ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΓΕΩΓΡΑΦΙΑΣ

Εφαρμοσμένη Γεωγραφία και Διαχείριση του Χώρου

‘Διαχείριση Φυσικών και Ανθρωπογενών Καταστροφών’

Τίτλος Διπλωματικής Εργασίας

ΜΕΛΕΤΗ ΤΟΥ ΠΛΑΙΣΙΟΥ ΔΙΑΧΕΙΡΙΣΕΩΣ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ

(Business Continuity Management)

Κατής Ν. Άγγελος

Αθήνα, 2017

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΓΕΩΓΡΑΦΙΑΣ

Εφαρμοσμένη Γεωγραφία και Διαχείριση του Χώρου

'Διαχείριση Φυσικών και Ανθρωπογενών Καταστροφών'

Τριμελής Εξεταστική Επιτροπή

Αλεξάνδρα Τραγάκη (Επιβλέπουσα)

Αναπληρώτρια Καθηγήτρια, Τμήμα Γεωγραφίας, Χαροκόπειο Πανεπιστήμιο

Ευθύμιος Καρύμπαλης

Αναπληρωτής Καθηγητής, Τμήμα Γεωγραφίας, Χαροκόπειο Πανεπιστήμιο

Πέτρος Κατσαφάδος

Επίκουρος Καθηγητής, Τμήμα Γεωγραφίας, Χαροκόπειο Πανεπιστήμιο

Ο Κατής Άγγελος,

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

Αφιερώνεται στους γονείς μου.

«Πριν τι κακόν παθέειν. Ρεχθέν δε τε νήπιος έγνω».

Πάντα ο φρόνιμος πριν πάθει λογαριάζει. Ιλιάδα, Ρ 32

ΕΥΧΑΡΙΣΤΙΕΣ

Όταν φτάνεις στο τέλος ενός μεγάλου στόχου διαπιστώνεις ότι ένα μεγάλο μέρος της επιτυχίας σου οφείλεται σε ένα πλήθος ανθρώπων. Στο σημείο αυτό αισθάνομαι την υποχρέωση να ευχαριστήσω θερμά όλους τους ανθρώπους που με βοήθησαν να ολοκληρώσω την διπλωματική αυτή. Καταρχήν θα ήθελα να ευχαριστήσω μέσα από την καρδιά μου την επιβλέπουσα καθηγήτρια κυρία Αλεξάνδρα Τραγάκη για τις ανεκτίμητες συμβουλές καθώς και την πολύτιμη καθοδήγηση που μου παρείχε κατά την διάρκεια συγγραφής της παρούσας διπλωματικής. Εν συνέχεια θα ήθελα να ευχαριστήσω όλους τους καθηγητές του συγκεκριμένου μεταπτυχιακού προγράμματος για την γνώση και εμπειρία που μας προσέφεραν όλο αυτό το διάστημα. Ένα μεγάλο ευχαριστώ ανήκει στους συμφοιτητές και συναδέλφους μου για τις κοπιαστικές καθώς και όμορφες στιγμές που περάσαμε μαζί τον περασμένο χρόνο. Οι θερμότερες ευχές ανήκουν στην οικογένειά μου για την αμέριστη στήριξη που μου προσέφερε όλο αυτό το διάστημα καθώς και σε κάθε μου βήμα.

ΠΕΡΙΛΗΨΗ

Οι καταστροφές μπορεί να συμβούν ανά πάσα στιγμή και συνήθως χωρίς προειδοποίηση. Μπορεί να οφείλονται σε φυσικά αίτια ή ανθρώπινες ενέργειες και έχουν την δυνατότητα να προκαλέσουν από προσωρινή αναστολή εργασιών έως και οριστική διακοπή μιας επιχείρησης. Την τελευταία δεκαετία έντονα έχει διαπιστωθεί ότι εταιρίες και οργανισμοί που παρέχουν κρίσιμες υπηρεσίες οφείλουν να εξασφαλίσουν την διαθεσιμότητα αυτών σε κάθε περίπτωση. Αυτό επιτυγχάνεται με τον σχεδιασμό κα την εφαρμογή ενός πλαισίου Επιχειρησιακής Συνέχειας (Business Continuity Management).

Στην παρούσα εργασία θα γίνει μελέτη και παρουσίαση ενός ολοκληρωμένου πλαισίου Επιχειρησιακής Συνέχειας. Θα ακολουθήσει εκτενής αναφορά των διαδικασιών που περιλαμβάνει ,όπως :

- Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis)
- Εκτίμηση Απειλών και Κινδύνων (Threat and Risk Assessment)
- Καθορισμός Στρατηγικής Επιχειρησιακής Συνέχειας (Business Continuity Strategy)
- Ανάπτυξη Σχεδίων
- Δοκιμαστική Εφαρμογή Σχεδίων
- Συντήρηση Σχεδίων

Στην συνέχεια θα αναφερθούν οι μέθοδοι που χρησιμοποιούνται για την ανάλυση , την αξιολόγηση , και την πιθανότητα εμφάνισης κινδύνων. Πρόσθετα, θα μελετηθούν περιπτώσεις αντιμετώπισης κρίσεων από φυσικές καταστροφές που έχουν καταγραφεί στην ελληνική καθώς και την διεθνή βιβλιογραφία, θα αξιολογηθούν τα αποτελέσματα, καθώς και τα οφέλη εφαρμογής ενός πλαισίου Επιχειρησιακής Συνέχειας. Κατόπιν θα προσδιοριστούν βέλτιστες πρακτικές για την αποτελεσματική αντιμετώπιση κρίσεων και τον σχεδιασμό πλάνων .

Μέσω ιστορικής αναδρομής θα μελετηθεί η εξέλιξη της Επιχειρησιακής Συνέχειας και στα πλαίσια ενός θεωρητικού Χρηματοπιστωτικού ιδρύματος θα αναφερθούν τα πλεονεκτήματα εφαρμογής της.

Την τελευταία δεκαετία αποκτά μεγάλη αξία και βαρύτητα, η δημιουργία ενός συστήματος ετοιμότητας έναντι φυσικών και ανθρωπογενών καταστροφών που έχει ως πρώτο μέλημα την υγεία και την ασφάλεια των εργαζομένων και κατόπιν την επιχειρησιακή συνέχεια ενός οργανισμού. Για τον λόγο αυτό αποτελεί ιδιαίτερο ενδιαφέρον η μελέτη εξέλιξης καθώς και οι μελλοντικές απαιτήσεις στο συγκεκριμένου τομέα των Χρηματοπιστωτικών Ιδρυμάτων όπου η αδιάλειπτη λειτουργία τους κρίνεται περισσότερο απαραίτητη όσο ποτέ.

Λέξεις κλειδιά: Επιχειρησιακή Συνέχεια, Ανάκαμψη από Καταστροφή, Σχέδια Ανάκαμψης Καταστροφών, Έκτακτη Ανάγκη, Κρίση

ABSTRACT

Catastrophes may occur at any moment and usually without any warning. These may be generated by natural causes or human actions which could lead to temporary suspension of a company's operations and its termination of its license. Over the last decade, it has been designated that companies or organizations that provide hazard / high risk services must ensure to obtain their availability of critical information at any case. This is achieved by designing and implementing an effective Business Continuity Management.

Research and analysis of Business Continuity Management will be elaborated throughout this report, including procedures such as:

- Business Impact Analysis
- Threat and Risk Assessment
- Business Continuity Strategy
- Business Continuity Plans
- Testing of Plans
- Corrective Actions

Furthermore, information will be expanded on methods used for an analysis, evaluation and probable risks arising. Case studies will be examined in managing crisis derived by natural catastrophes, as these were recorded in the Greek and International bibliography. Results will be assessed, as well as the advantages of the use of a Business Continuity Management using best practises in mitigating crisis risks and designing plans.

Historically, the evolution of a Business Continuity Management will be studied on a theoretical Financial Institution, denoting its benefits when applying.

Over the last decade the value and importance for the creation of preparedness system against natural and human catastrophes has proven highly important, having as priority the health and safety of the employees, as well as the continuity of an organization. For this reason it is particularly interesting to study the evolution and future requirements in the sector of financial institutions where their continued operation is considered more essential than ever.

Keywords: Business Continuity, Disaster Recovery, Disaster Recovery Plans, Emergency, Crisis

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1. *Εξέλιξη της Επιχειρησιακής Συνέχειας από το 1970 έως σήμερα.* 26
ΕΙΚΟΝΑ 2. *Ανθρώπινες απώλειες από φυσικές καταστροφές το 2016* 31
Εικόνα 3. *Συχνότητα εμφάνισης των τεσσάρων τύπων μεγάλων καταστροφών στον κόσμο (Μέσος όρος ανά χώρα) (http://www.rieti.go.jp/en/rieti_report/134.html).* 32
Εικόνα 4**.** Χιονοπτώσεις, Δασικές πυρκαγιές, Σεισμός, Ταραχές και οι αντίστοιχες διαχρονικές μέσες τιμές. *(Πηγή Ε.Α.Ε.Ε)* 33
Εικόνα 5. *Συσχετισμός Σχεδίων αντιμετώπισης περιστατικών* 38
Εικόνα 6. *Ο κύκλος του Deming* 40
Εικόνα 7. *Στοιχεία διαχείρισης κύκλου ζωής ενός ΣΕΣ.* 45
Εικόνα 8. *Κύκλος ζωής Διαχείρισης Επιχειρηματικής Συνέχειας - ΔΕΣ Πηγή: Διεθνές Ινστιτούτο Αποκατάστασης από Καταστροφή - ΔΙΑΚ (Disaster Recovery Institute International - DRII* 47
Εικόνα 9. *Το τρίπτυχο ασφαλείας "CIA" καθορίζει την κρισιμότητα μιας λειτουργίας.* 52
Εικόνα 10. *Διαγραμματική απεικόνιση RTO,RPO & MTPD.* 54
Εικόνα 11. *Χρονική διαγραμματική απεικόνιση διαχείρισης ενός καταστροφικού περιστατικού.* 54
Εικόνα 12. *Χρονική διαγραμματική απεικόνιση διαχείρισης ενός καταστροφικού περιστατικού με χρήση αλλά και χωρίς Σχεδίου Ανάκαμψης.* 55
Εικόνα 13. *Διαδικασία προσδιορισμού Στρατηγικής Επιχειρησιακής Συνέχειας.* 56
Εικόνα 14. *Διαφορές μεταξύ Σχεδίου Επιχειρησιακής Συνέχειας και Σχεδίου Ανάκαμψης από Καταστροφή* 61
Εικόνα 15. *Επίδραση ύπαρξης ΣΑΚ σε περίπτωση καταστροφής.* 63
Εικόνα 16. *Διάγραμμα αποτίμησης κινδύνου.* 73
Εικόνα 17. *Αναφορά κινδύνων - απειλών για μια εταιρία σήμερα, ALCO (Business Continuity Forum 2016).* 76
Εικόνα 18. *Ύπαρξη πλάνων διαχείρισης έκτακτων γεγονότων , σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO (Business Continuity Forum 2016).* 76
Εικόνα 19. *Ύπαρξη ομάδων διαχείρισης έκτακτων γεγονότων , σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO (Business Continuity Forum 2016).* 77
Εικόνα 20. *Βαθμός εξοικείωσης με τον όρο "Επιχειρησιακή Συνέχεια", σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO(Business Continuity Forum 2016).* 77
Εικόνα 21. *Οι σπουδαιότερες αιτίες που ΔΕΝ έχουν προχωρήσει σε σύστημα Business Continuity, σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO (Business Continuity Forum 2016).* 78

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1. *Οι 10 χώρες με τις μεγαλύτερες ανθρώπινες και οικονομικές απώλειες από καταστροφές το 2016* 31
Πίνακας 2. *Πλήθος δηλωθεισών ζημιών και το ποσό απαίτησης καταστροφών μεγάλης έκτασης 1993-2014 σύμφωνα με την (Πηγή Ε.Α.Ε.Ε).* 33
Πίνακας 3. *Είδη σχεδίων αντιμετώπισης περιστατικών* 38
Πίνακας 4. *Ταξινόμηση κρίσιμων λειτουργιών σε σχέση με τον χρόνο αποκατάστασης MTPD* 55
Πίνακας 5. *Τύποι Εγκαταστάσεων εφεδρικής τοποθεσίας.* 57
Πίνακας 6. *Πίνακας Ανάλυσης – Διαχείρισης Κινδύνου.* 68
Πίνακας 7. *Πίνακας Εκτίμηση- Πιθανότητας* 70
Πίνακας 8. *Πίνακας Εκτίμηση επιπτώσεων.* 71
Πίνακας 9. *Μήτρα Πιθανότητας/Επιπτώσεων Κινδύνων* 71
Πίνακας 10. *Πίνακας Αποτίμηση Κινδύνου.* 72

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1 13
1.Εισαγωγή & Κίνητρα 13
1.1 Σκοπός & Αντικείμενο 14
1.2 Δομή 15
Κεφάλαιο 2 17
2.1 Βασικές έννοιες-Ορολογία Επιχειρησιακής Συνέχειας 17
2.2 Ένα σύντομο Ιστορικό της Επιχειρησιακής Συνέχειας & Εξέλιξη 23
Κεφάλαιο 3 27
3.1 Βασικά είδη καταστροφών 27
3.2 Επιπτώσεις καταστροφών σε επίπεδο επιχειρήσεων 28
3.3 Καταγραφή Φυσικών και Τεχνολογικών καταστροφών 30
3.4 Κατηγορίες σχεδίων αντιμετώπισης περιστατικών 34
3.5 Ο κύκλος ζωής σχεδίων - PDCA 39
3.5.1 Μεθοδολογία του Κύκλου του Deming - PDCA 39
Κεφάλαιο 4 41
4.1 Πρότυπα Business Continuity 41
Κεφάλαιο 5 45
5.1 Μεθοδολογία Ανάπτυξης ΣΕΣ 45
5.1 .1 Το Πλαίσιο του Έργου 45
5.1.2 Στοιχεία Διαχείρισης Κύκλου Ζωής του ΣΕΣ 46
5.2.1 Ανάπτυξη Πολιτικής Επιχειρησιακής Συνέχειας 48
5.3 Κατανόηση του Οργανισμού 49
5.3.1 Ανάλυση Επιπτώσεων Επιχειρησιακής Συνέχειας 50
5.3.2 Εκτίμηση Απειλών και Κινδύνων (Threat and Risk Assessment) 51
5.3.5 Ιεράρχηση Κρίσιμων Εργασιών και Συστημάτων 55
5.4 Προσδιορισμός Στρατηγικής Επιχειρησιακής Συνέχειας 56
5.5 Εφαρμογή Σχεδίων Επιχειρησιακής Συνέχειας 58
5.5.2 Σχεδιασμός της επιχειρηματικής συνέχειας 60
5.6 Δοκιμή και Συντήρηση των Σχεδίων 63
5.6.2 Κατηγορίες και Δοκιμές των Σχεδίων 64
5.7 Ενσωμάτωση στην κουλτούρα του οργανισμού 65
Κεφάλαιο 6 66
6.1 Διαχείριση Κρίσεων (Risk Management) 66
6. 2 Μεθοδολογία Ανάλυσης Κινδύνου (Risk Analysis) 67

6.3 Μεθοδολογία Διαχείρισης Κινδύνου 73
Κεφάλαιο 7 75
7.1 Συμπεράσματα -Επίλογος 79
7.2 Συνεισφορά της Έρευνας 82
7.3 Μελλοντική Μελέτη 83
ΒΙΒΛΙΟΓΡΑΦΙΑ 84

Κεφάλαιο 1

1.Εισαγωγή & Κίνητρα

Από τις αρχές ήδη του 21ου αιώνα θεωρείται επιτακτική ανάγκη των επιχειρήσεων να αντιμετωπίζουν σε επιθυμητό επίπεδο τις αρνητικές επιπτώσεις από μια ενδεχόμενη κρίση ή και καταστροφή. 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) .

Σύμφωνα με την διεθνής βιβλιογραφία, οι Καταστροφές διακρίνονται σε Φυσικές Καταστροφές (Natural disasters) και σε Τεχνολογικές ή Ανθρωπογενείς Καταστροφές (Technological ή Man – Made disasters) . Ο διαχωρισμός αυτός βασίζεται στο γενετικό αίτιο της Καταστροφής. Οι Φυσικές Καταστροφές περιλαμβάνουν σεισμούς, ηφαιστειακές εκρήξεις τσουνάμι, κατολισθήσεις, παγετώνες, πυρκαγιές, ξηρασίες, πλημμύρες, καύσωνες, παγετούς, τυφώνες κλπ. Αντίθετα, με τις καταστροφές που προκύπτουν ως απόρροια της τεχνολογικής ή άλλης ανθρώπινης δραστηριότητας και κατατάσσονται στις Τεχνολογικές ή Ανθρωπογενείς Καταστροφές (π.χ. εκρήξεις, τρομοκρατικές ενέργειες ,διαρροές επικίνδυνων ουσιών, ατυχήματα σε εργοστάσια κλπ.) .

Οι επιπτώσεις μιας καταστροφής επιφέρουν τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα, απώλειες σε έναν οργανισμό. Μελέτη της εταιρίας AXA το 2007 αναφέρει οτι το 80% των εταιριών που επλήγησαν από κάποιο καταστροφικό γεγονός είτε δεν επαναλειτούργησαν είτε διέκοψαν τη λειτουργία τους μετά από χρονικό διάστημα 18 μηνών. Στην ίδια κατεύθυνση καταλήγει έρευνα του Εμπορικού και Βιομηχανικού επιμελητηρίου Λονδίνου (London Chamber of Commerce) που πραγματοποιήθηκε το 2005 όπου αναφέρει ότι το 40% των οργανισμών που επηρεάστηκαν από μια καταστροφή δεν επαναλειτούργησαν ποτέ (Duncan, Yeager, Rucks, Ginter, 2011) .

Για να αποφευχθούν παρόμοιου είδους καταστροφικές συνέπειες καθώς και να διασφαλίσουν στο μέγιστο δυνατό βαθμό την συνέχεια των εργασιών τους, οι οργανισμοί θέσπισαν διαδικασίες που εντάχθηκαν σε ένα Πλαίσιο Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management – BCM). Αναπτύχθηκαν Σχέδια Επιχειρησιακής Συνέχειας (Business Continuity Plan) ώστε να εξασφαλίζουν ως ένα βαθμό ότι αμέσως μετά την εκδήλωση ενός απρόοπτου γεγονότος θα διασφαλιστεί σταδιακά η συνέχιση των κύριων και στην συνέχεια όλων των επιχειρησιακών λειτουργιών. Για την επιτυχή εφαρμογή, κυρίαρχο ρόλο φέρουν

τόσο οι άνθρωποι που το υλοποιούν, το γνωστοποιούν όσο και η κοινότητα που το αποδέχεται.

Στα πλαίσια της συγκεκριμένης εργασίας θα γίνει εκτενής μελέτη και παρουσίαση του συγκεκριμένου Πλαισίου καθώς των κανόνων που το διέπουν.

Πριν προχωρήσουμε, είναι ενδιαφέρον να εξετάσουμε τα κίνητρα εκπόνησης αυτής της διατριβής.

Τα τελευταία χρόνια, ορισμένα σοβαρά περιστατικά σε διεθνές επίπεδο (π.χ. φυσικές καταστροφές, τρομοκρατικές επιθέσεις) έχουν αναδείξει τη σπουδαιότητα της λειτουργικής αξιοπιστίας των υποδομών μιας επιχείρησης. Η προστασία μιας επιχείρησης , τόσο σε επίπεδο παγίων περιουσιακών στοιχείων, ιδιοκτησίας, υλικών και άυλων κεφαλαίων , ανθρωπίνου δυναμικού και φήμης επιτυγχάνεται με την εφαρμογή ενός αποτελεσματικού Σχεδίου Επιχειρησιακής Συνέχειας (Business Continuity Planning) το οποίο εμπεριέχεται στο πλαίσιο της Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management) .

Έχουν εντοπιστεί αρκετοί παράγοντες που επηρεάζουν την επιτυχία ή μη του σχεδίου. Επιγραμματικά αναφέρονται οι κυριότεροι :

- μη αποτελεσματική επικοινωνία στους εργαζόμενους
- λανθασμένη ιεράρχηση κρίσιμων λειτουργιών
- λανθασμένη ιεράρχηση κινδύνων
- μη τακτική συντήρηση-ανανέωση των σχεδίων
- κουλτούρα της επιχείρησης

Απόρροια των ανωτέρω αποτέλεσε η ύπαρξη ανάγκης για την μελέτη της κατάλληλης μεθοδολογίας για την ανάπτυξη ενός αποτελεσματικού Σχεδίου Επιχειρησιακής Συνέχειας ενός Χρηματοπιστωτικού Ιδρύματος.

1.1 Σκοπός & Αντικείμενο

Η παρούσα εργασία στοχεύει στην λεπτομερή μελέτη και ανάλυση του Πλαισίου Επιχειρησιακής Συνέχειας και του ειδικότερου Σχεδίου Επιχειρησιακής Συνέχειας (ΣΕΣ) . Θα γίνει απόπειρα να δοθούν απαντήσεις, στα κάτωθι ερωτήματα, όπου υφίστανται:

- Ποια τα πλεονεκτήματα ενός Σχεδίου Επιχειρησιακής Συνέχειας (ΣΕΣ) για μια επιχείρηση;
- Θεωρείται υποχρεωτική ή προαιρετική η ύπαρξη ενός τέτοιου σχεδίου;

- Ποια κατάλληλα πρότυπα και βέλτιστες πρακτικές υφίστανται για την αποτελεσματική εφαρμογή του;
- Ποιό είναι το οικονομικό κόστος υλοποίησης ενός ΣΕΣ ώστε να είναι αποτελεσματικό και αποδοτικό;

Αντικείμενο μελέτης αποτελεί η μεθοδολογία ανάπτυξης που θα υιοθετήσει από ένα Χρηματοπιστωτικό ίδρυμα για να εφαρμόσει γρήγορα και αποτελεσματικά ένα ΣΕΣ, περιορίζοντας στο ελάχιστο δυνατό βαθμό τις επιπτώσεις μιας ενδεχόμενης καταστροφής. Τα παραπάνω επιμέρους ερωτήματα θα αναπτυχθούν στα επόμενα κεφάλαια, προτού εστιάσουμε σε κάθε στόχο μεμονωμένα, θα αναφερθούμε στην συνέχεια στη δομή της εργασίας.

1.2 Δομή

Η εργασία είναι διαρθρωμένη με τρόπο ώστε αρχικά να αναλύεται η θεωρητική προσέγγιση του Πλαισίου Επιχειρησιακής Συνέχειας . Επιγραμματικά σε κάθε κεφάλαιο εντάσσονται:

Κεφάλαιο 1: Στο 1ο κεφάλαιο γίνεται μια εισαγωγική αναφορά στα κίνητρα, τον σκοπό και το αντικείμενο της διπλωματικής εργασίας. Συγκεκριμένα αναφέρεται η ανάλυση κατάλληλης μεθοδολογίας για την ανάπτυξη ενός ΣΕΣ στα πλαίσια ενός Χρηματοπιστωτικού Ιδρύματος.

Κεφάλαιο 2: Στο 2ο κεφάλαιο διευκρινίζονται βασικές έννοιες και ορισμοί που διέπουν το Πλαίσιο Επιχειρησιακής Συνέχειας προκειμένου να γίνει καλύτερα αντιληπτό. Στην συνέχεια γίνεται μια αναφορά στην εξέλιξη της Επιχειρησιακής Συνέχειας μέσω ενός σύντομου ιστορικού. Ξεκινώντας από το 1970, συνεχίζοντας στην 11η Σεπτεμβρίου 2001 και καταλήγοντας στην σημερινή της μορφή.

Κεφάλαιο 3: Στο 3^{ο} κεφάλαιο αναφέρονται τα είδη των καταστροφών ,οι επιπτώσεις που προκαλούν στις επιχειρήσεις καθώς γίνεται επιγραμματική αναφορά σε καταστροφικά γεγονότα που έλαβαν χώρα σε διεθνές και εθνικό επίπεδο. Στην συνέχεια παρουσιάζονται τα είδη σχεδίων αντιμετώπισης περιστατικών σύμφωνα με το National Institute of Standards and Technology των Η.Π.Α . Το κεφάλαιο κλείνει με την αναφορά στον κύκλο του Deming . Κάθε σχέδιο, ως ένα σύνολο από διαδικασίες και ενέργειες, για να είναι αποτελεσματικό δεν θα πρέπει να αντιμετωπίζεται ως ένα στατικό αλλά ως ένα δυναμικά εξελισσόμενο μέτρο

προστασίας. Επομένως απαιτείται η συνεχής παρακολούθησή του και η προσαρμογή του στις εκάστοτε συνθήκες.

Κεφάλαιο 4: Στο 4ο κεφάλαιο περιγράφονται τα διεθνή πρότυπα που ισχύουν σχετικά με την Επιχειρησιακή Συνέχεια καθώς γίνεται αναφορά και στο Προεδρικό Διάταγμα σχετικά με τα Ελληνικά Χρηματοπιστωτικά ιδρύματα.

Κεφάλαιο 5: Το κεφάλαιο αυτό περιγράφει αναλυτικά τη μέθοδο που αποσκοπεί στην αποτελεσματική ανάπτυξη του Σχεδίου Επιχειρησιακής Συνέχειας σύμφωνα με τα διεθνή πρότυπα BS25999 και ISO22301.

Κεφάλαιο 6: Στο κεφάλαιο αυτό γίνεται μια αναφορά στην Διαχείριση Κρίσεων καθώς και την σπουδαιότητά της σχετικά με την λήψη άμεσα σημαντικών αποφάσεων για την ελαχιστοποίηση του κινδύνου εμφάνισης δυσάρεστων γεγονότων και στην συνέχεια περιγράφεται η μεθοδολογία ανάλυσης, αναγνώρισης και εκτίμησης κινδύνου.

Κεφάλαιο 7: Στο 7^{ο} και τελευταίο κεφάλαιο αρχικά επισημαίνονται τα σπουδαιότερα αποτελέσματα έρευνας σχετικής με την επιχειρησιακή συνέχεια που έλαβε χώρα από την εταιρία ALCO στα πλαίσια του 3ου Business Continuity Management Forum για τα έτη 2014-2015-2016. Κλείνοντας συνοψίζονται συμπεράσματα που προέκυψαν από την παρούσα εργασία καθώς και πεδίο δράσης για μελλοντική έρευνα.

Κεφάλαιο 2

Το Κεφάλαιο αυτό περιλαμβάνει 2 ενότητες. Στην πρώτη ενότητα κρίθηκε σκόπιμη η αναφορά σε βασικές έννοιες που διέπουν το Πλαίσιο Επιχειρησιακής Συνέχειας έτσι όπως αποτυπώνονται στο γλωσσάρι του Business Continuity Institute (Ινστιτούτο Διαχείρισης Επιχειρησιακής Συνέχειας) , που είναι ένα από τα 3 μεγαλύτερα στον κόσμο, προκειμένου να γίνουν άμεσα και καλύτερα αντιληπτά τα επόμενα κεφάλαια.

Η δεύτερη ενότητα αναφέρεται στην εξέλιξη, μέσω ενός σύντομου ιστορικού των τελευταίων δεκαετιών, του Σχεδιασμού Επιχειρησιακής Συνέχειας προσεγγίζοντας τελικά της σημερινή της μορφή και επιβεβαιώνοντας το πόσο επιτακτική ανάγκη για τις επιχειρήσεις είναι η αποτελεσματική εφαρμογή της.

2.1 Βασικές έννοιες-Ορολογία Επιχειρησιακής Συνέχειας

Κρίση (Crisis event) : Κρίση αποτελεί ένα κρίσιμο συμβάν το οποίο ενδέχεται να επηρεάσει αρνητικά την κερδοφορία, τη φήμη ή τη δυνατότητα ενός οργανισμού να λειτουργεί. Ενδέχεται να μην επηρεάζεται από την πάροδο του χρόνου και συνήθως δεν στερεί την πρόσβαση στις εγκαταστάσεις και τις υποδομές.

Περιστατικό (Incident) : Είναι ένα συμβάν είτε τυχαίο είτε λόγω συνδυασμού απροσδόκητων περιστάσεων, το οποίο χωρίς τον κατάλληλο χειρισμό μπορεί να κλιμακωθεί σε μια έκτακτη κατάσταση, καταστροφή ή κρίση.

Διακοπή Εργασιών/Λειτουργίας : Διαταραχή αποτελεί η διακοπή των κανονικών επιχειρησιακών δραστηριοτήτων ή διεργασιών, η οποία μπορεί να ποικίλει από βραχυπρόθεσμη έως μακροπρόθεσμη μη διαθεσιμότητα.

Επιχειρησιακή συνέχεια (Business Continuity) :

1.Η Επιχειρησιακή Συνέχεια αποσκοπεί στην προστασία των συμφερόντων ενός οργανισμού και των κυριότερων ενδιαφερόμενων μερών προστατεύοντας τις κρίσιμες επιχειρησιακές δραστηριότητες από προκαθορισμένες διαταραχές.

2. Η δυνατότητα του οργανισμού να συνεχίσει να παρέχει τα προϊόντα και τις υπηρεσίες του σε προκαθορισμένα αποδεκτά επίπεδα μετά από κάποιο περιστατικό διακοπής.

Διαχείριση Επιχειρησιακής Συνέχειας (Business Continuity Management) :

1.Η Διαχείριση Επιχειρησιακής Συνέχειας αποτελεί ένα γνωστικό πεδίο που αφορά ολόκληρο τον οργανισμό και ένα πλήρες σύνολο διεργασιών το οποίο αναγνωρίζει πιθανές επιπτώσεις που απειλούν τον οργανισμό. Παρέχει τη δυνατότητα αποτελεσματικής απόκρισης που προστατεύει τα συμφέροντα των κυριότερων ενδιαφερόμενων μερών και τη φήμη του οργανισμού.

2. Είναι μια ολιστική διαδικασία διαχείρισης που εντοπίζει τις πιθανές απειλές σε ένα οργανισμό και τις δυνατές τους επιπτώσεις στις επιχειρηματικές λειτουργίες στην περίπτωση που συμβούν. Παρέχει ένα πλαίσιο για την ανάπτυξη της ανθεκτικότητας του οργανισμού με τη δυνατότητα αποτελεσματικής απόκρισης η οποία προστατεύει τα συμφέροντα των κύριων ενδιαφερόμενων μερών, τη φήμη, το εμπορικό σήμα και τις κερδοφόρες δραστηριότητες.

Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Plan) :

1. Ένα Σχέδιο Επιχειρησιακής Συνέχειας αποτελείται από σαφώς καθορισμένες και τεκμηριωμένες διαδικασίες και πληροφορίες προς χρήση κατά την εκδήλωση περιστατικού καταστροφής.

2. Τεκμηριωμένες διαδικασίες που καθοδηγούν τους οργανισμούς στην απόκριση, ανάκαμψη, επαναφορά και αποκατάσταση σε ένα προκαθορισμένο επίπεδο λειτουργίας μετά από μια διαταραχή.

Καταστροφή (Disaster) : Μία Καταστροφή αποτελεί ένα ξαφνικό μη προγραμματισμένο γεγονός το οποίο προκαλεί σημαντική ζημιά ή απώλεια σε ένα οργανισμό. Έχει σαν αποτέλεσμα την αποτυχία του οργανισμού να παρέχει κρίσιμες επιχειρησιακές δραστηριότητες για κάποιο προκαθορισμένο ελάχιστο χρονικό διάστημα. Εν συντομία, στερεί από τον οργανισμό πρόσβαση σε ανθρώπους, διεργασίες και υποδομές.

Ανάκαμψη από Καταστροφή (Disaster Recovery) : Η Ανάκαμψη από την Καταστροφή αποτελεί τη δυνατότητα ενός οργανισμού να παρέχει κρίσιμες πληροφοριακές και τηλεπικοινωνιακές δυνατότητες καθώς και υπηρεσίες, αφού διαταραχθεί από κάποιο περιστατικό, έκτακτη κατάσταση ή καταστροφή. Η Ανάκαμψη από τη Καταστροφή ανακάμπτει τις διαταραγμένες πληροφοριακές και τηλεπικοινωνιακές δυνατότητες με σκοπό να διασφαλίσει ότι οι Κρίσιμες Επιχειρησιακές Δραστηριότητες μπορούν να συνεχισθούν μέσα σε

ένα ελάχιστο χρονικό διάστημα, προκαθορισμένο από τον οργανισμό, σε καθορισμένα επίπεδα υπηρεσίας.

Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery Plan / DRP) :

1. Το Σχέδιο Ανάκαμψης από Καταστροφή αποτελεί μια τεκμηριωμένη διεργασία ή σύνολο διαδικασιών για την ανάκαμψη και την προστασία της πληροφοριακής υποδομής μιας επιχείρησης στην περίπτωση Καταστροφής.
2. Πρόκειται για ένα σαφώς καθορισμένο και τεκμηριωμένο σχέδιο σύμφωνα με το οποίο ανακάμπτουν οι πληροφοριακές και οι τηλεπικοινωνιακές δυνατότητες μετά από μία καταστροφή. Συνήθως καλύπτει το κρίσιμο προσωπικό, τους πόρους, τις υπηρεσίες και τις ενέργειες που απαιτούνται ώστε τα πληροφοριακά συστήματα που υποστηρίζουν τις κρίσιμες επιχειρησιακές διεργασίες να συνεχίσουν να λειτουργούν σε προκαθορισμένα επίπεδα διαταραχής. Για ένα οργανισμό που στηρίζεται σε μεγάλο βαθμό από τα πληροφοριακά συστήματα, το Σχέδιο Ανάκαμψης από Καταστροφή αποτελεί απαραίτητο στοιχείο του Σχεδίου Επιχειρησιακής Συνέχειας.

Χώρος Ανάκαμψης ή Εναλλακτικός χώρος λειτουργίας (Recovery Site) : Προσωρινές εγκαταστάσεις που συντηρεί η επιχείρηση, σε διαφορετικό χώρο από τον χώρο κανονικής λειτουργίας, με σκοπό την κάλυψη των αναγκών εναλλακτικής λειτουργίας σε περίπτωση διακοπής των εργασιών. Ο Εναλλακτικός χώρος λειτουργίας ή χώρος ανάκαμψης περιλαμβάνει και τις απαιτούμενες υποδομές ανάκαμψης (θέσεις εργασίας, δίκτυα, εξοπλισμό, τηλεπικοινωνίες κ.λπ.)

Ελάχιστο Επίπεδο Ανακάμψεως (Minimum Business Continuity Objective) :

1. Είναι το ελάχιστο επίπεδο υπηρεσιών ή/και προϊόντων το οποίο πρέπει να εξασφαλίσει ο Οργανισμός για να επιτύχει τους επιχειρησιακούς του στόχους μετά από ένα περιστατικό, έκτακτη κατάσταση ή καταστροφή. Ο Ελάχιστος Στόχος Επιχειρησιακής Συνέχειας καθορίζεται από την Διοίκηση του Οργανισμού και ενδέχεται να επηρεάζεται, ορίζεται ή/και να τροποποιείται με βάση τις απαιτήσεις του κανονιστικού πλαισίου ή τις πρακτικές που εφαρμόζονται στον Τομέα/Βιομηχανία που δραστηριοποιείται ο Οργανισμός.

2. Το Ελάχιστο επίπεδο υπηρεσιών ή/και προϊόντων το οποίο είναι αποδεκτό από τον Οργανισμό προκειμένου να επιτύχει τους επιχειρησιακούς του στόχους μετά από διακοπή εργασιών.

Επιθυμητός Χρόνος Ανάκαμψης (Recovery Time Objective) :

1. Είναι η μέγιστη αποδεκτή διάρκεια διακοπής που μπορεί να μεσολαβήσει, πριν η έλλειψη λειτουργίας μιας επιχειρησιακής δραστηριότητας έχει σοβαρή επίπτωση στον Οργανισμό. Αυτός είναι και ο μέγιστος συμφωνημένος χρόνος για την επαναφορά των κρίσιμων επιχειρησιακών λειτουργιών.

Ο Χρονικός Στόχος Ανάκαμψης (RTO- Recovery Time Objective) υπολογίζεται αφού αθροιστούν οι ακόλουθοι χρόνοι : Ο χρόνος από την στιγμή της καταστροφής, συμπεριλαμβανομένων των χρόνων για την ενεργοποίηση του Σχεδίου (κήρυξη της καταστροφής) και για την εκτέλεση των ενεργειών (που προβλέπονται στο Σχέδιο BCP ή DR), έως την στιγμή που υπάρχει ανάκαμψη των επιχειρησιακών λειτουργιών ή αποκατάσταση των συστημάτων και των δεδομένων τους.

2. Η Χρονική Διάρκεια που ακολουθεί μετά από κάποιο γεγονός, εντός της οποίας :

-Ένα προϊόν ή μία υπηρεσία πρέπει να επαναλειτουργήσει -Μια δραστηριότητα/λειτουργία πρέπει να επαναλειτουργήσει - Οι πόροι να αποκατασταθούν Σημείωση : Για προϊόντα, υπηρεσίες και δραστηριότητες, ο χρόνος ανάκαμψης (RTO) πρέπει να είναι μικρότερος από την Μέγιστη Ανεκτή Περίοδο Διακοπής (Maximum Tolerable Period of Disruption), δηλαδή την περίοδο μετά την οποία η διακοπή της υπηρεσίας ή του προϊόντος μπορεί να προκαλέσει ανεπανόρθωτη ζημιά στον Οργανισμό.

Χρονικό Σημείο Ανάκτησης Δεδομένων (Recovery Point Objective) :

1. Είναι το χρονικό σημείο πριν τη διακοπή, στο οποίο τα συστήματα και τα δεδομένα που περιέχουν πρέπει να ανακάμψουν μετά από τη διακοπή, ώστε να μην επηρεαστούν οι εργασίες.

Για παράδειγμα τα δεδομένα πρέπει να αποκατασταθούν στην αρχή της ημέρας. Περιλαμβάνει το σύνολο των δεδομένων που πρέπει να ανακτηθούν ή επανεισαχθούν μετά την επαναφορά των συστημάτων και των εργασιών σε λειτουργία. Σχετικοί όροι : Στόχοι ανάκαμψης, Χρονικό στόχος Ανάκαμψης (RTO).

Σημείο στο οποίο η πληροφορία που χρησιμοποιείται από μια δραστηριότητα πρέπει να αποκατασταθεί ώστε να καταστεί δυνατή η λειτουργία και η επαναφορά της. Σημείωση :

Αναφέρεται επίσης και ως "Μέγιστη Απώλεια Δεδομένων" (Maximum Data Loss) Πηγή: ISO22301

Μέγιστη Ανεκτή Περίοδος Διακοπής (Maximum Tolerable Period of Disruption) :

Είναι το μέγιστο χρονικό διάστημα κατά το οποίο είναι ανεκτό τα βασικά προϊόντα ή υπηρεσίες του Οργανισμού να μην είναι διαθέσιμα πριν η επίπτωση από τη μη διαθεσιμότητά να χαρακτηριστεί ως μη αποδεκτή ή / και να τεθεί θέμα επιβίωσης του Οργανισμού.

Κίνδυνος (Risk) :

1. Κίνδυνος είναι η πιθανή έκθεση σε ζημιά λόγω κάποιας απειλής, η οποία προκαλεί διακοπή στις επιχειρησιακές λειτουργίες και εμποδίζει την επίτευξη του ελάχιστου στόχου επιχειρησιακής συνέχειας.
2. Η επίπτωση της αβεβαιότητας στους στόχους.

Σημείωση (1) : Ένα αποτέλεσμα ή μια απόκλιση (θετική ή αρνητική) από το αναμενόμενο. Σημείωση (2) : Οι στόχοι μπορεί να έχουν πολλές πτυχές (π.χ. οικονομικοί, υγείας, ασφάλειας και περιβαλλοντικοί στόχοι) και μπορούν να εφαρμοστούν σε διάφορα επίπεδα (π.χ. στρατηγικό επίπεδο, σε επίπεδο Οργανισμού, έργου, προϊόντος, διαδικασίας) . Ένας στόχος μπορεί να εκφραστεί με άλλους τρόπους, π.χ. με βάση το επιδιωκόμενο αποτέλεσμα, επιχειρησιακά κριτήρια, στόχος επιχειρησιακής συνέχειας ή με την χρήση όρων που έχουν παρόμοια σημασία (π.χ. σκοπός). Σημείωση (3) : Ο κίνδυνος συχνά χαρακτηρίζεται σε σχέση με πιθανά γεγονότα και συνέπειες ή με συνδυασμό και των δύο. Σημείωση (4) : Ο κίνδυνος συχνά εκφράζεται από τον συνδυασμό των συνεπειών που προκύπτουν από κάποιο γεγονός (συμπεριλαμβανομένων των αλλαγών στις συνθήκες) και της σχετιζόμενης πιθανότητας εμφάνισης του κινδύνου Σημείωση (5) : Αβεβαιότητα είναι η κατάσταση, έστω και μερική, έλλειψης πληροφόρησης, κατανόησης ή γνώσης σχετικά με κάποιο γεγονός καθώς και των επιπτώσεων ή της πιθανότητας εμφανίσεώς του. Σημείωση (6) : Στο πλαίσιο των προτύπων για το Σύστημα Διαχειρίσεως Επιχειρησιακής Συνέχειας (Σ.Δ.Ε.Σ.) , οι στόχοι επιχειρησιακής συνέχειας καθορίζονται από τον Οργανισμό με βάση την πολιτική επιχειρησιακής συνέχειας και τα αποτελέσματα που επιδιώκει ο Οργανισμός. Ο όρος "κίνδυνος" σχετίζεται με τους στόχους του Οργανισμού και δεν περιορίζεται μόνο στους στόχους επιχειρησιακής συνέχειας.

Επίπτωση (Impact) :

Επίπτωση είναι η αξιολόγηση συνεπειών μιας συγκεκριμένης πράξης, όπως η εκδήλωση μιας απειλή.

Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis) :

1.Η Ανάλυση Επιχειρησιακών Επιπτώσεων αποτελεί μία φάση στη Μεθοδολογία Σχεδιασμού Επιχειρησιακής Συνέχειας.

Είναι η διεργασία ανάλυσης των αποτελεσμάτων της διακοπής των επιχειρησιακών λειτουργιών ή διεργασιών σε όλες τις επιχειρησιακές δραστηριότητες.

Μεθοδολογία Σχεδιασμού Ανάκαμψης από Καταστροφή.

Σημείωση 1 : Η Ανάλυση Επιχειρησιακών Επιπτώσεων θα πρέπει να εντοπίζει όλες τις κρίσιμες επιχειρησιακές δραστηριότητες, να εκτιμά ποιοτικά ή/και ποσοτικά τις απώλειες διακοπών και να καθορίζει τα επιτρεπτά διαστήματα μη διαθεσιμότητας και τους ελάχιστους πόρους που απαιτούνται για την ανάκαμψη των κρίσιμων επιχειρησιακών δραστηριοτήτων.

Σημείωση 2 : Συνήθως, στο πρώτο έργο Σχεδιασμού Επιχειρησιακής Συνέχειας σε ένα οργανισμό θα πρέπει να εμπλέκονται όλες οι επιχειρησιακές μονάδες στη φάση της Ανάλυσης Επιχειρησιακών Επιπτώσεων. Σε επόμενα έργα Σχεδιασμού Επιχειρησιακής Συνέχειας χρειάζεται η εμπλοκή μονάχα των επιχειρησιακών μονάδων που διεξάγουν κρίσιμες επιχειρησιακές δραστηριότητες, εφόσον δεν υπάρχουν σημαντικές οργανωτικές αλλαγές.

Μεθοδολογία Σχεδιασμού Διαχείρισης Επιχειρησιακής Συνέχειας (BCM Planning Process or Methodology) :

Η Μεθοδολογία Σχεδιασμού Διαχείρισης Επιχειρησιακής Συνέχειας αποτελεί την διαδικασία υλοποίησης κάθε Σχεδίου Επιχειρησιακής Συνέχειας. Αποτελείται από τις εξής φάσεις :

Διαχείριση Έργου Ανάλυση και Ανασκόπηση Κινδύνων Ανάλυση Επιχειρησιακών Επιπτώσεων Στρατηγική Επιχειρησιακής Συνέχειας Ανάπτυξη Σχεδίου Δοκιμές και Ασκήσεις Διαχείρισης Προγράμματος.

2. Σειρά δραστηριοτήτων επιχειρησιακής συνέχειας οι οποίες συνολικά καλύπτουν όλες τις διαστάσεις και τις φάσεις του προγράμματος Διαχείρισης Επιχειρησιακής Συνέχειας.

Κύκλος Ζωής Επιχειρησιακής Συνέχειας (Business Continuity Life Cycle) :

Ο Κύκλος Ζωής Επιχειρησιακής Συνέχειας αποτελείται από τα παρακάτω στάδια :

1. Πρόληψη : η περίοδος του χρόνου πριν την καταστροφή 2. Απόκριση : οι ώρες και μέρες αμέσως μετά την καταστροφή 3. Ανάκαμψη : η περίοδος από την εκδήλωση της καταστροφής έως την έναρξη προσωρινών εργασιών ή εναλλακτικής μεθόδου εργασίας 4. Επαναφορά : ο χρόνος στον οποίο οι επιχειρησιακές δραστηριότητες και λειτουργίες ανακάμπτουν από εναλλακτική τοποθεσία 5. Αποκατάσταση : η επαναφορά μη κρίσιμων δραστηριοτήτων και κατεστραμμένων υποδομών 6. Επιστροφή : ο χρόνος στον οποίο οι δραστηριότητες επιστρέφουν στην κανονική λειτουργία.

Κρίσιμες Επιχειρησιακές Δραστηριότητες (Critical Business Functions) :

Κρίσιμες Επιχειρησιακές Δραστηριότητες είναι εκείνες που θα πρέπει να αποκατασταθούν στην περίπτωση περιστατικού διαταραχής, ώστε να διασφαλιστεί η ικανότητα του οργανισμού να προστατεύσει του πόρους του, να καλύψει τις ανάγκες του και να τηρήσει τις νομικές / κανονιστικές του υποχρεώσεις.

Αποτελούν εταιρικές δραστηριότητες και πληροφορίες οι οποίες δεν θα πρέπει να διαταράσσονται σε βαθμό που να επηρεάζεται η ικανότητα του οργανισμού να επιτύχει τους Ελάχιστους Στόχους Επιχειρησιακής Συνέχειας που έχει θέσει.

2.2 Ένα σύντομο Ιστορικό της Επιχειρησιακής Συνέχειας & Εξέλιξη

Αν και ο ορισμός του Σχεδιασμού της Επιχειρησιακής Συνέχειας θεσπίστηκε την δεκαετία του 1970, παρολαυτά η έννοια του μπορούμε να αναφέρουμε ότι έχει χρησιμοποιηθεί στην αρχαιότητα. Ένας από τους μεγαλύτερους στρατηγούς όλων των εποχών που έδρασε πριν από 2.600 χρόνια περίπου ήταν ο Sun Tzu, ήταν ο πρώτος που επισήμανε την ανάγκη για αποθήκευση όπλων και τον σχεδιασμό σεναρίων που σκοπό είχαν την προετοιμασία για την αντιμετώπιση εχθρικών διενέξεων.

Ζωτικής σημασίας δεκαετίες οι 1970-1980-1990

Η εταιρία Royal Dutch Shell γνωστή ως Shell που δραστηριοποιείται σε όλους τους τομείς της βιομηχανίας πετρελαίου και φυσικού αερίου, συμπεριλαμβανομένη της εξερεύνησης και παραγωγής, διύλισης, τη διανομή και το εμπόριο υπήρξε ο αρωγός χρήσης σχεδίων επιχειρησιακής συνέχειας στις αρχές περίπου του 1970. Ο Pierre Wack στέλεχος της Shell και υπεύθυνος Επιχειρησιακού Σχεδιασμού πρόβλεψε ότι ο Ο.Π.Ε.Κ. (Οργανισμός Εξαγωγών

Πετρελαιοπαραγωγών Χωρών) θα απαιτούσε υψηλότερες τιμές στο πετρέλαιο μετά τον πόλεμο του Yom Kippur το 73 στην Μέση Ανατολή. Η ομάδα επιχειρησιακού σχεδιασμού της Shell κατάφερε να προετοιμαστεί κατάλληλα για την συγκεκριμένη ασυνέχεια και η Shell να μετατραπεί σε μια από τις ισχυρότερες εταιρίες του κλάδου. Η ομάδα όμως δεν σταμάτησε εκεί, μέσω της εταιρίας Iron Mountain προχώρησε στην φύλαξη και αποθήκευση των πληροφοριακών της δεδομένων αυτό σηματοδοτούσε την έναρξη του Επιχειρησιακού Σχεδιασμού και Αποκατάστασης Καταστροφών (Business Continuity / Disaster Recovery) στην αγορά.

Επιπλέον , ήδη την ίδια δεκαετία η εταιρία Sun Company που δραστηριοποιούνταν και εκείνη στην πετρελαϊκή αγορά, δημιούργησε μια θυγατρική εταιρία την SunGard. Η τελευταία δραστηριοποιούνταν κυρίως στο να παρέχει υποστήριξη μέσω απομακρυσμένης πρόσβασης επεξεργασίας δεδομένων στην μητρική εταιρία. Η Sun Company ήταν σε μεγάλο βαθμό εξαρτώμενη από τις τεχνολογικές υπηρεσίες της θυγατρικής με αποτέλεσμα οποιαδήποτε αποτυχία χρήσης Υ/Η να επέφερε απώλειες πολλών χιλιάδων δολαρίων . Αυτό είχε ως απώτερο αποτέλεσμα την καθημερινή αντιγραφή ταινιών ασφαλείας και την αποθήκευση δεδομένων σε εφεδρικούς υπολογιστές με σκοπό την εκμηδένιση ή και μετριασμό οποιασδήποτε διακοπής προσωρινής ή μόνιμης στον κεντρικό υπολογιστή. Σήμερα η SunGard Recovery Services είναι μια από τις μεγαλύτερες εταιρίες υπηρεσιών αποκατάστασης παγκοσμίως.

Προς το τέλος της δεκαετίας του 1980 περισσότερες από 100 εταιρίες παροχής αποκατάστασης από καταστροφή είχαν ιδρυθεί στις Η.Π.Α. με αρωγούς τις IBM, SunGard και Comdisco.

Στα μέσα της δεκαετίας του 1990, η Επιχειρησιακή Συνέχεια συνδέονταν κυρίως με την αποκατάσταση τεχνολογικών, επικοινωνιακών και δικτυακών περιστατικών, λίγοι οργανισμοί ήταν εκείνοι που εφάρμοζαν σχέδια αποκατάστασης καταστροφών. Οι Τραπεζικοί και Χρηματοπιστωτικοί Όμιλοι καθώς προετοίμαζαν τα σχέδια έκτακτης ανάγκης για το έτος 2000 επεσήμαναν την ανάγκη για επέκταση της Επιχειρησιακής Συνέχειας σε όλες τις επιχειρησιακές διαδικασίες και όχι μόνο στις τεχνολογικές.

Τα γεγονότα της 11ης Σεπτεμβρίου 2001 ήταν εκείνα που επαναπροσδιόρισαν την Επιχειρησιακή Συνεχεία σε μια νέα βάση. Η καταστροφή ήταν καθολική και ανεπανόρθωτη, οι συγκοινωνίες παρεμποδιζόταν, οι μεταφορές είχαν διακοπεί, και εξαιτίας αυτής την κατάστασης υπήρξε η συλλογική ανάγκη από όλους τους οργανισμούς και επιχειρήσεις να διαθέτουν ολοκληρωμένα σχέδια Επιχειρησιακής Συνέχειας. Προέκυψαν αρκετά διδάγματα που απώτερο σκοπό είχαν την βελτίωση των υφισταμένων σχεδίων . Πλέον τα σχέδια αυτά έπρεπε να ενημερώνονται σε τακτά χρονικά διαστήματα καθώς και να δοκιμάζονται. Οι υπεύθυνοι ασφαλείας των επιχειρήσεων όφειλαν να προετοιμάζονται ανάλογα για μια σειρά από πιθανές απειλές(φυσικές καταστροφές , τρομοκρατικές επιθέσεις κ.α.). Να λαμβάνονται υπόψη οι πιθανές αλληλεξαρτήσεις λειτουργιών και μη μιας επιχείρησης . Ο εναλλακτικός χώρος λειτουργίας να απέχει αρκετή απόσταση από τον παραγωγικό χώρο έτσι ώστε οποιαδήποτε καταστροφή να μην επιφέρει καταστροφές στον χώρο ανάκαμψης. Αντίγραφα των σχεδίων θα πρέπει να βρίσκονται και σε χώρους εκτός του παραγωγικού όπου στην καλύτερη περίπτωση ψηφιοποιημένα μπορούν να ανακτηθούν από οπουδήποτε.

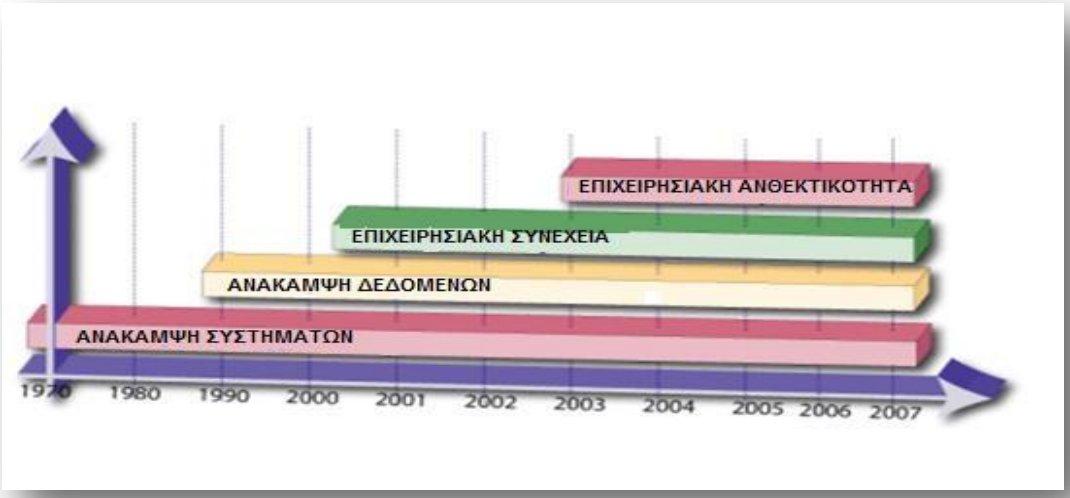
Από το τρομοκρατικό χτύπημα το 2001 στις Η.Π.Α. έχουν καταγραφεί στην διεθνή βιβλιογραφία μια σειρά από εξίσου καταστροφικά γεγονότα. 2004 τσουνάμι στην Ινδονησία, 2005 τυφώνας Κατρίνα, 2010 διαρροή πετρελαίου από λάθος ενέργεια της πετρελαϊκής εταιρίας BP στον κόλπο του Μεξικού, 2010 το ηφαιστειακό νέφος από την Ισλανδία που κάλυψε μεγάλο μέρος της Ευρώπης, 2012 ο τυφώνας Sandy που εξαιτίας του πολλές περιοχές των Η.Π.Α. τέθηκαν σε κατάσταση εκτάκτου ανάγκης 2013 σεισμός 7.2 της κλίμακας Ρίχτερ σειεί τις Φιλιππίνες σκορπώντας τον πανικό 2015 η μεγαλύτερη ασφαλισμένη ζημιά κατά περιουσίας το 2015 – ύψους περίπου 3,5 δισεκατομμυρίων δολαρίων - ήταν οι δύο μεγάλες εκρήξεις στο λιμάνι της Tianjin. Η πόλη είναι από τα σημαντικότερα βιομηχανικά κέντρα της Κίνας και ένα από τα πιο πολυσύχναστα λιμάνια του κόσμου. Περισσότερα από 700 άτομα τραυματίστηκαν και 150 άνθρωποι έχασαν τη ζωή τους από την έκρηξη που σημειώθηκε σε μια αποθήκη που περιείχε τοξικά χημικά. Καταστράφηκαν οικοδομικά τετράγωνα και κάηκαν χιλιάδες οχήματα**.** Η μελέτη της Swiss Re αξίζει να σημειωθεί περιέχει ειδικό κεφάλαιο για το Tianjin και την διαπιστωμένη συσσώρευση κινδύνου σε μεγάλα κέντρα μεταφορών όπως είναι οι λιμένες.

Το συμβάν στο λιμάνι της Tianjin, λόγω του μεγέθους της έκρηξης και της τεράστιας έκθεσης περιουσιακών στοιχείων στον κίνδυνο, καθίστανται ως η μεγαλύτερη ασφαλισμένη ζημιά

προερχόμενη από ανθρώπινο λάθος που έχει συμβεί ποτέ όχι μόνο στην Ασία αλλά και παγκοσμίως.

Εξέλιξη

Τα πρώτα σχέδια που εμφανίστηκαν ήταν τα Σχεδία Ανάκαμψης από Καταστροφή (Disaster Recovery Plan) την δεκαετία 1970 και επικεντρώνονταν κυρίως στην ανάκτηση των πληροφοριακών συστημάτων. Αρχές όμως της δεκαετίας του 1990 αναδεικνύεται η ανάγκη ανάκτησης επιχειρησιακών δεδομένων ,εντοπίζεται δηλαδή η αναγκαιότητα ανάπτυξης διαδικασιών και εφαρμογών για την ανάκτηση δεδομένων σε περίπτωση βλάβης των συστημάτων. Σήμερα βρισκόμαστε στην εποχή της επιχειρησιακής ανθεκτικότητας (Business Resiliency) που αφορά την πρόληψη της καταστροφής. Αυτό σημαίνει άμεση προσαρμογή και ανταπόκριση του οργανισμού σε καταστάσεις έκτακτης ανάγκης για την επιβίωση τους σε μία δύσκολη εποχή συνεχών προκλήσεων. Την τελευταία δεκαετία παρατηρείται ότι ο στρατηγικός σχεδιασμός των επιχειρήσεων για την συνέχεια των εργασιών τους και την ανάπτυξη επίσημων Σχεδίων Επιχειρησιακής Συνέχειας τους, έχει εξελιχθεί σε κύρια δραστηριότητα της εταιρικής διακυβέρνησης. Παράλληλα η χρήση του Διαδικτύου ως υποστηρικτικό εργαλείο στις επιχειρησιακές διαδικασίες έχει ως αποτέλεσμα τα θέματα των τεχνολογιών της πληροφορικής και των επικοινωνιών να βρίσκονται στο επίκεντρο των επιχειρησιακών αποφάσεων. Έτσι όπως διαμορφώνονται σήμερα οι συνθήκες για μια σύγχρονη επιχείρηση, η ανάπτυξη και υλοποίηση ενός ΣΕΣ βασισμένου σε ένα οργανωμένο πλαίσιο διαχείρισης κινδύνων είναι παραπάνω από απαραίτητη. Ενώ παλαιότερα αποτελούσε απλώς μία δράση σήμερα προβάλει ως επιτακτική ανάγκη συνυφασμένη με την ίδια τη βιωσιμότητα της ιδίας.



Εικόνα 1. *Εξέλιξη της Επιχειρησιακής Συνέχειας από το 1970 έως σήμερα.*

Κεφάλαιο 3

3.1 Βασικά είδη καταστροφών

Η αδιάκοπτη λειτουργία μιας επιχείρησης καθώς και η ανάκαμψη των κρίσιμων λειτουργιών της με το πέρας ή κατά την διάρκεια μιας καταστροφής αποτελεί πρώτιστο κίνητρο για την εφαρμογή ενός δομημένου Σχεδίου Επιχειρησιακής Συνέχειας . Ο ορισμός της καταστροφής διαφέρει σε κάθε οργανισμό και εξαρτάται από τον χώρο δραστηριότητάς του καθώς και την τεχνολογική του δομή. «Ο όρος καταστροφή χρησιμοποιείται για να περιγράψει το σύνολο των αρνητικών αποτελεσμάτων μεγάλης κλίμακας, ως αποτέλεσμα της εκδήλωσης ενός φαινομένου. Χαρακτηρίζουμε ένα φαινόμενο καταστροφικό όταν προκαλεί ευρείας κλίμακας είτε κοινωνικής είτε οικονομικής φύσεως απώλειες»(Κώστας Μακρόπουλος *Καθηγητής Σεισμολογίας Πανεπιστήμιο Αθηνών, Πρόεδρος του Οργανισμού Αντισεισμικού Σχεδιασμού και Προστασίας (ΟΑΣΠ)).*

Οι σημαντικότερες αιτίες που μπορούν να προκαλέσουν διακοπή εργασιών καθώς και διαρκή διακοπή πληροφοριακών συστημάτων διακρίνονται :

Στις **φυσικές** και αφορούν περιστατικά που οφείλονται σε περιβαλλοντικούς παράγοντες όπως :

- σεισμοί
- πυρκαγιές
- πλημμύρες
- τυφώνες
- κατολισθήσεις
- ηφαίστεια
- ακραία καιρικά φαινόμενα

Στις καταστροφές από **ανθρώπινη ενέργεια ,λάθη, παραλείψεις, άγνοια , δόλο** και αναφέρεται ενδεικτικά:

- Ανθρώπινο λάθος/άγνοια
- διαρροή επικίνδυνων ουσιών/μόλυνση
- Ανθρώπινος δόλος: τρομοκρατικές ενέργειες /hacking
- εξεγέρσεις/κοινωνικές αναταραχές

Σε τεχνολογικά σφάλματα μπορεί να οφείλονται σε :

- δυσλειτουργία εξοπλισμού
- λάθη συστήματος
- πτώση /απώλεια ενέργειας
- απώλεια επικοινωνιών

Και τέλος ενδεικτικά αναφέρονται καταστροφές όπως :

- πανδημίες
- οικονομική κατάρρευση

3.2 Επιπτώσεις καταστροφών σε επίπεδο επιχειρήσεων

Το μέγεθος της απώλειας από μία καταστροφή μπορεί να εκτείνεται από την διακοπή ορισμένων καθημερινών κρίσιμων και μη λειτουργιών ή συστημάτων ενός οργανισμού έως και την ακραία περίπτωση της απώλειας ανθρώπινων ζωών. Κατώθι γίνεται μια προσπάθεια κατηγοριοποίησης αυτών των συνεπειών.

Υγιεινή και Ασφάλεια

Η βασικότερη συνέπεια ύστερα από μια καταστροφή είναι εκείνη που σχετίζεται με τις περιβαλλοντικές επιπτώσεις καθώς και τις ανθρώπινες απώλειες. Οργανισμοί που διαθέτουν μηχανήματα που διαχειρίζονται ή ελέγχουν επικίνδυνα υλικά διακατέχουν ιδιαίτερη βαρύτητα επειδή μια πιθανή βλάβη τους μπορεί να προκαλέσει ανυπολόγιστες περιβαλλοντολογικές καταστροφές. Για τον λόγο αυτό έχει θεσπιστεί η Ευρωπαϊκή νομοθεσία που σχετίζεται με την Υγιεινή και την Ασφάλεια στο χώρο εργασίας(89/391/EEC(12/6/1989).

Νομικές

Η αλήθεια είναι ότι ζούμε στην ψηφιακή εποχή. Σχεδόν τα πάντα λειτουργούν με τη χρήση ενός πληροφοριακού συστήματος. Όλα τα συστήματα, δημόσιοι και ιδιωτικοί φορείς, κράτη, οργανισμοί, εταιρίες διαχειρίζονται μεγάλες ή μικρότερες ποσότητες ψηφιακών δεδομένων. Αυτός ο τεράστιος όγκος πληροφοριών χρειάζεται μια σωστή και ασφαλή διαχείριση. Τα δεδομένα αυτά μπορεί να είναι είτε δημόσιες πληροφορίες είτε εμπιστευτικές ή ακόμα περισσότερο προσωπικά δεδομένα τρίτων. Οποιοδήποτε καταστροφικό περιστατικό απώλειας ή και μη διαθεσιμότητας ψηφιακών δεδομένων και ιδιαίτερα εκείνων που είναι

χαρακτηρισμένα ως εμπιστευτικά μπορεί να οδηγήσει σε πρόστιμα και νομικές κυρώσεις βάσει νομικών και κανονιστικών υποχρεώσεων.

Λειτουργικές

Η προσωρινή απώλεια ή μη διαθεσιμότητα κρίσιμων πόρων μπορεί να οδηγήσει τόσο σε άμεσες όσο και σε έμμεσες καταστροφικές συνέπειες μιας κρίσιμης υπηρεσίας ή ακόμη και ολόκληρου το Οργανισμού. Το απρόοπτο γεγονός μπορεί να προκαλέσει καταστροφές στις εγκαταστάσεις του Οργανισμού ,στον Server ή ακόμα και στο φυσικό αρχείο. Η μόνιμη απώλεια σε συνδυασμό με την αδυναμία αντικατάστασης των πόρων δημιουργεί την ανάγκη για επιπρόσθετο χρόνο εκτέλεσης μιας εργασίας γεγονός το οποίο μπορεί να οδηγήσει σε ακόμη μεγαλύτερες επιπτώσεις.

Υστεροφημία

Η φήμη κάθε επιχείρησης αποτελεί κυρίαρχο στοιχείο και σχετίζεται άμεσα με την διαχείριση κρίσεων (Crisis Management) .Οι κρίσεις, όμως, ούτε «εξορκίζονται» ούτε αποσιωπούνται αλλά αντιμετωπίζονται με την προνοητικότητα και με τη συνεχή κατάλληλη προετοιμασία για να μην καταστρέψουν τη φήμη της επιχείρησης. Η συγκεκριμένη κατηγορία επιπτώσεων είναι από τις περισσότερο επικίνδυνες καθώς οι συνέπειες της είναι μακροχρόνιες και δύσκολα επουλώνονται. Ανεξάρτητα από τους οικονομικούς πόρους που διαθέτει μια επιχείρηση έννοιες της αξιοπιστίας και της εμπιστοσύνης δύσκολα αποκαθίστανται.

Άλλες

Εκτός από τις παραπάνω επιπτώσεις, υπάρχουν και επιπλέον επιπτώσεις οι οποίες σχετίζονται ανάλογα με τη φύση, το έργο και την αποστολή του οργανισμού. Χαρακτηριστικό παράδειγμα αποτελεί ένας αερολιμένας ή ένα νοσοκομείο. Σε τέτοιες περιπτώσεις η ύπαρξη διαδικασιών άμεσης ανάκαμψης θεωρείται απαιτητή, καθώς η απουσία τους μπορεί να έχει ανυπολόγιστο κόστος.

- Απώλεια πωλήσεων και άλλων εσόδων
- Επιπτώσεις στο όνομα και στη φήμη της εταιρίας
- Απώλεια ανταγωνιστικού πλεονεκτήματος

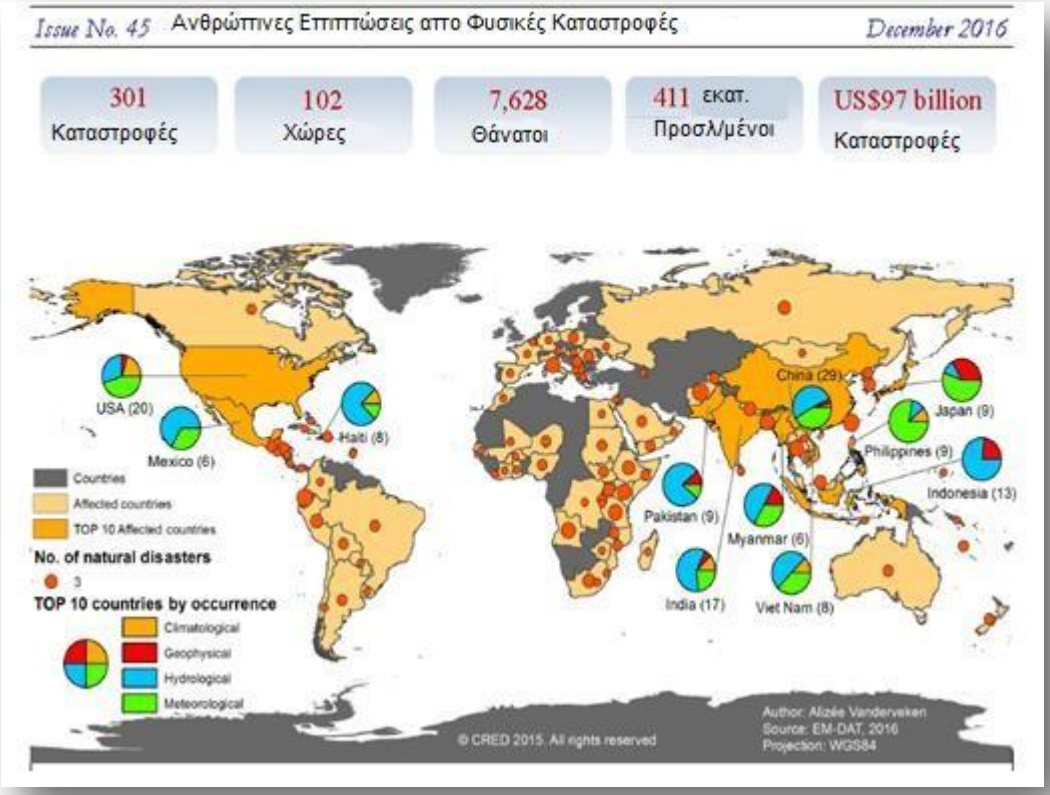
- Μείωση της εμπιστοσύνης των μετόχων / επενδυτών / πελατών
- Καθυστερήσεις στην εκτέλεση έργων / παραγγελιών / πληρωμών
- Αυξημένα ασφάλιστρα
- Νομικά / κανονιστικά προβλήματα
- Διοικητικές ευθύνες

Συμφώνα με έρευνα του Business Continuity Institute, το 25% των επιχειρήσεων που δεν ήταν «προετοιμασμένες για απρόβλεπτα γεγονότα» δεν ξανάνοιξαν ποτέ. Το 80% των επιχειρήσεων που δεν μπόρεσαν να λειτουργήσουν ξανά σε διάστημα ενός μηνός, τελικά έβαλαν λουκέτο. Και το 75% των επιχειρήσεων που μπόρεσαν να ξαναλειτουργήσουν, έκλεισαν οριστικά μέσα σε τρία χρόνια. Κάτι που επισημαίνεται στην έρευνα, είναι ότι όλες αυτές οι επιχειρήσεις ήταν ασφαλισμένες. Γίνεται άμεσα αντιληπτό επομένως ότι η σωστή και συστηματική πρόληψη αποτελεί φθηνότερη και αποτελεσματικότερη λύση από κάθε ενδεχόμενη ζημιά που θα μπορούσε να προσκληθεί χωρίς προετοιμασία.

3.3 Καταγραφή Φυσικών και Τεχνολογικών καταστροφών

Σε Διεθνές επίπεδο

Σε παγκόσμιο επίπεδο, είτε αναφερόμαστε σε ανεπτυγμένη είτε σε αναπτυσσόμενη χώρα, οι επιπτώσεις από φυσικές και τεχνολογικές καταστροφές είναι ανεπανόρθωτες. Αντλώντας στοιχεία από τη βάση δεδομένων περιστατικών έκτακτης ανάγκης (EM-DAT) που διατηρεί το Κέντρο Έρευνας για την Επιδημιολογία των Καταστροφών (Centre for Research on the Epidemiology of Disasters -CRED) καθώς και το Αμερικανικό Γραφείο Βοηθείας Καταστροφών Εξωτερικού (Office of U.S. Foreign Disaster Assistance-OFDA) εξάγονται οι κάτωθι χάρτες και πίνακες σε παγκόσμιο επίπεδο :



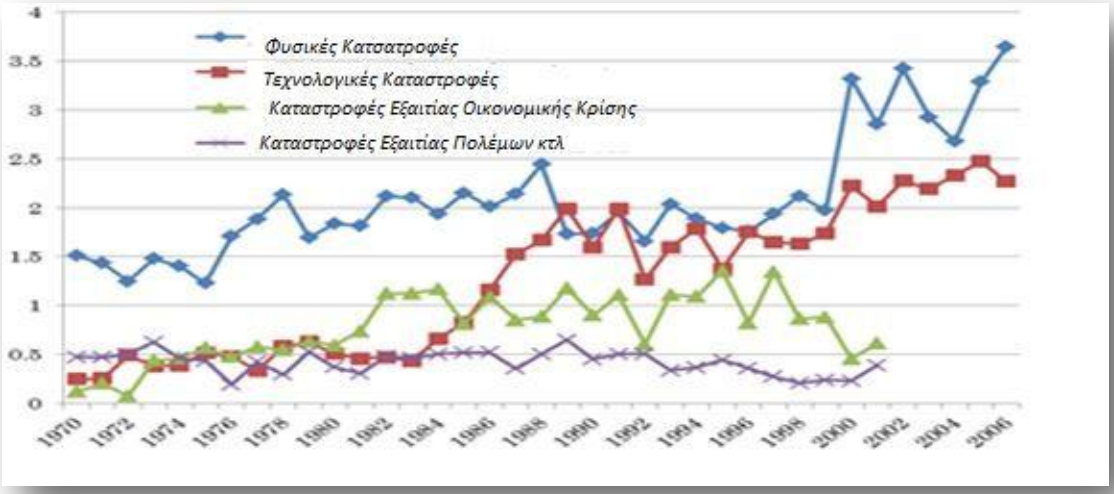
ΕΙΚΟΝΑ 2. *Ανθρώπινες απώλειες από φυσικές καταστροφές το 2016*

Οι 10 χώρες με τις περισσότερες ανθρώπινες και οικονομικές απώλειες από καταστροφές το 2016

Deaths		Deaths /100,000 inhabitants		Affected (million)		Affected/100,000 inhabitants	
China	1,151	Haiti	5.56	India	331.2	Micronesia	96,113
India	884	Fiji	5.16	China	13.0	Haiti	54,076
Ecuador	686	Ecuador	4.25	Ethiopia	10.2	Somalia	43,571
Korea Dem. Rep.	598	Korea Dem. Rep.	2.39	Malawi	6.5	Fiji	39,792
Haiti	596	Macedonia	1.06	Haiti	5.8	Marshall Islands	39,628
Pakistan	510	Rwanda	1.00	Somalia	4.7	Malawi	37,759
Italy	299	Sri Lanka	0.97	Zimbabwe	4.1	Mongolia	32,611
Indonesia	251	Taiwan	0.90	South Sudan	3.6	South Sudan	29,352
United States	250	Nepal	0.63	Viet Nam	3.6	Swaziland	27,196
Taiwan	212	Italy	0.49	Bangladesh	3.2	Zimbabwe	26,277

Πίνακας 1. *Οι 10 χώρες με τις μεγαλύτερες ανθρώπινες και οικονομικές απώλειες από καταστροφές το 2016*

Το κάτωθι σχήμα απεικονίζει την μέση εμφάνιση για καθένα από τα τέσσερα είδη καταστροφών, ανά χώρα, ετησίως. Διαπιστώνουμε ότι ενώ οι φυσικές και τεχνολογικές καταστροφές αυξάνονται με ταχείς ρυθμούς, η οικονομική κρίση και ο πόλεμος διατηρούν μια σταθερή και ελάχιστα αυξανόμενη τάση. Αυτές οι τάσεις καταστροφής δείχνουν πόσο απαραίτητη είναι η προετοιμασία αντιμετώπισης προκειμένου να ελαχιστοποιηθούν οι επιπτώσεις τους στο μέγιστο βαθμό που είναι εφικτό .



Εικόνα 3**.** *Συχνότητα εμφάνισης των τεσσάρων τύπων μεγάλων καταστροφών στον κόσμο (Μέσος όρος ανά χώρα) (http://www.rieti.go.jp/en/rieti_report/134.html).*

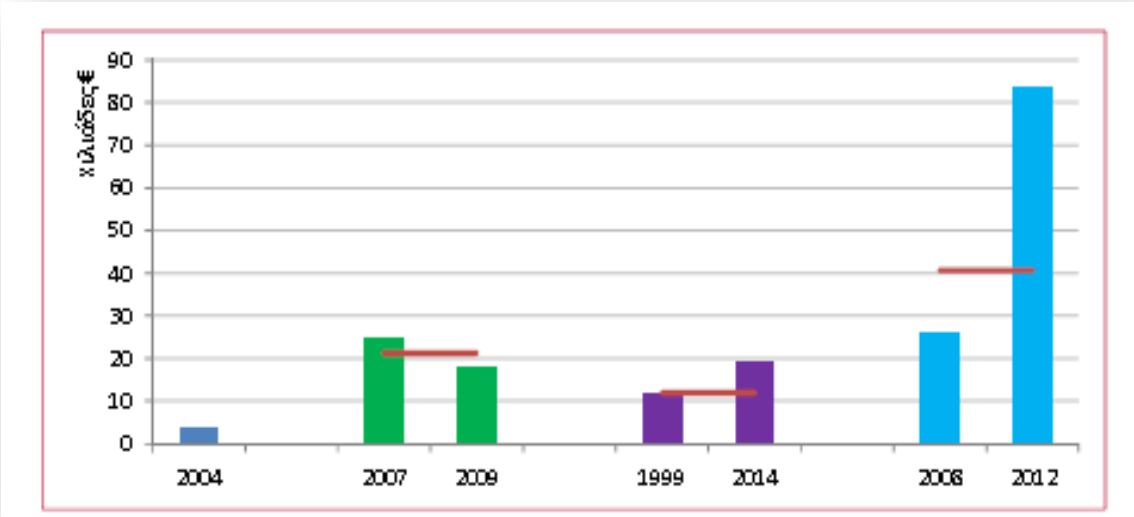
Σε Εθνικό επίπεδο

Σύμφωνα με μελέτη της Ε.Α.Ε.Ε. (Ένωση Ασφαλιστικών Εταιριών Ελλάδος) που έγινε μεταξύ των ασφαλιστικών επιχειρήσεων-μελών την χρονική περίοδο 1993-2014 αναφορικά με το πλήθος δηλωθέντων ζημιών και το ποσό απαίτησης καταστροφών μεγάλης έκτασης και έντασης το σύνολο των γεγονότων που έχουν συμβεί στην εν λόγω χρονική περίοδο υπολογίζεται σε 19.925 δηλωθείσες ζημιές με συνολικό ποσό απαίτησης περίπου 272,5 εκατ. €.

Α/Α	Ημερομηνία	Τόπος	Πλήθος Δηλωθέντων Ζημιών	Ποσό Απαίτησης (€)	Αιτία Ζημιάς
1.	30/11/1993	Αττική	358	4.554.600	Βροχοπτώσεις
2.	31/05/1994	Αττική	138	1.577.523	Βροχοπτώσεις
3.	21/10/1994	Αττική/Ελλάδα	1.159	26.077.872	Βροχοπτώσεις
4.	06/10/1996	Αττική	48	653.353	Βροχοπτώσεις
5.	30/11/1996	Θράκη	40	876.478	Βροχοπτώσεις
6.	12/01/1997	Αττική/Ελλάδα	311	6.909.486	Βροχοπτώσεις
7.	26/03/1998	Αττική/Ελλάδα	1.704	6.023.074	Βροχοπτώσεις
8.	07/09/1999	Αττική	9.480	110.934.694	Σεισμός
9.	08/07/2002	Αττική/Ελλάδα	1.350	28.621.262	Βροχοπτώσεις
10.	13/02/2004	Αττική/Ελλάδα	646	2.409.739	Χιονοπτώσεις
11.	17/09/2004	Θεσσαλονίκη	387	2.841.395	Βροχοπτώσεις
12.	05/11/2004	Αττική/Ελλάδα	209	1.930.133	Βροχοπτώσεις
13.	07-08/2007	Αττική/Ελλάδα	232	5.656.344	Δασικές Πυρκ.
14.	07/12/2008	Αττική/Ελλάδα	891	23.339.100	Ταραχές
15.	08/2009	Αττική	227	4.095.910	Δασικές Πυρκ.
16.	10/02/2012	Αττική	302	25.189.835	Ταραχές
17.	22/02/2013	Αττική	765	5.286.423	Βροχοπτώσεις
18.	22/11/2013	Ρόδος	93	3.441.998	Βροχοπτώσεις
19.	26/01/2014	Κεφαλονιά	415	7.824.348	Σεισμός
20.	24/10/2014	Αττική	1.170	4.296.297	Βροχοπτώσεις

Πίνακας 2. *Πλήθος δηλωθεισών ζημιών και το ποσό απαίτησης καταστροφών μεγάλης έκτασης 1993-2014 σύμφωνα με την (Πηγή Ε.Α.Ε.Ε).*

Στο παρακάτω γράφημα φαίνεται η μέση δηλωθείσα ζημία διαχρονικά, εκτός των βροχοπτώσεων.



Εικόνα 4. Χιονοπτώσεις, Δασικές πυρκαγιές, Σεισμός, Ταραχές και οι αντίστοιχες διαχρονικές μέσες τιμές. *(Πηγή Ε.Α.Ε.Ε)*

Η επέλευση φαινομένων φυσικών καταστροφών στην Ελλάδα γίνεται συχνά. Όμως, το ύψος των οικονομικών απωλειών τέτοιων φαινομένων παρουσιάζει έντονες διακυμάνσεις, γεγονός που προβληματίζει έντονα τις επιχειρήσεις, στο βαθμό που καλούνται να διαχειριστούν τέτοιας φύσεως κινδύνους. Όποιοι και να είναι οι λόγοι της αύξησης των καταστροφών, γίνεται φανερό ότι θα πρέπει να λαμβάνονται μέτρα με πιο εντατικούς ρυθμούς για την αντιμετώπιση της ολοένα αυξανόμενη συχνότητα εμφάνισης τους, αλλά και λόγω της μεγέθυνσης των επιπτώσεων τους.

3.4 Κατηγορίες σχεδίων αντιμετώπισης περιστατικών

Οι καταστροφές θα υπάρχουν στην ζωή μας έτσι και αλλιώς, δεν μπορούμε να τις προβλέψουμε όλες ούτε να αποτρέψουμε τον ερχομό τους, μπορούμε όμως με σχεδιασμό και κατάλληλη προετοιμασία να μετριάσουμε τις επιπτώσεις τους στο ελάχιστο. Η λειτουργία μιας επιχείρησης επηρεάζεται από πολλούς εξωτερικούς παράγοντες και γεγονότα που μπορούν να προκαλέσουν από μια αύξηση του φόρτου εργασίας, απώλειας εσόδων έως και την πλήρη διακοπή της λειτουργίας. Για τους άνωθι λόγους κρίνεται αναγκαία η εκπόνηση Σχεδίων Επιχειρησιακής Συνέχειας. Καταγραφή ενός συνόλου δηλαδή ενεργειών και διαδικασιών που θα επαναφέρουν τον οργανισμό σε άμεση λειτουργία και αποκατάσταση .Παρακάτω αναφέρονται τα είδη «σχεδίων αντιμετώπισης κρίσεων» όπως αυτά έχουν καταγραφεί από το NIST (National Institute of Standards and Technologies) .

Σχέδιο Επιχειρησιακής Συνέχειας

(Business Continuity Plan-BCP)
Το σχέδιο αυτό περιγράφει όλες τις διαδικασίες που οφείλει να ακολουθήσει μια επιχείρηση κατά την διάρκεια αλλά και με το πέρας ενός καταστροφικού γεγονότος ώστε να εξασφαλιστεί η αδιάλειπτη λειτουργία των κρίσιμων αλλά και μη εργασιών.

Σχέδιο Συνέχειας Λειτουργιών

(Continuity of Operations Plan-COOP)
Το σχέδιο αυτό αναφέρεται στην ανάκαμψη των κρίσιμων λειτουργιών ενός οργανισμού σε εναλλακτική τοποθεσία από την τοποθεσία παραγωγής. Ο Διεθνής Οργανισμός NIST προτείνει την ως στόχο του σχεδίου την δυνατότητα παροχής των εργασιών έως και 30 ημέρες πριν την πλήρη αποκατάσταση της αρχικής λειτουργίας. Διαφοροποιείται από το Σχέδιο Επιχειρησιακής

Συνέχειας στο ότι αφορά κυρίως τις κρίσιμες λειτουργίες και απευθύνεται σε κυβερνητικούς οργανισμούς και υπηρεσίες.

Σχέδιο Επικοινωνιών Κρίσης

(Crisis Communication Plan)
Το συγκεκριμένο σχέδιο περιγράφει τις απαραίτητες διαδικασίες που απαιτούνται για την επικοινωνιακή ενημέρωση του περιστατικού είτε εσωτερικά είτε εξωτερικά του οργανισμού. Στόχος του είναι η αποφυγή αρνητικής πληροφόρησης και ανήκει στις αρμοδιότητες του υπεύθυνου δημοσίων σχέσεων του οργανισμού.

Σχέδιο Προστασίας Κρίσιμων Υποδομών

(Critical Infrastructure Protection Plan-CIP)
Το σχέδιο αυτό αφορά κρίσιμες υποδομές εθνικής σημασίας. Ως κρίσιμες ορίζονται οι υποδομές που σχετίζονται με την ασφάλεια, την υγεία καθώς και την οικονομία ενός κράτους.

Σχέδιο Αντιμετώπισης Περιστατικών Κυβερνοχώρου

(Cyber Incident Response Plan-CIRP)
Το συγκεκριμένο σχέδιο λειτουργεί ως προσάρτημα του Σχεδίου Επιχειρησιακής Συνέχειας, αφορά κυρίως τμήματα πληροφορικής και ασφάλειας πληροφοριών καθώς καθορίζει τις διαδικασίες που πρέπει να ακολουθούμε σε περίπτωση μιας κυβερνοεπίθεσης.

Σχέδιο Ανάκαμψης από Καταστροφή

(Disaster Recovery Plan-DRP)
Το Σχέδιο Ανάκαμψης από Καταστροφή αφορά συνήθως καταστροφές που προσβάλλουν πληροφοριακά συστήματα ενός οργανισμού. Περιλαμβάνει καταγεγραμμένες διαδικασίες και οδηγίες όσον αφορά τη αποκατάσταση και συνέχιση της λειτουργίας των πληροφοριακών συστημάτων καθώς και μετάπτωση σε εφεδρικά συστήματα. Λειτουργεί ως συμπληρωματικά στο Σχέδιο Επιχειρησιακής Συνέχειας καθώς και στο Σχέδιο Συνέχειας Λειτουργιών.

Σχέδιο Αντιμετώπισης Καταστροφής Πληροφοριακών Συστημάτων

(Information System Contingency Plan-ISCP)
Αποτελεί μέρος ή παράρτημα του Σχεδίου Ανάκαμψης από Καταστροφή, αφορά την μερική ή και πλήρη ανάκαμψη ενός πληροφοριακού συστήματος και περιλαμβάνει όλες εκείνες τις διαδικασίες που πρέπει να ακολουθηθούν προς την συγκεκριμένη κατεύθυνση.

Σχέδιο Έκτακτης Ανάγκης Παρευρισκομένων

(Occupant Emergency Plan-OEP)

Εντός ενός Οργανισμού πλην των υπαλλήλων ίσως βρίσκονται και επισκέπτες, σκοπός του σχεδίου Έκτακτης Ανάγκης Παρευρισκομένων είναι η καταγραφή εκείνων των οδηγιών που πρέπει να ακολουθήσουν οι παρευρισκόμενοι κατά την εκδήλωση ενός απρόοπτου καταστροφικού γεγονότος, ώστε να εκκενωθεί με ασφάλεια το κτίριο. Το σχέδιο αυτά είναι προσαρμοσμένα κάθε φορά στις εκάστοτε ιδιαιτερότητες των κτιριακών εγκαταστάσεων του οργανισμού.

Σχέδιο Αντιμετώπισης Πανδημίας

(Pandemic Business Continuity Plan)

Βασική προϋπόθεση των εταιριών είναι η ανάπτυξη σχεδίου έκτακτης ανάγκης ώστε να περιοριστεί ο αντίκτυπος μιας επιδημίας γρίπης στους εργαζομένους και την επιχειρηματική δραστηριότητα. Αυτό πρέπει να εφαρμοσθεί για τρεις βασικούς λόγους :

Κοινωνική ευθύνη – πολλές επιχειρήσεις παρέχουν ζωτικής σημασίας υπηρεσίες που δεν μπορούν να ανασταλούν στη διάρκεια πανδημίας (π.χ. τρόφιμα, νερό, διάθεση απορριμμάτων) . Αυτές οι εταιρείες έχουν την κοινωνική ευθύνη να διασφαλίσουν τη συνέχιση της λειτουργίας τους ακόμη και αν το προσωπικό τους μειωθεί δραματικά.

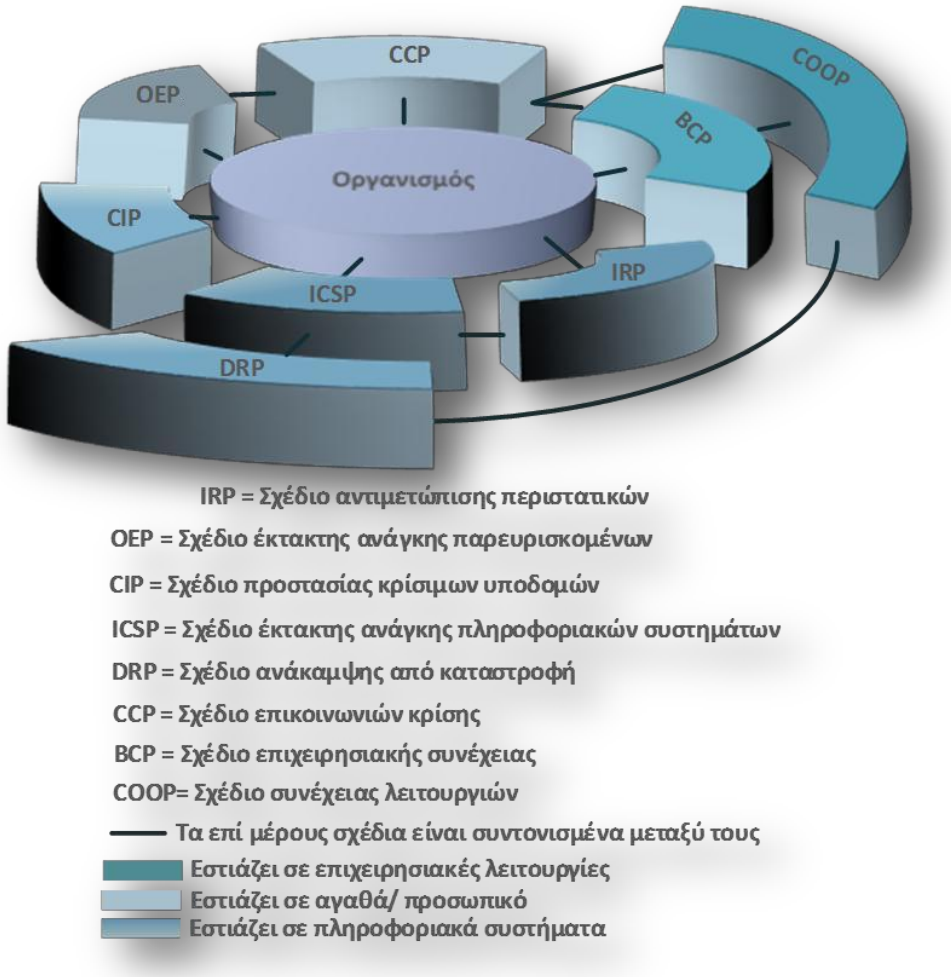
Ευεξία των εργαζομένων – δεν είναι οι εταιρείες που παράγουν αλλά οι άνθρωποι. Ο ανθρώπινος παράγοντας είναι ο πλέον σημαντικός πόρος σε οποιαδήποτε επιχείρηση. Η σωστή προετοιμασία για το ενδεχόμενο πανδημίας δεν μπορεί παρά να συμπεριλάβει και μέτρα για την προστασία αυτού του σημαντικού πόρου.

Αξία για τους μετόχους – η πανδημία γρίπης δεν είναι ένας κίνδυνος του οποίου την ύπαρξη αγνοούμε. Είναι λοιπόν υποχρέωση των ιθυνόντων των εταιρειών να ελαχιστοποιήσουν τον δυνητικό του αντίκτυπο. Στον κάτωθι πίνακα αναφέρεται συνοπτικά ο σκοπός, το πεδίο αναφοράς και ο συσχετισμός των σχεδίων αυτών.

Σχέδιο	Περιγραφή	Πεδίο Εφαρμογής	Συσχετισμός με άλλο Σχέδιο
Σχέδιο Επιχειρησιακής Συνέχεια (BCP)	Περιγράφει τις διαδικασίες που πρέπει να ακολουθήσει ο οργανισμός, ώστε να εξασφαλιστεί η αδιάλειπτη παροχή υπηρεσιών κατά τη διάρκεια ενός περιστατικού, αλλά και μετά από αυτό	Το σχέδιο αυτό μπορεί να περιλαμβάνει είτε μόνο τη συνέχεια παροχής των κρίσιμων λειτουργιών του οργανισμού είτε να περικλείει όλες τις λειτουργίες του οργανισμού, εστιάζοντας στις επιχειρησιακές λειτουργίες του οργανισμού	Δρα συμπληρωματικά με τα υπόλοιπα Σχέδια και κυρίως με το COOP
Σχέδιο Συνέχειας Λειτουργιών(COOP)	Αναφέρεται στην αποκατάσταση των κρίσιμων λειτουργιών του οργανισμού σε εναλλακτική τοποθεσία	Διαφοροποιείται από το BCP στο ότι αφορά κυρίως τις κρίσιμες λειτουργίες. Εστιάζει στις επιχειρησιακές λειτουργίες του οργανισμού.	Δρα συμπληρωματικά με τα υπόλοιπα Σχέδια και κυρίως με το BCP
Σχέδιο Επικοινωνιών Κρίσης (CCP)	Περιγράφει τις διαδικασίες που πρέπει να ακολουθήσει ο οργανισμός για τους επικοινωνιακούς χειρισμούς του σχετικά με το περιστατικό, τόσο εσωτερικά όσο και στο εξωτερικό περιβάλλον του.	Στόχος του σχεδίου είναι ο έλεγχος της διάχυσης πληροφοριών, με σκοπό την αποφυγή παραπληροφόρησης. Το σχέδιο αυτό συνήθως είναι στην περιοχή ευθύνης του υπεύθυνου δημοσίων σχέσεων του οργανισμού.	Δρα συμπληρωματικά με τα υπόλοιπα Σχέδια .
Σχέδιο Προστασίας Κρίσιμων Υποδομών (CIP)	Αφορά κρίσιμες υποδομές και περιλαμβάνει σειρά από πολιτικές και διαδικασίες για την προστασία αυτών από τον κίνδυνο καταστροφών, τον περιορισμό των ευπαθειών αλλά και την αποκατάστασή τους σε περίπτωση προσβολής τους.	Εστιάζει στις υποδομές του οργανισμού	Δρα συμπληρωματικά με τα υπόλοιπα Σχέδια
Σχέδιο Αντιμετώπισης Περιστατικών Κυβερνοχώρου (CIRP)	Καθορίζει τις διαδικασίες που πρέπει να ακολουθούνται σε περίπτωση εκδήλωσης περιστατικών που μπορεί να πλήξουν τα πληροφοριακά συστήματα ενός οργανισμού	Συνήθως, αυτό το σχέδιο αποτελεί προσάρτημα του BCP. Εστιάζει στα πληροφοριακά συστήματα του οργανισμού	Δρα συμπληρωματικά με τα υπόλοιπα Σχέδια
Σχέδιο Ανάκαμψης από Καταστροφή (DRP)	Αφορά συνήθως καταστροφές μεγάλης έκτασης, οι οποίες προσβάλλουν κυρίως τα πληροφοριακά συστήματα ενός οργανισμού.	Σκοπός του είναι να καθορίσει πολιτικές και διαδικασίες ώστε να διασφαλιστεί η αποκατάσταση και η συνέχιση της λειτουργίας των πληροφοριακών συστημάτων, ακόμα και μέσω της μεταφοράς της λειτουργίας τους σε εναλλακτικές εγκαταστάσεις	Συμπληρώνει τα σχέδια BCP ή COOP ενώ μπορεί να συμπεριλαμβάνει επιμέρους σχέδια ISCP. Εστιάζει στα πληροφοριακά συστήματα του οργανισμού
Σχέδιο Αντιμετώπισης Καταστροφής Πληροφοριακών Συστημάτων (ISCP)	Στοχεύει στην ανάκαμψη κάποιου πληροφοριακού συστήματος μετά από μερική ή πλήρη καταστροφή.	Περιλαμβάνει αναλυτικά όλα τα ειδικά μέτρα και τις διαδικασίες που πρέπει να ακολουθηθούν προκειμένου να ανακάμψει η λειτουργία κάποιου συγκεκριμένου συστήματος, χωρίς να είναι απαραίτητη η χρήση εναλλακτικής εγκατάστασης.	Συνήθως αποτελεί επιμέρους σχέδιο του DRP. Εστιάζει στα πληροφοριακά συστήματα του οργανισμού
Σχέδιο Έκτακτης Ανάγκης Παρευρισκομένων (OEP)	Περιγράφει εκείνες τις ενέργειες που πρέπει να ακολουθηθούν από τους παρευρισκόμενους (εργαζόμενους-επισκέπτες) κατά την εκδήλωση κάποιας καταστροφής.	Σκοπός του είναι να καθορίσει τις άμεσες αντιδράσεις των παρευρισκομένων με στόχο την ασφάλεια των ατόμων, του περιβάλλοντος.	Τα σχέδια είναι προσαρμοσμένα στις εκάστοτε ιδιαιτερότητες των κτιριακών εγκαταστάσεων του οργανισμού. Εστιάζουν στο προσωπικό του οργανισμού.

Πίνακας 3. *Είδη σχεδίων αντιμετώπισης περιστατικών.*

Τα σχέδια αυτά δρουν συμπληρωματικά και στόχο έχουν την αντιμετώπιση περιστατικών που μπορεί να θέσουν σε κίνδυνο την μερική ή ολική λειτουργία ενός οργανισμού. Στο επόμενο Σχήμα απεικονίζεται αυτός ο συσχετισμός σύμφωνα με τον NIST



Εικόνα 5. *Συσχετισμός Σχεδίων αντιμετώπισης περιστατικών.*

3.5 Ο κύκλος ζωής σχεδίων - PDCA

Για να είναι αποτελεσματικό ένα σχέδιο πρέπει να αντιμετωπίζεται ως ένα εξελισσόμενο μέτρο προστασίας. Ακόμα και το καλύτερο σχέδιο μια χρονική στιγμή, δεν θα είναι το καλύτερο για πάντα. Επομένως απαιτείται η συνεχής παρακολούθησή του .

Για να επιτευχθεί αυτό ενδείκνυται η εφαρμογή της μεθοδολογίας του κύκλου PDCA (Plan-Do-Check-Act) ή του Demings όπως είναι ευρέως γνωστή. Η μεθοδολογία αυτή αποτελείται από τέσσερα επαναλαμβανόμενα στάδια, τα οποία εφαρμοζόμενα στα εκάστοτε σχέδια και μπορούν να προσδιορίσουν τον κύκλο ζωής τους.

3.5.1 Μεθοδολογία του Κύκλου του Deming - PDCA

Ο Deming παριστάνει την διαδικασία συνεχούς βελτίωσης με έναν κύκλο.

Ο κύκλος αυτός ονομάζεται κύκλος Deming και αποτελείται από τέσσερα βασικά στάδια, που το ένα ακολουθεί το άλλο με μια καθορισμένη σειρά που επαναλαμβάνεται διαρκώς. Ο κύκλος ονομάζεται PDCA, από την σύντμηση των τεσσάρων σταδίων : plan, do, check, act ή στα ελληνικά : σχεδίασε, κάνε, έλεγξε, δράσε.

PLAN (ΣΧΕΔΙΑΣΕ)

Αναφέρεται στον σχεδίασμά της πορείας των ενεργειών που θα ακολουθηθούν.

DO (ΚΑΝΕ)

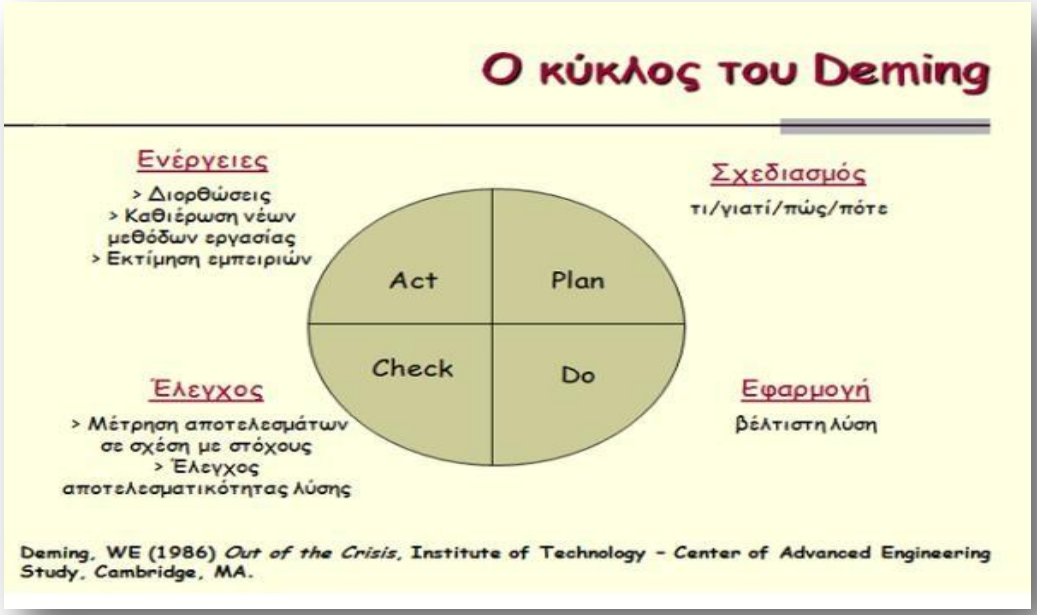
Αφορά την εφαρμογή του σχεδιασμού, όπου θα αναμιχθούν όλοι. Το στάδιο αυτό περιλαμβάνει την εκπαίδευση πάνω στις επιστημονικές μεθόδους, την έρευνα για τις ανάγκες και τις προσδοκίες των πελατών, την συλλογή των στατιστικών πληροφοριών, τον σχηματισμό ομάδων κλπ.

CHECK (ΕΛΕΓΞΕ)

Ο έλεγχος της εξέλιξης του σχεδιασμού αποτελεί ένα σημαντικό μέρος του κύκλου. Περιλαμβάνει την μέτρηση και παρατήρηση των αποτελεσμάτων, την ανά-πληροφόρηση και την επανεξέταση.

ACT (ΔΡΑΣΕ)

Οι αλλαγές υιοθετούνται ή εγκαταλείπονται ανάλογα με τα αποτελέσματα του προηγούμενου σταδίου.



Εικόνα 6. *Ο κύκλος του Deming*

Αυτά τα βήματα μπορούν να περιγραφούν συνοπτικά ως εξής εφαρμοσμένα αναλόγως στα Σχέδια Αντιμετώπισης κρίσιμων περιστατικών :

Plan: Το στάδιο κατά το οποίο δημιουργείται το σχέδιο και προσδιορίζονται οι στόχοι και τα αναμενόμενα αποτελέσματα. Σε αυτό το στάδιο επίσης καθορίζεται και ο τρόπος με τον οποίο θα εκτελεστούν τα βήματα του κύκλου PDCA (ποιός, τι, πού, πότε) .

Do: Στο στάδιο αυτό εφαρμόζεται και τίθεται σε πλήρη λειτουργία το σχέδιο. Καταγράφονται και αναλύονται τα προβλήματα που εμφανίζονται.

Check: Ολοκληρώνεται η καταγραφή και ανάλυση των απροσδόκητων αποτελεσμάτων από το προηγούμενο στάδιο. Στην συνέχεια ακολουθείται σύγκριση των πραγματικών αποτελεσμάτων με εκείνων που είχαν προσδιοριστεί κατά το πρώτο στάδιο . Αναλύονται οι αποκλίσεις και γίνεται προσπάθεια εξαγωγής συμπερασμάτων για να χρησιμοποιηθούν στο επόμενο στάδιο.

Act: Αποφασίζονται οι διορθωτικές ενέργειες που πρέπει να ακολουθηθούν ώστε να αντιμετωπιστούν αποτελεσματικά οι παραπάνω αποκλίσεις. Παράλληλα πραγματοποιείται η αξιολόγηση της αποτελεσματικότητας του ίδιου του κύκλου PDCA και εφόσον απαιτείται , δίδεται το έναυσμα για την εφαρμογή ενός νέου.

Ο κύκλος PDCA θεωρείται επιτυχής μόνο όταν με την ολοκλήρωσή του υπεισέρχονται διορθωτικές ενέργειες, αποτελώντας έτσι μια ιδανική μεθοδολογία για τη συνεχή αξιολόγηση και βελτίωση των σχεδίων.

Κεφάλαιο 4

4.1 Πρότυπα Business Continuity

Η σχεδίαση ανάκαμψης από καταστροφές , δεν αποτελεί εύκολη υπόθεση για κανέναν οργανισμό, αντίθετα μπορεί να αποδειχθεί ιδιαίτερα πολύπλοκη διαδικασία. Η πολυπλοκότητα αυτή σχετίζεται τόσο με την σχεδίαση όσο και την αποτελεσματική εφαρμογή του. Επιβάλλεται επομένως να ακολουθείται μια προκαθορισμένη μεθοδολογία που να εξασφαλίζει μέσα από την τυποποίηση ότι το αποτέλεσμα δεν θα έχει κενά, παραλείψεις, ή εσφαλμένες προσεγγίσεις.

Προκειμένου να καλυφθούν όλες αυτές οι απαιτήσεις έχουν εκδοθεί ορισμένα πρότυπα από οργανισμούς πιστοποίησης όπως ο διεθνής "International Organization for Standardization" (ISO) και ο "National Institute of Standards and Technology" (NIST) των Η.Π.Α. Τα πρότυπα αυτά περιγράφουν τις διαδικασίες που πρέπει να ακολουθεί ένας οργανισμός, ανάλογα με τις ανάγκες του και τις ιδιαίτερες συνθήκες –απαιτήσεις που υφίστανται σε κάθε περίπτωση.

Τα τελευταία χρόνια η χρήση ενός προτύπου αποτελεί τον πλέον ενδεδειγμένο τρόπο είτε για την αξιολόγηση είτε τη σχεδίαση ενός νέου Σχεδίου Ανάκαμψης. Πολλές φορές η αποτελεσματική εφαρμογή κάποιου προτύπου μπορεί να κρίνεται απαραίτητη για τη συμμόρφωση ενός οργανισμού με νομικές απαιτήσεις, όπως συμβαίνει συνήθως, για παράδειγμα, με τις Sarbanes–Oxley Act of 2002 (SOX) για τα χρηματοπιστωτικά ιδρύματα.

Παρακάτω περιγράφονται συνοπτικά τα κυριότερα πρότυπα που υπάρχουν αυτή τη στιγμή και σχετίζονται με την Επιχειρησιακή Συνέχεια.

27001:2005 -"Information Security Management System"

Ένα από τα πιο αναγνωρισμένα διεθνή πρότυπα σχετικά με την ασφάλεια πληροφοριών είναι το ISO 27001:2005 το οποίο περιέχει όλα όσα απαιτείται να πληροί ένας οργανισμός για την εφαρμογή ενός αποτελεσματικού Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Σκοπός του είναι να διασφαλίσει ότι η επιχείρηση έχει υιοθετήσει και εφαρμόζει μέτρα, πρακτικές και ελέγχους ώστε να προστατεύονται επαρκώς οι πληροφορίες και τα δεδομένα των «ενδιαφερόμενων μερών». Τα ενδιαφερόμενα μέρη μπορεί να είναι πελάτες, άλλες επιχειρήσεις, προσωπικό καθώς και συνεργάτες. Το πρότυπο δίνει έμφαση στην εμπιστευτικότητα (confidentiality) , την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) των πληροφοριών. Οι περιγραφόμενες απαιτήσεις ενέργειες είναι προληπτικού κυρίως χαρακτήρα και όχι διορθωτικού. Είναι διαρθρωμένο σε 10 θεματικές ενότητες μια εκ

των οποίων αφορά το αντικείμενο της διαχείρισης της Επιχειρησιακής Συνέχειας (**Business Continuity Planning**) σύμφωνα με το οποίο θα πρέπει :

- Καταγεγραμμένη και ελεγχόμενη διαδικασία να καθορίζει τις απαιτήσεις ασφάλειας πληροφοριών για την επιχειρησιακή συνέχεια του οργανισμού.
- (Threat & Risk Assessment) . Αναγνώριση όλων των πιθανών απειλών, υπολογισμός πιθανότητας να συμβούν και τέλος εκτίμηση των επιπτώσεών τους στην ασφάλεια πληροφοριών του Οργανισμού.
- Καταγραφή τόσο ενιαίων πλάνων επιχειρησιακής συνέχειας όσο και ειδικών που σκοπό έχουν την ενιαία αντιμετώπιση των απαιτήσεων ασφάλειας πληροφοριών.

Τα πλάνα αυτά πρέπει να ενημερώνονται και να δοκιμάζονται σε τακτά χρονικά διαστήματα ώστε να παραμένουν επικαιροποιημένα και αποτελεσματικά.

BS 25999:2007 - British Standard for Business Continuity Management"

Το πρότυπο BS 25999 εκδόθηκε από το British Standards Institution με σκοπό τη δημιουργία πιστοποιήσιμου πλαισίου απαιτήσεων για την εφαρμογή, λειτουργία και βελτίωση Συστήματος Διαχείρισης της Επιχειρηματικής Συνέχειας (BCM) . Το πρότυπο μπορεί να εφαρμοσθεί από οποιαδήποτε επιχείρηση, ανεξάρτητα από τον επιχειρηματικό τομέα στον οποίο δραστηριοποιείται. Περιέχει οδηγίες σχετικά με τις απαιτήσεις που πρέπει να ικανοποιούνται προκειμένου να διασφαλίζεται η επιχειρησιακή λειτουργία ενός οργανισμού σε περίπτωση ενός καταστροφικού γεγονότος. Αποτελεί βάση , γιατί αναλύει τις αρχές και τις απαιτήσεις της επιχειρησιακής συνέχειας. Δεν εξειδικεύει θέματα σχετικά με την ανάκαμψη των Πληροφοριακών του Συστημάτων. Παρόλο που περιγράφονται διεξοδικά οι απαιτήσεις της επιχειρησιακής συνέχειας, δεν περιγράφεται ο τρόπος με τον οποίο αυτές εφαρμόζονται και οι πρακτικές που πρέπει να ακολουθούνται.

BS 25777:2008 - Code of Practice for IT Service Continuity Management

Το BS 25777 θεωρείται παράρτημα του BS 25999 καθώς ειδικεύεται στη διασφάλιση της συνέχισης της λειτουργίας των Πληροφοριακών Συστημάτων ενός οργανισμού. Αποτέλεσε την εξέλιξη του προτύπου PAS 77:2006.

ISO 24762:2008 - Guidelines for Information and Communications Technology Disaster Recovery Services

Το πρότυπο ISO 24762 περιγράφει τις βέλτιστες πρακτικές που σχετίζονται με σχέδια ανάκαμψης πληροφοριακών και επικοινωνιακών συστημάτων. Αναφέρεται σε θέματα ελαχιστοποίησης κινδύνων (όπως είναι η προστασία από πυρκαγιά, πτώση τάσης) . Απευθύνεται κυρίως σε οργανισμούς που επιθυμούν να παρέχουν την ανάκαμψη ως υπηρεσία σε τρίτους.

ISO 27301:2011 - Guidelines for Information and Communications Technology Readiness for Business Continuity

Το ISO 27301 αποτελεί το νεότερο πρότυπο που σχετίζεται με την ανάκαμψη από καταστροφές, περιγράφει βασικές αρχές για την ετοιμότητα των πληροφοριακών συστημάτων ώστε να διασφαλίζουν την επιχειρησιακή συνέχεια. Περιγράφει επιπλέον μεθόδους και διαδικασίες για τη διαχείριση περιστατικών ασφαλείας αλλά και για το σχεδιασμό ετοιμότητας των Πληροφοριακών Συστημάτων. Αποτελεί ένα πρότυπο το οποίο περιλαμβάνει το συγκερασμό της επιχειρησιακής συνέχειας (BS 25999) με τη διαχείριση της συνέχειας των Πληροφοριακών Συστημάτων (BS 25777) και την ανάκαμψή τους από καταστροφές (ISO 24762) , προσαρμοσμένο έτσι ώστε να είναι συμβατό με το πλαίσιο που περιγράφεται στο ISO 27001.

NIST SP800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

Ο οργανισμός NIST εξέδωσε το 2002 τον οδηγό 800-34 για να κατευθύνει τους οργανισμούς που επιθυμούν να επιτύχουν επιχειρησιακή συνέχεια στις λειτουργίες των Πληροφοριακών τους Συστημάτων. Αποτελεί έναν καταξιωμένο, κατανοητό και εμπεριστατωμένο οδηγό ο οποίος αναφέρεται σε διοικητικά, λειτουργικά και τεχνικά ζητήματα που σχετίζονται με τον ΣΑΚ. Η οδηγία SP800-34 αναθεωρήθηκε πρόσφατα με την έκδοση Rev.1 (2010) και, αντίθετα με τα υπόλοιπα αναγνωρίσιμα πρότυπα και οδηγίες, διατίθεται δωρεάν προς χρήση.

Προεδρικό Διάταγμα 2577 - Παράρτημα 2 - Αρχές Ασφαλούς και Αποτελεσματικής Λειτουργίας των Συστημάτων Πληροφορικής στα Πλαίσια της Διαχείρισης του Λειτουργικού Κινδύνου από τα Πιστωτικά Ιδρύματα

Το συγκεκριμένο Προεδρικό διάταγμα θέτει ένα δομημένο και λεπτομερές πλαίσιο γενικών αρχών και κριτηρίων για την ασφαλή και αποτελεσματική λειτουργία των Πληροφοριακών Συστημάτων (ΠΣ) των Πιστωτικών Ιδρυμάτων (ΠΙ) . Το πλαίσιο αποτελεί τη βάση αξιολόγησης των ΠΙ στο συγκεκριμένο τομέα και συμβάλλει σημαντικά στην αποτελεσματική διαχείριση του λειτουργικού κινδύνου που σχετίζεται με τα Πληροφοριακά Συστήματα. Σύμφωνα με το Π.Δ. Το Πιστωτικό ίδρυμα πρέπει να διαθέτει εγκεκριμένα από τη Διοίκηση Σχέδια Επιχειρησιακής Συνέχειας για τα Πληροφοριακά Συστήματα, ενταγμένα στα γενικότερα εταιρικά ΣΣΕ, έτσι ώστε να εξασφαλίζεται η συνέχεια των κρισιμότερων λειτουργιών τους. Επιπλέον, το ΠΙ πρέπει να διαθέτει αποτελεσματικά Σχέδια Ανάκαμψης από Καταστροφή που θα εφαρμόζονται στις περιπτώσεις καταστροφικών συμβάντων που μπορεί να προκαλέσουν παρατεταμένη διακοπή της λειτουργίας ενός κρίσιμου συστήματος, ή ακόμη και ολόκληρου του μηχανογραφικού κέντρου.

Προτού δημιουργηθούν Σχέδια Επιχειρησιακής Συνέχειας και Σχέδια Ανάκαμψης από Καταστροφή θα πρέπει να προηγούνται διαδικασίες ανάλυσης επιχειρησιακών επιπτώσεων (business impact analysis) και ανάλυσης κινδύνων (risk assessment). Βάσει αυτών :

- θα προσδιορίζονται όλες οι κρίσιμες λειτουργίες καθώς και τα συστήματα-πόροι που χρησιμοποιούν
- θα προσδιορίζονται όλοι οι κίνδυνοι που απειλούν τις κρίσιμες λειτουργίες και θα κατατάσσονται σύμφωνα με την πιθανότητα εμφάνισής τους και τις πιθανές επιπτώσεις τους στα συστήματα και τις λειτουργίες
- θα σταθμίζεται το λειτουργικό κόστος από ενδεχόμενη διακοπή των κρίσιμων λειτουργιών και το κόστος ενεργοποίησης του ΣΕΣ & ΣΑΚ για να προσδιορίζονται οι συνθήκες που θα θέτουν σε εφαρμογή το αντίστοιχο σχέδιο
- θα προσδιορίζεται ο χρόνος ανάκαμψης των κρισίμων λειτουργιών – συστημάτων (Recovery Time) αλλά και το σημείο ανάκαμψης (Recovery Point) , δηλαδή σε πόσο χρόνο και σε ποια εικόνα χρονικά θα επανέλθουν τα συστήματα μετά την ανάκαμψη.

Κεφάλαιο 5

5.1 Μεθοδολογία Ανάπτυξης ΣΕΣ

Στο κεφάλαιο αυτό θα προσπαθήσουμε να προσεγγίσουμε την μεθοδολογία που αποσκοπεί στην αποτελεσματική δημιουργία ενός Σχεδίου Επιχειρησιακής Συνέχειας. Η μεθοδολογία που ακολουθείται είναι βασισμένη στις κατευθυντήριες γραμμές και βέλτιστες πρακτικές των πρότυπων BS 25999 και ISO 27301 που είναι και τα πιο συνήθης καθώς χρησιμοποιούνται ευρύτατα για πετυχημένη εφαρμογή Επιχειρησιακής Συνέχειας.

5.1 .1 Το Πλαίσιο του Έργου

Αρχική προϋπόθεση για ένα Σχέδιο Επιχειρησιακής Συνέχειας (ΣΕΣ) είναι να υποστηρίζει τους στόχους και την κουλτούρα ενός οργανισμού καθώς και να υποστηρίζεται από την πλευράς της Διοίκησης. Έχει ήδη αναφερθεί σε προηγούμενο κεφάλαιο ότι ένα (ΣΕΣ) έχει κυκλικό χαρακτήρα. Οι συνθήκες που επικρατούν στις σύγχρονες επιχειρήσεις αλλάζουν με ταχύτατους ρυθμούς επομένως η αρχική διαμόρφωση ενός ΣΕΣ δεν αρκεί για να εξασφαλιστεί η αποτελεσματικότητα του. Επιβάλλεται συχνή επικαιροποίηση βάση των εκάστοτε επιχειρησιακών απαιτήσεων.

Εικόνα 7. *Στοιχεία διαχείρισης κύκλου ζωής ενός ΣΕΣ.*

5.1.2 Στοιχεία Διαχείρισης Κύκλου Ζωής του ΣΕΣ

Ο κύκλος ζωής ενός ΣΕΣ αποτελείται από τα ακόλουθα στοιχεία τα οποία μπορούν να εφαρμοσθούν σε οποιοδήποτε οργανισμό ανεξάρτητα από το μέγεθος, τον τομέα ειδίκευσης και την μορφή του (Goh Moh Heng,2008) .

- **Διαχείριση Έργου Επιχειρησιακής Συνέχειας (BCM program management)**

  Αποτελεί την ουσία της διαδικασίας υλοποίησης ενός ΣΕΣ, ποικίλει και μεταβάλλεται ανάλογα με το μέγεθος και την πολυπλοκότητα του οργανισμού.

- **Κατανόηση του Οργανισμού (Understanding the Organization)**

  Σε πρώτο στάδιο κατανόηση των δραστηριοτήτων και εργασιών του οργανισμού και σε επόμενο ιεράρχηση των κρίσιμων λειτουργιών καθώς και του χρόνου εκτίμησης για την αποκατάστασής τους.

- **Προσδιορισμός Στρατηγικής Επιχειρησιακής Συνέχειας (Determining BCM Strategy)**

  Προσδιορίζεται η στρατηγική που θα ακολουθηθεί. Η καταλληλότερη στρατηγική για κάθε κρίσιμη λειτουργία επιλέγεται έτσι ώστε να επηρεάσει όσο το δυνατόν λιγότερο την επιχειρησιακή συνέχεια του οργανισμού.

- **Ανάπτυξη και Εφαρμογή Σχεδίων Επιχειρησιακής Συνέχειας (Developing and Implementing a BCM response)**

  Το συγκεκριμένο στοιχείο αναφέρεται στην ανάπτυξη και εφαρμογή κατάλληλων σχεδίων / βημάτων για την εξασφάλιση της συνέχειας των κρίσιμων λειτουργιών και την διαχείριση ενός έκτακτου καταστροφικού συμβάντος.

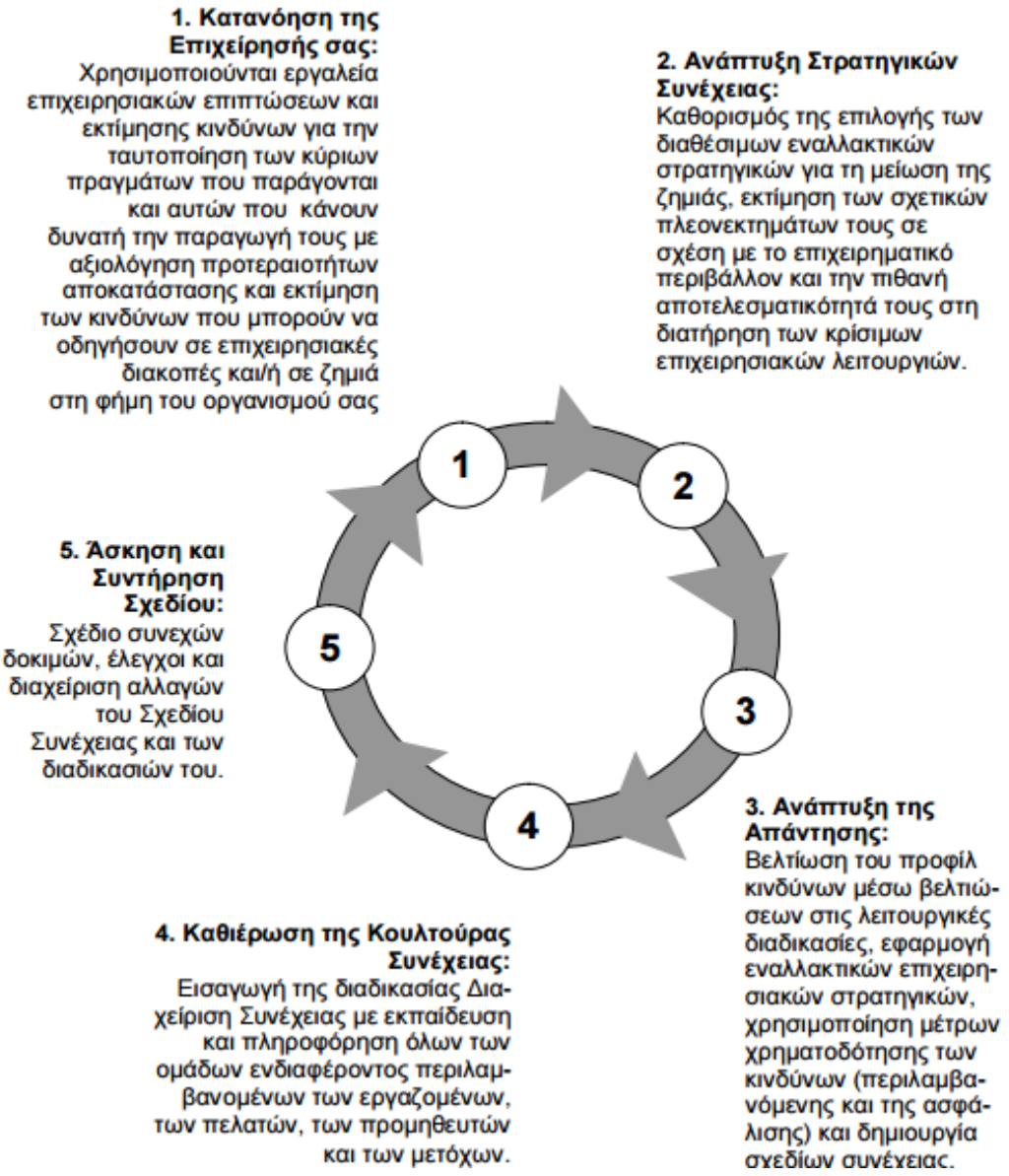
- **Δοκιμή και Ενημέρωση των Σχεδίων (Exercising, Maintaining and Reviewing)**

  Σκοπός του στοιχείου είναι η ανάπτυξη εκείνων των διαδικασιών, ενημέρωσης τόσο του προσωπικού όσο και εξωτερικών συνεργατών καθώς και δοκιμής των σχεδίων ώστε να αποδεικνύεται η ετοιμότητα και αποτελεσματικότητά τους όπως και να εντοπίζονται σημεία προς βελτίωση.

- **Ενσωμάτωση στην Κουλτούρα του Οργανισμού (Embedding in the organization's culture)**

  Για να θεωρείται αποτελεσματικό το έργο της επιχειρησιακής συνέχειας εκτός των άλλων πρέπει να τύχει ευρύτερης αποδοχής από το προσωπικό του οργανισμού

Όλα τα παραπάνω στοιχεία περιλαμβάνουν τις ενέργειες εκείνες που απαιτούνται ώστε να εξασφαλιστεί ότι ένα έργο ΣΕΣ υλοποιείται προς τις σωστές κατευθυντήριες γραμμές.



Εικόνα 8. *Κύκλος ζωής Διαχείρισης Επιχειρηματικής Συνέχειας - ΔΕΣ Πηγή: Διεθνές Ινστιτούτο Αποκατάστασης από Καταστροφή - ΔΙΑΚ (Disaster Recovery Institute International - DRII.*

Διαχείριση Έργου Επιχειρησιακής Συνέχειας

Η διαχείριση του έργου αποτελεί το πρώτο στάδιο υλοποίησης του ΣΕΣ. Στο στάδιο αυτό ο οργανισμός θέτει τους στόχους αλλά και την πολιτική εντός της οποίας θα ενταχθεί το ΣΕΣ. Ένα ορθά δομημένο έργο λειτουργεί προς την σωστή κατεύθυνση για την πετυχημένη ολοκλήρωση των επόμενων σταδίων.

5.2.1 Ανάπτυξη Πολιτικής Επιχειρησιακής Συνέχειας

Εντός της Πολιτικής Επιχειρησιακής Συνέχειας που έχει ορίσει η Διοίκηση θα καθαρισθεί το πεδίο εφαρμογής του ΣΕΣ. Η υποστήριξη της Διοίκησης ενός οργανισμού θεωρείται βασική προϋπόθεση για την επιτυχία της δημιουργίας, της συντήρησης καθώς και δοκιμής τους ΣΕΣ. Αρχικά οφείλει να ορίσει μια ομάδα ανθρώπων, υπευθύνων παρέχοντας τις βασικές κατευθυντήριες γραμμές για το σχεδιασμό, τον προϋπολογισμό καθώς και τις ειδικές απαιτήσεις του οργανισμού. Αξίζει να σημειωθεί ότι πρέπει να γίνεται αντιληπτός εξαρχής ο στόχος του ΣΕΣ και το πεδίο εφαρμογής του.

Υποστήριξη της Διοίκησης

Η Επιχειρησιακή Συνέχεια σχετίζεται με την βιωσιμότητα του οργανισμού έπειτα από ένα απρόοπτο καταστροφικό γεγονός. Για τον λόγο αυτό η Διοίκηση οφείλει να γνωρίζει όλους εκείνους τους κινδύνους που εν δυνάμει μπορεί να απειλήσουν την εύρυθμη λειτουργία του οργανισμού και να δεσμευτεί ως προς την δημιουργία ενός ΣΕΣ παρέχοντας τις απαραίτητες οικονομικές και τεχνικές υποδομές. Η γνωστοποίηση του σχεδίου καθώς και της σπουδαιότητάς του τόσο στην κοινότητα όσο και στις εμπλεκόμενες ομάδες οφείλεται να είναι σαφής, ρητή και να έχει την ίδια βαρύτητα με αντίστοιχες που γίνονται για άλλους επιχειρησιακούς λόγους. Η συντήρησή του σχεδίου πρέπει να ανατεθεί σε ανώτατο στέλεχος και σε καμία περίπτωση δεν θα πρέπει να αποτελεί πάρεργο των βασικών καθηκόντων του αλλά να θεωρείται βασικό καθήκον.

Επιλογή Ομάδας

Ακριβώς μετά την δέσμευση από την πλευρά της Διοίκησης, ανώτατο στέλεχος του οργανισμού αναλαμβάνει την επίβλεψη του έργου. Αρχικά επιλέγει τα μέλη που θα

συγκροτήσουν την ομάδα του. Τα συγκεκριμένα μέλη θα ανήκουν σε διάφορες μονάδες του οργανισμού και το μέγεθος της ομάδας θα εξαρτάται από το γενικότερο μέγεθος της εταιρίας. Όπως κάθε ομάδα μιας επιχείρησης έτσι και η συγκεκριμένη έχει ρόλους, αρμοδιότητες και στόχους. Για την συγκεκριμένη βασική προϋπόθεση αποτελεί η ορθή ανάλυση και εκτίμηση των επιπτώσεων και απειλών των κρίσιμων επιχειρησιακών λειτουργιών για την αποτελεσματική υλοποίησης ενός ΣΕΣ. Και σε επόμενο στάδιο η αποδοχή και δοκιμή του σχεδίου από την κοινότητα του οργανισμού. Δεν υπάρχει προκαθορισμένος χρόνος ολοκλήρωσης ενός έργου επιχειρησιακής συνέχειας λόγο της πολυπλοκότητας που το διακρίνει.

Παρά ταύτα μια μέθοδος που μπορεί να χρησιμοποιηθεί για την καλύτερη κατανόηση της κατάστασης του οργανισμού της οργάνωσης και τον προσδιορισμό των προσδοκιών του σε θέματα επιχειρησιακής συνέχειας είναι η δημιουργία και διανομή ενός ερωτηματολόγιου στα πρώτα εγκριτικά επίπεδα της κοινότητας του οργανισμού.

5.3 Κατανόηση του Οργανισμού

Για να είναι ένα έργο επιχειρησιακής συνέχειας ευθυγραμμισμένο με τους στόχους του οργανισμού τα αρμόδια στελέχη του έργου οφείλουν να έχουν προσδιορίσει πλήρως όλες τις λειτουργίες, τα περιουσιακά στοιχεία και τους ανθρώπινους πόρους του οργανισμού. Έπειτα να αξιολογήσουν της κρίσιμες εργασίες καθώς και το αποδεκτό χρονικό εκείνο διάστημα που δεν θα αποφέρει ζημιογόνες επιπτώσεις στην λειτουργία του οργανισμού στην περίπτωση που έχει επέλθει διακοπή τους. Επιπλέον υπάλληλοι που γνωρίζουν τις λειτουργικές διαδικασίες του οργανισμού σε συνεργασία με την ομάδα του έργου οφείλουν να προσφέρουν τις γνώσεις τους κατά την διαδικασίας σχεδιασμού του ΣΕΣ .

5.3.1 Ανάλυση Επιπτώσεων Επιχειρησιακής Συνέχειας

(Business Impact Analysis)

Η σημαντικότερη ίσως διαδικασία πάνω στην οποία δομείται το ΣΕΣ είναι η Ανάλυση Επιχειρησιακών Επιπτώσεων. Αποτελεί την διαδικασία κατά την οποία ο οργανισμός εντοπίζει όλες τις κρίσιμες επιχειρησιακές δραστηριότητες, εκτιμά ποιοτικά ή / και ποσοτικά τις απώλειες διακοπών και να καθορίζει τα επιτρεπτά διαστήματα μη διαθεσιμότητας και τους ελάχιστους πόρους που απαιτούνται για την ανάκαμψη των κρίσιμων επιχειρησιακών δραστηριοτήτων (Goh Moh Heng,2008) .

Η Ανάλυση Επιχειρησιακών Επιπτώσεων εξυπηρετεί για να προσδιορίσει το αποδεκτό χρονικό διάστημα μη λειτουργίας και το επιτρεπτό όριο απώλειας δεδομένων, έως ότου δεν επηρεάζεται η εύρυθμη λειτουργία του οργανισμού.

Βασικοί στόχοι της είναι:

- Η καταγραφή των εργασιών/δραστηριοτήτων του οργανισμού καθώς και της κρισιμότητάς τους που διεκπεραιώνονται τόσο εντός όσο και με τρίτους: εποπτικές αρχές, εξωτερικές εταιρίες, πελάτες κτλ.
- Εκτίμηση των συνεπειών (π.χ. λειτουργικές επιπτώσεις) που μπορεί να έχει τυχόν διακοπή εργασιών του οργανισμού.
- Καθορισμός του μέγιστου χρόνου (Recovery Time Objective) για την ανάκαμψη των εργασιών, ώστε να μην επηρεασθεί η λειτουργία του Οργανισμού.
- Καθορισμός του ελάχιστου επιπέδου λειτουργίας με την ολοκλήρωση της διαδικασίας ανακάμψεως.
- Καταγραφή των απαιτήσεων σε εξοπλισμό και εφαρμογές σε περίπτωση διακοπής λειτουργίας από ένα καταστροφικό γεγονός.
- Καταγραφή τυχόν αλληλεξαρτήσεων μεταξύ των εργασιών τόσο εντός του οργανισμού όσο και με εξωτερικούς συνεργάτες (παρόχους / προμηθευτές).
- Προβλέψεις για τη συνέχιση της λειτουργίας σε περίπτωση που έχουν ανατεθεί εργασίες σε τρίτους συνεργάτες (outsourcing) και εκείνοι εμφανίσουν διακοπή εργασιών.

5.3.2 Εκτίμηση Απειλών και Κινδύνων (Threat and Risk Assessment)

Επόμενο στάδιο μετά την Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis) αποτελεί η εκτίμηση Απειλών και Κινδύνων (Threat and Risk Assessment) . Εξετάζονται και αξιολογούνται τυχόν κίνδυνοι, απειλές ή ευπάθειες που μπορούν να έχουν επίπτωση στην ομαλή λειτουργία του οργανισμού .

Η αξιολόγηση πραγματοποιείται για τους ακόλουθους τομείς :

- Κτηριακές εγκαταστάσεις :
  - θέματα ασφαλείας / πυρασφαλείας εγκαταστάσεων,
  - δίκτυα και συστήματα παροχής ηλεκτρισμού/κλιματισμού / τηλεπικοινωνιών ,
  - έκθεση τους σε έκτακτα γεγονότα / κακόβουλες ενέργειες / ακραία καιρικά φαινόμενα.
- Λειτουργία πληροφοριακών πόρων και κρίσιμα σημεία αστοχίας.
- Ασφάλεια Πληροφοριών.
- Διαδικασίες τηρήσεως αντιγράφων ασφαλείας.
- Κρίσιμοι συνεργάτες/προμηθευτές/πάροχοι υπηρεσιών (outsourcing) .
- Εκπαίδευση Προσωπικού σε διαδικασίες έκτακτης ανάγκης.
- Ασφαλιστικές καλύψεις έναντι κινδύνων.

Εκτενής αναφορά σχετικά με την μεθοδολογία ανάλυσης κίνδυνου παρατίθεται σε επόμενο κεφάλαιο , παρακάτω αναφέρονται ενδεικτικά τα βήματα διαχείρισης κινδύνων .

- **Καθορισμός του σκοπού και της εμβέλειας της ανάλυσης**

Καθορίζεται ο σκοπός και τι ακριβώς θα περιληφθεί στην ανάλυση κινδύνων καθώς και ποιά αποτελέσματα αναμένονται να παραχθούν.

- **Αξιολόγηση των κρίσιμων λειτουργιών**

Σ’ αυτό το στάδιο προσδιορίζονται οι κρίσιμες λειτουργιές / εργασίες στον οργανισμό.

- **Ανάλυση των απειλών κρίσιμων λειτουργιών**

Στην συνέχεια προσπαθούμε να αναγνωρίσουμε τις πιθανές απειλές για κάθε μια κρίσιμη λειτουργία καθώς και τις επιπτώσεις μου θα επιφέρει .

- **Ανάλυση ευπαθειών**

Κάθε λειτουργία και κυρίως οι κρίσιμες μπορεί να είναι λιγότερο ή περισσότερο ευπαθής προς μια απειλή. Στο συγκεκριμένο στάδιο προσδιορίζεται η ευπάθεια της κάθε λειτουργίας προς κάθε απειλή ξεχωριστά .

- **Υπολογισμός του κινδύνου**

Υπολογίζεται ο κίνδυνος για κάθε λειτουργία από κάθε απειλή .

- **Επιλογή τρόπου αντιμετώπισης των κινδύνων**

Ενώ έχουν εντοπιστεί οι κίνδυνοι σε προηγούμενο στάδιο επιλέγεται ο τρόπος αντιμετώπισής τους. Τρείς είναι οι τρόποι αντιμετώπισης ενός κινδύνου.

- Η Αποφυγή ή Μεταφορά
- Η Αποδοχή και
- Ο μετριασμός μέσω κατάλληλων μέτρων

«CIA» και Κρίσιμες λειτουργίες

Η κρισιμότητα μιας λειτουργίας ενός οργανισμού σχετίζεται και με τον βαθμό εμπιστευτικότητας των δεδομένων που χρησιμοποιεί. Όσο πιο ευαίσθητα είναι τα δεδομένα, τόσο πιο κρίσιμη είναι η εργασία. Στο σημείο αυτό αξίζει να σημειωθεί το τρίπτυχο ασφαλείας" CIA – Confidentiality- Integrity – Availability" μέσω του οποίου πραγματοποιείται η συγκεκριμένη διαδικασία.

Εικόνα 9. *Το τρίπτυχο ασφαλείας "CIA" καθορίζει την κρισιμότητα μιας λειτουργίας.*

Εμπιστευτικότητα (Confidentiality)

Σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα.

Ακεραιότητα (Integrity)

Η *ακεραιότητα* μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

Διαθεσιμότητα (Availability)

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών.

Κόστος Επιπτώσεων

Σύμφωνα με τα παραπάνω η ανάλυση επιχειρησιακών επιπτώσεων εκτιμά το μέγεθος της επιχειρηματικής απώλειας από την μη ομαλή λειτουργία ορισμένων κρίσιμων ή μη λειτουργιών. Η απώλεια αυτή μπορεί να υπολογίζεται σε χρήμα, ανθρωποώρες, αρνητική δημοσιότητα, μείωση παραγωγής και παραγωγή ελαττωματικού προϊόντος.

Παραδείγματα εξισώσεων παρουσιάζονται κάτωθι :

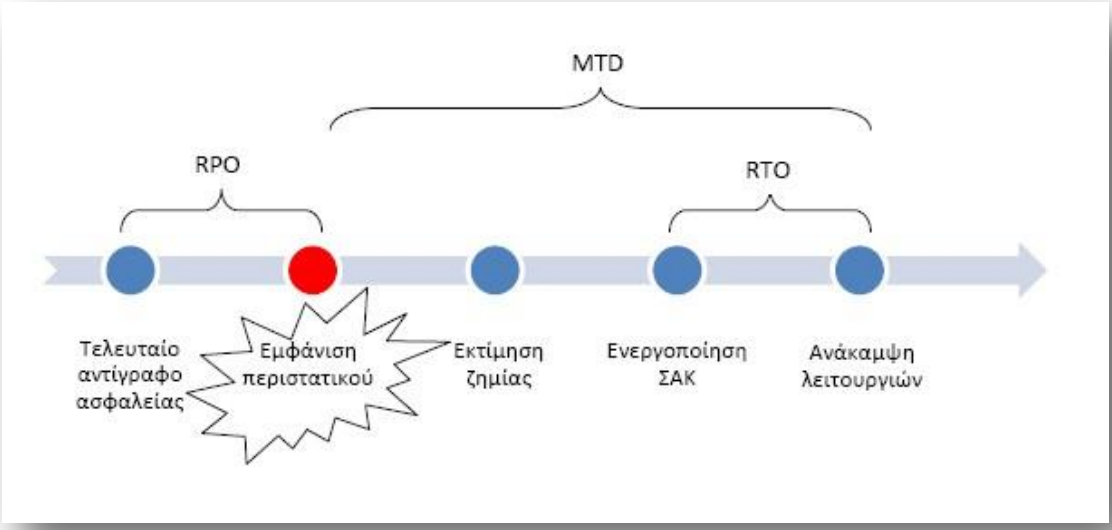
Απώλειες κερδών = Συχνότητα x Διάρκεια x Ωριαίο κόστος

Ανθρωποώρες = Ωρομίσθιο x Διάρκεια

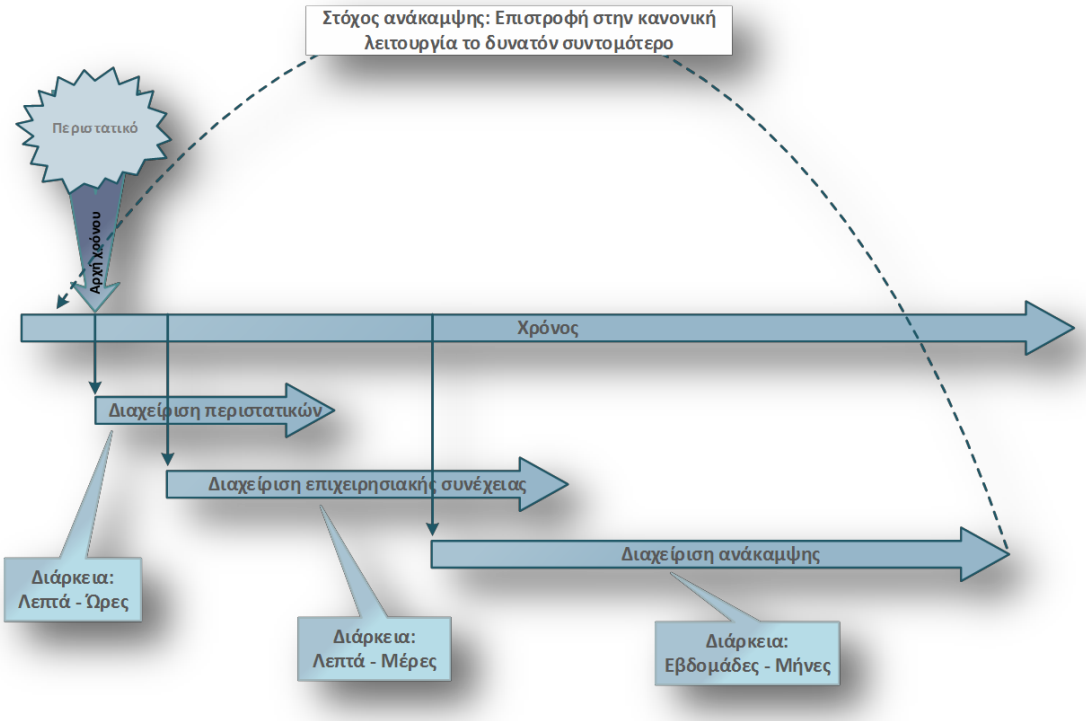
Κόστος ελαττωματικού προϊόντος = Ποσότητα Ελαττωματικού x Κόστος Καταστροφής

Μέσω της ανάλυσης επιπτώσεων (BIA) της επιχειρησιακής συνέχειας προκύπτουν δύο παράμετροι μέσω των οποίων γίνεται ο η ταξινόμηση των κρίσιμων λειτουργιών :

- Το RTO (Recovery Time Objective) : «αποδεκτό χρονικό πλαίσιο αποκατάστασης των κρίσιμων επιχειρησιακών λειτουργιών μετά από καταστροφή» και
- Το RPO (Recovery Point Objective) : «επιτρεπτό όριο απώλειας δεδομένων για χρονικό διάστημα το οποίο δεν επηρεάζει την επιχειρησιακή συνέχεια ».



Εικόνα 10. *Διαγραμματική απεικόνιση RTO,RPO & MTPD.*



Εικόνα 11. *Χρονική διαγραμματική απεικόνιση διαχείρισης ενός καταστροφικού περιστατικού.*

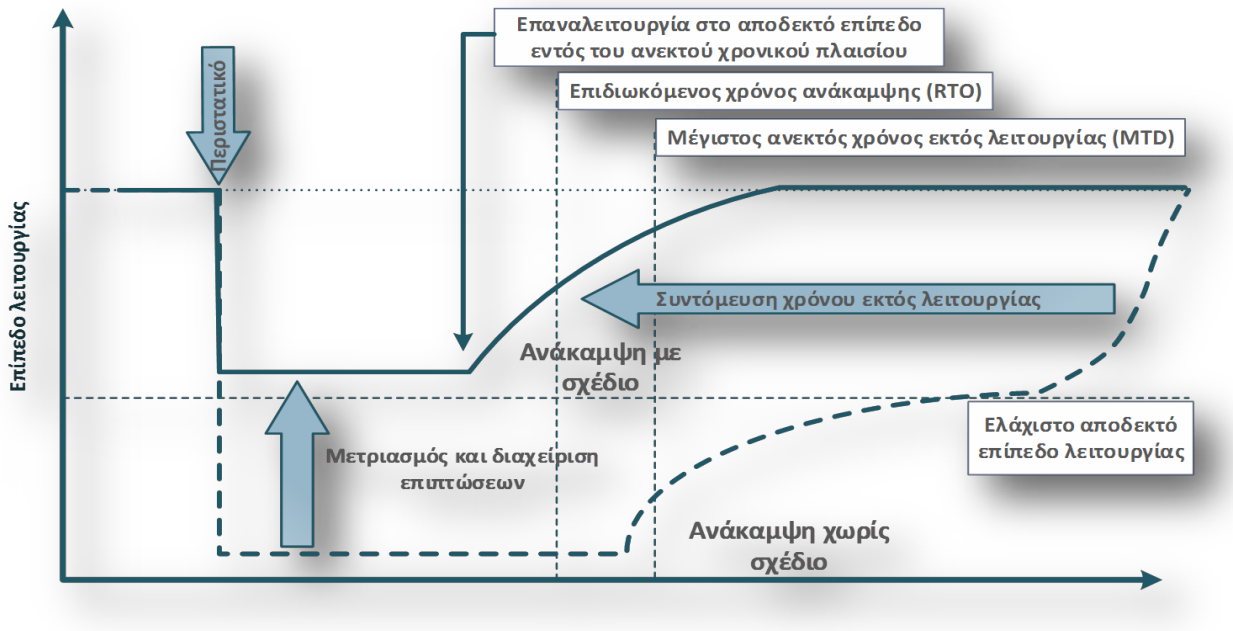
5.3.5 Ιεράρχηση Κρίσιμων Εργασιών και Συστημάτων

Η ιεράρχηση της κρισιμότητας των λειτουργιών / εργασιών οποιοδήποτε οργανισμού πρέπει να ακολουθεί μία μέθοδος μέτρου σύγκρισης. Αυτό θα μπορούσε να υλοποιηθεί με την δημιουργία ενός ερωτηματολογίου, σκοπός του οποίου θα ήταν να προσδιορίσει την επίπτωση που θα προκαλέσει στον οργανισμό η μη ομαλή λειτουργία μιας εργασίας. Μια τυπική ταξινόμηση όλων των εργασιών ενός οργανισμού είναι η κλίμακα του κάτωθι πίνακα σε συνδυασμό με τον Μέγιστο Ανεκτό Χρόνο Διακοπής.

Κατηγορία Κρισιμότητας	Περιγραφή Κρισιμότητας	MTPD
Α	Εξαιρετική	0 – 24 ώρες
Β	Πολύ Υψηλή	1 -3 ημέρες
Γ	Υψηλή	3 – 7 ημέρες
Δ	Σημαντική	1 – 4 εβδομάδες
Ε	Σημαντική αλλά μη κρίσιμη	1 + Μήνας

Πίνακας 4. *Ταξινόμηση κρίσιμων λειτουργιών σε σχέση με τον χρόνο αποκατάστασης MTPD*.

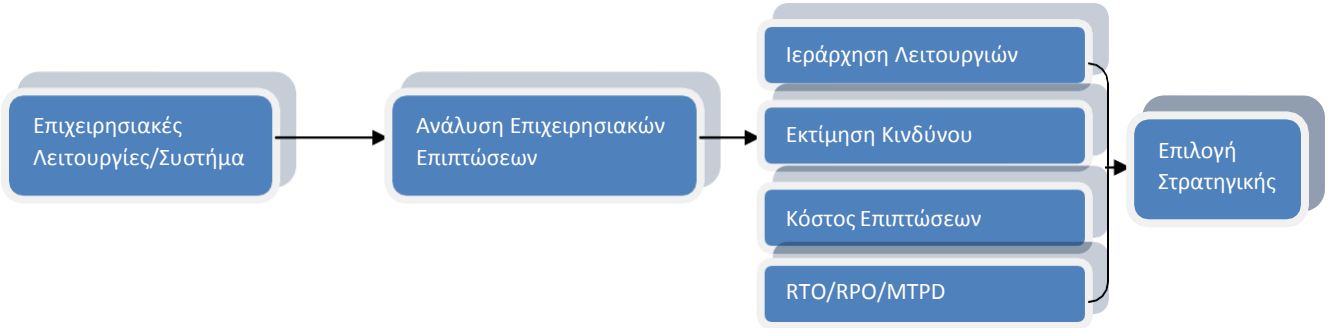
Η ομάδα έργου που έχει στόχο την υλοποίηση του ΣΕΣ σε συνεργασία με τους ιδιοκτήτες κάθε συστήματος/λειτουργίας του οργανισμού μπορούν να καθορίσουν το κατάλληλο «Μέγιστο Ανεκτό Χρόνο Διακοπής» (MTPD) .



Εικόνα 12. *Χρονική διαγραμματική απεικόνιση διαχείρισης ενός καταστροφικού περιστατικού με χρήση αλλά και χωρίς Σχεδίου Ανάκαμψης.*

5.4 Προσδιορισμός Στρατηγικής Επιχειρησιακής Συνέχειας

Ενώ έχει ολοκληρωθεί η ανάλυση επιχειρησιακών επιπτώσεων, έχουν προσδιοριστεί, εκτιμηθεί, καθοριστεί οι χρονικοί στόχοι ανάκτησης και οι επιπτώσεις τους , επόμενο στάδιο είναι η επιλογή της κατάλληλης στρατηγικής επιχειρησιακής συνέχειας.



Εικόνα 13. *Διαδικασία προσδιορισμού Στρατηγικής Επιχειρησιακής Συνέχειας.*

Η επιλογή της κατάλληλης στρατηγικής σχετίζεται με ένα σύνολο παραγόντων όπως :

1. Το μέγεθος του οργανισμού
2. Κόστος εφαρμογής
3. Αναπροσαρμογή συμβολαίων προμηθευτών / παρόχων
4. Τον Μέγιστο Ανεκτό Χρόνο Διακοπής (MTPD) κάθε λειτουργίας και συστήματος.

Στρατηγικές Επιλογές

Η επιλογή οποιασδήποτε στρατηγικής δεν θα εξαλείψει την καταστροφή αλλά θα μετριάσει τον κίνδυνο, να μετατραπεί σε καταστροφή. Για την υλοποίηση της αποτελεσματικότερης και αποδοτικότερης στρατηγικής απαιτείται η λήψη μέτρων για τα ακόλουθα :

Δραστηριότητες αποκατάστασης προσωπικού: Οποιαδήποτε καταστροφή κα αν επέλθει, κατά την διάρκεια ή μη ωρών εργασίας, θα επιφέρει προβλήματα στο ανθρώπινο δυναμικό . Για τον λόγο αυτό ο οργανισμός θα πρέπει να έχει προσδιορίσει την ομάδα εκείνη του οργανισμού ή να έχει συνάψει συμβόλαιο με εξωτερική εταιρία έτσι ώστε να συνεχισθεί η εκτέλεση των εργασιών στον εναλλακτικό τόπο λειτουργίας μετά την καταστροφή .

Εγχειρίδιο διαδικασιών εργασίας: Υπάρχουν περιπτώσεις διακοπής λειτουργίας εργασιών και πληροφοριακών συστημάτων και παρόλαυτα οι εργασίες που υποστηρίζουν μπορεί να γίνουν χειρονακτικά .

Το εγχειρίδιο διαδικασιών οφείλει να είναι κατανοητό, λειτουργικό και προσφάτως επικαιροποιημένο ώστε να εξυπηρετεί τον στόχο του. Όσο πιο ευκολονόητο και ενδελεχής είναι τόσο πιο αποτελεσματική είναι η επαναφορά του οργανισμού σε κανονική λειτουργία. Για τον λόγο αυτό θα πρέπει να περιλαμβάνει :

- Τις ενέργειες αποκατάστασης και επαναφοράς σε αρχική λειτουργία.
- Στοιχεία επικοινωνίας των εμπλεκομένων ατόμων στην επιχειρησιακή συνέχεια ή εξωτερικών συνεργατών.

Αποκατάσταση των πληροφοριακών συστημάτων: Η λύση που θα χρειαστεί για την αποκατάσταση των πληροφοριακών συστημάτων. Ορισμένες κρίσιμες εργασίες έχουν την δυνατότητα αποκατάστασής τους με χειρονακτικές , ενώ άλλες έχουν πλήρη εξάρτηση από τα πληροφοριακά συστήματα για τον λόγο αυτό οι στρατηγικές οφείλουν να εναρμονιστούν με το Μέγιστο Ανεκτό Χρόνο Διακοπής (MTPD) . Στόχος είναι να βρεθεί η καλύτερη και πιο οικονομικώς αποδεκτή λύση αποκατάστασης των συστημάτων.

Ανάθεση δραστηριοτήτων σε τρίτους: Διεργασίες που μπορούν να εκτελεστούν από τρίτους εξωτερικούς συνεργάτες. Η επιλογή του κατάλληλου εξωτερικού συνεργάτη απαιτεί προσεκτική αξιολόγηση, ώστε να διασφαλιστεί η ποιότητα και η συνέπεια του προϊόντος της κρίσιμης λειτουργίας. Θεωρείται απαιτείτο είναι να υπάρχουν συμβόλαια δέσμευσης υποστήριξης με τους εξωτερικούς συνεργάτες (Service Level Agreements) όπου σε περίπτωση διακοπής (καταστροφής) να είναι υποχρεωμένοι να εκπληρώσουν τις υποχρεώσεις του, στο ανάλογο συμφωνηθέν χρονικό διάστημα.

Εγκατάσταση εφεδρικής τοποθεσίας : Μια από τις πιο σημαντικές πτυχές της αποκατάστασης μιας καταστροφής είναι η ύπαρξη εφεδρικής τοποθεσίας μέχρι την αποκατάσταση της κύριας τοποθεσίας. Αυτή η εφεδρική τοποθεσία μπορεί να ανήκει στον οργανισμό ή να ενοικιάζεται. Παρουσιάζονται οι παρακάτω επιλογές τύπου εγκατάστασης :

Τοποθεσία	Θέση	Κόστος	Υπάρχουσα IT υποδομή	Τηλ/νιες	Χρόνος
Cold	Σταθερή	Χαμηλό	-	-	Μεγάλος
Warm	Σταθερή	Μέτριο	Μερικώς	Μερικώς/ Πλήρως	Μέσος
Hot	Σταθερή	Μέτριο/ Υψηλό	Πλήρως	Πλήρως	Μικρός
Mobile	Κινητή	Υψηλό	Εξαρτάται	Εξαρτάται	Εξαρτάται

Πίνακας 5. *Τύποι Εγκαταστάσεων εφεδρικής τοποθεσίας.*

Cold Site : Χώρος **με βασικές υποδομές.** Οι θέσεις εργασίας, ο εξοπλισμός και τα συστήματα θα πρέπει να εγκατασταθούν.

Warm Site: Χώρος **μερικώς** εξοπλισμένος ο οποίος καλύπτει τις ανάγκες για ανάκαμψη εργασιών σε σύντομο χρονικό διάστημα. Διαθέτει εγκατεστημένο εξοπλισμό και συστήματα κατόπιν σύντομων ρυθμίσεων μπορούν να λειτουργήσουν.

Hot Site: Χώρος **πλήρως** εξοπλισμένος ο οποίος καλύπτει τις ανάγκες για άμεση ανάκαμψη. Στο χώρο αυτό, οι θέσεις εργασίας, ο εξοπλισμός και τα συστήματα είναι εγκατεστημένα και έτοιμα προς χρήση.

Mobile Site : είναι ένας κινητός χώρος με όλο των απαραίτητο εξοπλισμό αφού διαθέτουν και εφεδρικές γεννήτριες για την παροχή ρεύματος. Ο χρόνος αποκατάστασης χρησιμοποιώντας αυτήν την προσέγγιση είναι λίγες εβδομάδες.

Ωστόσο πρέπει να ληφθούν υπόψη η απόσταση της εφεδρικής εγκατάστασης καθώς δεν θα πρέπει να βρίσκονται κοντά στην παραγωγική εγκατάσταση. Η αποκλειστική χρήση του χώρου θα πρέπει να τεκμηριώνεται γραπτώς εάν ενοικιάζεται από κοινού με άλλες οργανώσεις/εταιρείες για την αποφυγή προβλήματος διαθεσιμότητας της εγκατάστασης.

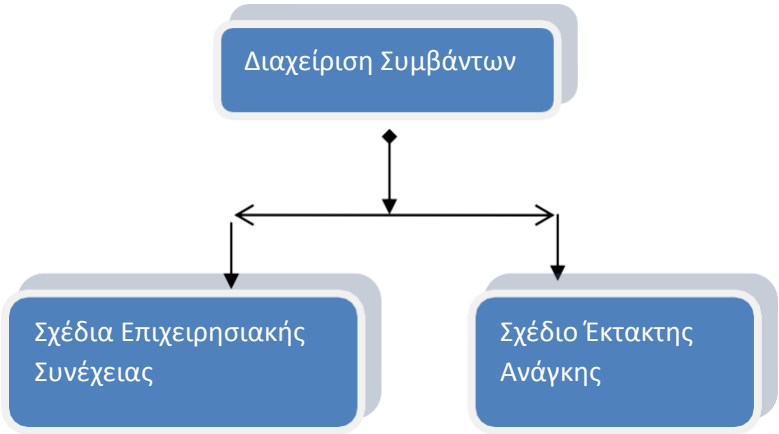
5.5 Εφαρμογή Σχεδίων Επιχειρησιακής Συνέχειας

Κάθε Σχέδιο Επιχειρησιακής Συνέχειας θα πρέπει είναι έτοιμο προς χρήση έχοντας μέσα όλα τα απαραίτητα στοιχεία ώστε να επιτύχει τον στόχο του σε περίπτωση καταστροφής.

Η υλοποίηση των σχεδίων πρέπει να ανατίθεται σε άτομα με ειδικευμένες γνώσεις που γνωρίζουν τις διαδικασίες του οργανισμού. Κάθε σχέδιο θα πρέπει να είναι συνετό, κατανοητό και όσο το δυνατόν λειτουργικό και να περιλαμβάνει βήμα προς βήμα οδηγίες για το τι πρέπει να γίνει, και ποιος θα το κάνει.

Σχέδιο Διαχείρισης Συμβάντων

Για την άμεση αντιμετώπιση μια καταστροφής ο οργανισμός οφείλει να καθορίσει μία δομή διαχείρισης των συμβάντων. Με αυτό τον τρόπο θα επιτρέπεται η έγκαιρη αναγνώριση της έκτασης και το περιεχόμενο της καταστροφής, ο καλύτερος έλεγχος της κατάστασης και η άμεση επικοινωνία των εμπλεκομένων φορέων. Ανάλογα με τον συμβάν οι αντίστοιχες ομάδες διαχείρισης κρίσεων οφείλουν να διαχειριστούν το συμβάν. Το κάτωθι διάγραμμα παρουσιάζει την κατηγοριοποίηση των συμβάντων ανάλογα με το τύπο της καταστροφής.



Εικόνα 4.5: Διαχωρισμός Σχεδίων διαχείρισης έκτακτων καταστροφικών περιστατικών .

Το **Σχέδιο Έκτακτης Ανάγκης** είναι το έγγραφο εκείνο στο οποίο καταγράφονται οι διαδικασίες που πρέπει να εφαρμοσθούν σε περιπτώσεις έκτακτης ανάγκης, όπως εκκένωσης κτιρίων ,σεισμού, πυρκαγιάς, ή τρομοκρατικής ενέργειας όπου υπάρχει ο κίνδυνος απώλειας ανθρώπινων ζωών .

Τα **Σχέδια Επιχειρησιακής Συνέχειας** είναι τα έγγραφα εκείνα που αναφέρονται μόνο σε καταστροφές που επηρεάζουν την διεκπεραίωση της επιχειρησιακής δραστηριότητας όπως την απώλεια πληροφοριακού συστήματος ή δεδομένων .

Στην συνέχεια αναφέρουμε τις αρμοδιότητες των ομάδων κρίσεων επιχειρησιακής συνέχειας :

Ομάδα Ασφαλείας: Διεξάγει την αρχική εκτίμηση της κατάστασης και ενημερώνει εφόσον απαιτείται την Διοίκηση αναφορικά με το μέγεθος της καταστροφής, ευθύνεται για την ενεργοποίηση των σχεδίων σε κατάσταση έκτακτης ανάγκης , την διεξαγωγή δοκιμών και ενημέρωση και συντήρηση των σχεδίων.

Ομάδα Έκτακτης Ανάγκης: Η ομάδα που διαχειρίζεται καταστάσεις έκτακτης ανάγκης όπως, πλημμύρες, σεισμούς κτλ.

Ομάδα Ανάκτησης Συστημάτων: Αρμοδιότητα της συγκεκριμένης ομάδας είναι η αποκατάσταση των πληροφοριακών συστημάτων σύμφωνα με τις διαδικασίες των σχεδίων.

Ομάδα Επικοινωνίας: Η ομάδα επικοινωνίας διαχειρίζεται την επικοινωνία με όλα τα ενδιαφερόμενα μέρη όπως πελάτες, ή την κοινότητα του οργανισμού με εκτέλεση καθορισμένων τρόπων επικοινωνίας.

Περιεχόμενα των Σχεδίων

Το περιεχόμενο ενός Σχεδίου Επιχειρησιακής Συνέχειας διαφέρει ανάλογα με τον τομέα της ειδικότητας του οργανισμού. Ποικίλοι από ένα έγγραφο για μικρούς οργανισμούς έως χωριστά για κάθε κρίσιμη λειτουργία. Σε κάθε περίπτωση περιλαμβάνουν :

Τον σκοπό του σχεδίου : Ο σκοπός του κάθε σχεδίου καθορίζεται όπως έχει συμφωνηθεί από την Διοίκηση και έχει γίνει κατανοητό από όλους τους εμπλεκόμενους.

Ρόλους και αρμοδιότητες : Ποιοι είναι οι ρόλοι και οι αρμοδιότητες των μεμονωμένων ατόμων και ομάδων κατά την διάρκεια του συμβάντος. Τα εμπλεκόμενα πρόσωπα και ομάδες ορίζονται με λεπτομέρεια.

Ενεργοποίηση του Σχεδίου : Ποιος και πότε δίνει την εντολή ενεργοποίησης του σχεδίου.

Ιδιοκτήτης/Υπεύθυνος του Σχεδίου : Ορισμός ενός υπεύθυνου για την εξέταση, τροποποίηση, και ενημέρωση των σχεδίων σε τακτά διαστήματα.

Επαναφορά στην κανονική κατάσταση : Τις ενέργειες που ακολουθούμε για να επιστρέψουμε από την εναλλακτική σε παραγωγική κατάσταση.

Λίστα επαφών (Call Tree): Κάθε σχέδιο περιέχει λίστα με όλους τους εμπλεκόμενους φορείς είτε αυτοί είναι φυσικά πρόσωπα, ομάδες, ή εξωτερικές εταιρείες.

5.5.2 Σχεδιασμός της επιχειρηματικής συνέχειας

Ο σχεδιασμός της επιχειρηματικής συνέχειας είναι μια ολιστική διαδικασία, η οποία εντοπίζει τους κίνδυνους και τις επιπτώσεις τους για την επιχείρηση, αυξάνει την αντοχή της σε αυτές , ενώ παράλληλα ενισχύει την ικανότητα αποτελεσματικής αντίδρασης σε καταστροφικά γεγονότα. Πρόκειται για ένα αμιγώς επιχειρηματικό ζήτημα, το οποίο ενοποιεί ένα ευρύ φάσμα επιχειρηματικών και διοικητικών τομέων. Συγκεκριμένα παρέχει το στρατηγικό και λειτουργικό πλαίσιο για την ανασκόπηση και πιθανή βελτίωση των διαδικασιών παραγωγής και διάθεσης προϊόντων και υπηρεσιών, αυξάνοντας παράλληλα την αντοχή της επιχείρησης σε περίπτωση καταστροφής, διακοπής λειτουργίας η απωλειών.

Το λάθος που γίνεται συχνά είναι η ταύτιση του Σχεδίου Επιχειρηματικής

Συνέχειας - Business Continuity Planning (BCP) με το Σχέδιο Ανάκαμψης από Καταστροφή – Disaster Recovery Plan (DRP) , και καλύπτει το σενάριο καταστροφής του κέντρου πληροφορικής. Κινητήρια δύναμη για την επίτευξη του στόχου του BCP είναι η ευθύνη και η δέσμευση της διοίκησης απέναντι στους εργαζόμενους, στους πελάτες και στους μέτοχους της επιχείρησης. Ωστόσο, ενώ μπορεί να είναι εύκολη η κάλυψη της οικονομικής ζημίας, η πιο σημαντική επίπτωση μιας λανθασμένης διαχείρισης ενός περιστατικού είναι η απώλεια φήμης η εμπιστοσύνης των πελατών. Αντιθέτως, η καλά οργανωμένη αντιμετώπιση μιας κρίσης μπορεί να αυξήσει την φήμη της, καθώς και την εμπιστοσύνη των μετόχων και πελατών στην διοικητική ομάδα.

Διαφορές DRP(Disaster Recovery Plan) – BCP (Business Continuity Plan)

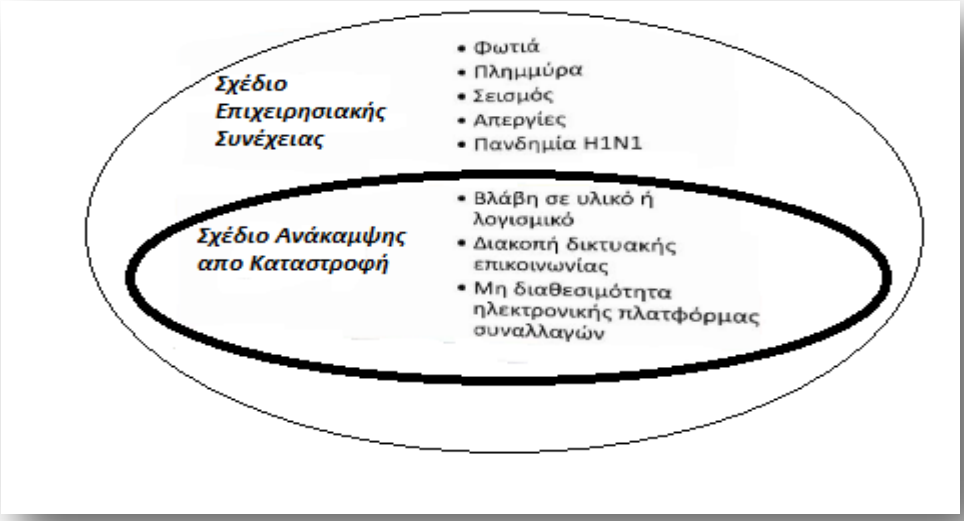
Αξίζει να αναφερθεί η διαφορά μεταξύ δύο βασικών σχεδίων του DRP (Disaster Recovery Plan) και του BCP (Business Continuity Plan) .

Το DRP:

- Εστιάζεται μόνο στα Πληροφοριακά Συστήματα (Π.Σ.)
- Ασχολείται με την αξιολόγηση της ζημιάς στα Π.Σ. μετά από μια καταστροφή, τη διάσωση και την αποκατάσταση εξοπλισμού και εγκαταστάσεων πληροφορικής

Το BCP :

- Περιλαμβάνει και ζητήματα που δεν αφορούν τα Π.Σ.
- Αφορά την επικοινωνία με το προσωπικό μετά από μια καταστροφή, και την οργάνωση ενδεχόμενης μετακίνησής του σε εναλλακτικές εγκαταστάσεις
- Εστιάζεται στην αποκατάσταση κρίσιμων λειτουργιών (π.χ. λήψη παραγγελιών, αποστολή / παραλαβή εμπορευμάτων) που απαιτούνται για την συνέχεια εργασιών του οργανισμού.

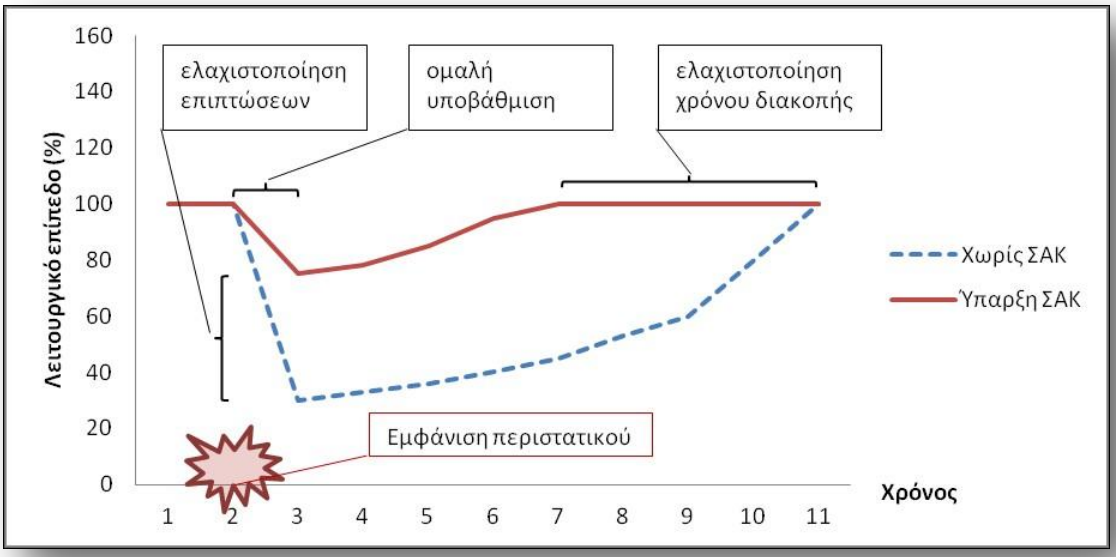


Εικόνα 14. *Διαφορές μεταξύ Σχεδίου Επιχειρησιακής Συνέχειας και Σχεδίου Ανάκαμψης από Καταστροφή.*

Άμεσα και έμμεσα οφέλη

Ο βασικός σκοπός του BCP είναι λοιπόν να διασφαλίσει ότι η επιχείρηση θα αντιδράσει σε μεγάλες καταστροφές που απειλούν την ύπαρξη της. Αυτό βέβαια είναι σημαντικό από μόνο του, αλλά υπάρχουν και άλλα «παράπλευρα» οφέλη. Ας διευκρινίσουμε σε αυτό το σημείο, συνοπτικά, πού βρίσκονται τα άμεσα και τα έμμεσα οφέλη του Business Continuity Management. Τα άμεσα οφέλη - για παράδειγμα αυτά που μπορεί να 'απολαύσει' μια εταιρεία σε περίπτωση μιας καταστροφής ή κρίσης - έχουν να κάνουν με τη μείωση του λειτουργικού αντίκτυπου της κρίσης. Τα έμμεσα οφέλη από την άλλη - αυτά τα οποία μπορεί να αποκομίσει η εταιρεία ακόμα και στη απουσία καταστροφής ή κρίσης - σχετίζονται με τη βελτιωμένη ανθεκτικότητα και με τη σε βάθος κατανόηση του οργανισμού και των βασικών προϊόντων και υπηρεσιών του. Αυτό σημαίνει ότι η εταιρεία θα έχει καθορίσει τους κινδύνους και τον αντίκτυπο αυτών, και κατ' επέκταση θα είναι σε θέση να αφιερώσει τους διαθέσιμους πόρους της σε στρατηγικές επιχειρηματικές περιοχές, καθώς και σε έργα που θα διασφαλίζουν την ετοιμότητά της να ανταποκριθεί στο μη αναμενόμενο. Αυτή η γνώση των κινδύνων σημαίνει ότι το οικονομικό «ανάχωμα» για τις απρόβλεπτες αναταράξεις και διακοπές της επιχειρηματικής λειτουργίας μπορεί να μειωθεί περαιτέρω και να αξιοποιηθεί για επιχειρηματικά έργα. Επιπρόσθετα, πολλές επιχειρήσεις οφείλουν να συμμορφώνονται με κανονιστικές και ρυθμιστικές διατάξεις, είτε ειδικά για το BCP είτε συνολικά για την διαχείριση κινδύνων. Ένα σωστό BCP ικανοποιεί τον νομοθέτη ενώ ταυτόχρονα εκπαιδεύει το προσωπικό να συνειδητοποιεί τους κίνδυνους και να αντιδρά μεθοδικά και ψύχραιμα. Για να δημιουργήσουμε το BCP πρέπει να ξεκαθαρίσουμε τι πρέπει να προστατεύσουμε και από τι. Εξετάζουμε λοιπόν όλες τις λειτουργικές και παραγωγικές διαδικασίες της επιχείρησης, ώστε να εντοπίσουμε τις κρισιμότερες και να υπολογίσουμε τις απαιτήσεις τους για συνεχή λειτουργία. Κατά την διάρκεια αυτής της φάσης προκύπτουν αδυναμίες, παραλείψεις, λάθη, κενά στην ασφάλεια η ακόμη υπερβολικά κόστη, τα οποία σε άλλη περίπτωση μπορεί να μην είχαν εντοπιστεί. Η ύπαρξη BCP χρησιμοποιείται ως ανταγωνιστικό πλεονέκτημα σε αγορές και συγχωνεύσεις εταιρειών, γιατί προσελκύει νέους πελάτες και δίνει εικόνα επιχείρησης που νοιάζεται για το προσωπικό και τους πελάτες της. Οι εταιρείες παροχής υπηρεσιών ή αγαθών, αναγνωρίζουν ότι είναι φθηνότερο να κρατάνε τους πελάτες τους παρέχοντας αξιόπιστες υπηρεσίες, παρά να προσπαθούν να τους ξανακερδίσουν μετά από μια διακοπή λειτουργίας. Το ομαδικό πνεύμα που δημιουργείται κατά την αντιμετώπιση ενός γεγονότος, βελτιώνει συνολικά την αποδοτικότητα της επιχείρησης, ακόμη και αρκετό καιρό μετά. Οπωσδήποτε όμως, ο κύριος λόγος δημιουργίας του BCP είναι η προστιθέμενη αξία σε μια επιχείρηση, στις

υπηρεσίες και τα προϊόντα που αυτή παρέχει στους πελάτες της, παρά την συμμόρφωση με κανονισμούς ή η βελτίωση των διαδικασιών λειτουργίας της.



Εικόνα 15. *Επίδραση ύπαρξης ΣΑΚ σε περίπτωση καταστροφής.*

5.6 Δοκιμή και Συντήρηση των Σχεδίων

Το Σχέδιο Επιχειρησιακής Συνέχειας είναι ένα δυναμικά εξελισσόμενο έγγραφο, μεταλλάσσεται παράλληλα μαζί με τον οργανισμό και οφείλει να αναπροσαρμόζεται στις εξελίξεις του. Ένα βασικό μειονέκτημα που παρατηρείται είναι η μη τακτική συντήρηση και δοκιμή του. Αν και επενδύονται πολλά χρήματα και ανθρωποώρες για την υλοποίησή του και σε ορισμένες περιπτώσεις δεν δοκιμάζεται. Αξίζει να σημειωθεί ότι η δοκιμή αποσκοπεί στην ανάπτυξη ικανοτήτων, γνώσεων, ομαδικού πνεύματος και εμπιστοσύνης τα οποία είναι απαραίτητα σε περίπτωση που συμβεί κάποιο γεγονός μεταξύ των ατόμων της κοινότητας του οργανισμού.

Συντήρηση των Σχεδίων

Όλα τα σχέδια πρέπει να επικαιροποιούνται σε τακτά χρονικά διαστήματα, τουλάχιστον σε ετήσια βάση, ώστε να είναι πάντοτε ενημερωμένα και αξιόπιστα τα ακόλουθα :

- Η ισχύς των υποθέσεων και παραδοχών που υπάρχουν.
- Οι κρισιμότητες των συστημάτων/λειτουργιών/διεργασιών/συστημάτων.
- Διαθεσιμότητα και επάρκεια των πόρων που απαιτούνται για την αποκατάσταση του συμβάντος.
- Επανεξέταση της διαθεσιμότητας του προσωπικού.

5.6.2 Κατηγορίες και Δοκιμές των Σχεδίων

Υπάρχουν 5 κατηγορίες δοκιμών ΣΕΣ , ορισμένες υλοποιούνται σε θεωρητικό και άλλες σε πρακτικό επίπεδο . Παρακάτω αναφέρονται επιγραμματικά :

- (Orientation Test): Θεωρητική Παρουσίαση των διαδικασιών ανάκαμψης
- (Tabletop Test) : Δοκιμή επί χάρτου των διαδικασιών ανάκαμψης
- (Functional Test) :Λειτουργία στο χώρο ανάκαμψης με χρήση συστημάτων Παραγωγής
- (Full Scale Test) : Ευρείας Κλίμακας δοκιμή, με πλήρη και ταυτόχρονη λειτουργία στο χώρο ανάκαμψης όσο το δυνατόν περισσότερων τμημάτων και προσωπικού
- (Disaster Test) : Λειτουργία στο χώρο εργασίας (χωρίς μετακίνηση Λειτουργών) αλλά με χρήση Εφεδρικών Συστημάτων

Κάτωθι αναφέρονται οι γενικοί στόχοι της δοκιμής των ΣΕΣ :

- Δοκιμάζονται οι διαδικασίες και ενέργειες ανακάμψεως που προβλέπει το Σχέδιο Επιχειρησιακής Συνέχειας (οργάνωση, διοικητική διάρθρωση και επικοινωνία, ενέργειες για την προετοιμασία, εφαρμογή και λειτουργία του Σχεδίου) .
- Δοκιμάζονται οι ρόλοι και τα καθήκοντα των Ομάδων Περιστατικών Κρίσεως, καθώς και της διαθεσιμότητας και κατάρτισης των ατόμων που τις στελεχώνει. Η δοκιμή της δυνατότητας των μελών των Ομάδων καθώς και των αναπληρωματικών μελών ως προς την εκτέλεση των καθηκόντων τους.
- Δοκιμάζονται οι υποδομές στους χώρους ανακάμψεως συμπεριλαμβανομένων των υποδομών πληροφορικής (εφαρμογές, τερματικά, περιφερειακός εξοπλισμός, κ.λπ.) των τηλεπικοινωνιών, των δικτύων (επικοινωνιών και δεδομένων) καθώς και των υποδομών ασφαλείας πληροφοριών.

- Επιβεβαιώνεται ο χρόνος και η αποτελεσματικότητα ανακάμψεως των εργασιών και κυρίως εκείνων που είναι κρίσιμες.
- Δημιουργείται κλίμα εμπιστοσύνης, ομαδικού πνεύματος και συνεργασίας μεταξύ των συμμετεχόντων στις δοκιμές.
- Βελτιώνεται η αποτελεσματικότητα του Σχεδίου με βάση τον εντοπισμό και την επίλυση τυχόν θεμάτων που προκύπτουν κατά τη διενέργεια των δοκιμών.

Η συχνότητα των δομικών εξαρτάται από τις ανάγκες του οργανισμού, το περιβάλλον που δραστηριοποιείται και τις απαιτήσεις των μετόχων και πελατών.

5.7 Ενσωμάτωση στην κουλτούρα του οργανισμού

Ένα από τα σημαντικότερα στοιχεία για την αποτελεσματικότητα του ΣΕΣ όπου η επιτυχία του εξαρτάται από την ενσωμάτωση του στην κουλτούρα του οργανισμού. Η ενσωμάτωσης αυτή δεν θεωρείται μια εύκολη υπόθεση αλλά αποτελεί μια είναι δύσκολη και χρονοβόρα διαδικασία. Το προσωπικό οφείλει να αποδεχτεί ότι έχει πρωταρχικό ρόλο στην επιτυχία αυτού του σημαντικού σχεδίου και έχει την ίδια βαρύτητα με άλλα αντίστοιχα έργα που πραγματοποιούνται για αμιγώς επιχειρησιακούς σκοπούς. Η ενσωμάτωση κουλτούρας των ΣΕΣ στον οργανισμό σχετίζεται με την :

- Τη Διοίκηση
- Ανάθεση αρμοδιοτήτων ρόλων για περιστατικά έκτακτων αναγκών
- Εκπαίδευση δεξιοτήτων του προσωπικού και
- Πραγματοποίηση δοκιμών των σχεδίων

Κεφάλαιο 6

6.1 Διαχείριση Κρίσεων (Risk Management)

Εξαιτίας των πρόσφατων τρομοκρατικών επιθέσεων αλλά και φυσικών καταστροφών έκανε την εμφάνισή της στο προσκήνιο των επιχειρήσεων η Διαχείριση Κρίσεων (Risk Management) . Κύριο μέλημά της είναι να λαμβάνουν άμεσα σημαντικές αποφάσεις και να ελαχιστοποιείται ο κίνδυνος εμφάνισης δυσάρεστων αποτελεσμάτων κατόπιν ενός απρόοπτου καταστροφικού γεγονότος. Σύμφωνα με τον Bob Darretta, CEO της Johnson & Johnson το 1999, «η φήμη της εταιρείας είναι το σημαντικότερο στοιχείο της» . Η Διαχείριση Κρίσεων ορίζεται ως η μεθοδολογία εκείνη που περιλαμβάνει συγκεκριμένο σχέδιο, οργάνωση, καθοδήγηση και έλεγχο τόσο κατά την διάρκεια αλλά και μετά από ένα καταστροφικό γεγονός.

Κάθε Σχέδιο Διαχείρισης Κρίσεων περιλαμβάνει

- Την αναγνώριση κινδύνων
- Την εκτίμηση κινδύνων
- Την κατάστρωση του Σχεδίου Διαχείρισης Κρίσεων
- Την άμεση αντίδραση του οργανισμού
- ‘’Ανάρρωση’’ του οργανισμού μετά την καταστροφικό γεγονός και τέλος τον
- Έλεγχο του Σχεδίου Διαχείρισης Κρίσεων

Αξίζει να επισημανθεί ότι πριν από την έναρξη της διαδικασίας κατάστρωσης του Σχεδίου Διαχείρισης Κρίσεων είναι απαραίτητο να ορισθεί το αρμόδιο πρόσωπο που θα φέρει την ευθύνη υλοποίησης του σχεδίου καθώς και τον συντονισμό των μελών της Ομάδας Διαχείρισης Κρίσεων.

Ορισμένοι από τους πιο πιθανούς κινδύνους που μπορούν να επηρεάσουν αρνητικά και να εκθέσουν ανεπανόρθωτα έναν οργανισμό είναι ένας πιθανός εμπρησμός, η εμφάνιση ιών στους Ηλεκτρονικούς Υπολογιστές, ο σεισμός, η φωτιά, η πλημμύρα κλπ. Η εκτίμηση των κινδύνων μπορεί να πραγματοποιηθεί είτε με ποιοτική είτε ποσοτική μεθοδολογία, εφόσον είναι εφικτό . Ένα Σχέδιο Διαχείρισης Κρίσεων οφείλει να βρίσκεται σε γραπτή μορφή και να περιλαμβάνει όλα τα προαναφερθέντα σχετικά με τους κινδύνους και την εκτίμησή τους. Να καθορίζει λεπτομερώς και ευδιάκριτα ρόλους και αρμοδιότητες. Το στοιχείο αυτό θεωρείται πολύ σημαντικό καθώς υπάρχει ο κίνδυνος μεσούσης κάποιας κρίσης διάφορα άσχετα με το αντικείμενο στελέχη της εταιρείας να προσπαθούν να πάρουν τον έλεγχο καταστάσεων καθώς αυτοί δεν είναι σωστά και πλήρως ενημερωμένοι. Η εκπαίδευση όλων των εμπλεκομένων σε αυτά τα ζητήματα και θεωρείται εξίσου σημαντική. Το στάδιο της “ανάρρωσης” της

επιχείρησης από μία πιθανή κρίση είναι πολύ σημαντικό. Σε αυτό το στάδιο πρέπει να τίθενται οι προτεραιότητες και τα σχέδια της επιχείρησης για την μετά – την – κρίση - περίοδο (Post Crisis Recovery Period) και να καθορίζεται το μήκος αυτής της περιόδου.

Ίσως το κρίσιμο στάδιο στη Διαχείριση Κρίσεων είναι η επαφή με τα Μέσα Μαζικής Ενημέρωσης. Όταν ένα απρόοπτο γεγονός με αρνητικές διαστάσεις εμφανισθεί ο οργανισμός οφείλει να προστατέψει την φήμη του καθώς και την αξιοπιστία του στην αγορά. Για τον λόγο αυτό πρωταρχικός στόχος του είναι η δημιουργία των ομάδων εκείνων που θα ενεργοποιηθούν, ο προσδιορισμός ενός και μόνου ατόμου το οποίο θα έρχεται σε επαφή με τα Μ.Μ.Ε. κατά τη διάρκεια αλλά και μετά την κρίση θεωρείται απαραίτητη. Συμπερασματικά η Διαχείριση Κρίσεων είναι μία πολύπλοκη και δυναμική μεθοδολογία που απαιτεί πολύ επίπεδη προσέγγιση. Εξαιτίας του γεγονότος ότι οι οργανισμοί διαφέρουν μεταξύ τους ως προς τις υποδομές και την οργάνωση, αντίστοιχα και τα Σχέδια Διαχείρισης Κρίσεων διαφέρουν για τον λόγο αυτό και δεν υπάρχει πανάκεια στην κατάστρωσή τους.

6. 2 Μεθοδολογία Ανάλυσης Κινδύνου (Risk Analysis)

Σε προηγούμενο κεφάλαιο έχει γίνει ενδεικτική αναφορά στην ανάλυση κινδύνου, εδώ θα γίνει μια εκτενής αναφορά της μεθοδολογίας ανάλυσης κινδύνου καθώς και των σταδίων διαχείρισής του . Η Ανάλυση κινδύνου μπορεί να υπολογισθεί ποσοτικά ή ποιοτικά αναφορικά με την πιθανότητα εμφάνισης και την πιθανή συνέπεια του. Η ποσοτική ανάλυση προσδιορίζεται με αριθμητικές τιμές όπως χρηματικά ποσά, π.χ. υπολογισμός της χρηματικής αξίας των απειλών ή του αριθμού μείωσης της παραγωγής του οργανισμού σε μια ενδεχόμενη απειλή.

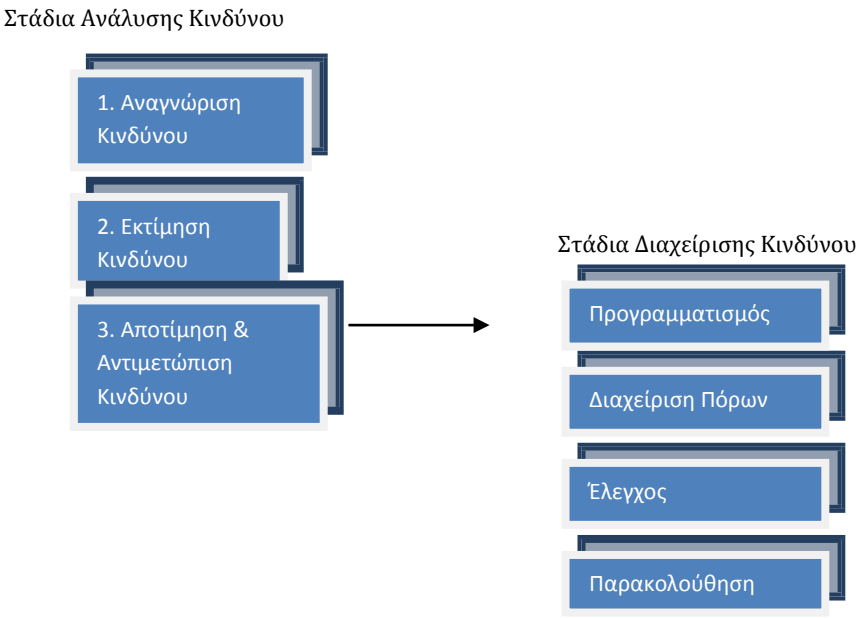
Από την άλλη , η ποιοτική ανάλυση δεν προσδίδει αριθμητικές τιμές. Αντίθετα δίνει τιμές από μια προαποφασισμένη κλίμακα, παρακάμπτοντας έτσι πολύπλοκους υπολογισμούς. Αν και οι κίνδυνοι δεν μπορούν να υπολογισθούν ακριβώς επιτυγχάνετε η ταξινόμησή τους καθώς και η προτεραιότητα για την αντιμετώπισή τους. Αξίζει να σημειωθεί ότι η ποιοτική ανάλυση βασίζεται στην εμπειρία των ανθρώπων που συμμετέχουν για τον προσδιορισμό των κινδύνων και σε ιστορικά δεδομένα. Πρόκειται προφανώς για μια υποκειμενική μέθοδο. Έχει αποδειχτεί με τον καιρό ότι η ποιοτική ανάλυση παράγει ικανοποιητικά αποτελέσματα εφόσον τα άτομα που συμμετέχουν έχουν την απαιτούμενη γνώση και εμπειρία σχετικά με το έργο που εξετάζεται.

Αρχική προϋπόθεση της Ανάλυσης Κινδύνου είναι η κατανόηση της οργανωτικής δομής και ο καταμερισμός των δραστηριοτήτων του Οργανισμού, οι οποίοι μπορούν να χωριστούν σε εργασίες/διαδικασίες ή και χαμηλότερου επιπέδου δραστηριότητες.

Η μεθοδολογία Ανάλυσης Κινδύνου περιλαμβάνει τρία βασικά στάδια :

- **Αναγνώριση Κινδύνου (Risk Identification) :** Προετοιμασία ενός καταλόγου με όλους τους πιθανούς κινδύνους που θα μπορούσε να αντιμετωπίσει ο Οργανισμός.
- **Εκτίμηση Κινδύνου (Risk Estimation) :** Προσδιορισμός της έκθεσης σε κάθε παράγοντα κινδύνου, βασισμένος στην εκτίμηση της πιθανότητας να συμβεί και της πιθανής επίπτωσής του.
- **Αποτίμηση Κινδύνου (Risk Evaluation) :** Εκτίμηση της αποδοχής κάθε παράγοντα κινδύνου, με σκοπό να αποφασιστεί τι μέτρα / ενέργειες πρέπει να ληφθούν.

Τα τρία παραπάνω βασικά στάδια παρουσιάζονται στον επόμενο πίνακα. Το τελευταίο Στάδιο Ανάλυσης , η αποτίμηση ,επικαλύπτεται με τα τέσσερα Στάδια Διαχείρισης ως κάτωθι .



Πίνακας 6. *Πίνακας Ανάλυσης – Διαχείρισης Κινδύνου.*

Αναγνώριση Κινδύνου

Στο πρώτο στάδιο γίνεται προσπάθεια προσδιορισμού των επικίνδυνων εκείνων γεγονότων καθώς και των συνθηκών που αποτελούν απειλή για τον οργανισμό. Σκοπός στο στάδιο αυτό είναι πέρα από την μέθοδο εν τέλει που θα χρησιμοποιηθεί να διατηρηθεί και η γνώση έτσι ώστε ο εντοπισμός οποιουδήποτε κινδύνου στο μέλλον να γίνεται άμεσα αντιληπτός. Κάτωθι παρουσιάζονται ορισμένες μέθοδοι εντοπισμού των κινδύνων :

- Μέσω συνεντεύξεων με ειδικευμένα στελέχη του οργανισμού ώστε να διαπιστωθούν κίνδυνοι που θα επηρέαζαν την ομαλή λειτουργία μιας διαδικασίας / εργασίας.
- Στο ίδιο μήκος κύματος με το προηγούμενο αλλά μέσω ομαδικών συζητήσεων μεταξύ στελεχών του οργανισμού. Το πλεονέκτημα της συγκεκριμένης μεθόδου είναι η ομαδική σκέψη που υπερτερεί της ατομικής.
- Μέσα από υπάρχων καταλόγους καταγραφής κινδύνων και καταστροφικών περιστατικών .
- Μέσω ανάλυσης υποθέσεων . Με την δημιουργία ενός έργου γίνονται κάποιες σωστές και κάποιες εσφαλμένες υποθέσεις. Η ανάλυση υποθέσεων αποσκοπεί στον εντοπισμό κινδύνων που γεννώνται μετά από εσφαλμένες υποθέσεις.

Εκτίμηση Κινδύνου

Εφόσον εντοπισθούν οι κίνδυνοι , το επόμενο στάδιο αφορά την εκτίμησή τους. Είναι εξίσου πολύ σημαντικό στάδιο διότι οποιαδήποτε λάθος απόφαση μπορεί να εκτινάξει το κόστος του έργου. Χρησιμοποιούνται δύο μέθοδοι εκτίμησης κινδύνου.

1. Η ποσοτική ανάλυση που βασίζεται κυρίως σε μαθηματικούς υπολογισμούς και ενδεικτικά αναφέρονται οι εξής :
   - Αναμενόμενη τιμή (expected value) : Βασίζεται στην αρχή ότι κάθε γεγονός που συμβαίνει ,επηρεάζει θετικά ή αρνητικά τους στόχους του έργου.
   - Δένδρα σφαλμάτων (fault tree). Πρόκειται για μια μέθοδο κατά την οποία αρχικά καθορίζονται τα γεγονότα που δεν επιθυμούμε να συμβούν, κατόπιν αναλύονται οι αιτίες που τα προκάλεσαν, κατασκευάζεται μια αλληλουχία γεγονότων σε μορφή δέντρου και ύστερα γίνεται ποσοτική ανάλυση.

2. Η ποιοτική ανάλυση κατά την οποία εκτιμάται η πιθανότητα εμφάνισης κάποιου κινδύνου και της αντίστοιχης συνέπειάς του. Η πιθανότητα εμφάνισης εκφράζεται με διαβάθμιση τύπου : Σχεδόν Βέβαιο, Πολύ Πιθανό, Πιθανό ,Σπάνιο, Απίθανο και η επίπτωση αντίστοιχα : Επικίνδυνη, Σοβαρή , Μέτρια, Μικρή.

Η πιθανότητα εμφάνισης ενός κινδύνου (probability), αναφέρεται στο ενδεχόμενο εμφάνισης του, κατά την διάρκεια λειτουργίας του οργανισμού. Εξαιτίας του ότι δύσκολα υπολογίζεται αριθμητικά η πιθανότητα εμφάνισης για τον λόγο αυτό εκφράζεται ποιοτικά βάση εμπειρίας και ιστορικών δεδομένων.

Παρόμοιο τρόπο στον υπολογισμό παρουσιάζει και η **επίπτωση (impact)** όπου τις περισσότερες φορές η εκτίμηση της βασίζεται σε υποκειμενικές εμπειρίες και ιστορικά δεδομένα επίσης.

Όσον αφορά την **έκθεση σε κίνδυνο** , έχει ορισθεί με βάση τον συνδυασμό της πιθανότητας μιας απειλείς να πραγματοποιηθεί και των επιπτώσεων που θα έχει σε αυτή την περίπτωση.

Τέλος η σοβαρότητα ενός κινδύνου (**severity**) μπορεί να υπολογιστεί ως το γινόμενο της πιθανότητας και των επιπτώσεων της.

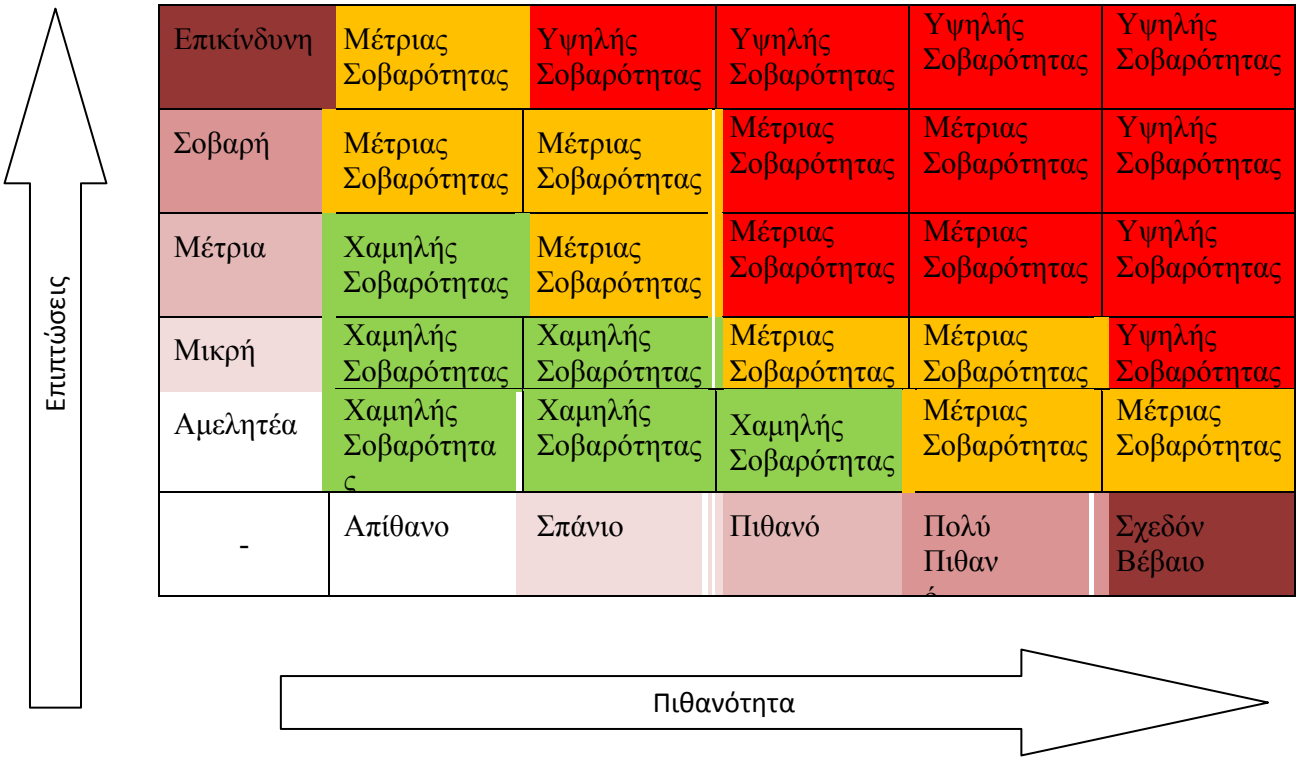
Παρακάτω παρουσιάζονται οι κλίμακες βαθμολόγησης που χρησιμοποιούνται για την εκτίμηση της πιθανότητας εμφάνισης και των επιπτώσεών των κινδύνων όπως και η μήτρα Πιθανότητα – Επιπτώσεων Κινδύνου.

Πιθανότητα εμφάνισης	Κλίμακα μετρήσεως	Περιγραφή
Σχεδόν Βέβαιο (Extremely High)	>80%	Η συχνότητα/πιθανότητα εμφάνισης της απειλής είναι πολύ μεγάλη (πάνω από 1 φορά το έτος) και υπάρχει μεγάλος κίνδυνος
Πολύ Πιθανό (Very High)	51% - 79%	Η συχνότητα/πιθανότητα εμφάνισης της απειλής είναι μεγάλη (1 φορά το έτος) και υπάρχει εξίσου μεγάλος κίνδυνος.
Πιθανό (High)	21% - 50%	Η συχνότητα εμφάνισης της απειλής είναι πιθανή
Σπάνιο (Medium)	6% - 20%	Η απειλή εμφανίζεται συχνά (π.χ. 1 φορά κάθε 2 έως 5 έτη) ,υπάρχει κίνδυνος.
Απίθανο (Low)	0% - 5%	Η απειλή δεν εμφανίζεται συχνά (π.χ. 1 φορά κάθε 5 έως 10 έτη) ή/και δεν υπάρχει κίνδυνος .

Πίνακας 7. *Πίνακας Εκτίμηση- Πιθανότητας* .

Βαρύτητα Επιπτώσεων	Περιγραφή Επιπτώσεων
Επικίνδυνη	Το συμβάν δύναται να προκαλέσει ανεπανόρθωτη απώλεια πόρων ή να βλάψει καταστροφικά τις παρεχόμενες υπηρεσίες, την αποστολή ή τη φήμη του οργανισμού ή να οδηγήσει σε απώλεια ζωής υπαλλήλου/πελάτη.
Σοβαρή	Το περιστατικό πιθανόν να προκαλέσει σοβαρό τραυματισμό υπαλλήλου / πελάτη του οργανισμού με περαιτέρω συνέπειες, ή σημαντική απώλεια πόρων ή να έχει σημαντικές επιπτώσεις στις παρεχόμενες υπηρεσίες, το ρόλο ή και τη φήμη του οργανισμού.
Μέτρια	Το συμβάν δύναται να προκαλέσει τραυματισμό υπαλλήλου/πελάτη του Οργανισμού με περαιτέρω συνέπειες, ή απώλεια πόρων, ή να έχει μέτριες επιπτώσεις στις παρεχόμενες υπηρεσίες.
Μικρή	Το συμβάν δύναται να προκαλέσει ελαφρύ τραυματισμό ή ατύχημα υπαλλήλου/πελάτη χωρίς περαιτέρω νομικές διεκδικήσεις, ή μικρή απώλεια πόρων ή να έχει περιορισμένη επίπτωση στις παρεχόμενες υπηρεσίες.
Αμελητέα	Το συμβάν δεν θα προκαλέσει επιπτώσεις ούτε τραυματισμούς

Πίνακας 8. *Πίνακας Εκτίμηση επιπτώσεων.*



Πίνακας 9. *Μήτρα Πιθανότητας/Επιπτώσεων Κινδύνων .*

Αποτίμηση και Αντιμετώπιση Κινδύνου

Το συγκεκριμένο στάδιο έχει ως αντικείμενο την αποτίμηση του βαθμού της αποδοχής ή μη κάθε παράγοντα κινδύνου. Θεωρείται ζωτικής σημασίας βήμα για την Διαχείριση Κινδύνου διότι χωρίς αυτό οι υπεύθυνοι δεν θα έχουν γνώση των σημαντικότερων κινδύνων για τους οποίους έχουν να λάβουν μέτρα. Πρωταρχικός στόχος αποτελεί ο εντοπισμός των μέτρων εκείνων που θα μειώσουν τις απειλές για τον λόγο αυτό συντάσσεται ένας κατάλογος με τους κινδύνους που έχουν εντοπισθεί και αναλυθεί. Σημαντικό κριτήριο για την επιλογή των κινδύνων που πρέπει να αντιμετωπισθούν πρώτοι είναι η χρονική στιγμή που εμφανίζεται ένας κίνδυνος και η δυνατότητα αντιμετώπισης του σε σχέση με έναν άλλον.

Οι τρόποι αντιμετώπισης ενός κινδύνου αναφέρονται στο κάτωθι πίνακα :

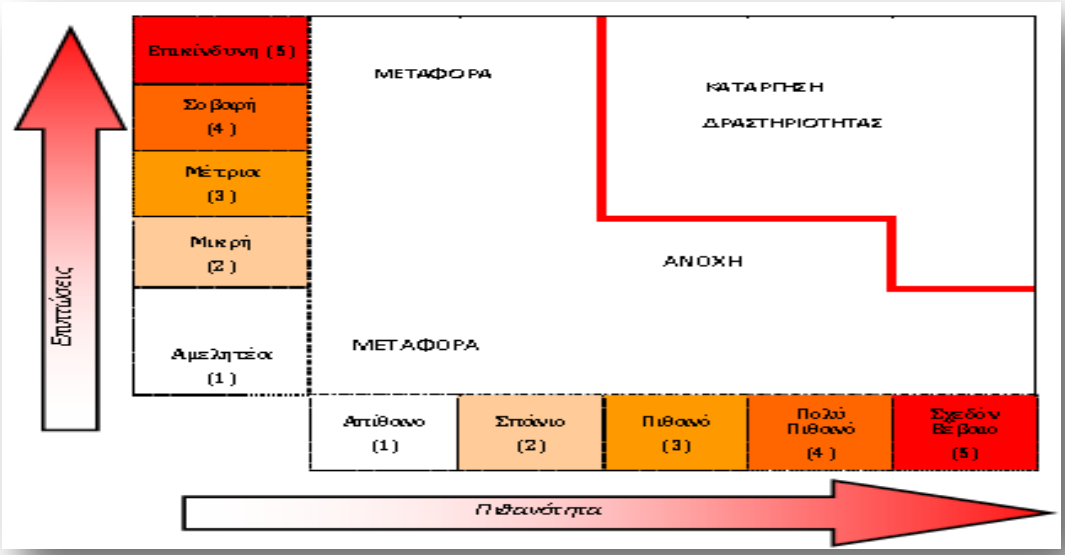
Στάδια Διαχείρισης	Ανάλυση Σταδίων
Αποφυγή	• Εφόσον προκύψει αλλαγή στο έργο/στην διαδικασία(Θεωρείται ο καλύτερος τρόπος αντιμετώπισης αλλά ισχύει με την προϋπόθεση)
Μεταφορά του κινδύνου	• Μεταφορά σε τρίτους
Ελάφρυνση του κίνδυνου	• Λήψη μέτρων
Αποδοχή	• Παρακολούθηση της εξέλιξης του κινδύνου και εναλλακτικά πλάνα

Πίνακας 10. *Πίνακας Αποτίμηση Κινδύνου.*

Στην περίπτωση που η ανάλυση κινδύνου έχει πραγματοποιηθεί σε ποσοτική βάση, τότε είναι εύκολο να συγκριθούν τα αριθμητικά επίπεδα έκθεσης με τα αποδεκτά όρια αφού εκφράζονται σε ίδιες μονάδες.

Στην αντίθετη περίπτωση με τις ποιοτική ανάλυση όπου υιοθετούνται υποκειμενικές μέθοδοι εκτίμησης, όπως είναι η γραμμή ανοχής που φαίνεται στο επόμενο Σχήμα .

Η γραμμή ανοχής, είναι η μέγιστη πιθανή έκθεση σε κίνδυνο, που μπορεί να γίνει αποδεκτή, με βάση τις πιθανές συνέπειες. Η ανοχή απέναντι σε μια απειλεί ποικίλει βάση ορισμένων παραγόντων όπως του μεγέθους, του χρόνου, και του τόπου που θα συμβεί.



Εικόνα 16. *Διάγραμμα αποτίμησης κινδύνου.*

6.3 Μεθοδολογία Διαχείρισης Κινδύνου

Στο στάδιο της Διαχείρισης Κινδύνου εφαρμόζονται τα μέτρα εκείνα που είναι απαραίτητα για να μειωθεί η σοβαρότητα των παραγόντων κινδύνου που έχουν προσδιοριστεί κατά τη διάρκεια της Ανάλυσης και συγκεκριμένα της αποτίμησης. Τα βασικά στάδια της Διαχείρισης Κινδύνου είναι :

1. Ο Προγραμματισμός (Planning) – Ανάπτυξη των κατάλληλων μέτρων για κάθε κίνδυνο και προετοιμασία ενός σχεδίου Διαχείρισης Κινδύνου.
2. Διαχείριση Πόρων (Resourcing) – Σχετίζεται με την κατανομή των υφιστάμενων πόρων και τον επιμερισμό ευθυνών σε αρμόδια στελέχη ή / και ομάδες για την υλοποίηση του σχεδίου.
3. Έλεγχος (Controlling) – Ελέγχεται η ορθότητα των σχεδιαζόμενων μέτρων και της κατανομής πόρων του σχεδίου καθώς και ο μεταξύ τους συντονισμός.
4. Παρακολούθηση (Monitoring) – Παρακολούθηση της αποτελεσματικότητας της εφαρμογής του σχεδίου. Αποτελεί το κλειδί που επιβεβαιώνει την αποτελεσματικότητα της εφαρμογής του σχεδίου Διαχείρισης Κινδύνου συνολικά. Σε αυτό το στάδιο παρακολουθείται και καταγράφεται ποιοι παράγοντες κινδύνου εμφανίστηκαν τελικά και πότε, καθώς επίσης και ποιες ενέργειες διαχείρισης τους λήφθηκαν τελικά, από ποιους και τι αποτελεσματικότητα είχαν. Τα καταγραφόμενα στοιχεία συγκρίνονται με αυτά του Σχεδίου Διαχείρισης Κινδύνου και εξετάζονται τυχόν αποκλίσεις από αυτό, σε

συνδυασμό με τους λόγους που οδήγησαν στις εν λόγω διαφοροποιήσεις. Με βάση όλα τα ανωτέρω στοιχεία παρακολουθείται η ανάγκη αναθεώρησης του Σχεδίου Διαχείρισης Κινδύνου. Η αναθεώρηση του Σχεδίου Διαχείρισης Κινδύνου είναι επιβεβλημένη, όταν, είτε εμφανιστεί ένας παράγοντας κινδύνου που δεν έχει προβλεφθεί, είτε αποδειχθεί ότι η υπάρχουσα εκτίμηση του μεγέθους της σοβαρότητας των παραγόντων κινδύνου βρίσκεται συστηματικά εκτός των ανεκτών ορίων διακύμανσης, είτε διαπιστωθεί ότι η αποτελεσματικότητα των σχεδιαζόμενων δράσεων είναι μειωμένη σε σχέση με τις προσδοκίες. Επομένως το σταδίου της Παρακολούθησης εξασφαλίζει ότι : Οι σχεδιασθείσες ενέργειες για τη μείωση της πιθανότητας εμφάνισης του παράγοντα κινδύνου είναι όντως αποτελεσματικές.

Στόχος της Διαδικασίας Διαχείρισης Κινδύνου αποτελεί η χρησιμοποίηση των συμπερασμάτων των προηγούμενων σταδίων της Ανάλυσης Κινδύνου για την παραγωγή ενός Βασικού Σχεδίου Δράσης. Εκτός του Βασικού Σχεδίου, αντίστοιχα της Διαδικασίας Διαχείρισης Κινδύνου αποτελούν και τα Σχέδια Έκτακτης Ανάγκης που έχουμε αναφέρει σε προηγούμενο κεφάλαιο .Τα τελευταία περιλαμβάνουν τις ενέργειες αντιμετώπισης ενός κινδύνου, μετά την εκδήλωσή του, στο σημείο αυτό έγκειται και η βασική διαφορά με το Βασικό Σχέδιο .

Κεφάλαιο 7

Κάθε χρόνο στην Ελλάδα λαμβάνει χώρα το Συνέδριο Επιχειρησιακής Συνέχειας (Business Continuity Forum) . Φέτος διεξήχθη το τρίτο κατά σειρά, αποτελεί το μοναδικό που πραγματοποιείται στην Ελλάδα και αφορά κάθε οργανισμό. Σκοπός του είναι να αναλύει σε βάθος τις νέες απειλές, όπως τρομοκρατία και κυβερνο-έγκλημα καθώς και τον ρόλο της επιχειρησιακής συνέχειας, να προτείνει ρεαλιστικές στρατηγικές, λύσεις, νέες τεχνολογίες που ενισχύουν και διασφαλίζουν την βιωσιμότητα του οργανισμού και τέλος να αναδεικνύει τη σημασία των συνεργειών και της συνεργασίας μεταξύ ομοειδών αλλά και ετερόκλητων φορέων από τον δημόσιο και ιδιωτικό τομέα για την αποφυγή ή την επιτυχή αντιμετώπιση σοβαρών καταστροφικών γεγονότων.

Σύμφωνα με έρευνα σχετικά με την Επιχειρησιακή Συνέχεια (Business Continuity) που πραγματοποίησε η ALCO με τη Fidel & Fortis και παρουσιάστηκε στο 3rd Business Continuity Management Forum τον περασμένο Δεκέμβριο, με στόχο

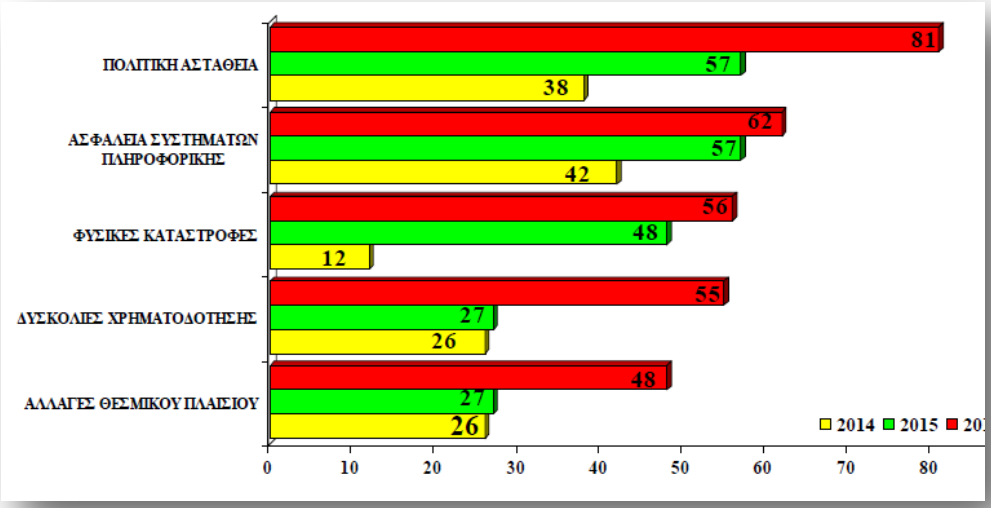
- την καταγραφή της εξέλιξης των αντιλήψεων 60 ανώτατων στελεχών από ισάριθμες πολύ μεγάλες επιχειρήσεις της χώρας (άνω των 500 εργαζομένων) ,
- την καταγραφή των σημαντικότερων κινδύνων που αντιμετωπίζουν και θα αντιμετωπίσουν στο μέλλον,
- καθώς και το επίπεδο ετοιμότητάς τους σε περίπτωση μεγάλων απρόβλεπτων γεγονότων οι επιχειρήσεις

προέκυψαν τα ακόλουθα ,

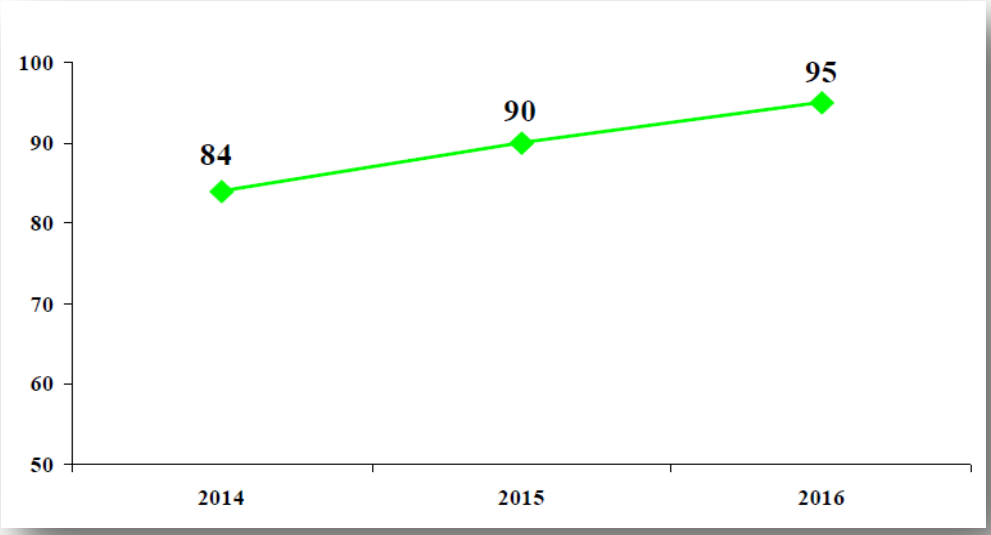
Οι τρείς σημαντικοί κίνδυνοι είναι :

1. πολιτική αστάθεια (81%) ,
2. απειλές που έχουν σχέση με την ασφάλεια (62%) ,
3. οι φυσικές καταστροφές (56%) ,

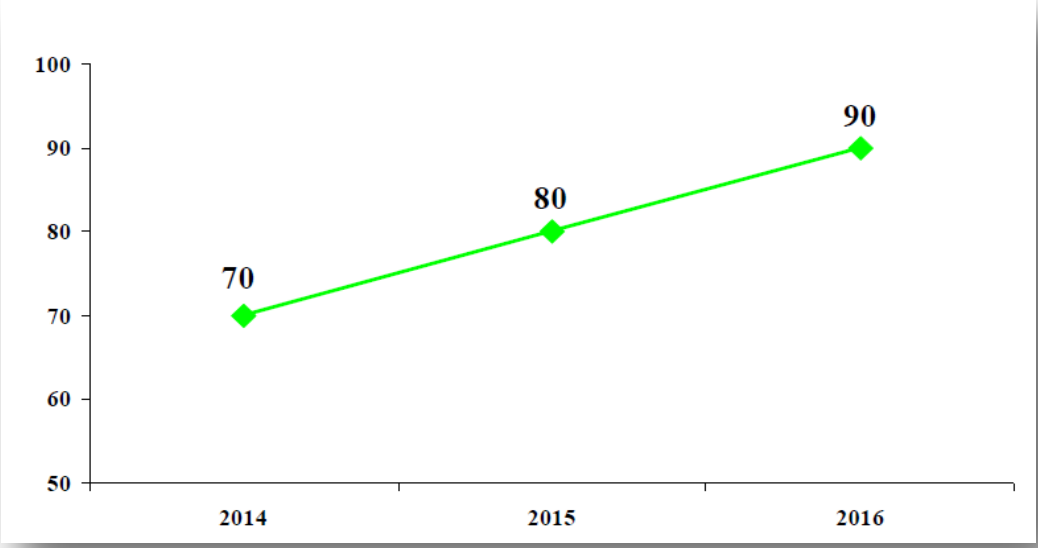
Τα αποτελέσματα του ερωτηματολογίου συνοψίζονται στα παρακάτω διαγράμματα διακρινόμενο σε τέσσερις θεματικές ενότητες :



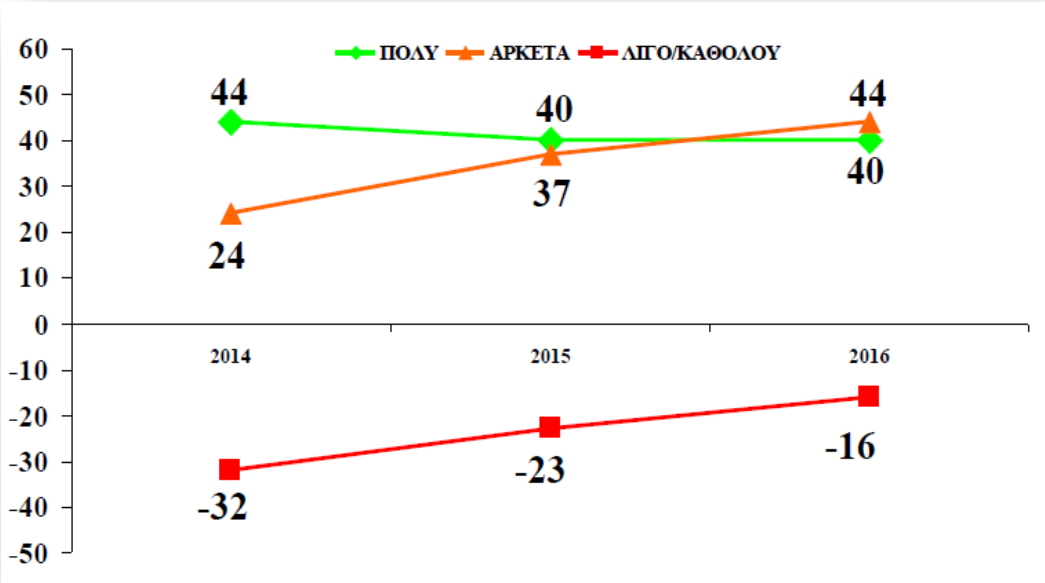
Εικόνα 17. *Αναφορά κινδύνων - απειλών για μια εταιρία σήμερα, ALCO (Business Continuity Forum 2016).*



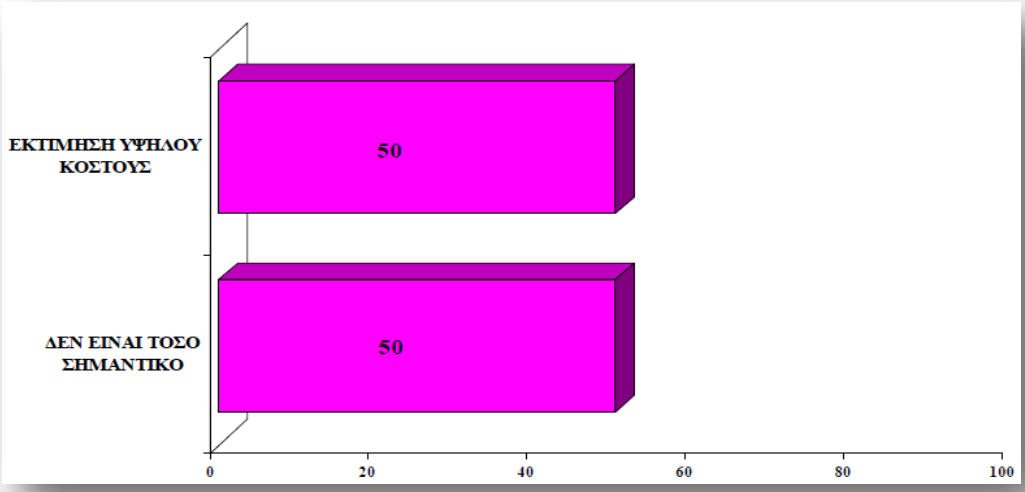
Εικόνα 18. *Ύπαρξη πλάνων διαχείρισης έκτακτων γεγονότων , σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO (Business Continuity Forum 2016).*



Εικόνα 19. *Ύπαρξη ομάδων διαχείρισης έκτακτων γεγονότων , σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO (Business Continuity Forum 2016).*



Εικόνα 20. *Βαθμός εξοικείωσης με τον όρο "Επιχειρησιακή Συνέχεια", σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO(Business Continuity Forum 2016).*



Εικόνα 21. *Οι σπουδαιότερες αιτίες που ΔΕΝ έχουν προχωρήσει σε σύστημα Business Continuity, σύμφωνα με έρευνα που πραγματοποιήθηκε από την εταιρία ALCO (Business Continuity Forum 2016).*

Η έρευνα αποτυπώνει τις αντιλήψεις για απειλές, κινδύνους και επιχειρησιακή συνέχεια στις μεγάλες και πολύ μεγάλες ελληνικές επιχειρήσεις, (το 62% από όσες συμμετείχαν απασχολεί πάνω από 500 εργαζόμενους και το σύνολο πάνω από 50 εργαζόμενους) , σε μία πολύ συγκεκριμένη χρονική συγκυρία, μετά από ένα χρόνο πολύ σημαντικών. Πλέον σημαντικά από τα ευρήματα της είναι :

- Η συνολική αίσθηση αυξημένων κινδύνων.
- Πολιτική αστάθεια (καθολική αίσθηση) , δυσκολίες χρηματοδότησης και αλλαγές θεσμικού πλαισίου εμφανίζουν πολύ αυξημένα (ακόμη και διπλάσια) ποσοστά, ενώ σταθερά υψηλά είναι τα ποσοστά για ασφάλεια συστημάτων και φυσικές καταστροφές.
- Κατά μέσο όρο κάθε επιχείρηση χρειάστηκε να αντιμετωπίσει 3,5 απειλές στο πρόσφατο παρελθόν.
- Δυσκολίες χρηματοδότησης και πολιτική αστάθεια κυριαρχούν (με υπερδιπλάσια ποσοστά σε σχέση με το 2015) , ενώ έκτακτα συμβάντα, διακοπή λειτουργίας συστημάτων, ακραία καιρικά φαινόμενα και αλλαγή θεσμικού πλαισίου φαίνεται να αποτελούν διαχρονικά υπαρκτούς κινδύνους.

Ανάλογη (προφανώς και επηρεασμένη από το πρόσφατο παρελθόν) , είναι η αντίληψη των επιχειρήσεων για τις απειλές στο μέλλον. Πολιτική αστάθεια (με σταθερά αυξητική τάση) και ασφάλεια συστημάτων αποτελούν τις κύριες απειλές και ταυτοχρόνως τους δύο μεγαλύτερους κινδύνους, αφού θεωρείται ότι μπορούν να επιφέρουν τις πλέον αρνητικές συνέπειες.

Η έρευνα αποδεικνύει ότι οι επιχειρήσεις προετοιμάζονται όλο και περισσότερο για να αντιμετωπίσουν κινδύνους και απειλές. Πλάνα διαχείρισης έκτακτων γεγονότων, άτομα / ομάδες που θα τα διαχειριστούν, διασφάλιση λειτουργίας κρίσιμων συστημάτων, ασφάλεια εργαζομένων, προληπτικοί έλεγχοι των πλάνων, συνεργασία με τις αρμόδιες αρχές, αποτελούν μέρος της λειτουργίας του 80% - 90% των μεγάλων και πολύ μεγάλων επιχειρήσεων στην Ελλάδα. Στο ευρύτερο αυτό πλαίσιο, η έννοια της επιχειρησιακής συνέχειας γίνεται όλο και πιο οικεία, ενώ η ύπαρξη, στην πράξη, ολοκληρωμένου συστήματος κινείται σταθερά αυξητικά, καλύπτοντας πλέον το 65% των μεγάλων και πολύ μεγάλων επιχειρήσεων, με μόνο το 50%, όμως, να διαθέτει ειδική σχετική ομάδα. Η περιορισμένη αντίληψη χρησιμότητας και η αίσθηση πολύ υψηλού κόστους, αποτελούν τα εμπόδια για την ανάπτυξη ολοκληρωμένου συστήματος επιχειρησιακής συνέχειας στο σύνολο των επιχειρήσεων αυτής της ομάδας. Στα τρία τελευταία χρόνια, οι μεγάλες και πολύ μεγάλες επιχειρήσεις κινούνται αργά στην κατεύθυνση της υιοθέτησης συστημάτων επιχειρησιακής συνέχειας. Η έρευνα δεν μπορεί να αποτυπώσει στην πράξη πόσο ολοκληρωμένα και πόσο λειτουργικά είναι τα συστήματα αυτά. Αρκείται στις σχετικές δηλώσεις όσων συμμετείχαν. Αποτυπώνει τη σαφή πρόοδο τόσο στην εξοικείωση με τον όρο επιχειρησιακή συνέχεια, όσο και στην (καθολική πλέον) αντίληψη για τη χρησιμότητα της, επισημαίνει όμως ότι σε ένα περιβάλλον τεράστιας έντασης κινδύνων και απειλών, η υιοθέτηση ολοκληρωμένων συστημάτων επιχειρησιακής συνέχειας, κινείται με σαφώς βραδύτερους ρυθμούς απ’ όσο θα ανέμενε κανείς .

7.1 Συμπεράσματα -Επίλογος

Στην Ελλάδα που μαστίζεται από την οικονομική κρίση πρωταρχικός σκοπός για κάθε επιχείρηση είναι η διαφύλαξη των εσόδων της, με παράλληλη προστασία της εταιρικής της εικόνας και φήμης. Μπορούμε να αναφέρουμε ότι διανύουμε την εποχή που η Επιχειρησιακή συνέχεια δεν είναι πολυτέλεια αλλά επιτακτική ανάγκη για τη βιωσιμότητα των επιχειρήσεων. Αποτελεί βασική προϋπόθεση η δυνατότητα ενός οργανισμού, να αντιμετωπίζει έκτακτα συμβάντα με τις μικρότερες δυνατές απώλειες καθώς και να προβλέπει τις κατάλληλες εκείνες ασπίδες αντιμετώπισης για τη συνέχιση της λειτουργίας της γενικότερα.

Η Επιχειρησιακή Συνέχεια αφορά όλες τις επιχειρήσεις, ασχέτως κλάδου και μεγέθους. Στις μέρες μας θεωρείται ιδιαίτερα επιτακτική απαίτηση για τα Χρηματοπιστωτικά Ιδρύματα εξαιτίας της σύνθετης οργανωτικής δομής που παρουσιάζουν καθώς η αδιάλειπτη λειτουργία τους κρίνεται απαραίτητη περισσότερο από ποτέ. Μέσω της διασφάλισης της ομαλής

λειτουργίας των συστημάτων πληρωμών, εκκαθάρισης και διακανονισμού, διασφαλίζεται η οικονομική σταθερότητα εντός και εκτός ακόμη των εθνικών συνόρων καθώς η λειτουργία ορισμένων συστημάτων ξεπερνά τα εθνικά σύνορα σε χώρες της Ευρωπαϊκής Ένωσης. Τα περασμένα χρόνια επικρατούσε η θεωρία ότι η Επιχειρησιακή Συνέχεια ανήκε αποκλειστικά στον τομέα ευθύνης των τμημάτων μηχανογράφησης . Ωστόσο τα τελευταία χρόνια τα δεδομένα έχουν αλλάξει καθώς οι επιχειρήσεις στρέφονται όλο και περισσότερο στο Business Continuity για τη δημιουργία ανθεκτικών επιχειρήσεων. Η Επιχειρησιακή Συνέχεια έχει εξελιχθεί σήμερα σε ένα ολοκληρωμένο Σύστημα Διοίκησης, με σκοπό τη δημιουργία ενός προστατευτικού πλαισίου γύρω από τις κρίσιμες λειτουργίες του οργανισμού, ανθρώπους, κτιριακές και τεχνολογικές υποδομές και συστήματα. Αξίζει να σημειωθεί και η σπουδαιότητα της συστηματικής καλλιέργειας της ατομικής ευθύνης του εργαζομένου απέναντι στην επιχείρηση για τη συνέχιση της ομαλής λειτουργίας της. Στο εξωτερικό κυρίως, οι επιχειρήσεις δίνουν ιδιαίτερη βαρύτητα στη συστηματική εκπαίδευση υπαλλήλων καθώς και της διοίκησης για την αναβάθμιση του επιπέδου ετοιμότητας και ανθεκτικότητάς τους, τόσο σε προσωπικό όσο και σε πρακτικό, λειτουργικό επίπεδο με στόχο την αποτελεσματική αντιμετώπιση πιθανών εκτάκτων κρίσεων πάσης φύσεως. Συνήθως, οι πρακτικές αυτές εντάσσονται στο γενικότερο Σύστημα Διοίκησης Επιχειρησιακής Συνέχειας, που οι επιχειρήσεις εφαρμόζουν. Εντούτοις η επιτυχία του συστήματος εξαρτάται σε μια σειρά από προϋποθέσεις που αφορούν κυρίως τον ανθρώπινο παράγοντα αρχής γενόμενης από τη διοίκηση και το κατά πόσον είναι οικειοθελώς δεσμευμένη να εντάξει το Σύστημα Επιχειρησιακής Συνέχειας στις αρχές εταιρικής στρατηγικής της επιχείρησης. Ιδιαιτέρως σε περιόδους ύφεσης, να αξιολογήσει την ευρύτερη σημασία της Επιχειρησιακής Συνέχειας ως επένδυση στη μελλοντική βιωσιμότητα της επιχείρησης. Όμως, τα καλύτερα πλάνα Επιχειρησιακής Συνέχειας θα παραμείνουν απλά πλάνα, αν ο κόσμος μέσα στην επιχείρηση δεν πεισθεί για την πραγματική αξία που προσφέρουν.

Επομένως, κυρίαρχη προϋπόθεση επιτυχίας είναι η δημιουργία της κατάλληλης κουλτούρας μέσα από την ενημέρωση, την ευαισθητοποίηση και την εκπαίδευση. Η εμπειρία έχει δείξει ότι όσο πιο πολύ συνεργάζονται οι μονάδες μεταξύ τους για την υλοποίηση ενός λογικού και αποτελεσματικού πλάνου επιχειρησιακής συνέχειας, τόσο περισσότερο ενισχύεται η ομαδικότητα και ενδυναμώνεται η κουλτούρα επιχειρησιακής πρόληψης και συνέχειας στον οργανισμό. Θεωρείται αυτονόητο ότι η Διαχείριση Επιχειρησιακής Συνέχειας ελέγχεται συστηματικά για τυχόν κενά και παραλείψεις.

Όσο πιο στενά συνεργάζονται διαφορετικές μονάδες της επιχείρησης μεταξύ τους για την υλοποίηση ενός αποτελεσματικού πλάνου επιχειρησιακής συνέχειας, τόσο μεγαλύτερη είναι η ευαισθητοποίηση και η ενδυνάμωση της κουλτούρας επιχειρησιακής συνέχειας στον επιχείρηση . Στα κυριότερα εμπόδια που καταγράφονται προκειμένου ένα Σύστημα Διοίκησης Επιχειρησιακής Συνέχειας να είναι ολοκληρωμένο και επιτυχημένο, είναι η εσφαλμένη αντίληψη να θεωρούνται ορισμένες μονάδες ότι είναι ξεχωριστές, με αποτέλεσμα να μην επιτυγχάνεται η στενή συνεργασία μεταξύ τους, κάτι που αποτελεί προϋπόθεση επιτυχίας.

Πέρα από τα προφανή πλεονεκτήματα που αναφέρθηκαν άνωθι, υπάρχουν και τα εγγενή, τα οποία αναγνωρίζονται μέσα από τις διαδικασίες που πραγματοποιούνται για την ανάπτυξη του Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας :

- Κατά την αποτύπωση της υποδομής του Οργανισμού, εμφανίζονται προβλήματα / κενά στην αρχιτεκτονική της υποδομής, είτε αυτά αφορούν τη ροή μιας διεργασίας είτε την οργάνωση της ροής εργασιών. Τα προβλήματα αυτά κατανοούνται και διορθώνονται.
- Κατά την Ανάλυση Επιχειρησιακών Επιπτώσεων, γίνεται βαθύτερη κατανόηση των διεργασιών του Οργανισμού. Αυτό μπορεί να βοηθήσει στο πρόγραμμα βελτιστοποίησης των διαδικασιών και κατά συνέπεια στη μείωση δαπανών για τον Οργανισμό.
- Το ποσοστό επιτυχούς ανάκαμψης της λειτουργικής συνέχειας από ένα περιστατικό ασφάλειας, σχετίζεται άμεσα με την απλότητα των διαδικασιών που την υποστηρίζουν. Ένα Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας θα βοηθήσει στην απλούστευση των διαδικασιών και κατά συνέπεια θα εξασφαλίσει την ευκολότερη ανάκαμψή τους σε περίπτωση κρίσης.
- Κατά τη διάρκεια εμφάνισης περιστατικών κρίσεων που μπορούν να προκαλέσουν διαταραχή στην επιχειρησιακή συνέχεια, ενδέχεται να επηρεαστούν όλα τα επίπεδα στην ιεραρχία ενός Οργανισμού. Με την υιοθέτηση ενός επιτυχημένου Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας δημιουργείται ένα εύκολο και άμεσο σύστημα επικοινωνίας και ενημέρωσης του προσωπικού, για τη διαχείριση κάθε περιστατικού.
- Με την κατανόηση του χρόνου αλλά και του επιπέδου αποκατάστασης των κρίσιμων δραστηριοτήτων του Οργανισμού, προσδιορίζεται η αναγκαιότητα για την ύπαρξη συγκεκριμένης υποδομής πληροφοριακών συστημάτων. Ο προσδιορισμός της υποδομής βοηθά τους Οργανισμούς, ώστε κατά τη σύνταξη του προϋπολογισμού τους να αναθέτουν το απαιτούμενο ποσό, προκειμένου να υποστηρίζεται η μέγιστη ανθεκτικότητα της υποδομής.

7.2 Συνεισφορά της Έρευνας

Από την ολοκλήρωση της παρούσας μεταπτυχιακής εργασίας διαπιστώθηκε ότι υπάρχουν ελάχιστες βιβλιογραφικές αναφορές σε διάσπαρτα κείμενα που αφορούν την διαχείριση πραγματικών περιστατικών κρίσεων και ενεργοποίησης πλάνων Επιχειρησιακής Συνέχειας. Για ευνόητους λόγους οι οργανισμοί δεν δημοσιεύουν τέτοιου είδους περιστατικά.

Το θεωρητικό μέρος της έρευνας αυτής προσδοκά στο να αφυπνίσει, να ενημερώσει τα αρμόδια στελέχη στην ύπαρξης μιας μεθόδου σύνταξης και ανάπτυξης Σχεδίου Επιχειρησιακής Συνέχειας. Αυτό συμβάλει στη δυνατότητα της διασφάλισης του οργανωτικού πλαισίου για τον καθορισμό του ΣΕΣ και στην ενσωμάτωση του στην κουλτούρα του οργανισμού, έτσι ώστε να έχει την ίδια βαρύτητα με άλλες αντίστοιχες που γίνονται για αμιγώς επιχειρησιακούς σκοπούς. Οι διαδικασίες αυτές αποτελούν σημαντική γνώση για τον οργανισμό. Από την Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis) σε συνδυασμό με τις βέλτιστες πρακτικές, εφόσον συνδυαστούν κατάλληλα μπορούν να χτίσουν την διαδικασία υλοποίησης του ΣΕΣ, αφού αξιολογούν το μέγεθος της επιχειρησιακής απώλειας και της μη ομαλής λειτουργίας τόσο των κρίσιμων πληροφοριακών συστημάτων όσο και των διαφόρων επιχειρησιακών λειτουργιών.

Κλείνοντας, κρίνουμε αναγκαίο να αναφέρουμε πως στόχος της προσπάθειας μας ήταν να αποτελέσει αντικείμενο προβληματισμού και ενδιαφέροντος για την εφαρμογή ενός δομημένου σχεδίου δράσης έτσι ώστε να διασφαλιστεί η επιχειρησιακή συνέχεια επιφέροντας μία προστιθέμενη αξία που μπορεί να επιφέρει σημαντικά πλεονεκτήματα , όπως εξοικονόμηση χρημάτων, χρόνου και πόρων στον οργανισμό. Η Σχεδίαση Επιχειρησιακής Συνέχειας αποτελεί περιουσιακό στοιχειό, το οποίο αν χρησιμοποιηθεί κατάλληλα, έχει τη δυνατότητα να αναδειχθεί ως σημαντικό στρατηγικό πλεονέκτημα για έναν οργανισμό.

7.3 Μελλοντική Μελέτη

Στην προηγούμενη ενότητα παρουσιάστηκαν τα κυριότερα αποτελέσματα της παρούσας εργασίας. Αναμφίβολα, οι ευρύτερες περιοχές έρευνας στις οποίες ανήκουν τα αποτελέσματα αυτά προσφέρουν πολλές προοπτικές. Κάτωθι παρατίθενται τα σημεία βελτίωσης και οι μελλοντικές προοπτικές έρευνας που θα μπορούσαν να πραγματοποιηθούν βάσει των αποτελεσμάτων που προέκυψαν από την παρούσα εργασία.

Παρόλα αυτά, μέσα από την συγκεκριμένη εργασία παρατηρήθηκαν σημεία βελτίωσης που όμως δεν θα μπορούσαν να υλοποιηθούν μέσω των διαθέσιμων βιβλιογραφικών αναφορών. Η κατασκευή μιας βάσης δεδομένων, καταγραφής αληθινών συμβάντων περιλαμβάνοντας τους κινδύνους και τις απαιτούμενες ενέργειες προς αντιμετώπιση αυτών, θα συμπλήρωνε ιδανικά την αποτελεσματική αντίδραση οποιουδήποτε οργανισμού σε καταστάσεις έκτακτης ανάγκης. Η ανταλλαγή πληροφοριών σε θέματα Επιχειρησιακής Συνέχειας θεωρείται πολύ σημαντική για την προετοιμασία και αποδοτικότητα σε περιπτώσεις έκτακτης ανάγκης ή κρίσης. Η συνεργασία μεταξύ αρμόδιων αρχών και συστημάτων είναι πολύ σημαντική για την διαχείριση διασυνοριακών προβλημάτων ή και κρίσεων.

Βασικό στοιχείο που χρήζει περισσότερης διερεύνησης αποτελεί ο εντοπισμός της ανάδειξης των κατάλληλων κινήτρων μεταξύ των συμμετεχόντων και μάλιστα σε σχέση με την εμπιστοσύνη τους προς τους υπευθύνους αποφάσεων. Όπως και να διεξαχθεί έρευνα σε οργανισμούς διαφορετικού μεγέθους οπού θα συγκρίνονται τα αποτελέσματα αυτών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Δρίβας, Γ.(2012).Σχεδιασμός Ανάκαμψης από Καταστροφές. Πανεπιστήμιο Πειραιώς– Τμήμα Ψηφιακών Συστημάτων, Πειραιάς

Καλαματιανός, Σ. (2011). Διασφάλιση Επιχειρησιακής Συνέχειας και Ανάκαμψης Συστημάτων. IT Professional Security Τεύχος Νοέμβριος – Δεκέμβριος: 10-12

Πετρόπουλος, Γ.(2012). Business Continuity Planning και η εφαρμογή του στις σύγχρονες επιχειρήσεις. Α.Τ.Ε.Ι. Μακεδονίας – Τμήμα Διοίκησης Επιχειρήσεων, Κοζάνη

ΠΔ/ΤΕ 2577 Πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργάνωσης και των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων και σχετικές αρμοδιότητες των διοικητικών τους οργάνων, 9 Μαρτίου 2006.

Σκιάνης,Χ.(2013).Μηχανική Κινδύνων και Σχεδιασμός Επιχειρησιακής Συνέχειας. Ε.Μ.Π.- Σχολή Μηχανολόγων Μηχανικών Τομέας Β.Δ. & Ε.Ε., Αθήνα

Φασόλης,Ε.(2012).Σύστημα Διαμόρφωσης και Σχεδιασμού Επιχειρησιακής Συνέχειας (Business Continuity Plan) Υποστηριζόμενο από Συλλογική Ευφυΐα (Collective Intelligence). Ανοιχτό Πανεπιστήμιο Κύπρου - Σχολή Θετικών και Εφαρμοσμένων Επιστημών, Κύπρος

Χαριτίδη, Μ. (2006) Business Continuity & Disaster Recovery Plan. Τεύχος Σεπτέμβριου: 8-10

ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Barnes, P. 2007. Business Impact Analysis. In The definitive handbook of business continuity management, ed. A. Hiles, 145-160

BCM Institute, BCM 8530 – BCM Audit and Governance course, ISO22301 BCM Lead Auditor Handbook, 2014

Bradbury, C. (2008) Disaster! Creating and testing an effective Recovery Plan. The British Journal of Administrative Management, 14-16

BS 25999 – 1 2006: Business Continuity Management – Part 1 Code of practice. British Standards.

Business Continuity Institute, The BCI Good Practice Guidelines 2010

Chisholm, P. (2008) Disaster Recovery Planning Is Business-Critical. *CPA Journal*, 78(7), 11

CISA Review Manual (2007) Business Continuity and Disaster Recovery, pp. 441-478

Dey, M., (2011). Business Continuity Planning (BCP) methodology — Essential for every business. GCC Conference and Exhibition (GCC), 2011 IEEE, p.229-232

Goh Moh Heng, GMH Continuity Architects, Business Continuity Management Series, 2nd Edition, 2006 and 2008

ISO/IEC 27031:2011: Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

ISO/IEC 22301:2012: Societal security – Business continuity management systems – Requirements

ISO/IEC 31000:2009, Risk management – Principles and guidelines

NIST Contingency Planning Guide for Information Technology Systems

Nollau, B. (2009) Disaster Recovery and Business Continuity. Journal of GXP Compliance, 13(3), 51-58

Stamatopoulou,S. (2012).Business Continuity. University of Piraeus– Department of Digital Systems, Piraeus

Thomas, A., & Fritz, L. (2006) Disaster Relief, Inc. Harvard Business Review, pp. 114-122

ΔΙΑΔΥΚΤΙΑΚΕΣ ΠΗΓΕΣ

Κέντρο Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α.). < http://www.kemea.gr >
ημερομηνία τελευταίας πρόσβασης (15/12/2016)

Business Continuity Institute: 'Glossary of Generic Business Continuity Management Terms' <http://www.thebci.org/glossary.pdf>
ημερομηνία τελευταίας πρόσβασης (15/12/2016)

Business Continuity Management Forum
<http://www.bcmforum.gr/ >
ημερομηνία τελευταίας πρόσβασης (15/01/2017)

Centre for Research on the Epidemiology of Disasters (CRED) < http://www.cred.be/>
ημερομηνία τελευταίας πρόσβασης (15/12/2016)

Centre for Research on the Epidemiology of Disasters (CRED). EM-DAT: The International Disaster Database <http://www.emdat.be/>
ημερομηνία τελευταίας πρόσβασης (15/12/2016)

Continuity Central: 'The International business continuity Information portal'. http://www.continuitycentral.com/
ημερομηνία τελευταίας πρόσβασης (15/12/2016)

Disaster Recovery Institute. < https://www.drii.org/>
ημερομηνία τελευταίας πρόσβασης (05/02/2017)

ISO - International Organization for Standardization
Business continuity management systems.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038 >
ημερομηνία τελευταίας πρόσβασης (15/12/2016)

ISO - International Organization for Standardization
The International Standard for Business Continuity – ISO 22301:2012 (Διαθέσιμο από τον Μάϊο 2012). < http://www.iso.org>
ημερομηνία τελευταίας πρόσβασης (15/01/2017)

Resiliency Group :'Historical Context'
<http://resiliencygroup.com/brmEvolution.html> ημερομηνία τελευταίας πρόσβασης (15/12/2016)

Wikipedia the free Encyclopedia: 'The Business continuity Planning'
<http://en.wikipedia.org/wiki/Business_continuity_planning>
ημερομηνία τελευταίας πρόσβασης (05/12/2016)

Wikipedia the free Encyclopedia: 'History of disaster recovery'
http://en.wikipedia.org/wiki/Disaster_recovery
ημερομηνία τελευταίας πρόσβασης (05/12/2016)