ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ

<<IT RISK MANAGEMENT: Η ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ ΣΕ ΕΤΑΙΡΕΙΕΣ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΠΛΗΡΟΦΟΡΙΚΗΣ>>

ΜΠΙΚΗΣ ΠΑΝΑΓΙΩΤΗΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΓΙΑΚΟΥΣΤΙΔΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΘΕΣΣΑΛΟΝΙΚΗ 2018

ΠΕΡΙΛΗΨΗ

Ο κίνδυνος αποτελεί ένα τεράστιο πεδίο έρευνας, ενώ οι θεωρίες και οι εφαρμογές του βρίσκουν ανταπόκριση σε πολλούς τομείς της οικονομίας.Για να γίνει, όμως, αποτελεσματική και σωστή διαχείριση των κινδύνων θα πρέπει να λάβουν χώρα δύο πράγματα. Το ένα είναι να γίνει κατανοητό τι είδους κίνδυνοι εμπλέκονται σε μια συγκεκριμένη οικονομική πράξη και το άλλο είναι να βρεθούν επαρκείς και αποτελεσματικές μέθοδοι έτσι ώστε να μετρηθούν οι κίνδυνοι αυτοί.

Η μέτρηση των κινδύνων διαφέρει ανάλογα με το είδος του κινδύνου. Είναι αντιληπτό ότι δεν είναι δυνατό να μετρηθεί, άρα και να διαχειριστεί, σωστά κάποιος κίνδυνος εάν δεν ξέρουμε ποια είναι η πηγή του και ποιο το είδος του. Στην πράξη υπάρχουν πολυάριθμοι κίνδυνοι που προέρχονται από ανάλογες πολυάριθμες πηγές. Εντούτοις, είναι δυνατό να ομαδοποιηθούν με κάποιον τρόπο δημιουργώντας «ομάδες» κινδύνων, που μπορούν να μετρηθούν με τον ίδιο τρόπο όσοι κίνδυνοι έχουν πηγή που προέρχονται από την ίδια ομάδα. Το επίκεντρο της καλής διαχείρισης κινδύνου είναι η αναγνώριση και ο χειρισμός αυτών των κινδύνων. Αυξάνει την πιθανότητα επιτυχίας, και μειώνει αμφότερα, την πιθανότητα αποτυχίας και την αβεβαιότητα επίτευξης των συνολικών στόχων.

Τα τελευταία χρόνια διαπιστώνεται ραγδαία εξέλιξη στην ανάπτυξη των συστημάτων πληροφορικής. Πολλοί από τους οργανισμούς του Δημοσίου και του Ιδιωτικού τομέα, βασίζονται στην ύπαρξη των πληροφοριακών συστημάτων. Αξιοποιώντας τα συστήματα αυτά σε καθημερινή βάση ανταλλάζουν πληροφορίες, προσφέρουν και αναπτύσσουν υπηρεσίες μεταφέροντας μεγάλο όγκο δεδομένων. Η ασφάλεια των πληροφοριακών συστημάτων είναι κρίσιμος παράγοντας για τη λειτουργία αλλά και τη βιωσιμότητα ενός οργανισμού. Η παραμικρή δυσλειτουργία, η διακοπή και η παράνομη διείσδυση στα

πληροφοριακά συστήματα έχουν ως αντίκτυπο να υπάρχουν οικονομικές απώλειες ακόμα και αδυναμία του οργανισμού να λειτουργήσει ομαλά. Ακόμα, τα σοβαρότερα προβλήματα ασφαλείας των πληροφοριακών συστημάτων επικεντρώνονται περισσότερο στο κομμάτι των συστημάτων εκείνων, όπου υπάρχουν καταγεγραμμένα ευαίσθητα δεδομένα, πληροφορίες και σημαντικές λειτουργίες. Για να επιτευχθεί η ασφάλεια χρειάζεται να εφαρμοστούν κατάλληλα μέτρα απέναντι στις διάφορες απειλές και κινδύνους που μπορεί να δεχθούν.

Σκοπός της παρούσας πτυχιακής εργασίας είναι να αναλυθεί διεξοδικά ο τρόπος αντιμετώπισης και διαχείρισης των επιμέρους κινδύνων που μπορεί να κληθεί να αντιμετωπίσει ένας οργανισμός, ιδιαίτερα αν πρόκειται για επιχείρηση που σχετίζεται με την πληροφορική και τα πληροφοριακά συστήματα, να γίνει καταμέτρηση των κινδύνων αυτών και να διευκρινιστεί η τεράστια σημασία της ασφάλειας των πληροφοριακών συστημάτων κατά των χειρισμό των εκάστοτε κινδύνων που είναι πιθανό να εμφανιστούν.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1:ΕΙΣΑΓΩΓΗ

Το θέμα «εκτίμηση κινδύνου» αποτελεί ένα τεράστιο πεδίο έρευνας, ενώ οι θεωρίες και οι εφαρμογές του βρίσκουν ανταπόκριση σε πολλούς τομείς της οικονομίας. Η εκτίμηση κινδύνου είναι μια διαδικασία ιδιαίτερα σημαντική όπου η σημασία της έχει συνειδητοποιηθεί πλήρως τα τελευταία χρόνια από όλους τους φορείς στις παγκόσμιες οικονομίες (κυβερνήσεις, μεγάλες επιχειρήσεις, επιχειρηματίες, ιδιώτες, κτλ.) και για αυτό το σκοπό έχουν αναπτυχθεί έντονα τα τελευταία χρόνια διάφορα υποδείγματα μέτρησης εκτίμησης και γενικότερης διαχείρισης του κινδύνου.

Ο στρατηγικός σχεδιασμός δράσης (Business plan) κάθε οικονομικής μονάδας, που βασίζεται στην υλοποίηση των στόχων, λόγω των ραγδαίων εξελίξεων στο διεθνές προσκήνιο, (την παγκοσμιοποίηση, την ανοιχτή αγορά, τη νομισματική ένωση,) για να επιτύχει χρειάζεται τον πλήρη καθορισμό, την διερεύνηση, την ανάλυση και την όσο το δυνατόν πιο επιτυχή αντιμετώπιση των κινδύνων που επιφυλάσσει κάθε λειτουργία της οικονομικής μονάδας.

Σήμερα ο ανταγωνισμός λόγω της διεθνούς αγοράς και της συνεχούς εξέλιξης καθιστά απαραίτητη την διαχείριση κινδύνων για την επιβίωση και την επιτυχή πορεία ενός οικονομικού οργανισμού.

Το risk management (διαχείριση κινδύνων) εξετάζει την δυνατότητα που έχει κάποιο συμβάν να προκαλέσει ζημιά. Μέσα από επιλεγμένες στρατηγικές, για κάθε παράγοντα κινδύνου, το risk management εκτιμάει την πορεία του σχεδίου δράσης (business plan) του οικονομικού οργανισμού, μελετάει την επικινδυνότητα κάθε ρίσκου που ο οικονομικός οργανισμός, πρόκειται να πάρει. Δεν προβλέπει απλά, αλλά αναλύει τους παράγοντες και τους κινδύνους και εκτιμάει το κόστος που θα προκληθεί σε κάθε περίπτωση.

Η διαχείριση κινδύνου είναι ένας γρήγορα αναπτυσσόμενος κλάδος και υπάρχουν πολλές και ποικίλες απόψεις και περιγραφές για το τι εμπεριέχει η διαχείριση κινδύνου, πώς πρέπει να διεξαχθεί και για ποιο σκοπό. Κάποια μορφή προτύπου είναι αναγκαία για να διασφαλίσει ότι υπάρχουν συμφωνημένα τα εξής:

- ορολογία σχετικά με τις λέξεις που χρησιμοποιούνται.
- διεργασία μέσω της οποίας μπορεί να διεξαχθεί η διαχείριση κινδύνου.
- οργανωτική δομή για τη διαχείριση κινδύνου.
- στόχος για τη διαχείριση κινδύνου.

Η διαχείριση κινδύνου δεν είναι μόνο κάτι για εταιρείες ή δημόσιους οργανισμούς, αλλά για οποιαδήποτε δραστηριότητα είτε βραχυπρόθεσμη είτε μακροπρόθεσμη. Τα οφέλη και οι ευκαιρίες πρέπει να εξετασθούν όχι μόνο εντός του πλαισίου της ίδιας της δραστηριότητας, αλλά σε σχέση με τους πολλούς και διαφορετικούς ενδιαφερόμενους που μπορεί επηρεασθούν.

Στην εποχή μας η ραγδαία τεχνολογική ανάπτυξη των πληροφοριακών συστημάτων και οι υπηρεσίες που μας παρέχουν καθημερινά είναι γεγονός. Πολλοί οργανισμοί βασίζονται στα πληροφοριακά συστήματα τα οποία αποτελούν καθοριστικό παράγοντα για τη λειτουργία και την ανάπτυξή τους. Ταυτόχρονα η συλλογή, η επεξεργασία, η αποθήκευση και η διάθεση δεδομένων αποτελούν σημαντικό αγαθό για τον κάθε οργανισμό. Τα τελευταία χρόνια και λόγω της αυξημένης χρήσης τους, τα πληροφοριακά συστήματα είναι ευάλωτα σε διαφόρων ειδών απειλών, είτε από το εσωτερικό, είτε από το εξωτερικό τους περιβάλλον. Οι απειλές αυτές μπορεί να έχουν ως συνέπεια να προκύψουν ανυπολόγιστα προβλήματα που πολλές φορές μεταφράζονται σε οικονομικές απώλειες ή με την παρεμπόδιση της σωστής λειτουργίας τους.

Πέρα όμως από τις οικονομικές επιπτώσεις τα προβλήματα ασφαλείας γίνονται πιο κρίσιμα σε συστήματα όπου υπάρχουν ευαίσθητα δεδομένα και σε συστήματα όπου πραγματοποιούνται και επεξεργάζονται σημαντικές λειτουργίες (π.χ συστήματα στρατού). Λόγω όμως της ιδιαιτερότητας των συστημάτων και της γρήγορης ανάπτυξής τους σε ένα σύνθετο περιβάλλον μεταβλητών και παραγόντων δημιουργείται μεγαλύτερη πολυπλοκότητα ως προς την ασφάλειά τους. Επομένως η ανάγκη για ασφάλεια στα πληροφοριακά συστήματα αποτελεί σημαντική προτεραιότητα για όσους τα σχεδιάζουν και τα υλοποιούν καθώς και γι' αυτούς που τα χρησιμοποιούν και τα διαχειρίζονται.

ΚΕΦΑΛΑΙΟ 2:Η ΕΝΝΟΙΑ ΤΟΥ RISK MANAGEMENT

Είναι αντιληπτό και κατανοητό ότι η έννοια του κινδύνου συνδέεται ιδιαίτερα στενά με την λογική και την έννοια της αβεβαιότητας,η οποία πολλές φορές επηρεάζει τις αποφάσεις και τις πράξεις ενός ανθρώπου/οργανισμού,επιφέροντας επιθυμητά ή ανεπιθύμητα αποτελέσματα. Η διαχείρηση κινδύνων ενσωματώνεται σε ένα απέραντο φάσμα λήψης αποφάσεων από την κατανομή περιουσιακών στοιχείων σε επίπεδο χαρτοφυλακίου μέχρι

την διασφάλιση της δημόσιας υγείας,από την εξόρυξη πετρελαίου μέχρι την προστασία του περιβάλλοντος και από την πληρωμή ασφαλίστρων μέχρι την χρήση ζώνης ασφαλείας στα αυτοκίνητα.Σε κάθε περίπτωση,κίνδυνος σημαίνει έκθεση στην αβεβαιότητα και αφορά τόσο τις ανθρώπινες δραστηριότητες(καθημερινός τρόπος ζωής και σκέψης) όσο και τις εκάστοτε επιχειρήσεις,γι'αυτό και θα πρέπει να είμαστε προετοιμασμένοι για την αντιμετώπισή του. Η διαφορά μεταξύ ρίσκου και αβεβαιότητας είναι ότι το ρίσκο συμβαίνει σε κάποιον συγκεκριμένο άνθρωπο ή επιχείρηση,ενώ η αβεβαιότητα είναι ένα γενικό χαρακτηριστικό που αφορά πολλούς ανθρώπους ή πολλές επιχειρήσεις.

Σε όλους τους τύπους των δραστηριοτήτων, υπάρχει το ενδεχόμενο για γεγονότα και συνέπειες που συνιστούν ευκαιρίες προς όφελος (upside) ή απειλές της επιτυχίας (downside). Η διαχείριση κινδύνου, αναγνωρίζεται, όλο και περισσότερο, ότι έχει σχέση με αμφότερες τις θετικές και τις αρνητικές πλευρές του κινδύνου. Στον τομέα της ασφάλειας, αναγνωρίζεται γενικά ότι οι συνέπειες είναι μόνο αρνητικές και γι' αυτό η διαχείριση του κινδύνου ασφάλειας εστιάζει στην πρόληψη και τον μετριασμό της ζημιάς.

Η διαχείριση κινδύνου είναι κεντρικός πυρήνας της διαχείρισης στρατηγικής κάθε οργανισμού. Είναι η διεργασία με την οποία οι οργανισμοί προσεγγίζουν μεθοδικά τους κινδύνους που σχετίζονται με τις δραστηριότητές τους, με σκοπό την επίτευξη αειφόρου οφέλους σε κάθε δραστηριότητα και επί του χαρτοφυλακίου όλων των δραστηριοτήτων.

Το επίκεντρο της καλής διαχείρισης κινδύνου είναι η αναγνώριση και ο χειρισμός αυτών των κινδύνων. Στόχος της είναι να προσθέσει τη μέγιστη αειφόρο αξία σε όλες τις δραστηριότητες του οργανισμού. Ταξινομεί την κατανόηση των πιθανών οφελών (upside) και απειλών (downside) όλων εκείνων των παραγόντων που μπορούν να επηρεάσουν τον οργανισμό. Αυξάνει την πιθανότητα επιτυχίας, και μειώνει αμφότερα, την πιθανότητα

αποτυχίας και την αβεβαιότητα επίτευξης των συνολικών στόχων του οργανισμού.

Η διαχείριση κινδύνου θα έπρεπε να είναι μία συνεχής και αναπτυσσόμενη διεργασία, η οποία διατρέχει τη στρατηγική του οργανισμού και την υλοποίηση αυτής της στρατηγικής. Θα έπρεπε να προσεγγίζει μεθοδικά όλους τους κινδύνους που περιβάλλουν τις παλαιότερες, τρέχουσες και ιδιαιτέρως τις μελλοντικές δραστηριότητες του οργανισμού. Πρέπει να μεταφράζει τη στρατηγική σε τακτικούς και επιχειρησιακούς στόχους, καθορίζοντας υπευθυνότητες σε κάθε επίπεδο του οργανισμού, με κάθε διοικητικό στέλεχος και εργαζόμενο υπεύθυνο για τη διαχείριση του κινδύνου ως μέρος της περιγραφής της εργασίας του. Υποστηρίζει την ευθύνη, την μέτρηση επίδοσης και την ανταμοιβή, έτσι ώστε να προωθείται η λειτουργική αποδοτικότητα σε όλα τα επίπεδα.

Ο κίνδυνος αποτελεί μια από τις πιο συνήθεις παραμέτρους της καθημερινής ζωής και υφίσταται σε όλες εκείνες τις περιπτώσεις που δεν μπορεί να προβλεφθεί με βεβαιότητα το αποτέλεσμα μιας δραστηριότητας. Η έννοια του κινδύνου σε σχέση με μια συγκεκριμένη δραστηριότητα είναι η πιθανότητα εμφάνισης ενός μη επιθυμητού αποτελέσματος και μπορεί να οριστεί ως η έκθεση στην αβεβαιότητα. Η έννοια της αβεβαιότητας με την σειρά της είναι στενά συνδεδεμένη με την έννοια της μεταβλητότητας (variability) ή της αστάθειας (volatility). Οι κίνδυνοι από εσφαλμένες εκτιμήσεις έχουν συχνά ανεπιθύμητες συνέπειες για τις επιχειρήσεις (π.χ. κόστος), με αποτέλεσμα η διοίκηση να προβαίνει σε ενέργειες για την διαχείρηση των κινδύνων, που δεν σχετίζονται με την στρατηγική ή με τους αρχικούς στόχους που έχουν τεθεί.

Ο κίνδυνος συχνά συνδέεται με τις παρακάτω έννοιες:

- Απειλή (threat): είναι οποιαδήποτε πράξη ή γεγονός που θα μπορούσε να παραβιάσει την ασφάλεια ενός συστήματος και να προκαλέσει ζημιά.
- Ευπάθεια (vulnerability): είναι μια αδυναμία του συστήματος, η ύπαρξη της οποίας

μπορεί να επιτρέψει την πραγματοποίηση της απειλής .

- Επίπτωση (consequence): είναι το αποτέλεσμα της παραβίασης της ασφάλειας και η έκταση της ζημιάς που έχει προκληθεί.

Στις επιχειρήσεις ο κίνδυνος διαδραματίζει έναν κρίσιμο ρόλο για τον λόγο ότι είναι εμφανής σε όλες τις δραστηριότητες, ανεξάρτητα από τον σκοπό και από την διάρθρωση των λειτουργιών τους. Σχεδόν κάθε επιχειρηματική απόφαση απαιτεί από την διοίκηση την εξισορρόπηση των κινδύνων, μια διαδικασία που είναι απαραίτητη για την επιτυχία μιας επιχείρησης. Μπορούμε να διακρίνουμε τρεις κατηγορίες επιχειρήσεων σύμφωνα με τον τρόπο που συμπεριφέρονται στα πλαίσια της αβεβαιότητας που αντιμετωπίζουν,ως προς τις συνθήκες του περιβάλλοντος και τη διαμόρφωση της πολιτικής που ακολουθούν:

1. Επιχειρήσεις που έχουν την πεποίθηση ότι δεν μπορούν να αλλάξουν τον τρόπο διαμόρφωσης των μελλοντικών συνθηκών, με αποτέλεσμα να αδυνατούν να λάβουν κάποιο μέτρο για την αντιμετώπιση της αβεβαιότητας.
2. Επιχειρήσεις που θεωρούν αδύνατη την τροποποίηση των μελλοντικών συνθηκών, αλλά υποστηρίζουν την συνεχή προσαρμογή τους σε αυτές ως βασική μέθοδο εξασφάλισης της βιωσιμότητάς τους.
3. Επιχειρήσεις που υποστηρίζουν την ενεργή διαμόρφωση των μελλοντικών συνθηκών τους, βάση των παρόντων και των μελλοντικών δυνατοτήτων τους.

Ένας κίνδυνος μιας επιχείρησης μπορεί να συσχετιστεί με τις ακόλουθες έννοιες:

- Αποτυχία: ανικανότητα έργου, υποέργου ή υπηρεσίας να ολοκληρώσει την απαιτούμενη λειτουργία του.
- Ασφάλεια ποιότητας: Πιθανότατα να μην ανταποκρίνεται το έργο στους σκοπούς για τους οποίους ετοιμάστηκε.

- Αξιοπιστία: Πιθανότητα το έργο να πραγματοποιήσει τους σκοπούς για τους οποίους σχεδιάστηκε, για συγκεκριμένο χρονικό διάστημα ή κάτω από συγκεκριμένες συνθήκες.
- Ασφάλεια εργασιών: Τεχνικές ελαχιστοποίησης της πιθανότητας να συμβεί ατύχημα ή περιορισμού των συνεπειών του ατυχήματος με σχεδιασμό και προληπτική συντήρηση.
- Αβεβαιότητα: Μέτρο των ορίων γνώσης σε τεχνικό τομέα. Τα τέσσερα κύρια στοιχεία της αβεβαιότητας είναι η στατιστική εμπιστοσύνη (μέτρο της ακρίβειας των δειγμάτων), η ανεκτικότητα (μέτρο της διαθέσιμης πληροφορίας), τα ημιτελή και ανακριβή δεδομένα εισόδου και η ασάφεια στην μοντελοποίηση του έργου.

Η εκτέλεση της διαδικασίας διαχείρισης κινδύνων ακολουθεί 6 βήματα τα οποία είναι τα εξής:

- Ανάπτυξη σχεδίου διαχείρισης Κινδύνων.
- Ανίχνευση και εντοπισμός Κινδύνων.
- Ανάλυση Κινδύνων.
- Αντιμετώπιση Κινδύνων.
- Παρακολούθηση Κινδύνων.
- Αναφορά και Αξιολόγηση Κινδύνων.

Το αρχικό στάδιο της διαδικασίας διαχείρισης κινδύνων περιέχει την ανάπτυξη σχεδίου διαχείρισης κινδύνων (Growth of drawing of management of Dangers) το οποίο είναι βασικό στοιχείο που υλοποιεί τη διαδικασία διαχείρισης κινδύνων. Ο σχεδιασμός του και η πληρότητα είναι σημαντικός παράγοντας για την επιτυχία και αποτυχία του. Το σχέδιο αυτό παρουσιάζει τον τρόπο με τον οποίο υλοποιούνται τα στάδια της διαδικασίας της διαχείρισης κινδύνων. Το μέγεθος του σχεδίου είναι ισοδύναμο με το μέγεθος του έργου

και είναι αναγκαίο όσο μικρό και αν είναι το έργο. Τα περιεχόμενα του σχεδίου ανάλυσης κινδύνων κατηγοριοποιούνται ως εξής:

- Η Τεχνική (Technique): Η τεχνική περιέχει μεθόδους καταγραφής ώστε να οριστεί ο τρόπος προσέγγισης της διαχείρισης των κινδύνων και τα εργαλεία καθώς και οι πηγές για την αναζήτηση στοιχείων. Για παράδειγμα σε μια τεχνική θα πρέπει να καθοριστεί αν ο εντοπισμός των κινδύνων θα γίνει από τον ίδιο οργανισμό που είναι αρμόδιος για την υλοποίηση του έργου.
- Οι Ρόλοι και Αρμοδιότητες (Roles and Responsibilities): Έχοντας επιλέξει την τεχνική μπορεί αμέσως να συγκροτηθεί η ομάδα της διαχείρισης του κινδύνου και να γίνει η μοιρασιά των αρμοδιοτήτων. Μετά εγκρίνεται ο αρμόδιος της διαδικασίας και αποφασίζεται αν η ομάδα είναι εσωτερική ή εξωτερική. Ως προς την εσωτερική ομάδα δεν προκύπτει πρόβλημα στην εξουσία διότι τα στελέχη έχουν τις κατάλληλες γνώσεις για τα δεδομένα του οργανισμού. Αντιθέτως στην εξωτερική ομάδα πρέπει να υλοποιείται πλήρως το πρόγραμμα του έργου και να υπάρχει καλή συνεννόηση της ομάδας και της διοίκησης για το καλύτερο αποτέλεσμα.
- Ο Οικονομικός Προϋπολογισμός (Financial Budget): Για να οριστεί ο οικονομικός προϋπολογισμός της διαχείρισης των κινδύνων υπάρχουν πολλοί τρόποι. Ένας από αυτούς είναι να καθοριστεί ένα ποσό του κόστους του έργου για την αντιμετώπιση του κινδύνου. Το μειονέκτημα είναι ότι δεν μπορούν να καθοριστούν από πριν οι κίνδυνοι άρα το ποσό μπορεί να ξεπεράσει το ύπαρχον με συνέπεια να προκαλέσει λάθος αποτέλεσμα. Ένας δεύτερος τρόπος είναι η ανάλυση των κινδύνων και η εκτίμηση μιας συνολικής έκθεσης. Το μειονέκτημα και σε αυτήν την περίπτωση είναι ότι ο προϋπολογισμός θα υπολογιστεί σε ανάλογο χρόνο έτσι ώστε να προσδιοριστούν καλύτερα ο εντοπισμός και η ανάλυση τω κινδύνων.Μια παραλλαγή και τρόπων αυτών είναι η επιλογή και των δύο. Από τη μια θα είναι γνωστό το κόστος της διαχείρισης των κινδύνων και από την άλλη το κόστος θα πρέπει να συνυπολογίζεται στο συνολικό κόστος για τη διαχείριση των

κινδύνων του έργου.

- Ο Χρονισμός (Timing): Θα πρέπει να διεξάγονται περιοδικές συναντήσεις για τη συζήτηση των αναφορών σχετικά με την εξέλιξη, εντοπισμό και την αντιμετώπιση των νέων κινδύνων.
- Η Εκπαίδευση (Education): Θα πρέπει να διεξάγονται προγράμματα εκπαίδευσης για τα στελέχη της διαχείρισης έργων είτε από εσωτερικούς ή από εξωτερικούς συμβούλους προβάλλοντας τεχνικές και εργαλεία αντιμετώπισης για τους κινδύνους.
- Η Επικοινωνία (Communication): Είναι ο τρόπος που διέπει την καταγραφή, ανάλυση και την κοινοποίηση των αποτελεσμάτων της διαχείρισης των κινδύνων στους ενδιαφερομένους του έργου.
- Η Τεχνική Μέτρησης και Κλίμακες (Technique of measurement and scales): Εδώ προσδιορίζονται οι τεχνικές μέτρησης (ποσοτικές, ποιοτικές) που θα χρησιμοποιηθούν καθώς και οι κλίμακες (συνέπεια, πιθανότητα) που προσδιορίζουν τα χαρακτηριστικά των κινδύνων.
- Τα Όρια (Limits): Πρέπει να προσδιορίζονται τα όρια για τους κινδύνους. Υπάρχουν τρεις κατηγορίες κινδύνων οι ασπυαντοι. οι υέσοι και οι σπυαντικοί. Τα όρια αυτά είναι διαφορετικά για κάθε οργανισμό και προσδιορίζουν την κατηγορία στην οποία βρίσκεται ο κίνδυνος. Είναι σημαντικό να προσδιορίζονται τα όρια πριν την εκτέλεση του έργου.

ΚΕΦΑΛΑΙΟ 3:ΕΙΔΗ,ΑΝΑΛΥΣΗ,ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΧΕΙΡΙΣΜΟΣ-ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ

3.1 ΕΙΔΗ ΚΙΝΔΥΝΟΥ

Υπάρχουν διάφορα είδη κινδύνου. Ανάλογα με την οικονομική πράξη και το είδος του περιουσιακού στοιχείου ο κίνδυνος σχετικά με κάποιο μελλοντικό αποτέλεσμα μπορεί να λάβει διαφορετικές μορφές.

Ένας πρώτος διαχωρισμός είναι βάσει της φύσης και της προέλευσής τους. Όσον αφορά τη φύση τους οι κίνδυνοι διακρίνονται σε ευκαιρίες και απειλές ενώ όσον αφορά την προέλευσή τους εσωτερικούς ή εξωτερικούς κινδύνους. Εσωτερικός είναι ένας κίνδυνος που επηρεάζεται από τις ενέργειες του ίδιου του οργανισμού/επιχείρησης, ενώ εξωτερικός αυτός του οποίου η πιθανότητα εμφάνισης δεν μπορεί να αλλάξει από κάποια ενέργεια του οργανισμού/επιχείρησης.

Οι ***εσωτερικοί κίνδυνοι*** διακρίνονται σε τεχνολογικούς, οργανωτικούς και απρόβλεπτους. Με τον όρο **τεχνολογικός** εννοείται η αδυναμία συμμόρφωσης ενός έργου με τις απαιτούμενες προδιαγραφές. Αυτό μπορεί να συμβαίνει εξ'αιτίας της λανθασμένης τεχνολογίας που επελέγη, του σχεδιασμού, της παραγωγής ή της λειτουργίας του έργου. Επίσης, οι εσωτερικοί τεχνολογικοί κίνδυνοι μπορεί να οφείλονται στην εγγενή αβεβαιότητα ή σε γεγονότα. Η εγγενής αβεβαιότητα είναι η διακύμανση ενός μεγέθους γύρω από μια μέση τιμή η οποία προκύπτει λόγω των εκάστοτε συνθηκών που μπορεί να λάβουν χώρα κατά τη διάρκεια εκτέλεσης ενός έργου.

Οι **εσωτερικοί οργανωτικοί** κίνδυνοι οφείλονται στους εξής παράγοντες:

1) στην αδυναμία εμπρόθεσμης ολοκλήρωσης ενός έργου
2) στην αδυναμία ολοκλήρωσης του έργου στο προϋπολογισθέν κόστος
3) στην αποτυχία της οργανωτικής δομής του οργανισμού/επιχείρησης
4) στην ακαταλληλότητα των διαθέσιμων πόρων
5) στην διακοπή της χρηματοδότησης

Οι **εσωτερικοί απρόβλεπτοι** κίνδυνοι είναι αυτοί που μπορεί να προκύωουν καθ'όλη τη διάρκεια ζωής ενός έργου και οι οποίοι δεν έχουν προσδιοριστεί εκ των προτέρων.

Οι ***εξωτερικοί κίνδυνοι*** διακρίνονται σε **προβλέψιμους** και **απρόβλεπτους**. Οι **προβλέψιμοι** βρίσκονται έξω από τη σφαίρα επιρροής της ομάδας έργου. Σχετικά παραδείγματα είναι η συμπεριφορά των αγορών πρώτων υλών που καθορίζει τις τιμές, την

διαθεσιμότητα και την ζήτηση, η εκάστοτε φορολογική πολιτική καθώς και τυχόν συναλλαγματικές διαφορές. Οι εξωτερικοί **απρόβλεπτοι** κίνδυνοι μπορούν να απαριθμηθούν αλλά δεν μπορεί να προβλεφθεί αν και πότε θα εμφανιστούν. Τέτοιοι κίνδυνοι είναι οι αλλαγές κυβερνήσεων, οι πόλεμοι, οι φυσικές καταστροφές, οι έκτακτες καταστάσεις, η πτώχευση του πελάτη ή ενός υπεργολάβου.

Οι κίνδυνοι οι οποίοι δεν μπορούν να προβλεφθούν και να υπολογισθούν αντικειμενικά, και οι οποίοι κυρίως οφείλονται στην ατελή γνώση και την αβεβαιότητα που κατέχουν οι λήπτες των αποφάσεων, δεν ασφαλίζονται και δεν συμπεριλαμβάνονται στο κόστος λειτουργίας της επιχείρησης. Η ύπαρξη των κινδύνων αυτών αποτελεί στοιχείο αιτιολόγησης, από την πλευρά των οικονομολόγων, του κέρδους των επιχειρήσεων.

Θα πρέπει ακόμη να σημειωθεί ότι τα άτομα και ειδικότερα οι λήπτες των αποφάσεων σε μία επιχείρηση, συμπεριφέρονται διαφορετικά έναντι του κινδύνου. Άλλοι προτιμούν να αντιμετωπίσουν μεγάλο ύψος κινδύνου, με την προσδοκία μεγάλου ύψους κέρδους, ενώ άλλοι προτιμούν ένα μέτριο ύψος κέρδους, που να συνοδεύεται από μικρό ύψος κινδύνου. Στην οικονομική θεωρία διακρίνονται τρία είδη πιθανής συμπεριφοράς των ατόμων έναντι του κινδύνου:

- Οι επιδιώκοντες τον κίνδυνο
- Οι αποστρεφόμενοι τον κίνδυνο και
- Οι αδιάφοροι έναντι του κινδύνου.

Ένας δεύτερος διαχωρισμός είναι σε επιχειρηματικούς (Business Risk) και χρηματοοικονομικούς (Financial Risk) κινδύνους. Οι πρώτοι έχουν να κάνουν με την δυνατότητα της κάθε επιχείρησης να λειτουργεί αποδοτικά και να καταφέρνει, βάση της βασικής λειτουργίας, να παράγει σημαντικά έσοδα και ταμειακές ροές. Κάθε επιχείρηση

λειτουργεί σε κάποιο κλάδο ή αγορά που έχει πλήθος κινδύνων είτε σε επίπεδο αγοράς, είτε σε επίπεδο ατομικό επιχειρησιακό. Η μεταβλητότητα των ταμειακών ροών θεωρείται ότι έχει πηγή τον λεγόμενο επιχειρηματικό κίνδυνο.

Οι δεύτεροι κίνδυνοι έχουν να κάνουν με την αστάθεια και μεταβλητότητα των διάφορων χρηματοοικονομικών αγορών (χρηματιστήρια, αγορά χρήματος, συναλλάγματος κτλ). Τέτοιοι κίνδυνοι επηρεάζουν χρηματοοικονομικούς οργανισμούς (τράπεζες, εταιρίες επενδύσεων, αμοιβαία κεφάλαια, ασφαλιστικές εταιρίες κτλ) και όσες άλλες επιχειρήσεις, οργανισμούς ή και ιδιώτες εμπλέκονται με αυτές. Οι χρηματοοικονομικοί κίνδυνοι θεωρείται ότι έχουν μια σειρά από πηγές ανάλογα και με τη φύση του περιουσιακού στοιχείου που εμπλέκεται σε μια οικονομική πράξη.

3.1.1 ΚΙΝΔΥΝΟΣ ΑΓΟΡΑΣ

Στο πλαίσιο του κίνδυνου προς τα κάτω (downside risk), ο κίνδυνος αγοράς θεωρείται ότι είναι ο κίνδυνος που προέρχεται από ανεπιθύμητες μεταβολές στην αγοραία αξία των διάφορων περιουσιακών στοιχείων εξ' αιτίας των διάφορων μεταβολών που λαμβάνουν χώρα στην αγορά όπου διαπραγματεύονται τα διάφορα περιουσιακά στοιχεία, κατά τη διάρκεια που είναι δυνατό να ρευστοποιηθεί κάποιο περιουσιακό στοιχείο. Η περίοδος ρευστοποίησης θεωρείται πολύ σημαντική στο πλαίσιο της εκτίμησης του κινδύνου αγοράς, καθώς όσο πιο μεγάλη είναι αυτή η περίοδος τόσο περισσότερο υπάρχουν ευκαιρίες για μεγάλη μεταβολή της αξίας του υποκείμενου περιουσιακού στοιχείου.

Σύμφωνα με διάφορους οικονομολόγους ο κίνδυνος αγοράς μπορεί να αντιμετωπιστεί είτε με απλό τρόπο, ρευστοποιώντας τα διάφορα περιουσιακά στοιχεία για να αποφευχθεί απώλεια από πιθανή πτώση της αξίας τους, εάν βέβαια αυτό μπορεί να γίνει, δηλαδή εάν η περίοδος ρευστοποίησης είναι από τη φύση του περιουσιακού στοιχείου μικρή, είτε με πιο σύνθετο τρόπο αντισταθμίζοντας τον με χρήση κατάλληλων συναλλαγών και παραγώγων

χρηματοοικονομικών εργαλείων.

Σημαντικό ρόλο στον κίνδυνο αγοράς παίζει και ο κίνδυνος ρευστότητας. Υποστηρίζεται ότι σε αγορές με υψηλή ρευστότητα, άρα και ευκολία στις συναλλαγές η μεταβλητότητα στην τιμή –άρα και την αξία- προς τα κάτω ενός περιουσιακού στοιχείου δεν είναι τόσο μεγάλη. Αντίθετα, σε αγορές με χαμηλή ρευστότητα, ο κίνδυνος να πέσει πολύ η αξία ενός περιουσιακού στοιχείου είναι σαφώς μεγαλύτερος. Έτσι, φαίνεται καθαρά και στην πράξη ότι τα είδη των κινδύνων αναμεταξύ τους συνδέονται στενά και ότι ο συνολικός κίνδυνος ενός περιουσιακού στοιχείου σε επίπεδο αξίας ή απόδοσης δεν είναι ένα απλό άθροισμα κινδύνων. Ανεξάρτητα, πάντως, από τον κίνδυνο ρευστότητας, ο «καθαρός» κίνδυνος αγοράς έχει τις πηγές του από τις μεταβολές που λαμβάνουν χώρα στις διάφορες παραμέτρους των αγορών που επηρεάζουν ένα περιουσιακό στοιχείο.

Σε επίπεδο μέτρησης του κινδύνου αγοράς έχει προταθεί η μεθοδολογία «Αξία σε Κίνδυνο» (Value at Risk – VaR). Σύμφωνα με αυτή τη μεθοδολογία, εκτιμάται μια πιθανή (με μεγάλη πιθανότητα πραγματοποίησης 95% ή 99%) προς τα κάτω απώλεια. Για την ακρίβεια εκτιμάται η μέγιστη προς τα κάτω απώλεια που λαμβάνει χώρα σε ένα συγκεκριμένο χρονικό ορίζοντα και οφείλεται καθαρά στις μεταβολές των παραμέτρων της αγοράς που επηρεάζουν ένα συγκεκριμένο περιουσιακό στοιχείο.

3.1.2 ΠΙΣΤΩΤΙΚΟΣ ΚΙΝΔΥΝΟΣ

Η φύση του πιστωτικού κινδύνου διακρίνεται διακρίνεται στις τρεις παρακάτω κατηγορίες:

1) κίνδυνος αθέτησης
2) κίνδυνος έκθεσης
3) κίνδυνος ανάκτησης

ΚΙΝΔΥΝΟΣ ΑΘΕΤΗΣΗΣ

Ο κίνδυνος αθέτησης θεωρείται ότι είναι μια σημαντική πηγή απώλειας. Ο κίνδυνος αυτός ορίζεται σαν ο κίνδυνος αθέτησης από την μεριά κάποιου που είναι δανειολήπτης με κάποιο τρόπο (δάνειο από τράπεζα, έκδοση ομολόγου, κτλ) και πραγματεύεται το ενδεχόμενο αποτυχίας του δανειολήπτη ,μια συγκεκριμένη στιγμή, να είναι συνεπής με τις υποχρεώσεις που έχει ως προς την αποπληρωμή του δανείου σχετικά με τις δόσεις και του τόκους. Ο κίνδυνος αθέτησης μετράται από την πιθανότητα αθέτησης, όπου μετράει την πιθανότητα να αθετήσει κάποιος δανειολήπτης μια συγκεκριμένη πληρωμή. Ο κίνδυνος αθέτησης έχει ως αποτέλεσμα μερική ή ολική απώλεια του ποσού που εκείνη τη στιγμή ο δανειολήπτης οφείλει στον δανειστή.

Μια άλλη διάσταση του πιστωτικού κινδύνου αθέτησης θεωρείται ότι είναι ο κίνδυνος να μειωθεί η πιστοληπτική ικανότητα κάποιου τωρινού ή υποψήφιου δανειολήπτη. Βέβαια, μια τέτοια μείωση δεν σημαίνει αθέτηση πληρωμής, αλλά σημαίνει ότι η πιθανότητα αθέτησης αυξάνεται και η μείωση της πιστοληπτικής ικανότητας περνάει στο κόστος του δανεισμού το οποίο αυξάνει για να αντισταθμίσει αυτήν την αύξηση του κινδύνου για τον δανειολήπτη.

Θα πρέπει στο σημείο αυτό να τονιστεί ότι υπάρχουν διάφορα είδη αθετήσεων:

- Καθυστέρηση στην πληρωμή. Απλές καθυστερήσεις στην πληρωμή δεν μετατρέπονται απαραίτητα σε αθέτηση, καθώς η ανικανότητα για αποπληρωμή σε πολλές περιπτώσεις είναι πρόσκαιρη.
- Ανασχηματισμός των δανειακών υποχρεώσεων εξ' αιτίας σημαντικής πτώσης στην πιστοληπτική ικανότητα. Θεωρείται ότι είναι πολύ κοντά σε αυτό που ονομάζεται οριστική καθυστέρηση των οφειλών, καθώς συνήθως προέρχεται από δομικά προβλήματα στην ικανότητα του δανειολήπτη στο να αντιμετωπίσει τις δανειακές του υποχρεώσεις. Εντούτοις, σε κάποιες περιπτώσεις, ένας τέτοιος ανασχηματισμός βοηθάει τον δανειολήπτη να μπορεί να αποπληρώσει τις υποχρεώσεις του και την τράπεζα να μην

υποστεί απώλειες λόγω πιστωτικού κινδύνου.

- Χρεωκοπία. Ο δανειστής κινείται, βάσει νόμου, για να διεκδικήσει τα οφειλόμενα μέσω της ρευστοποίησης των όποιων περιουσιακών στοιχείων έχει στην κατοχή του ο δανειολήπτης. Σε μια τέτοια περίπτωση, το γεγονός της αθέτησης είναι δεδομένο.

Στον πιστωτικό κίνδυνο, θα πρέπει να αναφέρουμε ένα ακόμα κίνδυνο ο οποίος μοιάζει, με τον πιστωτικό κίνδυνο. Ο κίνδυνος αυτός είναι ο κίνδυνος χώρας (Country Risk). Ο κίνδυνος χώρας θεωρείται ότι είναι ο κίνδυνος που οφείλεται σε μια κρίση που συμβαίνει σε μια χώρα και μπορεί να προκαλέσει απώλειες σε κατόχους περιουσιακών στοιχείων που αποτιμώνται στο νόμισμα αυτής της χώρας. Πιο συγκεκριμένα, ο κίνδυνος χώρας περιλαμβάνει:

- Κίνδυνο αθέτησης πληρωμών του δημοσίου σε εξωτερικούς δανειστές λόγω αύξησης των ελλειμμάτων κτλ.
- Δυσμενή μεταβολή των οικονομικών συνθηκών που προκαλεί πτώση της πιστοληπτικής ικανότητας των διάφορων τοπικών δανειοληπτών.
- Μεγάλη πτώση της συναλλαγματικής αξίας του τοπικού νομίσματος.
- Αδυναμία μεταφοράς κεφαλαίων εκτός χώρας.

Θα πρέπει να τονιστεί ότι ο κίνδυνος χώρας αποτελεί βάση για τον πιστωτικό κίνδυνο, όπως μετράται από τις πιστωτικές διαβαθμίσεις, όλων των εγχώριων δανειοληπτών. Έτσι, ο κάθε δανειολήπτης εκτιμάται ως προς την πιστοληπτική του ικανότητα και μέσω της πιστοληπτικής ικανότητας της χώρας που ανήκει.

ΚΙΝΔΥΝΟΣ ΕΚΘΕΣΗΣ

Σε γενικές γραμμές ο κίνδυνος έκθεσης μπορεί να θεωρηθεί ως μια εκτίμηση του βαθμού στον οποίο η τράπεζα μπορεί να βρεθεί εκτεθειμένη από κάποιον αντισυμβαλλόμενο ,π.χ.

δανειολήπτη, σε χρονική στιγμή και για χρηματικό ποσό που οφείλει ο αντισυμβαλλόμενος κατά τη στιγμή της αθέτησης και ονομάζεται «έκθεση κατά τη στιγμή της αθέτησης». Ο υπολογισμός του κινδύνου έκθεσης διαφέρει αν επιτευχθεί με τη βασική προσέγγιση (foundation approach) σε σχέση με την προηγμένη προσέγγιση (advanced approach). Στο πλαίσιο της βασικής προσέγγισης ο υπολογισμός της έκθεσης κινδύνου διέπεται από ρυθμιστικές αρχές ,ενώ σύμφωνα με την εξελιγμένη προσέγγιση (A-IRB) οι τράπεζες έχουν μεγαλύτερη ευελιξία σχετικά με το ποια μέθοδο θα εφαρμόσουν για να υπολογιστεί ο κίνδυνος έκθεσης, βάσει της φύσεως της εκάστοτε συναλλαγής και των χαρακτηριστικών της. Ο κίνδυνος έκθεσης χρησιμοποιείται κυρίως στις επιχειρήσεις τραπεζικού τομέα.

ΚΙΝΔΥΝΟΣ ΑΝΑΚΤΗΣΗΣ

Ο κίνδυνος ανάκτησης περιγράφει ποιο μέρος από το ποσό που οφείλεται κατά τη στιγμή της αθέτησης κατάφερε ο δανειστής να ανακτήσει από τον δανειολήπτη. Το ποσοστό του ποσού που κατάφερε να ανακτήσει ως προς την συνολική οφειλή ονομάζεται ποσοστό ανάκτησης (Recovery Rate), ενώ το ποσοστό του ποσού που δεν κατάφερε να ανακτήσει ως προς την συνολική οφειλή ονομάζεται «απώλεια δεδομένης της αθέτησης»

3.1.3 ΚΙΝΔΥΝΟΣ ΡΕΥΣΤΟΤΗΤΑΣ

Ο κίνδυνος ρευστότητας παίζει σημαντικό ρόλο στην διαμόρφωση του κινδύνου αγοράς. Πιστεύεται ότι ο κίνδυνος ρευστότητας επιδεινώνει περισσότερο τις αρνητικές συνέπειες που προκαλεί ουσιαστικά ο κίνδυνος αγοράς ο οποίος αναφέρεται σε πολλές διαστάσεις όπως αδυναμία να αντληθούν κεφάλαια σε κάποιο λογικό κόστος, κίνδυνος ρευστότητας περιουσιακού στοιχείου ,κίνδυνος ρευστότητας αγοράς, κτλ.

Ο κίνδυνος άντλησης κεφαλαίων εξαρτάται από το πόσο επικίνδυνο θεωρεί η αγορά κάποια οικονομική μονάδα που θέλει να αντλήσει κεφάλαια. Ουσιαστικά, η επικινδυνότητα κάποιου στο θέμα της άντλησης κεφαλαίων έχει να κάνει, σε πολλές περιπτώσεις με την πιστοληπτική του ικανότητα. Κάποιος που χρειάζεται κεφάλαια, αλλά δεν έχει καλή

πιστοληπτική ικανότητα αντιμετωπίζει περισσότερες δυσκολίες να βρει αυτά τα κεφάλαια που χρειάζεται. Έτσι, ο κίνδυνος ρευστότητας σε τέτοιο επίπεδο αυξάνει το κόστος άντλησης κεφαλαίων και έτσι μειώνει κάποια επικείμενη κερδοφορία και επιπλέον μελλοντική διευκόλυνση στην άντληση επιπλέον κεφαλαίων.

Ο κίνδυνος ρευστότητας περιουσιακού στοιχείου έχει να κάνει με το κατά πόσο εύκολη είναι η αγοροπωλησία ενός συγκεκριμένου περιουσιακού στοιχείου ανεξάρτητα από την ρευστότητα που υπάρχει στην συγκεκριμένη αγορά που διαπραγματεύεται. Είναι δυνατό, για ειδικούς λόγους, κάποιο περιουσιακό στοιχείο να είναι δύσκολο να διαπραγματευτεί για να γίνει αντικείμενο αγοροπωλησίας. Επίσης, είναι δυνατό να μην μπορεί να διαπραγματευτεί για λόγους συμφωνίας. Για παράδειγμα, μια προθεσμιακή κατάθεση έχει πρόστιμο εάν ο καταθέτης θελήσει να έχει τα χρήματα πριν την προκαθορισμένη ημερομηνία. Ομοίως, ένα δάνειο να μην μπορεί να αποπληρωθεί πριν την προκαθορισμένη λήξη ακόμα και εάν ο δανειζόμενος μπορεί και επιθυμεί να το εξοφλήσει πλήρως. Είναι προφανές ότι ο κίνδυνος ρευστότητας περιουσιακού στοιχείο έχει ισχυρή αλληλεπίδραση τόσο με τον κίνδυνο ρευστότητας αγοράς, όσο και με τον κίνδυνο άντλησης κεφαλαίων.

Ο κίνδυνος ρευστότητας της αγοράς έχει να κάνει με το κατά πόσο συχνές είναι οι αγοροπωλησίες σε μια συγκεκριμένη αγορά. Έχει παρατηρηθεί ότι ο κίνδυνος ρευστότητας σε τέτοιο επίπεδο προκαλεί υψηλό προς τα κάτω, αλλά και προς τα πάνω κίνδυνο, όταν κάποιος αντισυμβαλλόμενος είναι απρόθυμος, για τους δικούς του λόγους, να προβεί σε κάποια συναλλαγή. Πάντως, θεωρείται ότι ο κίνδυνος άντλησης κεφαλαίων και ο κίνδυνος ρευστότητας αγοράς είναι ισχυρά συνδεδεμένοι και θεωρείται ότι ουσιαστικά ο ένας είναι αιτία εμφάνισης του άλλου και το αντίθετο.

Ο κίνδυνος ρευστότητας θεωρείται ένας πολύ σημαντικός κίνδυνος που πρέπει να διαχειριστεί αποτελεσματικά, καθώς είναι δυνατό, σε μια ακραία μορφή του, να οδηγήσει

ακόμα και στην χρεωκοπία. Βέβαια, θα πρέπει να τονιστεί ότι αυτή η ακραία μορφή του κινδύνου ρευστότητας είναι συχνά αποτέλεσμα των άλλων κινδύνων. Εντούτοις, η αντιμετώπισή του δεν θεωρείται μια διαδικασία ιδιαίτερα δύσκολη και επίπονη. Σκοπός είναι να υπάρχουν ρευστά και ποιοτικά περιουσιακά στοιχεία, έτσι ώστε να καλύπτονται τα «κενά ρευστότητας», είτε με ρευστοποίηση των υπαρχόντων περιουσιακών στοιχείων, είτε με άντληση ρευστών κεφαλαίων σε λογικό κόστος, λόγω της καλής ποιότητας των υπαρχόντων περιουσιακών στοιχείων που προσδίδουν καλή πιστοληπτική ικανότητα.

3.1.4 ΛΕΙΤΟΥΡΓΙΚΟΣ ΚΙΝΔΥΝΟΣ

Ο λειτουργικός κίνδυνος δεν θεωρείται ένας χρηματοοικονομικός κίνδυνος. Εντούτοις, λαμβάνει χώρα στο πλαίσιο της λειτουργίας όχι απλά όλων των επιχειρήσεων, αλλά και στο πλαίσιο όλων των λειτουργιών μέσα σε μια επιχείρηση για αυτό και κρίνεται σκόπιμο να εξεταστεί σαν ένα είδος κινδύνου. Με την εξάπλωση και την χρήση νέων τεχνολογιών και καινοτομιών σχεδόν σε όλους τους κλάδους της οικονομίας, ο λειτουργικός κίνδυνος έχει αποκτήσει μια ιδιαίτερη σημασία στο γενικότερο πλαίσιο της διαχείρισης κινδύνων, και έτσι όλο και περισσότεροι ασχολούνται με την φύση του, τη διαδικασία μέτρησης και εκτίμησής του, καθώς και την αντιμετώπισή του στο γενικότερο πλαίσιο της διαχείρισης του λειτουργικού κινδύνου.

Ο λειτουργικός κίνδυνος έχει, λοιπόν, τις πηγές του σε υπολειτουργίες, και ιδιαίτερα κακές λειτουργίες, των πληροφοριακών συστημάτων που χρησιμοποιούνται από κάποιο οργανισμό, όπως τα διάφορα συστήματα αναφορών, τα εσωτερικά συστήματα παρακολούθησης κινδύνου και τις όποιες εσωτερικές διεργασίες έχουν σχεδιαστεί για να παράγουν έγκυρα και έγκαιρα αποτελέσματα συμμορφωμένα με τους κανόνες που διαμορφώνονται εσωτερικά σχετικά με την διαχείριση κινδύνων.

Η γενική αρχή της μέτρησης του λειτουργικού κινδύνου θεωρείται ότι είναι να εκτιμηθεί η πιθανότητα εμφάνισης κάποιου δυσάρεστου απρόοπτου και η απώλεια που θα επιφέρει ένα τέτοιο απρόοπτο. η διαδικασία αυτή δεν είναι τόσο εύκολη, καθώς η ταξινόμηση των πηγών του λειτουργικού κινδύνου είναι υποκειμενική, όπως και η διαδικασία της συλλογής των κατάλληλων δεδομένων δεν είναι ιδιαίτερα εύκολή.

Στην πραγματικότητα ο λειτουργικός κίνδυνος είναι αποτέλεσμα κάποιων γεγονότων και συγκυριών που έχουν ως αποτέλεσμα μια απώλεια. Υπάρχει ένας τεράστιος αριθμός γεγονότων, στο πλαίσιο του λειτουργικού κινδύνου, που μπορεί να προκαλέσουν απώλειες. Για μια αποτελεσματική διαχείριση του λειτουργικού κινδύνου έχει προταθεί να ταξινομηθούν, με κάποια κριτήρια, τα γεγονότα που προκαλούν την εμφάνισή του. Στο πλαίσιο αυτής της ταξινόμησης, ο λειτουργικός κίνδυνος εμφανίζεται στα παρακάτω διαφορετικά επίπεδα:

- Άνθρωποι
- Ανθρώπινο λάθος
- Απειρία ή/ και ανικανότητα
- Απάτη
- Διαδικασίες
- Ανεπαρκείς διαδικασίες και έλεγχοι στην αναφορά, την επίβλεψη και την λήψη αποφάσεων
- Ανεπαρκείς διαδικασίες στην προώθηση πληροφοριών, λάθη στην καταγραφή συναλλαγών, κτλ
- Οργανωτικές ανεπάρκειες
- Ανεπάρκειες διαχείρισης στην επίβλεψη κινδύνου
- Τεχνικές ανεπάρκειες των πληροφοριακών συστημάτων ή των συστημάτων διαχείρισης κινδύνου
- Λάθη στα μοντέλα

- Λάθη στην υλοποίηση τεχνικών συστημάτων
- Απουσία επαρκών εργαλείων για μέτρηση κινδύνων
- Υπολειτουργία (κακή λειτουργία) των πληροφοριακών συστημάτων
- Βλάβες στα πληροφοριακά συστήματα

Πάντως, η διαδικασία συλλογής δεδομένων είναι το πρώτο βήμα στο πλαίσιο της μέτρησης και εκτίμησης του λειτουργικού κινδύνου. Τα δεδομένα που συλλέγονται αναλύονται στατιστικά με τέτοιο τρόπο έτσι ώστε να αποκαλυφθούν κάποιες συσχετίσεις και αιτιώδεις σχέσεις που να συνδέουν την εμφάνιση κάποιου απρόοπτου γεγονότος που προκάλεσε απώλειες με κάτι συγκεκριμένο που δεν δούλεψε καλά σε εκείνη την περίπτωση. Η ανάλυση ολοκληρώνεται με την εκτίμηση των απωλειών στην χειρότερη περίπτωση, κάτι που παραπέμπει στη λογική της εκτίμησης της αξίας σε κίνδυνο.

3.2 ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ

3.2.1 Αναγνώριση Κινδύνου

Η αναγνώριση κινδύνου σκοπό έχει την ταυτοποίηση της έκθεσης του οργανισμού στην αβεβαιότητα. Αυτό απαιτεί μία βαθιά γνώση του οργανισμού, της αγοράς στην οποία δραστηριοποιείται, το νομικό, κοινωνικό, πολιτικό και πολιτισμικό περιβάλλον στο οποίο υπάρχει, καθώς και στην ανάπτυξη μιας ορθής κατανόησης των στρατηγικών και λειτουργικών στόχων, και παραγόντων κρίσιμων για την επιτυχία τους και τις απειλές και ευκαιρίες που σχετίζονται με την επίτευξη αυτών των στόχων.

Η αναγνώριση κινδύνου θα έπρεπε να προσεγγισθεί με ένα μεθοδικό τρόπο για να διασφαλίσει ότι όλες οι σημαντικές δραστηριότητες εντός του οργανισμού και ότι όλοι οι κίνδυνοι που απορρέουν από αυτές τις δραστηριότητες έχουν προσδιορισθεί. Οι επιχειρηματικές δραστηριότητες και αποφάσεις μπορούν να κατηγοριοποιηθούν ως εξής:

• Στρατηγικές - Αφορούν τους μακροχρόνιους στρατηγικούς στόχους του οργανισμού. Μπορεί να επηρεασθούν από θέματα όπως η διαθεσιμότητα κεφαλαίων, κρατικούς και πολιτικούς κινδύνους, νομικές και ρυθμιστικές αλλαγές, φήμη και αλλαγές στο φυσικό περιβάλλον.

• Λειτουργικές - Αφορούν τα καθημερινά θέματα που αντιμετωπίζει ένας οργανισμός στην προσπάθειά του να εκπληρώσει τους στρατηγικούς του στόχους.

• Χρηματο-οικονομικές - Αφορούν την αποτελεσματική διαχείριση και έλεγχο των χρηματο-οικονομικών του οργανισμού και τις επιδράσεις εξωτερικών παραγόντων όπως η διαθεσιμότητα πίστωσης, οι τιμές ξένου συναλλάγματος, οι τάσεις των επιτοκίων και άλλες εκθέσεις σε κινδύνους της αγοράς.

• Διαχείρισης γνώσης - Αφορούν την αποτελεσματική διαχείριση και έλεγχο των πόρων γνώσης, της παραγωγής, προστασίας και επικοινωνίας αυτών των πόρων.

Εξωτερικοί παράγοντες που επηρεάζουν τις σχετικές αποφάσεις και δραστηριότητες μπορεί να περιλαμβάνουν την μη εγκεκριμένη χρήση ή κακή χρήση της πνευματικής ιδιοκτησίας, την τοπική πτώση ισχύος, και την ανταγωνιστική τεχνολογία. Εσωτερικοί παράγοντες μπορεί να είναι μία δυσλειτουργία του συστήματος ή η απώλεια βασικών στελεχών η θέματα όπως η υγεία και η ασφάλεια, το περιβάλλον, οι εμπορικές περιγραφές προϊόντος, η προστασία του καταναλωτή, η προστασία δεδομένων, οι πρακτικές εργασιακής απασχόλησης και τα ρυθμιστικά θέματα.

Ενώ η αναγνώριση κινδύνου μπορεί να διεξαχθεί από εξωτερικούς συμβούλους, μία εκ των έσω προσέγγιση με διεργασίες καλά ανακοινωμένες, συνεκτικές και συντονισμένες , είναι ίσως πιο αποτελεσματική. Η εσωτερική "ιδιοκτησία" της διεργασίας διαχείρισης κινδύνου είναι πολύ σημαντική και θεμελιώδης.

3.2.2 Περιγραφή Κινδύνου

Ο στόχος της περιγραφής κινδύνου είναι η απεικόνιση των αναγνωρισμένων κινδύνων σε μία δομημένη μορφή, για παράδειγμα, με τη χρήση ενός πίνακα. Ο πίνακας περιγραφής κινδύνων μπορεί να χρησιμοποιηθεί για να διευκολύνει την περιγραφή και αποτίμηση των κινδύνων. Η χρήση μίας καλά σχεδιασμένης δομής είναι αναγκαία για να διασφαλίσει μία περιεκτική διεργασία αναγνώρισης, περιγραφής και αποτίμησης κινδύνου. Λαμβάνοντας υπόψη την συνέπεια και πιθανότητα καθενός από τους κινδύνους που είναι καταγεγραμμένοι στον πίνακα, θα έπρεπε να είναι δυνατόν να τεθούν προτεραιότητες στους βασικούς κινδύνους που χρειάζονται να αναλυθούν σε μεγαλύτερη λεπτομέρεια. Η αναγνώριση των κινδύνων που σχετίζονται με επιχειρηματικές δραστηριότητες και λήψη αποφάσεων μπορεί να κατηγοριοποιηθεί σε στρατηγικούς, έργου/τακτικούς, λειτουργικούς. Είναι σημαντικό να ενσωματωθεί η διαχείριση κινδύνων στην αρχική, εννοιολογικά σχεδιαστική φάση των έργων καθώς και σε ολόκληρο τον κύκλο ζωής ενός συγκεκριμένου έργου.

Πίνακας 1. Περιγραφή Κινδύνου

1. Ονομασία	
2. Πεδίο Κινδύνου	Ποιοτική περιγραφή του μεγέθους, του τύπου, του αριθμού και των συσχετίσεων των γεγονότων.
3. Φύση Κινδύνου	π.χ. στρατηγικός, λειτουργικός, χρηματο-οικονομικός, γνωστικός, συμμόρφωσης.
4.Έχοντες έννομο ενδιαφέρον (stakeholders)	Οι έχοντες έννομο ενδιαφέρον και οι προσδοκίες τους.
5. Ποσοτικοποίηση Κινδύνου	Σημαντικότητα και Πιθανότητα.
6. Ανοχή / Όρεξη στον Κίνδυνο	Η δυνητική απώλεια και η χρηματο-οικονομική επίδραση του κινδύνου. Αξία (περιουσιακών ή άλλων στοιχείων) σε κίνδυνο. Πιθανότητα και μέγεθος των δυνητικών ζημιών / κερδών. Στόχος ή στόχοι για τον έλεγχο του κινδύνου και επιθυμητό επίπεδο επίδοσης.
7. Χειρισμός Κινδύνου & Μηχανισμοί Ελέγχου	Βασικά μέσα με τα οποία ο κίνδυνος σήμερα διαχειρίζεται.

	Επίπεδα εμπιστοσύνης στον υφιστάμενο έλεγχο. Αναγνώριση πρωτοκόλλων παρακολούθησης και ανασκόπησης.
8. Δυνητική Ενέργεια Βελτίωσης	Συστάσεις για μείωση κινδύνου.
9. Ανάπτυξη Στρατηγικής και Πολιτικής	Αναγνώριση της υπεύθυνης λειτουργίας του οργανισμού για την ανάπτυξη στρατηγικής και πολιτικής.

3.2.3 Εκτίμηση Κινδύνου

Η εκτίμηση κινδύνου μπορεί να είναι ποσοτική, μερικώς ποσοτική ή ποιοτική όσον αφορά την πιθανότητα εμφάνισης και την πιθανή συνέπεια. Για παράδειγμα, συνέπειες, σε αμφότερες απειλές (downside risks) και ευκαιρίες (upside risks) μπορεί να είναι υψηλές, μεσαίες ή χαμηλές. Η πιθανότητα μπορεί να είναι υψηλή, μεσαία ή χαμηλή αλλά απαιτεί διαφορετικούς ορισμούς σχετικά με τις απειλές και τις ευκαιρίες.

Παραδείγματα παρουσιάζονται στους παρακάτω πίνακες .Διαφορετικοί οργανισμοί θα βρουν ότι διαφορετικά κριτήρια για την συνέπεια και την πιθανότητα θα εξυπηρετήσουν καλύτερα τις ανάγκες τους. Για παράδειγμα, πολύ οργανισμοί βρίσκουν ότι η αποτίμηση της συνέπειας και της πιθανότητας ως υψηλή, μεσαία ή χαμηλή, είναι αρκετά ικανοποιητική για τις ανάγκες του και μπορεί να παρουσιασθεί σε έναν 3x3 πίνακα.

Πίνακας 2. Συνέπειες - Αμφότερες Απειλές και Ευκαιρίες

Υψηλή	Χρηματο-οικονομική επίδραση στον οργανισμό που αναμένεται να υπερβαίνει τα x€. Σημαντική επίδραση στην στρατηγική του οργανισμού ή στις επιχειρησιακές Δραστηριότητες. Σημαντική ανησυχία των εχόντων έννομο ενδιαφέρον (stakeholders).
Μεσαία	Χρηματο-οικονομική επίδραση στον οργανισμό που αναμένεται μεταξύ x€ και y€. Μέτρια επίδραση στην στρατηγική ή τις επιχειρησιακές δραστηριότητες του Οργανισμού. Μέτρια ανησυχία των εχόντων έννομο ενδιαφέρον (stakeholders).

Χαμηλή	Χρηματο-οικονομική επίδραση στον οργανισμό που αναμένεται μικρότερη των γ€. Χαμηλή επίδραση στην στρατηγική ή τις επιχειρησιακές δραστηριότητες του Οργανισμού. Χαμηλή ανησυχία των εχόντων έννομο ενδιαφέρον (stakeholders).

Πίνακας 3. Πιθανότητα Εμφάνισης – Απειλές

Υψηλή (Πιθανή)	Πιθανόν να συμβεί κάθε χρόνο ή περισσότερο με πιθανότητα εμφάνισης 25%	Είναι δυνατό να συμβεί πολλές φορές μέσα σε μία χρονική περίοδο (π.χ. δέκα χρόνια). Έχει συμβεί πρόσφατα.
Μεσαία (Δυνατή)	Πιθανόν να συμβεί σε μία περίοδο 10 ετών ή μικρότερη με πιθανότητα να εμφανισθεί 25%.	Θα μπορούσε να συμβεί περισσότερο από μία φορά μέσα σε μία χρονική περίοδο (π.χ. δέκα χρόνια). Θα μπορούσε να είναι δύσκολο να ελεγχθεί λόγω κάποιων εξωτερικών επιρροών. Υπάρχει ιστορικό συμβάντων;
Χαμηλή (Ελάχιστη)	Όχι πιθανόν να συμβεί σε μία περίοδο 10 ετών ή μικρότερη με πιθανότητα να εμφανισθεί 2%.	Δεν έχει συμβεί. Απίθανο να συμβεί.

Πίνακας 4. Πιθανότητα Εμφάνισης – Ευκαιρίες

Εκτίμηση	Περιγραφή	Δείκτες
Υψηλή (Πιθανή)	Ευνοϊκό αποτέλεσμα είναι πιθανόν να επιτευχθεί σε ένα χρόνο ή μεγαλύτερη με πιθανότητα εμφάνισης 75%.	Σαφής ευκαιρία, που μπορεί να είναι βάσιμη με αιτιολογημένη βεβαιότητα, και είναι να επιτευχθεί βραχυπρόθεσμα μέσω των υφισταμένων διαχειριστικών διεργασιών.
Μεσαία (Δυνατή)	Λογικές προσδοκίες για ευνοϊκά αποτελέσματα σε ένα χρόνο με πιθανότητα εμφάνισης από 25% έως 75%.	Ευκαιρίες που μπορεί να είναι επιτεύξιμες αλλά που απαιτούν προσεκτική διαχείριση. Ευκαιρίες που μπορεί να αναδειχθούν πέραν του επιχειρηματικού σχεδίου.

Χαμηλή (Ελάχιστη)	Μικρή πιθανότητα ευνοϊκού Αποτελέσματος μεσοπρόθεσμα ή λιγότερο με πιθανότητα εμφάνισης 25%.	Πιθανή ευκαιρία η οποία δεν έχει ακόμη εξετασθεί πλήρως από την διοίκηση. Ευκαιρία η οποία έχει χαμηλή πιθανότητα επιτυχίας στη βάση των διοικητικών πόρων που χρησιμοποιούνται επί του παρόντος.

Στη διάρκεια της εκτίμησης των κινδύνων πρέπει να λαμβάνουμε υπόψη τα μειονεκτήματα και τα πλεονεκτήματα της ποσοτικής αξιολόγησης ως προς την ποιοτική αξιολόγηση. Το μειονέκτημα της ποιοτικής ανάλυσης είναι ότι δεν υπάρχουν κάποια ορισμένα μεγέθη υπολογίσιμα για να εκτιμηθεί το μέγεθος των επιπτώσεων, με συνέπεια η ανάλυση κέρδους-κόστους για προτεινόμενες δράσεις είναι πολύ δύσκολη. Το σημαντικότερο πλεονέκτημα όμως της ποιοτικής αξιολόγησης είναι ότι βάζει προτεραιότητες μεταξύ των κινδύνων καθώς και να εντοπίζει τα τμήματα του έργου που χρειάζονται γρήγορη βελτίωση, προσδιορίζοντας τις ευαίσθητες περιοχές αυτού.

Σε αντίθεση στην ποσοτική ανάλυση το μειονέκτημα είναι ότι τα αριθμητικά αποτελέσματα υπάρχει περίπτωση να μην καταλήγουν σε λογικά και ξεκάθαρα συμπεράσματα και έτσι να απαιτείται επιπλέον ποιοτική ανάλυση των αποτελεσμάτων αυτών. Το πλεονέκτημα της ποσοτικής ανάλυσης είναι ότι προσφέρει τέτοιες πληροφορίες, διευκολύνοντας τις αναλύσεις κέρδους-κόστους παρέχοντας συγκεκριμένες τιμές για την δράση μας. Στο σημείο αυτό πρέπει να τονιστεί ότι στην ποσοτική αξιολόγηση το επίπεδο της πολυπλοκότητας και του κόστους είναι υψηλότερα από αυτά της ποιοτικής αξιολόγησης.

Ανακεφαλαιώνοντας, η ποιοτική ανάλυση στηρίζεται στην εμπειρία και τη λογική καθώς και στις δυνατότητες των ατόμων που τις παρουσιάζουν, ενώ η ποσοτική ανάλυση στηρίζεται στα αριθμητικά αποτελέσματα καθώς και στην αξιοπιστία των τεχνικών και μοντέλων που χρησιμοποιούνται. Όταν παρουσιάζεται θέμα κόστους χρησιμοποιείται η ποσοτική αξιολόγηση για να βγουν συμπεράσματα, αλλά όταν το κόστος δεν θεωρείται σημαντικός

παράγοντας παρουσιάζονται και οι δύο τρόποι για να βγουν πιο ορθότερα και ασφαλέστερα συμπεράσματα. Επομένως για την πλήρη αξιολόγηση των κινδύνων είτε μιλάμε για ποσοτική είτε για ποιοτική, είναι απαραίτητο να ληφθεί υπόψη και ο παράγοντας της συνεχής εμφάνισης ενός κινδύνου στα πλαίσια μια συγκριμένης χρονικής περιόδου έχοντας υπόψη και τις επιπτώσεις που έχει σε κάθε εμφάνισή του.

3.2.4 Προφίλ Κινδύνου

Το αποτέλεσμα της διεργασίας ανάλυσης κινδύνου μπορεί να χρησιμοποιηθεί για να παραχθεί ένα προφίλ κινδύνου το οποίο δίνει ένα βαθμό σημαντικότητας σε κάθε κίνδυνο και παρέχει ένα εργαλείο για την θέσπιση προτεραιότητας των προσπαθειών χειρισμού κινδύνων. Κατατάσσει κάθε αναγνωρισμένο κίνδυνο για να δώσει μία άποψη της σχετικής σημαντικότητας.

Αυτή η διεργασία επιτρέπει τη χαρτογράφηση του κινδύνου στην επιχειρηματική περιοχή που επηρεάζει, περιγράφει τις βασικές διαδικασίες ελέγχου σε εφαρμογή και υποδεικνύει περιοχές όπου το επίπεδο επένδυσης ελέγχου του κινδύνου μπορεί να αυξηθεί, να μειωθεί ή να ανακατανεμηθεί. Η υπευθυνότητα βοηθάει στη διασφάλιση του γεγονότος ότι η "περίπτωση" του κινδύνου έχει αναγνωρισθεί και ότι οι κατάλληλοι διοικητικοί πόροι έχουν κατανεμηθεί.

Πιο συγκεκριμένα,στα πληροφοριακά συστήματα οι επιπτώσεις που θα προέλθουν κατά την υλοποίηση ενός έργου πρέπει να προσδιορίζονται από τους υπεύθυνους για την πραγματοποίησή τους και από το διοικητικό τομέα του οργανισμού, για να έχουν μια ολοκληρωμένη αντίληψη για τις επιπτώσεις καθώς και να διασφαλίσουν σημαντικές αρχές ασφαλείας του συστήματος. Οι σημαντικές απώλειες που μπορεί να εμφανιστούν:

- Η Απώλεια Ακεραιότητας (Loss of Integrity): Η ακεραιότητα στα συστήματα και στις πληροφορίες έχει ως στόχο να προστατεύονται αυτά από κάποιες τροποποιήσεις και

καταστροφές καθώς και την άμεση επιδιόρθωση της λειτουργίας σε περίπτωση προβλήματος. Η απώλεια ακεραιότητας μπορεί να γίνει είτε στο λογισμικό είτε στη βάση δεδομένων του συστήματος. Αυτό συνεπάγεται με τη μη σωστή λειτουργία και την προστασία των πληροφοριών του συστήματος, το μη γρήγορο εντοπισμό σφαλμάτων που μπορεί να έχει ως συνέπεια τις λανθασμένες αποφάσεις της διοίκησης. Ακόμα η απώλεια της ακεραιότητας μπορεί να οδηγήσει, στο πρώτο στάδιο, σε μια επιτυχημένη επίθεση κατά της εμπιστευτικότητας και ακεραιότητας των συστημάτων.

- Η Απώλεια Διαθεσιμότητας (Loss of Availability): Σε περίπτωση μη διαθεσιμότητας όλου ή κάποιου τμήματος του συστήματος λόγω κάποιας βλάβης που παρουσιάστηκε κατά τη διάρκεια της λειτουργίας του,μπορεί να οδηγήσει το έργο εκτός λειτουργίας μέχρι να γίνει επιδιόρθωση. Η απώλεια της διαθεσιμότητας μπορεί να αποτελεί επακόλουθο της απώλειας ακεραιότητας του συστήματος. Επομένως, όπως είναι γνωστό, μπορεί να φέρει μια σειρά από αρνητικά αποτελέσματα όπως τη μείωση της αξιοπιστίας και κύρους του οργανισμού ακόμα και την αποδιοργάνωση των διαδικασιών αυτών.
- Η Απώλεια Εμπιστευτικότητας (Loss of Confidentiality): Η απώλεια εμπιστευτικότητας μπορεί να πραγματοποιηθεί με την παράνομη κοινοποίηση δεδομένων ή πληροφοριών του οργανισμού. Οι επιπτώσεις σε τέτοια περίπτωση μπορεί να είναι η διαρροή μελλοντικών σχεδίων του οργανισμού, προσωπικά δεδομένα στελεχών ή άλλα στοιχεία που υπάρχουν στη βάση δεδομένων του συστήματος. Εκτός αυτών η παράνομη κοινοποίηση τέτοιων πληροφοριών θα μπορούσε να έχει αντίκτυπο της απώλειας της δημόσιας εμπιστοσύνης ακόμα και τη νομική δράση εναντίον του οργανισμού για την κοινοποίηση αυτή.

3.3 ΑΞΙΟΛΟΓΗΣΗ ΚΙΝΔΥΝΟΥ

Όταν η διεργασία ανάλυσης κινδύνου έχει ολοκληρωθεί, είναι αναγκαίο οι εκτιμημένοι κίνδυνοι να συγκριθούν έναντι των κριτηρίων κινδύνου που έχει εγκαταστήσει ο

οργανισμός. Τα κριτήρια κινδύνου μπορεί να περιλαμβάνουν σχετικά κόστη και οφέλη, νομικές απαιτήσεις, κοινωνικό-οικονομικούς και περιβαλλοντικούς παράγοντες, ανησυχίες των εχόντων έννομο ενδιαφέρον (stakeholders), κλπ. Η αξιολόγηση κινδύνου επομένως, χρησιμοποιείται για τη λήψη αποφάσεων σχετικά με την σημαντικότητα των κινδύνων στον οργανισμό και για το κατά πόσον ο κάθε συγκεκριμένος κίνδυνος θα έπρεπε να γίνει αποδεκτός ή να αντιμετωπισθεί.

Επίσης χορηγούνται στοιχεία ελέγχου που έχουν τη δυνατότητα να μετριάσουν ή να απαλείψουν όλους τους κίνδυνους που εμφανίζονται. Ο σκοπός των ελέγχων αυτών είναι να μειωθεί το επίπεδο των κινδύνων σε ένα πληροφοριακό σύστημα σε αποδεκτό επίπεδο. Οι παρακάτω παράγοντες πρέπει να λαμβάνονται υπόψη για τη μείωση ή την απαλοιφή των εντοπισμένων κινδύνων:

- Οι Κανονιστικές και οι Νομοθετικές Διατάξεις.
- Η Πολιτική Οργάνωσης.
- Η Αποτελεσματικότητα των Επιλογών που Προτάθηκαν.
- Οι Επιχειρησιακές Επιπτώσεις.
- Η Ασφάλεια και η Αξιοπιστία.

Οι συστάσεις ελέγχων προέρχονται από τη διαδικασία της αξιολόγησης των κινδύνων και εδώ πρέπει να σημειωθεί ότι όλοι οι πιθανοί έλεγχοι μπορούν να βοηθήσουν στην μείωση των απειλών του συστήματος. Για να αξιολογηθεί μια τεχνική πρέπει πρώτα να διεξαχθεί μια ανάλυση οφέλους - κόστους έτσι ώστε να καταδείξει ότι το κόστος της εφαρμογής μπορεί να δικαιολογήσει τη μείωση του επιπέδου του κινδύνου. Τέλος είναι απαραίτητο να αξιολογούνται οι συνέπειες που θα προκύψουν από τον έλεγχο στον οργανισμό.

Για να είναι μια αναφορά πλήρης πρέπει να συμπεριλαμβάνει τα εξής:

- Τις πηγές από τις οποίες προήρθαν οι πληροφορίες.
- Τα άτομα που συμμετείχαν στη διαδικασία αυτή.

- Τις τεχνικές που χρησιμοποιήθηκαν για τη διεξαγωγή αποτελεσμάτων.
- Τις παρατηρήσεις και τα σχόλια που διατυπώθηκαν σε κάθε βήμα της διαδικασίας από τους ειδικούς.
- Την τεκμηρίωση των τεχνικών συμπερασμάτων και των πηγών που χρησιμοποιήθηκαν.

Πρέπει να διασαφηνιστεί ότι τα παραπάνω βήματα της διαδικασίας των κινδύνων πρέπει να πραγματοποιούνται και να επαναλαμβάνονται σε όλη τη διάρκεια της υλοποίησης του έργου, για να υπολογίζονται οι αλλαγές των συνθηκών έτσι ώστε να υπολογίζονται πάλι οι εντοπισμένοι και αναγνωρισμένοι κίνδυνοι και να προσθέτονται και νέοι κίνδυνοι αν αυτό είναι και εκτιμηθεί αναγκαίο.

Εσωτερική Αναφορά

Τα διαφορετικά επίπεδα εντός του οργανισμού χρειάζονται διαφορετική πληροφορία από τη διεργασία διαχείρισης κινδύνου. Το Διοικητικό Συμβούλιο θα έπρεπε:

- να πληροφορείται τους πιο σημαντικούς κινδύνους που αντιμετωπίζει ο οργανισμός.
- να γνωρίζει τις πιθανές επιπτώσεις στη μετοχική αξία των αποκλίσεων από το αναμενόμενο εύρος επίδοσης.
- να διασφαλίζει τα κατάλληλα επίπεδα ενημέρωσης και ευαισθητοποίησης σε ολόκληρο τον οργανισμό.
- να γνωρίζει πώς ο οργανισμός θα διαχειρισθεί μία κρίση.
- να γνωρίζει την σημαντικότητα της εμπιστοσύνης των εχόντων έννομο ενδιαφέρον (stakeholders) στον οργανισμό.
- να γνωρίζει πώς να διαχειρίζεται επικοινωνίες με την επενδυτική κοινότητα, όπου έχει Εφαρμογή.
- να είναι πεπεισμένο ότι η διεργασία διαχείρισης κινδύνου λειτουργεί αποτελεσματικά.

- να εκδίδει μία ξεκάθαρη πολιτική διαχείρισης κινδύνου που να καλύπτει τη φιλοσοφία και τις υπευθυνότητες διαχείρισης κινδύνου.

Οι Επιχειρηματικές Μονάδες θα έπρεπε:

- να γνωρίζουν τους κινδύνους που εμπίπτουν στη δική τους περιοχή ευθύνης, τις πιθανές επιδράσεις που μπορεί να έχουν σε άλλες περιοχές και τις συνέπειες που άλλες περιοχές μπορεί να έχουν σε αυτές (τις επιχειρηματικές μονάδες).
- να έχουν δείκτες επίδοσης που τους επιτρέπουν να παρακολουθούν τις βασικές επιχειρηματικές και χρηματο-οικονομικές δραστηριότητες, την πρόοδο σε σχέση με τους στόχους και να προσδιορίζουν αναπτυξιακές προοπτικές που απαιτούν παρέμβαση (π.χ. προβλέψεις, προϋπολογισμοί).
- να έχουν συστήματα τα οποία επικοινωνούν τις διαφορές σε προυπολογισμούς και προβλέψεις με κατάλληλη συχνότητα για τη λήψη ενέργειας.
- να αναφέρουν συστηματικά και άμεσα στην ανώτατη διοίκηση κάθε νέο κίνδυνο ή αστοχία των υπαρχόντων μέτρων ελέγχου που γίνονται αντιληπτά.

Τα μεμονωμένα άτομα θα έπρεπε:

- να κατανοούν την υπευθυνότητά τους σε μεμονωμένους κινδύνους.
- να κατανοούν πως αυτοί μπορούν να ενδυναμώσουν την συνεχή βελτίωση της απόκρισης της διαχείρισης κινδύνου.
- να κατανοούν ότι η διαχείριση κινδύνου και η ευαισθητοποίηση στον κίνδυνο είναι ένα βασικό μέρος της κουλτούρας του οργανισμού.
- να αναφέρουν συστηματικά και άμεσα στην ανώτατη διοίκηση κάθε νέο κίνδυνο ή αστοχία των υπαρχόντων μέτρων ελέγχου που γίνονται αντιληπτά.

Εξωτερική Αναφορά

Η εταιρεία χρειάζεται να αναφέρεται στους έχοντες έννομο ενδιαφέρον (stakeholders) στις δικές της δραστηριότητες της σε τακτική βάση, περιγράφοντας εκτενώς τις πολιτικές της διαχείρισης κινδύνου και την αποτελεσματικότητα στην επίτευξη των στόχων της.

Όλο και περισσότερο, οι έχοντες έννομο ενδιαφέρον (stakeholders) αναμένουν τους οργανισμούς να παρέχουν τα αποδεικτικά στοιχεία για την αποτελεσματική διαχείριση της επίδοσης του οργανισμού σε μη χρηματο-οικονομικά θέματα σε πεδία όπως σχέσεις με την κοινότητα, ανθρώπινα δικαιώματα, εργασιακές πρακτικές, υγιεινή και ασφάλεια και περιβάλλον.

Η καλή εταιρική διακυβέρνηση απαιτεί, οι εταιρείες να υιοθετούν μία μεθοδική προσέγγιση στην διαχείριση κινδύνων η οποία:

- προστατεύει τα ενδιαφέροντα των δικών τους εχόντων έννομο ενδιαφέρον(stakeholders).
- διασφαλίζει ότι το Διοικητικό Συμβούλιο εκπληρώνει τα καθήκοντά του με το να κατευθύνει τη στρατηγική, να δημιουργεί αξία και να παρακολουθεί την επίδοση του οργανισμού.
- διασφαλίζει ότι οι διοικητικοί έλεγχοι είναι σε εφαρμογή και ότι αποδίδουν Ικανοποιητικά.

Οι ρυθμίσεις για την επίσημη αναφορά της διαχείρισης κινδύνου θα έπρεπε να είναι ξεκάθαρα διατυπωμένες και να είναι διαθέσιμες στους έχοντες έννομο ενδιαφέρον.
Η επίσημη αναφορά θα έπρεπε να αναφέρει:

- τις μεθόδους ελέγχου – ιδιαιτέρως τις διοικητικές υπευθυνότητες για τη διαχείριση κινδύνου
- τις διεργασίες που χρησιμοποιούνται για την αναγνώριση κινδύνων και πώς αυτοί

αντιμετωπίζονται από τα συστήματα διαχείρισης κινδύνων

• τα κύρια συστήματα ελέγχου που εφαρμόζονται για τη διαχείριση σημαντικών κινδύνων

• το σύστημα παρακολούθησης και ανασκόπησης σε εφαρμογή.

Οποιεσδήποτε σημαντικές ελλείψεις ανακαλύπτονται από το σύστημα ή στο σύστημα αυτό καθ' εαυτό, θα έπρεπε να αναφέρονται μαζί με τις ενέργειες που έχουν ληφθεί για να τις αντιμετωπίσουν.

3.4 ΧΕΙΡΙΣΜΟΣ-ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΙΝΔΥΝΟΥ

Ο χειρισμός κινδύνου είναι η διεργασία της επιλογής και εφαρμογής μέτρων για να τροποποιηθεί ο κίνδυνος. Ο χειρισμός κινδύνου περιλαμβάνει, ως το πιο σημαντικό του στοιχείο, τον έλεγχο / μείωση κινδύνου, αλλά εκτείνεται ακόμη, για παράδειγμα, στην αποφυγή κινδύνου, τη μεταφορά κινδύνου, τη χρηματοδότηση κινδύνου, κλπ.

Σημείωση: Σε αυτό το πρότυπο, η χρηματοδότηση κινδύνου αναφέρεται στους μηχανισμούς (π.χ. προγράμματα ασφάλισης) παροχής κεφαλαίων για τις χρηματοοικονομικές επιπτώσεις του κινδύνου. Η χρηματοδότηση κινδύνου δεν θεωρείται, σε γενικές γραμμές, να είναι η παροχή κεφαλαίων για την αντιμετώπιση του κόστους εφαρμογής του χειρισμού κινδύνου.

Οποιοδήποτε σύστημα χειρισμού κινδύνου θα έπρεπε να παρέχει, ως το ελάχιστο:

• αποτελεσματική και αποδοτική λειτουργία του οργανισμού.

• αποτελεσματικά εσωτερικά μέτρα ελέγχου.

• συμμόρφωση με νόμους και κανονισμούς.

Η διεργασία ανάλυσης κινδύνου βοηθάει την αποτελεσματική και αποδοτική λειτουργία

του οργανισμού με την αναγνώριση εκείνων των κινδύνων οι οποίοι απαιτούν την προσοχή της διοίκησης. Η διοίκηση θα πρέπει να θέσει προτεραιότητα στις ενέργειες ελέγχου κινδύνου με βάση τη δυνατότητά τους να ωφελήσουν τον οργανισμό. Η αποτελεσματικότητα των εσωτερικών μέτρων ελέγχου είναι ο βαθμός στον οποίο είτε ο κίνδυνος θα εξαλειφθεί ή θα ελαχιστοποιηθεί από τα προτεινόμενα μέτρα ελέγχου.

Η κοστολογική αποτελεσματικότητα των εσωτερικών μέτρων ελέγχου σχετίζεται με το κόστος της εφαρμογής των ελεγκτικών μέτρων σε σύγκριση με τα αναμενόμενα οφέλη της μείωσης του κινδύνου.

Οι προτεινόμενοι έλεγχοι χρειάζεται να μετρηθούν σε σχέση με τη δυνητική οικονομική επίπτωση εάν δεν ληφθεί οποιαδήποτε ενέργεια, έναντι του κόστους των προτεινόμενων ενεργειών και οι οποίες απαιτούν σταθερά περισσότερη λεπτομερή πληροφορία και υποθέσεις από ότι είναι άμεσα διαθέσιμες.

Πρώτον, το κόστος εφαρμογής πρέπει να καθορισθεί. Αυτό πρέπει να υπολογισθεί με κάποια ακρίβεια μιας και γρήγορα γίνεται η βάση έναντι της οποίας μετριέται η αποτελεσματικότητα του κόστους. Η ζημιά που αναμένεται εάν δεν ληφθεί οποιαδήποτε ενέργεια πρέπει επίσης να εκτιμηθεί και με τη σύγκριση των αποτελεσμάτων, η διοίκηση μπορεί να αποφασίσει εάν και κατά πόσον θα εφαρμοσθούν τα μέτρα ελέγχου κινδύνου.

Η συμμόρφωση με νόμους και κανονισμούς δεν είναι επιλογή. Ένας οργανισμός πρέπει να κατανοεί τους εφαρμόσιμους νόμους και πρέπει να εφαρμόζει ένα σύστημα μέτρων ελέγχου για να επιτύχει τη συμμόρφωση. Υπάρχει μόνον περιστασιακά κάποια ευελιξία όταν το κόστος μείωσης ενός κινδύνου μπορεί να είναι συνολικά δυσανάλογο με τον ίδιο τον κίνδυνο.

Μία μέθοδος απόκτησης χρηματο-οικονομικής προστασίας έναντι των επιπτώσεων των κινδύνων είναι μέσω της χρηματοδότησης των κινδύνων που περιλαμβάνει την ασφάλιση. Όμως, θα έπρεπε να αναγνωρισθεί ότι ορισμένες ζημιές ή μέρος ζημιών δεν θα επιδέχεται ασφάλιση, π.χ. το μη ασφαλισμένο κόστος που σχετίζεται με την εργασιακή υγεία, ασφάλεια ή με περιβαλλοντικά περιστατικά, τα οποία μπορεί να περιλαμβάνουν ζημιά στο ηθικό των εργαζομένων και στην φήμη του οργανισμού.

Η αποτελεσματική διαχείριση κινδύνου απαιτεί μία δομή αναφορών και ανασκόπησης για να διασφαλίσει ότι οι κίνδυνοι αναγνωρίζονται και αποτιμώνται αποτελεσματικά και ότι κατάλληλα μέτρα ελέγχου και αποκρίσεις είναι σε ισχύ. Τακτικές επιθεωρήσεις ελέγχου της πολιτικής και της συμμόρφωσης με τα πρότυπα θα έπρεπε να πραγματοποιούνται και η επίδοση ως προς τα πρότυπα να ανασκοπείται για να αναγνωρίζονται ευκαιρίες για βελτίωση. Θα έπρεπε να θυμόμαστε ότι οι οργανισμοί είναι δυναμικοί και λειτουργούν σε δυναμικά περιβάλλοντα. Οι αλλαγές στον οργανισμό και στο περιβάλλον στο οποίο λειτουργεί πρέπει να αναγνωρίζονται και οι κατάλληλες μεταβολές να γίνονται στα συστήματα.

Η διεργασία παρακολούθησης θα έπρεπε να παρέχει τη διασφάλιση ότι υπάρχουν μέτρα ελέγχου σε εφαρμογή κατάλληλα για τις δραστηριότητες του οργανισμού και ότι οι διαδικασίες κατανοούνται και ακολουθούνται. Οι αλλαγές στον οργανισμό και το περιβάλλον στο οποίο αυτός λειτουργεί πρέπει να αναγνωρίζονται και οι κατάλληλες αλλαγές να γίνονται στα συστήματα.

Οποιαδήποτε διεργασία παρακολούθησης και ανασκόπησης θα έπρεπε επίσης να καθορίζει εάν και κατά πόσον:

• τα μέτρα που υιοθετήθηκαν είχαν ως αποτέλεσμα ότι είχε τεθεί ως αρχική πρόθεση

• οι διαδικασίες που υιοθετήθηκαν και η πληροφορία που συλλέχθηκε για τη διεξαγωγή

της αποτίμησης ήταν οι κατάλληλες

- η βελτιωμένη γνώση θα είχε βοηθήσει να ληφθούν καλύτερες αποφάσεις και να αναγνωρισθεί τι διδάγματα θα μπορούσαν να αποκτηθούν για τις μελλοντικές αποτιμήσεις και τη διαχείριση των κινδύνων.

ΚΕΦΑΛΑΙΟ 4:ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

4.1 ΟΡΙΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Μέχρι και σήμερα αναφέρονται στη διεθνή βιβλιογραφία παραπάνω από ένας ορισμοί για την έννοια του πληροφοριακού συστήματος που διαφοροποιούνται μεταξύ τους. Πολλοί συγγραφείς δίνουν έμφαση μόνο στην τεχνική πλευρά του πληροφοριακού συστήματος, δηλαδή στην επεξεργασία δεδομένων και των πληροφοριών. Για παράδειγμα ο Aktas (1987) και ο Newman (1990) ορίζουν το πληροφοριακό σύστημα ως «ένα σύστημα το οποίο δέχεται πληροφορίες, τις αποθηκεύει, ανακτά, μετασχηματίζει, επεξεργάζεται και τις διανέμει στους διάφορους χρήστες του οργανισμού, χρησιμοποιώντας υπολογιστές ή άλλα μέσα ». Για έναν οργανισμό ένα πληροφοριακό σύστημα αποτελεί οικονομική αξία και αποτελεί σημαντικό παράγοντα για την λειτουργία και την ανάπτυξη της. Ο πλησιέστερος ορισμός του Πληροφοριακού Συστήματος για την παρούσα εργασία είναι αυτός, στηριζόμενος με υπολογιστές, σύμφωνα με τον οποίο:

« Πληροφοριακό Σύστημα είναι ένα σύνολο από πέντε στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες και δεδομένα), τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείρισης πληροφορίας, για την υποστήριξη των ανθρώπινων δραστηριοτήτων, στα πλαίσια του οργανισμού». Επομένως η χρήση του όρου αυτού σημαίνει ότι το πληροφοριακό σύστημα αποτελείται από επιμέρους στοιχεία που

αλληλεπιδρούν, χαρακτηρίζεται από οργάνωση και εξετάζεται ως μια ενιαία ολότητα.

Τα Πληροφορικά Συστήματα είναι πολύπλοκα τεχνουργήματα και λόγω της ιδιαιτερότητας που έχουν πρέπει να σχεδιάζονται και αναπτύσσονται με τέτοιον τρόπο έτσι ώστε να στοχεύουν και να υποστηρίζουν την ομαδική και την οργανωτική λήψη αποφάσεων. Επομένως για όσους τα σχεδιάζουν και τα υλοποιούν, τα συστήματα αυτά πρέπει να βασίζονται στα επιμέρους χαρακτηριστικά:

- Πρέπει να έχουν δυνατότητα ως προς την υποστήριξη μιας μεγάλης ποικιλίας από γνώσεις, στυλ και δεξιότητες.
- Πρέπει να είναι ευπροσάρμοστα και να παρέχουν επιλογές ως προς την αξιολόγηση πληροφοριών και χειρισμό δεδομένων.
- Πρέπει να είναι ισχυρά, να περιλαμβάνουν πολλά διαισθητικά και αναλυτικά μοντέλα αξιολόγησης δεδομένων καθώς και τη δυνατότητα παρατήρησηςαξιολόγησης εναλλακτικών ενεργειών και των επιπτώσεών τους.
- Πρέπει να είναι ευπροσάρμοστα και ευαίσθητα ως προς τις πολιτικές-γραφειοκρατικές απαιτήσεις του συστήματος.

4.2 ΣΤΟΧΟΙ ΚΑΙ ΠΑΡΑΓΟΝΤΕΣ ΑΠΟΤΥΧΙΑΣ ΕΝΟΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Όπως και κάθε άλλο σύστημα, έτσι και τα Πληροφοριακά Συστήματα έχουν ένα σκοπό στο περιβάλλον που λειτουργούν. Το περιβάλλον αυτό συνήθως είναι ο οργανισμός, οι βασικές λειτουργίες τις οποίες στηρίζει το πληροφοριακό σύστημα καθώς και τους στόχους που έχει ο οργανισμός. Οι σημαντικότεροι σκοποί των Πληροφοριακών Συστημάτων είναι οι εξής:

- Η συλλογή, επεξεργασία, αποθήκευση των δεδομένων για την εξαγωγή καθοριστικών πληροφοριών για τον οργανισμό.

- Η ενημέρωση και η χορήγηση λειτουργικής πληροφόρησης ως προς τους εργαζόμενους για να εκτελούν κατά το δυνατόν τρόπο τις δραστηριότητες σε καθημερινή βάση όπως συναλλαγές, προγραμματισμός και έλεγχος.
- Η χορήγηση στρατηγικής πληροφόρησης ως προς τα ανώτατα στελέχη, για την καλύτερη λήψη αποφάσεων για τη μελλοντική πορεία του οργανισμού.
- Η ανάπτυξη και η εξέλιξη των οργανισμών για την εδραίωσή τους στο χώρο των οργανισμών μέσω της σύνδεσης του πληροφοριακού συστήματος με εκείνα των προμηθευτών και πελατών για τη δημιουργία οφέλους από περισσότερη πληροφόρηση.

Τα Πληροφοριακά Συστήματα είναι συστήματα τα οποία στηρίζουν ανθρώπινες δραστηριότητες εστιάζοντας στις απαιτήσεις που αναφέρονται στις σχέσεις του ανθρώπου αλλά και του συστήματος. Επομένως οι σχεδιαστές θα πρέπει να σχεδιάζουν και να υλοποιούν τα πληροφοριακά συστήματα έχοντας υπόψη τους την ομαλή και σωστή λειτουργία του οργανισμού. Άρα ένας παράγοντας αποτυχίας των πληροφοριακών συστημάτων είναι ότι δίνεται ιδιαίτερη έμφαση ως προς την τεχνική πλευρά του συστήματος και όχι την κοινωνική. Επίσης ένα πληροφοριακό σύστημα μπορεί να έχει πλήρη επιτυχία από τεχνικής άποψης αλλά παράλληλα αποτυχημένο οργανωτικά.

Μερικοί σχεδιαστές δεν αναγνωρίζουν το πόσο σημαντικός παράγοντας είναι ο άνθρωπος, χωρίς να το λάβουν υπόψη κατά τη δημιουργία του πληροφοριακού συστήματος. Ακόμα ένας παράγοντας που οδηγεί στην αποτυχία των πληροφοριακών συστημάτων είναι ότι υπάρχει έλλειψη στο κομμάτι της εκπαίδευσης και της διαχείρισής τους. Επομένως στη διαδικασία της ανάπτυξης των πληροφορικών συστημάτων είναι σημαντικό κομμάτι ο προσδιορισμός των ανθρωπίνων αναγκών, η οποία προϋποθέτει ικανότητες που δεν υπάρχουν στους προγραμματιστές και αναλυτές. Αυτό γίνεται διότι οι αναλυτές και οι προγραμματιστές έχουν και βασίζονται μόνο στις τεχνικές γνώσεις και δε γνωρίζουν αλλά ούτε δίνουν ιδιαίτερη έμφαση ως προς το κομμάτι της ανθρώπινης ψυχολογίας και

συμπεριφοράς. Επομένως όποιος ασχολείται με τον τομέα των πληροφοριακών συστημάτων πρέπει να δίνει έμφαση και σε άλλους παράγοντες ώστε τα πληροφοριακά συστήματα να μπορούν να πετύχουν το σκοπό τους.

4.3 ΔΙΑΧΕΙΡΗΣΗ ΚΙΝΔΥΝΩΝ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Κάθε οργανισμός επιλέγει να εισάγει στο περιβάλλον του ένα πληροφοριακό σύστημα βασιζόμενος στη λειτουργία, ανάπτυξη, επίτευξη κερδών καθώς και τη δημιουργία ανταγωνιστικού κλίματος και πλεονεκτήματος. Ωστόσο η ενοποίηση του οργανισμού με ένα πληροφοριακό σύστημα δεν είναι μια απλή αλλά μια περίπλοκη διαδικασία, κι αυτό γιατί το περιβάλλον που λειτουργεί και εξελίσσεται ο οργανισμός είναι πολύ ευμετάβλητο και περίπλοκο.

Οι κίνδυνοι των πληροφοριακών συστημάτων μπορούν να προέρχονται από πολλές πηγές. Σε περίπτωση που αγνοηθούν μπορούν να αποβούν μοιραίοι. Τα κύρια σημεία που πρέπει να δώσουν ιδιαίτερη προσοχή, λόγω των κινδύνων, τα διοικητικά στελέχη είναι η πρόσβαση στο δίκτυο του οργανισμού, η ακεραιότητα των πληροφοριών και δεδομένων του και η απόκτηση και ανάπτυξη των λογισμικών.

Επομένως για να αντιμετωπιστούν ενδεχόμενοι κίνδυνοι, που μπορεί να προκύψουν, πρέπει να εφαρμοστεί και να εκτελεστεί μια σειρά από ενέργειες οι οποίες αναφέρονται και αναλύονται παρακάτω. Η ενότητα αυτή εστιάζεται στη διευκρίνηση και ανάλυση των κινδύνων καθώς και του σχεδίου το οποίο πρέπει να κατέχει ένας οργανισμός ώστε αρχικά να εντοπίσει και ύστερα να αντιμετωπίσει τους κινδύνους, έτσι ώστε να αποφύγει κάθε αποτυχία ή απόκλιση των στόχων του.

Οι κίνδυνοι οι οποίοι μπορούν να παρουσιαστούν κατά την περίοδο λειτουργίας ενός πληροφοριακού συστήματος καθώς και την περίοδο της ολοκλήρωσής του, μπορούν να ανιχνευτούν από εξειδικευμένο προσωπικό που κατέχει όχι μόνο γνώσεις και εμπειρίες αλλά και αντιληπτικότητα ώστε να αντιλαμβάνοται τους κινδύνους. Παρακάτω αναφέρονται έξι σημαντικές κατηγορίες κινδύνων που μπορούν να παρουσιαστούν σε ένα πληροφοριακό σύστημα:

- Οι Φυσικές Απειλές (Natural Threats): Οι φυσικές απειλές όπως οι πλημμύρες και οι σεισμοί δεν επικεντρώνονται μόνο στα πληροφοριακά συστήματα αλλά έχουν άμεση σχέση με τις κτηριακές υποδομές του οργανισμού αλλά και έμμεση με τα πληροφοριακά συστήματα που στεγάζονται εκεί. Αυτό έχει ως συνέπεια τέτοιες καταστροφές να δημιουργήσουν προβλήματα που θα ενισχύσουν το κόστος και το χρόνο πραγματοποίησης του έργου.
- Οι Ανθρώπινες Απειλές (Human Threats): Στις ανθρώπινες απειλές βρίσκονται τα άτομα τα οποία προκαλούν βλάβες στο λογισμικό του πληροφοριακού συστήματος αποτελούν είτε ανταγωνιστές που αποσκοπούν να βλάψουν την αξιοπιστία, ακεραιότητα και την εμπιστευτικότητα του οργανισμού και του έργου του, καθώς και άτομα που αποτελούν το ίδιο το προσωπικό του οργανισμού επιχείρησης που τα προκαλούν για προσωπικούς λόγους.
- Οι Κίνδυνοι Τεχνολογίας (Dangers of Technology): Οι κίνδυνοι της τεχνολογίας αποτελούν τους κινδύνους που μπορεί να προκληθούν από την εισαγωγή νέων συστημάτων σε έναν οργανισμό εξαιτίας την μη δυνατότητας να λειτουργήσουν σύμφωνα με τις απαιτήσεις τους.Ακόμα ο μη κατάλληλος εξοπλισμός της νέας τεχνολογίας μπορεί να δημιουργήσει διάφορα προβλήματα όπως το να βγει εκτός προγράμματος στους στόχους που έχει θέσει.
- Το Θεσμικό-Φυσικό Περιβάλλον Έργου (Institutional-Natural Environment Project): Με τον όρο «θεσμικό» περιβάλλον του έργου αναφερόμαστε σε εκείνους τους θεσμούς τους οποίους πρέπει να εφαρμόσει και αναπτύξει το πληροφοριακό σύστημα του οργανισμού έτσι ώστε να πειθαρχεί με αυτούς για να αποφύγει ενδεχόμενες κυρώσεις για θεσμική

ανυπακοή, αποτέλεσμα που θα προκαλέσει μεγάλες οικονομικές ζημίες αλλά και χάσιμο πολύτιμου χρόνου. Με τον όρο «φυσικό» περιβάλλον έργου αναφερόμαστε στις εγκαταστάσεις του οργανισμού που στεγάζονται τα πληροφοριακά συστήματα. Σε περίπτωση που στεγάζονται σε παλαιές εγκαταστάσεις προκύπτει το ενδεχόμενο να υπάρχει πρόβλημα σε θέματα όπως η παροχή ηλεκτρισμού το οποίο μπορεί να καταστεί δυνατό να επιφέρει τη διακοπή λειτουργίας αλλά και την καταστροφή του εξοπλισμού (λογισμικού, απώλεια δεδομένων).

- Οι Επιχειρησιακοί Κίνδυνοι (Dangers Operational): Οι κίνδυνοι αυτοί αναφέρονται στην αδυναμία της προσάρτησης νέας τεχνολογίας σε κάθε οργανισμό που έχει σαν αποτέλεσμα την εμπόδιση της λειτουργίας του πληροφοριακού συστήματος. Αυτός ο κίνδυνος προκαλείται από τις τυχόν καθυστερήσεις της υλοποίησης του έργου αλλά και της μη κατάλληλης εκπαίδευσης του προσωπικού του οργανισμού.
- Οι Κίνδυνοι Οργάνωσης Έργου (Dangers of Organisation of Work): Ο κίνδυνος αυτός αναφέρεται στην οργάνωση και τη δομή του έργου. Έχει σχέση άμεσα με τα άτομα τα οποία έχουν την ευθύνη για την υλοποίηση και το σχεδίασμά του. Σε περίπτωση που υπάρχει έλλειψη εκπαίδευσης των ειδικών, ανεπάρκεια τεχνογνωσιών και μη λήψη αποφάσεων μπορεί να προκαλέσει οικονομικά και χρονικά ζητήματα στον οργανισμό.

Το αρχικό στάδιο της διαχείρισης κινδύνων περιλαμβάνει τη συλλογή πληροφοριών του οργανισμού στον οποίο θα λειτουργήσει το πληροφοριακό σύστημα, τις ανάγκες που πρέπει να καλύψει και πληροφορίες για την πραγματοποίηση σχετικών έργων κατά το παρελθόν. Αυτός ο τρόπος συλλογής πληροφοριών θα βοηθήσει στη διερεύνηση κινδύνων που μπορεί να προκύψουν για το έργο καθώς και στην εξεύρεση μεθόδων για τη μείωσή τους ή και την εξάλειψη αυτών και των συνεπειών τους.

Επομένως πρέπει να συλλεχθούν πληροφορίες για το περιβάλλον του πληροφοριακού συστήματος. Η κατηγοριοποίηση των πληροφοριών γίνεται σύμφωνα με τα παρακάτω:

- Το Υλικό (Hardware): Η συλλογή πληροφοριών στον παρόντα εξοπλισμό αλλά και τον εξοπλισμό που θα χρησιμοποιηθεί από το νέο πληροφοριακό σύστημα.
- Το Λογισμικό (Software): Η συλλογή πληροφοριών για νέο και παλιό λογισμικό.
- Οι Διεπαφές Συστημάτων: 0 προσδιορισμός για τις εξωτερικές και εσωτερικές συνδέσεις του συστήματος.
- Οι Βάσεις Δεδομένων (Bases of data): Η αξία, ο όγκος και το είδος δεδομένων και πληροφοριών που θα αναλάβει το νέο λογισμικό.
- Η Υποστήριξη και η Μεταχείριση του Συστήματος από τα Στελέχη: Τα στελέχη πρέπει να κατέχουν τις κατάλληλες γνώσεις, ώστε να κατανοούν την αξία, τη χρησιμότητα του νέου συστήματος καθώς και το χειρισμό του λογισμικού.
- Ο Προορισμός του Νέου Συστήματος: Οι λειτουργίες που πρέπει να υλοποιήσει το πληροφοριακό σύστημα.
- Η Αξία του Νέου Συστήματος: Η σημαντικότητα της εγκατάστασης του νέου πληροφοριακού συστήματος για τη λειτουργία του οργανισμού.
- Η Ευαισθησία του Συστήματος: Το επίπεδο προστασίας που πρέπει να υπάρχει για τη διασφάλιση της ακεραιότητας, εμπιστευτικότητας, διαθεσιμότητας των πληροφοριών και συστημάτων.

Επιπρόσθετες πληροφορίες που έχουν σχέση με το λειτουργικό περιβάλλον του συστήματος και είναι το ίδιο σημαντικές για τη διαδικασία της διαχείρισης κινδύνων, είναι οι παρακάτω:

- Οι Λειτουργικές Απαιτήσεις του Συστήματος.
- Οι Πολιτικές Ασφαλείας των Συστημάτων: Οι πολιτικές που εφαρμόζει ο οργανισμός.
- Η Τωρινή Δικτυακή Τοπολογία: Το δίκτυο στο οποίο στηρίζεται το σύστημα.
- Η Προστασία των Αποθηκευμένων Πληροφοριών.
- Η Ροή Πληροφοριών Σχετικές με το Σύστημα: Οι διασυνδέσεις του συστήματος, πληροφορίες που εισέρχονται και εξέρχονται από το σύστημα.
- Οι Τεχνικοί Έλεγχοι που Εφαρμόζονται για το Πληροφοριακό Έργο: Εδώ αναφέρονται οι

διακριτοί ή αυστηροί έλεγχοι πρόσβασης, η προστασία πληροφοριών και τεχνικές κρυπτογράφησης.

- Οι Διοικητικοί Έλεγχοι για την Προστασία του Συστήματος.
- Οι Λειτουργικοί Έλεγχοι: Εδώ αναφέρονται ο έλεγχος πρόσβασης χρηστών (ιδιαίτερα σε αυτούς που έχουν πρόσβαση σε λειτουργίες και αρχεία πέρα από των υπαρχουσών), περιπτώσεις της αποκατάστασης και συντήρησης των συστημάτων, περιπτώσεις προσθήκης και διαγραφής δεδομένων.
- Η Ασφάλεια των Εγκαταστάσεων του Οργανισμού: Η ασφάλεια τόσο σε εσωτερικό όσο και εξωτερικό επίπεδο.
- Η Ασφάλεια σε Σχέση με το Φυσικό Περιβάλλον του Έργου: Εδώ τονίζονται οι έλεγχοι για τη διαχείριση ενέργειας, την έκθεση σε φυσικές καταστροφές.

4.4 Η ΔΙΑΔΙΚΑΣΙΑ ΣΥΛΛΟΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Για τα πληροφοριακά συστήματα τα οποία είναι στο στάδιο της έναρξης ή στο στάδιο του σχεδιασμού οι πληροφορίες προέρχονται είτε από την κατάσταση με τις απαιτήσεις του έργου είτε από το ίδιο το σχέδιο. Όταν το έργο αναπτύσσεται μπορεί να προέρχονται χρήσιμες πληροφορίες από τον προσδιορισμό των σημαντικών κανόνων και των στοιχείων ασφάλειας που προκαθορίζονται για το σύστημα. Για οποιαδήποτε έργο λογισμικού, οι πληροφορίες που προέρχονται από το περιβάλλον δημιουργίας του έργου, συμπεριλαμβάνουν τα στοιχεία που αφορούν την διαμόρφωση συστημάτων, την διασύνδεσή τους, και τις πρακτικές. Έτσι λοιπόν η περιγραφή των συστημάτων μπορεί να στηριχτεί στην ασφάλεια που δίνεται από την υπάρχουσα υποδομή ή τα σχέδια χρήσης για ασφάλεια στο μέλλον. Όμως αυτή η συγκέντρωση πληροφοριών δεν αποτελεί μια εύκολη διαδικασία και η εκτέλεση της πρέπει να είναι προσεκτική, να καθορίζεται σε επιστημονικό επίπεδο και να απαιτείται αυστηρή ενασχόληση από τα άτομα που θα συγκεντρώσουν αυτές τις πληροφορίες, έτσι ώστε τα αποτελέσματα να είναι αξιόπιστα για να μπορούν να

βοηθήσουν στην διαδικασία της διαχείρισης των κινδύνων και όχι να οδηγήσουν σε λάθος συμπεράσματα. Μερικές μέθοδοι για τον εντοπισμό και τη διαχείριση των κινδύνων είναι οι εξής:

- Τα Ερωτηματολόγια: Η ομάδα της διαχείρισης κινδύνων για να συγκεντρώσει πληροφορίες θα πρέπει να δημιουργήσει κάποια ερωτηματολόγια που θα επικεντρώνονται στους λειτουργικούς ελέγχους αλλά και στη διαχείριση που κανονίζονται για το νέο πληροφοριακό σύστημα ή των υπαρχόντων συστημάτων. Τα ερωτηματολόγια θα πρέπει να διανεμηθούν στο προσωπικό που θα ασχοληθεί με τη σχεδίαση και την υποστήριξη του πληροφοριακού συστήματος.
- Οι Συνεντεύξεις: Οι συνεντεύξεις που θα διενεργούνται τόσο στο προσωπικό υποστήριξης και σχεδίασης του συστήματος όσο και το προσωπικό της διοικήσεως του οργανισμού, μπορούν να παρέχουν στα άτομα τα οποία διεξάγουν την αξιολόγηση των κινδύνων σημαντικές πληροφορίες για την πολυτιμότητα και τον προορισμό του συστήματος καθώς και τις διαφωνίες των στελεχών για την εισαγωγή νέας τεχνολογίας. Ακόμα οι συνεντεύξεις βοηθάνε στην κατανόηση όσον αφορά τα λειτουργικά χαρακτηριστικά του οργανισμού και στην αποτίμηση του περιβάλλοντος που θα εγκατασταθεί το πληροφοριακό σύστημα.
- Το Πόρισμα Ειδικών: Εδώ αναφερόμαστε στη συγκέντρωση των πληροφοριών όσον αφορά το φυσικό και λειτουργικό περιβάλλον του έργου από την ομάδα της αξιολόγησης κινδύνων. Η αξία αυτού του πορίσματος είναι σημαντική διότι δεν συμπεριλαμβάνει τις προσωπικές απόψεις των στελεχών του οργανισμού, που υπάρχει περίπτωση να είναι απόλυτα αντικειμενικές, αλλά μόνο την παρακολούθηση και καταγραφή των γεγονότων με βασικό παράγοντα τη διορατικότητα και την ουδετερότητα των ειδικών.
- Η Αναθεώρηση Εγγράφων: Με την αναθεώρηση των εγγράφων εννοούμε τα έγγραφα που έχουν πολιτικό περιεχόμενο (νομοθεσίες, κρατικές οδηγίες), τα έγγραφα που αναφέρονται στο σύστημα (σχέδια τους συστήματος, οδηγοί χρήσεων, διοικητικά εγχειρίδια συστημάτων) και έγγραφα που αναφέρονται στην ασφάλεια (διαδικασίες και

σχεδιασμός συστημάτων, έκθεση λογιστικού και ελέγχου και αξιολόγηση κινδύνου) που παρέχουν πολλές και σημαντικές πληροφορίες που μπορούν να διαμορφώσουν μια άψογη εικόνα του οργανισμού και της ποιότητας της λειτουργικότητας του νέου έργου.

- Η Συγκέντρωση Πληροφοριών από Παρόμοια έργα Πληροφορικής που έχουν ήδη υλοποιηθεί: Οι πληροφορίες αυτές είναι πολύτιμες διότι μέσα από αυτές εξάγονται εμπειρίες από παρόμοια έργα και έτσι μπορούν να αποφθεχθούν κάποια λάθη και παραλήψεις από το παρελθόν δημιουργώντας έτσι μια πιο πρακτική εικόνα των τρόπων αντιμετώπισης των συνεπειών.
- Η Χρήση Αυτοματοποιημένου Ανιχνευτικού Εξοπλισμού: Μπορούν να αξιοποιηθούν δυναμικές μέθοδοι για τη συλλογή πληροφοριών.

ΚΕΦΑΛΑΙΟ 5: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

5.1 ΟΡΙΣΜΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Στην σύγχρονη εποχή, η χρήση πληροφοριακών συστημάτων είναι δεδομένη για κάθε οργανισμό. Η επανάσταση της συνδεσιμότητας είναι πλέον γεγονός. Η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Σαν αποτέλεσμα, στο μεγαλύτερο ποσοστό των οργανισμών η χρήση των πληροφοριακών συστημάτων είναι απολύτως αναγκαία για την επίτευξη των στόχων και της βασικής λειτουργικότητας τους. Έτσι, η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος, είτε από άμεσες οικονομικές απώλειες, είτε από την αδυναμία του οργανισμού να λειτουργήσει αποδοτικά.

Εκτός από τις οικονομικές επιπτώσεις όμως, τα προβλήματα ασφαλείας πληροφοριακών συστημάτων γίνονται ακόμα πιο αισθητά σε συστήματα που περιέχουν ευαίσθητα δεδομένα ή επιτελούν «ευαίσθητες» και σημαντικές λειτουργίες. Διάφορα παραδείγματα τέτοιων συστημάτων είναι:

• Συστήματα με απόρρητα στρατιωτικά δεδομένα

• Συστήματα ελέγχου εναέριας κυκλοφορίας

• Συστήματα με ευαίσθητα ιατρικά δεδομένα

• Συστήματα που περιέχουν ευαίσθητα προσωπικά δεδομένα

Είναι φανερό ότι η ρήξη της ασφάλειας τέτοιων πληροφοριακών συστημάτων μπορεί να προκαλέσει σοβαρότατα προβλήματα που απειλούν άμεσα την ανθρώπινη ζωή και την ασφάλεια σε τοπικό, εθνικό αλλά και σε παγκόσμιο επίπεδο. Δεν υπάρχει λοιπόν αμφιβολία ότι η ασφάλεια των πληροφοριακών συστημάτων έχει τεράστια σημασία στην σύγχρονη κοινωνία και πρέπει να παίζει πρωτεύον ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους.

Οι παραβιάσεις των πληροφοριακών συστημάτων οφείλονται τόσο σε εσωτερικούς,όσο και σε εξωτερικούς παράγοντες. Όσον αφορά τους εσωτερικούς παράγοντες αυτοί προέρχονται από εσωτερικές απειλές (Internal Threats) του οργανισμού. Αυτό συμπεριλαμβάνει όλους τους εργαζόμενους, τα στελέχη και τις εσωτερικές υποδομές επίσης. Οι εξωτερικοί παράγοντες προέρχονται από τις εξωτερικές απειλές όπως από τις πηγές εκτός του οργανισμού και από το δίκτυο των συνεργατών. Για παράδειγμα τα άτομα τα οποία μπορεί να είναι Hackers, πρώην εργαζόμενοι των φορέων ή και ακόμα εγκληματικές ομάδες. Εκτός αυτών υπάρχει και μια άλλη κατηγορία παραγόντων που έχει σχέση με τους συνεργάτες καθώς και τρίτα πρόσωπα που έχουν και μοιράζονται κάποια επιχειρησιακή σχέση με τον οργανισμό. Τα τρίτα πρόσωπα μπορεί να είναι πωλητές, προμηθευτές, υπηρεσίες υποστήριξης πληροφορικής κ.τ.λ. Εκτός των άλλων παραγόντων το ποσοστό των

εξωτερικών παραγόντων υπερέχει κατά πολύ. Στους εξωτερικούς παράγοντες μπορούν τοποθετούνται οι παρακάτω απειλές:

• Οι επιθέσεις από Hackers (Hacking).

• Παραβιάσεις που προέρχονται από τη χρήση κακόβουλων λογισμικών (Malware).

• Οι παραβιάσεις κοινωνικού περιεχομένου (Social).

• Οι περιβαλλοντικές και φυσικές απειλές (Environmental and Physical Threats).

• Η κακή χρήση των πληροφοριακών συστημάτων (Misuse).

• Διάφορα σφάλματα που προκύπτουν στα πληροφορικά συστήματα (Errors).

Επομένως οι κάθε είδους παραβιάσεις και επιθέσεις κατά των πληροφοριακών συστημάτων των οργανισμών οδηγούν στην απώλεια εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας των πληροφοριών και των δεδομένων που διαχειρίζονται καθώς και την παράβαση ολόκληρων των συστημάτων αυτών. Αυτό μπορεί να είναι και το σοβαρότερο πρόβλημα καθώς μπορεί να απειληθούν ζωές ανθρώπων αλλά και η ασφάλεια τόσο σε τοπικό, εθνικό και παγκόσμιο επίπεδο. Έτσι η ασφάλεια στα πληροφοριακά συστήματα αποτελεί σημαντικό παράγοντα στη σύγχρονη κοινωνία, που στηρίζεται σε αυτά, γι' αυτό και θα πρέπει να λαμβάνεται υπόψη από τα άτομα που ασχολούνται με τη σχεδίαση, υλοποίηση και τη χρήση τους.

Όπως είναι γνωστό,τα 5 συστατικά στοιχεία από τα οποία αποτελείται το πληροφοριακό σύστημα είναι οι άνθρωποι, οι διαδικασίες, τα δεδομένα, το υλικό, και το λογισμικό. Με τον όρο ασφάλεια πληροφοριακών συστημάτων (Information Systems Security) δίνεται έμφαση στην προστασία αυτών των στοιχείων ενός πληροφοριακού συστήματος και στο σύνολό του. Ως προς τον ορισμό είναι γεγονός ότι στη διεθνή επιστημονική βιβλιογραφία δεν υπάρχει ένας ορισμός της ασφάλειας των πληροφοριακών συστημάτων που να συμφωνούν όλοι. Ένας ορισμός που προσδιορίζει την έννοια της ασφάλειας είναι ο παρακάτω:

«Ασφάλεια Πληροφοριακού Συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή».

Ο παραπάνω ορισμός μας δίνει το πλεονέκτημα για την άμεση αναφορά στα παρακάτω βασικά στοιχεία:

- Επισήμανση όχι μόνο στο Πληροφοριακό Σύστημα ως σύνολο αλλά και στα επιμέρους στοιχεία του.
- Η προστασία σχετίζεται με κάθε είδους απειλής (τυχαία ή σκόπιμη).
- Η ασφάλεια του Πληροφοριακού Συστήματος σχετίζεται άμεσα με τις τεχνικές, διαδικασίες, τα διοικητικά μέτρα όσο και με τις αντιλήψεις, αρχές και παραδοχές.
- Το πλαίσιο αυτό χαρακτηρίζεται από οργάνωση.

Η ασφάλεια Πληροφοριακών Συστημάτων σχετίζεται με:

- Πρόληψη (Prevention): Τη λήψη μέτρων για την αποτροπή πραγματικής ή πιθανής απειλής που μπορεί να προκαλέσει φθορές στα συστατικά μέρη ενός πληροφοριακού συστήματος.
- Ανίχνευση (Detection):Η ανίχνευση είναι η λήψη μέτρων για την εμφάνιση ενός περιστατικού ή μιας παραβίασης που προκάλεσε φθορές σε κάποιο συστατικό μέρος του πληροφοριακού συστήματος.
- Αντίδραση (Reaction): Την υιοθέτηση κατάλληλων ενεργειών για την αποκατάσταση ή την ανάκτηση των συστατικών μερών ενός πληροφοριακού συστήματος.

5.2 Η ΑΣΦΑΛΕΙΑ ΩΣ ΑΠΑΙΤΗΣΗ ΤΩΝ ΔΙΚΑΙΟΥΧΩΝ

Στα Πληροφοριακά Συστήματα η ύπαρξη μέτρων εκτιμάται από πολλούς ότι έχουν άμεσο συμφέρον μόνο οι σχεδιαστές και οι ιδιοκτήτες. Όμως με το πέρασμα των χρόνων τα πληροφοριακά συστήματα παίζουν σημαντικό ρόλο μέσα στον οργανισμό καθώς και το δικαίωμα της απαίτησης στην ασφάλεια του Πληροφοριακού Συστήματος. Επομένως αυτοί που έχουν το δικαίωμα της απαίτησης να υπάρχουν μέτρα ασφαλείας και μηχανισμοί είναι οι εξής:

- Η Διοίκηση του Οργανισμού: Λόγω του ρόλου του πληροφοριακού συστήματος και της σπουδαιότητας των πληροφοριακών πόρων, σε σχέση με τις οικονομικές δαπάνες που πραγματοποιούντε για την απρόσκοπτη λειτουργία του συστήματος είναι λογικό η διοίκηση να ενδιαφέρεται για το επίπεδο ασφάλειάς του.
- Οι Ιδιοκτήτες και οι Διαχειριστές Δεδομένων και Διεργασιών: Σε περίπτωση μειωμένων μέτρων ασφαλείας κάνουν το σύστημα ευπαθές και ευπρόσβλητο σε κάθε είδους φύσεως απειλές από τρίτους.
- Οι Υπεύθυνοι της Λειτουργίας και της Ανάπτυξης του Πληροφοριακού Συστήματος: Στην κατηγορία αυτή ανήκουν τα άτομα που ασχολούνται με την ορθή λειτουργία του τεχνολογικού και υπολογιστικού εξοπλισμού.
- Οι Καταναλωτές των Τελικών Προϊόντων και Υπηρεσιών: Στην κατηγορία αυτή ανήκουν οι πολίτες ή τα απλά άτομα που χρησιμοποιούν το πληροφοριακό σύστημα για την πραγματοποίηση μιας ενέργειας του ή την λήψη μιας υπηρεσίας.
- Η Πολιτεία: Η πολιτεία έχει τον πρωταρχικό ρόλο για τη διαμόρφωση των μέτρων ασφαλείας με το να θεσπίζει κανόνες και πλαίσια για να τηρούνται οι κανόνες που πρέπει. Επομένως η σοβαρότητα των πιθανών αδικημάτων που μπορεί να διαπραχθούν από τη συλλογή, χρήση, μετάδοση καθώς και την επεξεργασία των πληροφοριών σε σχέση με τον κάθε απλό πολίτη να αντιμετωπίσει την πολυπλοκότητα της νέας τεχνολογίας, οδηγεί την πολιτεία να διορίσει Ανεξάρτητες Διοικητικές Αρχές (π.χ Επιτροπή Τηλεπικοινωνιών, Αρχή Προστασίας Δεδομένων),με σκοπό τον έλεγχο των πληροφοριακών συστημάτων.

Σε περίπτωση αποτυχίας της αντιμετώπισης μιας επίθεσης σε έναν οργανισμό, πέρα από την απώλεια ευαίσθητων ιδιωτικών ή δημόσιων δεδομένων και πληροφοριών από τα αρχεία του, θα έχει επιπτώσεις τόσο στη δημόσια εικόνα του καθώς και στην αξιοπιστία του. Είναι εμφανές ότι σε όλο το ζήτημα εμπλέκονται πολλοί παράγοντες καθώς και πολλοί ενδιαφερόμενοι. Όπως είπαμε και παραπάνω η διοίκηση είναι φυσικό να δίνει μεγάλη σημασία στις οικονομικές δαπάνες και στην περίπτωση του πιθανού αυτοσχεδιασμού δραστηριοτήτων που συνεπάγεται η εφαρμογή των μέτρων ασφαλείας. Από την άλλη μεριά η πολιτεία και οι τελικοί χρήστες δίνουν σημασία στην τελειότητα της ικανοποίησης των απαιτήσεων της ασφάλειας, χωρίς να τους ενδιαφέρει το κόστος. Οι υπεύθυνοι της λειτουργίας και οι διαχειριστές των διεργασιών ενδιαφέρονται, για τα μέτρα τα οποία προτείνονται, να ανταποκρίνονται στα χαρακτηριστικά της οργάνωσης και της ιδεολογίας του οργανισμού, έτσι ώστε να μην χρειάζονται πολλές αλλαγές στον τρόπο λειτουργίας και δομής του. Τέλος οι ειδικοί ασφαλείας και οι υπεύθυνοι της ανάπτυξης του πληροφοριακού συστήματος δίνουν σημασία σε μια σειρά από παράγοντες όπως ο ρόλος του αναλυτή, ο ρόλος του χρήστη, το οντολογικό και επιστημονικό πλαίσιο της κάθε οντολογικής προσέγγισης κ.α.

5.3 ΟΙ ΕΠΙΒΟΥΛΟΙ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Οι επιθέσεις κατά του συστήματος, αν κατηγοριοποιηθούν με βάση το σκοπό τους, δίνουν τις παρακάτω 5 κατηγορίες:

- Εισαγωγή ή μετατροπή δεδομένων χωρίς εξουσιοδότηση ή καταστροφή των δεδομένων και των προγραμμάτων ενός πληροφοριακού συστήματος.
- Αλλοίωση ή μείωση της αξιοπιστίας των δεδομένων ενός πληροφοριακού συστήματος.
- Παρεμπόδιση της ομαλής λειτουργίας του.
- Χωρίς άδεια εισβολή και αφαίρεση στοιχείων του.

• Παραβίαση των αποκλειστικών δικαιωμάτων του δημιουργού, του κατόχου, των δεδομένων, των προγραμμάτων και γενικά του πληροφοριακού υλικού.

Στις προαναφερθείσες κατηγορίες πρέπει να σημειωθεί και η επίθεση από κακόβουλο λογισμικά. Ποιοι είναι αυτοί όμως που απειλούν ένα πληροφοριακό σύστημα; Έρευνες δείχνουν ότι η κυριότερη απειλή προέρχεται μέσα από τον οργανισμό. Συνεταίροι, σύμβουλοι και δυσαρεστημένοι υπάλληλοι που θέλουν να διεκδικήσουν την διοίκηση για τις αποφάσεις της καθώς και χρήστες που έχουν λανθασμένη αντίληψη για τα προνόμια και τα δικαιώματα τους, είναι μερικές αιτίες που οδηγούν και προκαλούν αυτού του είδους τις ενέργειες.

5.4 ΟΙ ΙΔΙΟΤΗΤΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για να υλοποιηθεί ο στόχος της ασφάλειας πρέπει να υιοθετηθούν και να εφαρμοστούν τα αντίστοιχα μέτρα ασφαλείας (Safeguards). Χωρίς αυτά τα πληροφοριακά συστήματα είναι ευάλωτα απέναντι σε απειλές.

Η πρόσβαση σε πληροφορίες από μη εξουσιοδοτημένα άτομα καταργεί την εμπιστευτικότητα (Confidentiality) των πληροφοριών. Η τροποποίηση των πληροφοριών από μη εξουσιοδοτημένα άτομα έχει ως συνέπεια την καταστροφή της ακεραιότητας (Integrity) και τέλος η διαγραφή πληροφοριών και δεδομένων ή κατάργηση άλλων λειτουργιών του πληροφοριακού συστήματος από μη εξουσιοδοτημένα άτομα κάνουν αδύνατη τη διαθεσιμότητα (Availability) των πληροφοριών. Οι 3 αυτές έννοιες (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) αποτελούν τις πιο σημαντικές ιδιότητες της πληροφορίας ως αγαθό, όπου η διασφάλισή τους και η προστασία τους αποτελούν πρωταρχικό στόχο για την ασφάλεια των πληροφοριακών συστημάτων. Παρακάτω αναφέρονται οι 3 βασικές ιδιότητες ασφάλειας πιο αναλυτικά:

- Η Εμπιστευτικότητα (Confidentiality): Προφυλάσσει την αποκάλυψη ευαίσθητων πληροφοριών από μη εξουσιοδοτημένα άτομα. Τα ευάλωτα στοιχεία των πληροφοριακών συστημάτων (πληροφορίες, υπολογιστικοί πόροι) πρέπει να εμφανίζονται μόνο σε εξουσιοδοτημένα άτομα. Οι μηχανισμοί προστασίας που υπάρχουν πραγματοποιούν τους αναγκαίους ελέγχους, για να ελαττώσουν την πρόσβαση στα στοιχεία αυτά. Η εμπιστευτικότητα επιτυγχάνεται με την κρυπτογράφηση των δεδομένων η οποία κάνει τα δεδομένα μη αναγνώσιμα καθώς και με έλεγχο πρόσβασης στα δεδομένα. Άλλες μορφές της εμπιστευτικότητας είναι οι εξής:

  - Η μυστικότητα (Secrecy): Είναι η προστασία των δεδομένων που έχουν μορφή προσωπικού χαρακτήρα (αφορούν συγκεκριμένα άτομα).
  - Η ιδιωτικότητα (Privacy): Είναι η προστασία των δεδομένων σε ένα οργανισμό.

- Η Ακεραιότητα (Integrity): Είναι η διασφάλιση της ακρίβειας, της πληρότητας καθώς και των μεθόδων επεξεργασίας του πληροφοριακού συστήματος. Στόχος της ακεραιότητας είναι η κάθε αλλαγή και τροποποίηση στο πληροφοριακό σύστημα (π.χ τιμές πληροφοριών) να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας ενώ σε περίπτωση μη εξουσιοδοτημένης αλλαγής να μη γίνεται επιτρεπτή. Η ακεραιότητα επιτυγχάνεται με τις ψηφιακές υπογραφές, με τη χρήση των μηχανισμών αυθεντικοποίησης καθώς και με τον έλεγχο πρόσβασης.
- Η Διαθεσιμότητα (Availability): Είναι η ιδιότητα που κάνει αδιάλειπτη και απρόσκοπτη την πρόσβαση των εξουσιοδοτημένων χρηστών όταν τη χρειάζονται έτσι ώστε να μην υπάρχουν προβλήματα αδικαιολόγητης καθυστέρησης ή να μην είναι προσπελάσιμες οι υπηρεσίες ενός πληροφοριακού συστήματος. Στόχος της διαθεσιμότητας είναι:
  - Η έγκαιρη ανταπόκριση της διάθεσης των δεδομένων.
  - Η δίκαιη κατανομή των πόρων.
  - Η δυνατότητα χρησιμοποίησης των πόρων και των δεδομένων όπως σχεδιάστηκαν.
  - Ο κατάλληλος χρόνος διάθεσης πόρων.

- Η ικανότητα χειρισμού των απαραίτητων πόρων.

Επιπλέον έχει διαπιστωθεί πως οι παραπάνω 3 ιδιότητες δεν είναι αρκετές για να προσδιοριστεί η έννοια της ασφάλεια των πληροφοριών. Επιπρόσθετες ιδιότητες που συναντώνται είναι οι εξής:

- Η Ταυτοποίηση (Identification): Είναι η διαδικασία κατά την οποία μία οντότητα (π.χ άνθρωπος , υπολογιστής) αναγνωρίζει μια άλλη οντότητα.
- Η Αυθεντικοποίηση ή Πιστοποίηση TauTO^Taq(Authentication): Είναι η διαδικασία κατά την οποία μια οντότητα επιβεβαιώνει την ταυτότητα μιας άλλης οντότητας. Η διαδικασία αυτή χωρίζεται σε αυθεντικοποίηση μηνύματος και αυθεντικοποίηση της οντότητας.
- Η Εξουσιοδότηση (Authorization): Η παροχή σε ένα υποκείμενο το δικαίωμα πρόσβασης σε ένα αντικείμενο. Η παροχή αυτή γίνεται και τυπικά μετά την ταυτοποίηση και αυθεντικοποίηση του υποκειμένου.
- Η Απονομή ευθυνών (Accountability): Αποδεικνύει ότι μια οντότητα πρέπει να έχει αναγνωριστή και να είναι υπεύθυνη των πράξεων της.
- Η Μη αποποίηση (Non-repudiation): Είναι η διαθεσιμότητα των αδιάψευστων αποδείξεων που μπορούν να χρησιμοποιηθούν σε μια διαφωνία.

Οι διαφορετικές απόψεις που υπάρχουν για τις ιδιότητες της ασφάλειας δεν πρέπει να θεωρηθούν παράδοξες επειδή στον ευρύ τομέα της πληροφορικής η ασφάλεια αποτελεί μια αφηρημένη έννοια, οι οποία δέχεται διάφορες ερμηνείες. Επομένως η έννοια της ασφάλειας προσδιορίζεται σε ποικίλες ιδιότητες της πληροφορίας, με βάση το πώς το βλέπει ο ερευνητής και ως προς το πληροφοριακό σύστημα που αναφέρεται. Οι προαναφερθείσες ιδιότητες ασφαλείας των πληροφοριών δεν μπορούν μετρηθούν σε απόλυτα μεγέθη. Παρά το γεγονός ότι οι ορισμοί για τις 3 βασικές κατηγορίες που παρέχονται με απλότητα και σαφήνεια, δεν είναι πάντα εύκολο να προσδιορίσουμε ποιες από αυτές έχουν παραβιαστεί. Για παράδειγμα σε περίπτωση παραβίασης διαθεσιμότητας με τη μη διάθεση της πληροφορίας μπορεί να αξιολογηθεί με ποικίλους τρόπους σε

διαφορετικές περιπτώσεις, διότι ο χρόνος αναμονής διαφέρει από εφαρμογή σε εφαρμογή. Επομένως μια καθυστέρηση μιας συγκεκριμένης χρονικής περιόδου 5 λεπτών για την εξαγωγή μια σημαντικής ιατρικής πληροφορίας μπορεί να θεωρηθεί έλλειψη διαθεσιμότητας αλλά ο ίδιος χρόνος για την αναζήτηση κάποιων στοιχείων για ένα φορολογούμενο σε μια δημόσια υπηρεσία μπορεί να θεωρηθεί αποδεκτός.

5.5 Η ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Η πολιτική ασφαλείας σε έναν οργανισμό, ως προς τη λειτουργία των πληροφοριακών συστημάτων, περιλαμβάνει τους κανόνες, τις οδηγίες, τις διαδικασίες, τις αρμοδιότητες και γενικά με ότι έχει σχέση με την ασφάλεια και αφορά την προστασία των πληροφοριακών συστημάτων. Η πολιτική ασφαλείας παρουσιάζεται σε ένα έγγραφο το οποίο υποχρεούνται οι χρήστες των πληροφοριακών συστημάτων να το ξέρουν και να το εφαρμόζουν.

Ένας ρόλος έχει μια δομή και είναι η βάση της πολιτικής ελέγχου προσπέλασης. Ο ρόλος μπορεί να περιλαμβάνει εξουσιοδοτήσεις από αρμοδιότητες και ενέργειες που έχουν σχέση με τη λειτουργία του συστήματος, και παραχωρείται σε χρήστες, δίνοντας τους έτσι την δυνατότητα να εκτελέσουν τις ενέργειες για να λειτουργήσουν στα πλαίσια των αρμοδιοτήτων. Η πολιτική ασφαλείας εφαρμόζεται για να κατανοήσουμε τα παρακάτω ερωτήματα:

- Ποιος είναι οι στόχοι και ο σκοπός της πολιτικής;
- Ποια είναι τα αγαθά του συστήματος που χρειάζονται προστασία;
- Για την προστασία των αγαθών ποιοι είναι υπεύθυνοι και ποιες αρμοδιότητες έχουν;

5.6 ΕΛΕΓΧΟΣ ΠΡΟΣΠΕΛΑΣΗΣ

Το πρώτο στάδιο της άμυνας ενός πληροφοριακού συστήματος είναι η αναγνώριση και η επαλήθευση της ταυτότητας των χρηστών. Αυτές οι 2 ενέργειες είναι απαραίτητες και σημαντικές γιατί η ταυτότητα του χρήστη αποτελεί βασικό παράγοντα στις αποφάσεις του ελέγχου προσπέλασης. Το γεγονός όμως ότι κάποιος χρήστης έχει την εξουσιοδότηση να συνδεθεί με ένα πληροφοριακό σύστημα δεν συνεπάγεται ότι έχει και εξουσιοδότηση να κάνει ό,τι θέλει σε αυτό. Από την άλλη μεριά οι μη εξουσιοδοτημένες προσβάσεις χρηστών σε εγκαταστάσεις πληροφοριακού συστήματος επιφέρουν την καταστροφή των αγαθών. Επομένως, είναι σημαντικό να υπάρχει ένας μηχανισμός που να επιβλέπει τη δυνατότητα των χρηστών να κάνουν χρήση των πληροφοριών ή των υπολογιστικών πόρων κάποιου πληροφοριακού συστήματος. Ο μηχανισμός αυτός είναι γνωστός ως μηχανισμός προσπέλασης. Ο έλεγχος προσπέλασης είναι ένα κοινό μέτρο ασφαλείας ενός πληροφοριακού συστήματος και περιλαμβάνει τα παρακάτω:

> Το μηχανισμό αυθεντικοποίησης του χρήστη.

> Το μηχανισμό της διαχείρισης δικαιωμάτων των χρηστών.

> Το μηχανισμό του ελέγχου και της καταγραφής των ενεργειών.

> Το μηχανισμό λήψης απόφασης της εξουσιοδότησης.

> Το μηχανισμό της επιβολής του ελέγχου εξουσιοδότησης.

Ο έλεγχος προσπέλασης αποτελείται από δύο τμήματα:

- ένας μηχανισμός ο οποίος αποφασίζει αν θα δοθεί ή όχι άδεια προσπέλασης υποκειμένων σε αντικείμενα με βάση προσδιορισμένους κανόνες.
- και ένας μηχανισμός που ορίζει την απόφαση.

Υπάρχουν διάφορες πολιτικές ελέγχου προσπέλασης που έχουν δημιουργηθεί για να καλύψουν τις απαιτήσεις των διαφορετικών χώρων λειτουργίας των πληροφοριακών συστημάτων. Οι πολιτικές ελέγχου προσπέλασης διακρίνονται σύμφωνα με το βαθμό

εμπιστοσύνης και το βαθμό ευαισθησίας της πληροφορίας Αδιαβάθμητη (Infinitely), Εμπιστευτική (Confidential), Απόρρητη (Secret), Άκρως Απόρρητη (Top Secret).

5.7 ΤΑΥΤΟΠΟΙΗΣΗ ΚΑΙ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

Σε ένα πληροφοριακό σύστημα υπάρχουν ποικίλες τεχνικές και διαδικασίες για την ταυτοποίηση και αυθεντικοποίηση των διάφορων χρηστών. Η καλύτερη δυνατή επιλογή ανάμεσα σε πολλές τεχνικές παίζει σημαντικό ρόλο και αποτελεί βασικό στοιχείο για την ασφάλεια των επικοινωνιακών όσο και των υπολογιστικών συστημάτων.

- Ως προς τη διαδικασία της ταυτοποίησης (Identification) ενός λογικού υποκείμενου είναι εκείνη η διαδικασία στην οποία το υποκείμενο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που χρειάζεται για να συσχετιστεί με ένα από τα αντικείμενα που δικαιούται προσπέλασης στους πόρους του.
- Ως προς τη διαδικασία της αυθεντικοποίησης (Authentication) ενός λογικού υποκειμένου είναι εκείνη η διαδικασία στην οποία το υποκείμενο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που χρειάζεται ώστε να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.

Τα πιο συνηθισμένα μέσα αυθεντικοποίησης είναι τα εξής:

- Συνθηματικά (Passwords)
- Ψηφιακά Πιστοποιητικά (Digital Certificates)
- Έξυπνες Κάρτες (Smart Cards)
- Συστήματα Αυθεντικοποίησης
- Βιομετρικά Συστήματα(αναγνώριση προσώπου, δακτυλικά αποτυπώματα, ίριδα ματιού)
- Κρυπτογραφία (Cryptography)

Λόγω της ευαίσθητης πληροφορίας που εμπεριέχεται στα πληροφοριακά συστήματα και του μεγέθους των οργανισμών απαιτείται μια μεθοδευμένη διαχείριση κινδύνου που πρέπει να αναπτυχθεί εντός των οργανισμών. Άτομα με εξιδεικευμένες γνώσεις σε τεχνικά ζητήματα, καθώς και άνθρωποι του οργανισμού θα πρέπει να απασχολούνται εξ' ολοκλήρου με την διαχείριση αυτών των κινδύνων αφού είναι απειλές ύψιστης σημασίας για τον εκάστοτε οργανισμό.

ΕΠΙΛΟΓΟΣ

Με βάση τα σημερινά δεδομένα και την υψηλή επικινδυνότητα της αγοράς, οι κίνδυνοι αποτελούν ένα μεγάλο κεφάλαιο στον τομέα των οικονομικών μονάδων. Η ποικιλομορφία των κινδύνων συμβάλλει στην δυσκολία των λύσεων των ζητημάτων ρίσκου ενός οργανισμού. Από έρευνες διαπιστώνεται η αύξηση της σημασία του risk management σε οργανισμούς κάθε είδους. Ο εντεινόμενος ανταγωνισμός που είναι αποτέλεσμα της ενιαίας αγοράς, οι σαρωτικές τεχνολογικές αλλαγές και οι αλλαγές στον κοινοτικό και δημογραφικό τομέα είναι κάποιοι από τους παράγοντες που έχουν συμβάλλει σημαντικά στην απαραίτητη και γρήγορη εξέλιξη της διαχείρισης κινδύνου.

Η πολυδιάστατη μορφή του κινδύνου όμως δεν επιτρέπει στους οικονομικούς οργανισμούς την πλήρη και σωστή κατανόηση του κινδύνου και έχει ως αποτέλεσμα την αποτυχία πολλών σχεδίων επιχειρηματικού ρίσκου. Οι κίνδυνοι αλληλοσυνδέονται και επηρεάζουν πολλούς τομείς του περιβάλλοντος των οικονομικών οργανισμών. Η μελέτη αυτών λοιπόν απαιτεί σύνθετα και ενημερωμένα προγράμματα αντιμετώπισης και διορθωτικών αλλαγών για κάθε μεμονωμένο ζήτημα ρίσκου, όπως επίσης και την γνώση των άλλων οικονομικών θεωριών.

Πολλές μέθοδοι υπάρχουν ήδη ή προτείνονται από διάφορους ερευνητές για την λεπτομερή και όσο το δυνατόν απλούστερη ανάλυση και διαχείριση του κινδύνου. Όμως σημαντικό ρόλο παίζει και η κρίση του κάθε αποφασίζων για το κάθε βήμα σ' αυτές. Απολύτως λογικό είναι το γεγονός ότι από έναν οικονομικό οργανισμό σε έναν άλλον η αντίληψη για τον κίνδυνο διαφέρει και δίνεται διαφορετική έμφαση σ' αυτόν.

Η είσοδος πληροφοριακών συστημάτων για την διευκόλυνση των στρατηγικών της διαχείρισης κινδύνων είναι πολύ σημαντική τόσο για την αποφυγή συντακτικών λαθών όσο και για την εξοικονόμηση χρόνου, διότι η ταχύτερη επίλυση ενός προβλήματος συνδέεται άμεσα με την μείωση του κόστους. Η ραγδαία εξέλιξη στον τομέα της Τεχνολογίας Πληροφορικής και των Επικοινωνιών οφείλεται στην ανάπτυξη των υπηρεσιών που υποστηρίζουν την ανταλλαγή των δεδομένων από απόσταση καθώς και την επεξεργασία των πληροφοριών. Έτσι είναι επιτακτική η ανάγκη για δημιουργία πληροφοριακών συστημάτων τα οποία θα εξασφαλίζουν με ασφάλεια τη διακίνηση των δεδομένων που οδηγούν σε πληροφορίες και να διαθέτουν τις ιδιότητες της εμπιστευτικότητας (Confidentiality) της ακεραιότητας (Integrity) και τις διαθεσιμότητας (Availability). Τα δεδομένα αποτελούν το αγαθό μεγάλης αξίας σε κάθε οργανισμό. Επομένως η ασφάλεια των δεδομένων και των κρίσιμων πληροφοριών αποτελούν σημαντική πρόκληση σε όλα τα επίπεδα. Τα θέματα ασφαλείας των πληροφοριακών συστημάτων και των δικτύων που στηρίζοντα σε αυτά είναι μεγάλης αξίας και εξελίσσονται καθημερινά.

Η ασφάλεια των πληροφοριακών συστημάτων πάντα θα αποτελεί ένα μείζον θέμα. Στην ερώτηση αν υπάρχει ή αν θα υπάρξει πλήρης ασφάλεια στα πληροφοριακά συστήματα, η απάντηση δεν είναι θετική. Αν και οι οργανισμοί που στηρίζονται σε αυτά για να λειτουργήσουν σωστά αλλά και να γίνουν και πιο ανταγωνιστικοί τους παρέχουν την ουσιώδη προστασία με διάφορες τεχνικές, τα λογισμικά καθώς και το κατάλληλο εκπαιδευμένο προσωπικό (αναλυτές συστημάτων, προγραμματιστές), πάντα θα έχουν το πρόβλημα της ασφάλειας.

Λόγω της ραγδαίας τεχνολογικής εξέλιξης πάντα θα υπάρχουν οι κακόβουλοι χρήστες που θα προσπαθούν μέσω νέων πιο εξελιγμένων τεχνικών να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή τον έλεγχο σε συστήματα για να προκαλέσουν ζημιά. Επομένως για την ασφάλεια πρέπει να κινούνται όλοι οι εμπλεκόμενοι στο σωστό δρόμο ώστε να βελτιώνονται συνέχεια οι υποδομές τους, με τη χρήση των πιο σύγχρονων τεχνικών και λογισμικών που παρουσιάζονται στην αγορά ώστε να μπορούν να αντεπεξέλθουν στις πιθανές νέες απειλές. Επίσης οι εταιρίες θα πρέπει να εφαρμόζουν τις πολιτικές ασφαλείας και οι χρήστες να είναι ενήμεροι για τους υπάρχοντες κινδύνους καθώς και για τους πρωτοεμφανιζόμενους αλλά και να συμπεριφέρονται ανάλογα σε περίπτωση εμφάνισής τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- https://erm.ncsu.edu/library/categories/category/erm-and-information-technology-risk
- http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/16484/SDO_XRHMEL_00444_Medium.pdf?sequence=1
- https://ac.els-cdn.com/S1876610212005760/1-s2.0-S1876610212005760-main.pdf?_tid=46f71184-465f-4076-9697-a7d556c56a10&acdnat=1545004909_63efc9caa61a068d2003677f3bc3fb55
- http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/6177/Tsalamandris.pdf?sequence=2&isAllowed=y
- https://www.business.qld.gov.au/running-business/protecting-business/risk-management/it-risk-management
- https://eclass.uoa.gr/modules/document/file.php/D205/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/intro_risk_mgmt.pdf
- http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/12606/1/DT2014-0311.pdf
- http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/13433/STE_MHP_00188_Medium.pdf?sequence=1

- http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9310/Alexandri_Barbara.pdf?sequence=1&isAllowed=y
- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf
- https://www.theirm.org/media/886331/Risk_Management_Standard_Greek_000.pdf
- https://www.sciencedirect.com/science/article/pii/S0377221715011479?via%3Dihub
- http://nefeli.lib.teicrete.gr/browse/sdo/ba/2011/KapagioridisCharalampos/attached-document-1305620931-972325-13789/kapagioridis2011.pdf