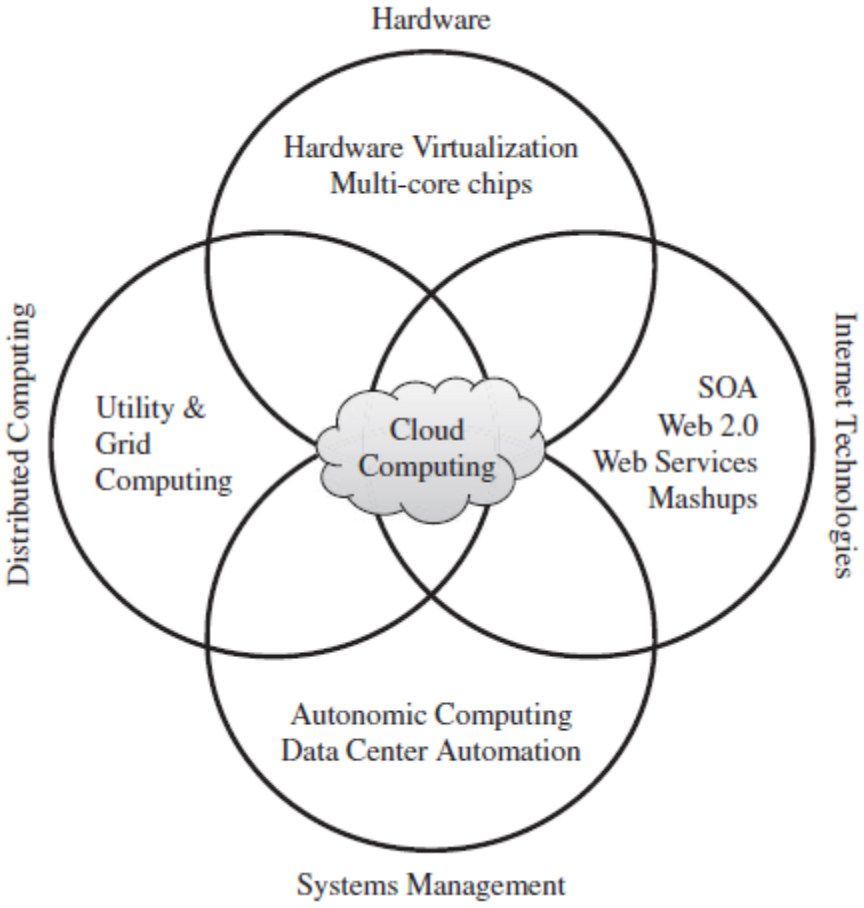


Σχήμα 9: «Storage virtualization» (EC-Council, 2011b, p 22).

Οι τρόποι με τους οποίους μπορεί η εικονοποίηση να συνεισφέρει στην ανάκαμψη από καταστροφές είναι πολλοί (EC-Council, 2011b, p29). Πρώτα απ' όλα, με τη χρήση της εικονοποίησης δημιουργείται πλεονάζων αποθηκευτικός χώρος για τα αντίγραφα ασφαλείας των δεδομένων της επιχείρησης. Επιτρέπει την εύκολη μεταφορά του λογισμικού της επιχείρησης και μειώνει τον όγκο του hardware που απαιτείται στις ειδικά σχεδιασμένες εγκαταστάσεις της επιχείρησης για αυτές τις περιπτώσεις (alternate sites). Προσφέρει αυτόματο συγχρονισμό των δεδομένων μεταξύ των μέσων αποθήκευσης που χρησιμοποιούνται και επιτρέπει στους χρήστες να συνεχίσουν σχεδόν αμέσως την εργασία τους, μετά από τυχόν πρόβλημα στο hardware. Γενικότερα λοιπόν, αυξάνει την «ευκινησία» της επιχείρησης και τη δυνατότητά της να ανταποκρίνεται άμεσα σε επείγουσες καταστάσεις.

Cloud computing

Η «υπολογιστική νέφους» (cloud computing) είναι ίσως η πιο πολυσυζητημένη σύγχρονη τεχνολογία, σύμφωνα με την οποία, οι υπολογιστικές εργασίες διαμοιράζονται σε έναν μεγάλο αριθμό υπολογιστών, έτσι ώστε όλες οι εφαρμογές να έχουν πρόσβαση στην υπολογιστική ισχύ, τον αποθηκευτικό χώρο και το λογισμικό (Zhang Jian-hua & Zhang Nan, 2011). Η βασική αρχή πίσω από αυτό το μοντέλο είναι η παροχή της υπολογιστικής ισχύς, της αποθήκευσης και του λογισμικού «ως υπηρεσίες».

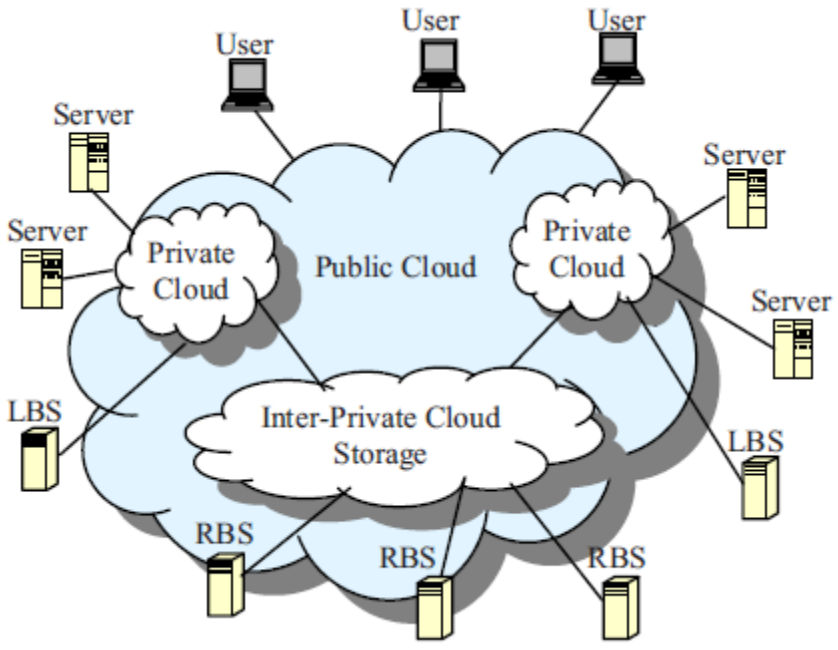


Σχήμα 10: «Convergence of various advances leading to the advent of cloud computing» (Buyya et al,2011, p 6).

Προέρχεται από το συνδυασμό και περιλαμβάνει τα χαρακτηριστικά αρκετών εξελίξεων, σε τομείς όπως είναι το hardware (πχ hardware virtualization), οι τεχνολογίες διαδικτύου (πχ Web 2.0), η διαχείριση συστημάτων (πχ autonomic computing) και η κατανεμημένη υπολογιστική (πχ grid computing) (Σχήμα 10).

Η «υπολογιστική νέφους» και ειδικά η «αποθήκευση στο νέφος» (cloud storage) προσφέρει πολλά πλεονεκτήματα όταν χρησιμοποιείται στο σχεδιασμό ανάκαμψης από καταστροφές. Οι επιχειρήσεις με χαμηλά έσοδα μπορούν να επωφεληθούν από την μαζική επεξεργασία και την αποθήκευση μεγάλου όγκου δεδομένων με πολύ χαμηλό κόστος. Επίσης, η αρχιτεκτονική «αποθήκευσης στο νέφος» διακρίνεται από υψηλή αποδοτικότητα και επεκτασιμότητα (άλλωστε πρόκειται για μια τεχνολογία που αναπτύσσεται συνεχώς και με ταχείς ρυθμούς τα τελευταία χρόνια) (Zhang Jian-hua & Zhang Nan, 2011; Menken, 2008, p51). Οι τεχνολογίες εικονοποίησης (virtualization) που βρίσκονται πίσω από το cloud computing αυτοματοποιούν τις διαδικασίες back-up και μειώνουν το κόστος τους, ενώ ταυτόχρονα μειώνουν την ανάγκη ύπαρξης των πλεοναζουσών εγκαταστάσεων, που αναφέρθηκαν στην προηγούμενη ενότητα (alternate sites)(Reese, 2009, p 128; Chee& Franklin, 2010, p87).

Το μοντέλο που χρησιμοποιείται για την ανάκαμψη από καταστροφές με τη χρήση του cloud computing φαίνεται στο σχήμα 11.



Σχήμα 11: «The model of disaster recovery system» (Zhang Jian-hua& Zhang Nan, 2011, p 631).

Τα δεδομένα των εφαρμογών του συστήματος αποθηκεύονται στους διακομιστές (servers). Όλοι οι διακομιστές έχουν κάποιους back-up servers. Οι back- up servers και οι βασικοί servers μπορούν να βρίσκονται σε διαφορετικές πόλεις. Ο back-up server

αποτελείται από τον τοπικό back-up server (LBS) και τον απομακρυσμένο back-up server (RBS). Τα δεδομένα αντιγράφονται πρώτα στον τοπικό back-up server και στην συνέχεια στον απομακρυσμένο ώστε οι διακομιστές να παραμένουν συγχρονισμένοι και τα δεδομένα να παραμένουν ασφαλή στην περίπτωση μιας καταστροφής.

Συμπεράσματα

Ο Σχεδιασμός Ανάκαμψης από Καταστροφές είναι απαραίτητο βήμα ώστε να διασφαλιστεί ότι μια επιχείρηση ή ένας οργανισμός θα συνεχίσει να λειτουργεί μακροχρόνια χωρίς προβλήματα. Η χρήση των εφαρμογών IT (Information Technology) συνεισφέρει στην προσπάθεια ο σχεδιασμός αυτός να γίνει πιο αποδοτικός και πιο αποτελεσματικός. Σύγχρονες τεχνολογίες όπως είναι η εικονοποίηση και το cloud computing, που αναπτύσσονται συνεχώς, αυτοματοποιούν και απλοποιούν τις διαδικασίες του Disaster Recovery ενώ ταυτόχρονα μειώνουν τα σχετικά κόστη. Η περαιτέρω ανάπτυξη των συγκεκριμένων τεχνολογιών όπως και η έρευνα και ανάπτυξη αναδυόμενων τεχνολογιών (πχ. green technology), μπορεί να βελτιστοποιήσει τη μεθοδολογία του Disaster Recovery Planning.

Βιβλιογραφία

1. Al-Khabbaz, F., Al-Zahir, H., Elwi, S., Al-Yousef, H. (2011). Disaster recovery planning & methodology for Process Automation Systems. *EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE* , pp.1-4, 27-29 April 2011. DOI: 10.1109/EUROCON.2011.5929151

2. Arduini, F. & Morabito, V., (2010). Business continuity and the banking industry. *Commun. ACM,* 53(3), March 2010, p121-125. DOI=10.1145/1666420.1666452

3. Barker, R. & Massiglia, P., (2002). *Storage Area Network Essentials: A Complete Guide to Understanding and Implementing SANs*. New York, USA: John Wiley & Sons, Inc.

4. Business Continuity- is it expensive and hard? (2006). *ITNOW,* March 2006, p12-13. DOI: 10.1093/itnow/bwi0156

5. Buyya, R., Broberg, J., Goscinski, A., (2011). *Cloud Computing: Principles and Paradigms.* New Jersey, USA: John Wiley & Sons, Inc.

6. Cervone, F. H., (2006). Disaster recovery and continuity planning for digital library systems. *OCLC Systems & Services, 22(3),* p 173-178. DOI:10.1108/10650750610686234

7. Chee, B. J.S. & Franklin, C. Jr, (2010). *Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center.* Boca Raton, FL, USA: CRC Press.

8. Cousins, T.J., (2007). Devising Post-Disaster Continuity Plans that Meet Actual Recovery Needs. *Technology and Society Magazine, IEEE, 26(3),* Fall 2007, p 13-23. DOI:10.1109/MTS.2007.906672

9. Dey, M., (2011). Business Continuity Planning (BCP) methodology — Essential for every business. *GCC Conference and Exhibition (GCC), 2011 IEEE, p.229-232, 19-22 Feb. 2011*. DOI: 10.1109/IEEEGCC.2011.5752503

10. Duncan, W. J., Yeager, V.A., Rucks, A.C, Ginter, P.M, (2011). Surviving organizational disasters. *Business Horizons, 54(2),* p 135-142. DOI: 10.1016/j.bushor.2010.10.005

11. EC-Council, (2011a). *Disaster Recovery*. New York, USA: Cengage Learning.

12. EC-Council, (2011b). *Virtualization Security,* New York, USA: Cengage Learning.

13. Fulmer, K. L., (2005). *Business Continuity Planning: A Step-by-Step Guide with Planning Forms, Third Edition*. Brookfield, Connecticut, USA: Rothstein Associates Inc.

14. Gibb, F., Buchanan, S., (2006). A framework for business continuity management. *International Journal of Information Management, 26(2),* April 2006, p 128-141. DOI:10.1016/j.ijinfomgt.2005.11.008

15. Herbane, B., (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History, 52(6),* p 978-1002. DOI:10.1080/00076791.2010.511185

16. Hoopes, J., (2009). *Virtualization for security: including sandboxing, disaster recovery, high availability.* Burlington, Massachusetts, USA: Syngress Publishing, Inc.

17. Lingeswara Tammineedi, R., (2010). Business Continuity Management: A Standards-Based Approach. *Information Security Journal: A Global Perspective, 19(1),* p 36-50. DOI:10.1080/19393550903551843

18. Liotine, M., (2003). *Mission-Critical Network Planning.* Norwood, MA, USA: Artech House, Inc.

19. Luetkehoelter, J., (2008). *Pro SQL Server Disaster Recovery*. Berkeley, California, USA: Apress.

20. McDonald, R., (2008). New considerations for security compliance, reliability and business continuity. *Rural Electric Power Conference, 2008 IEEE, p.B1-B1-7, 27-29 April 2008.* DOI: 10.1109/REPCON.2008.4520132

21. Menken, I., (2008). *Cloud Computing - The Complete Cornerstone Guide to Cloud Computing Best Practices: Concepts, Terms, and Techniques for Successfully Planning, ... Enterprise IT Cloud Computing Technology.* Newstead, Australia: Emereo Publishing.

22. Mikkilineni, R.; Kankanhalli, G., (2010). Using Virtualization to Prepare Your Data Center for "Real-Time Assurance of Business Continuity. *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on, p 76-81, 28-30 June 2010.* DOI:10.1109/WETICE.2010.18

23. Oberg, J.C.; Whitt, A.G.; Mills, R.M. (2011). Disasters will happen - are you ready? *Communications Magazine, IEEE, 49(1),* January 2011, p36-42. DOI:10.1109/MCOM.2011.5681012

24. Peterson, C.A., (2009). Business continuity management \& guidelines. In *2009 Information Security Curriculum Development Conference (InfoSecCD '09). ACM*, New York, NY, USA, 114-120. DOI=10.1145/1940976.1940999

25. Reese, G., (2009). *Cloud Application Architectures.* Sebastopol, CA, USA: O'Reilly Media, Inc.

26. Rittinghouse, J.W., &Ransome, J.F., (2005). *Business Continuity and Disaster Recovery for InfoSec Managers*. Burlington, Massachusetts, USA: Elsevier Digital Press.

27. Snedaker, S., (2007). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Burlington, Massachusetts, USA: Syngress Publishing, Inc.

28. Stanton, R., (2005). Beyond disaster recovery: the benefits of business continuity. *Computer Fraud & Security, Vol :2005(7)*, July 2005, p 18-19. DOI:10.1016/S1361-3723(05)70234-7

29. Zhang Jian-hua; Zhang Nan, (2011). Cloud Computing-based Data Storage and Disaster Recovery. *Future Computer Science and Education (ICFCSE), 2011 International Conference on, p629-632, 20-21 Aug. 2011.* DOI:10.1109/ICFCSE.2011.157