ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

RISK MANAGEMENT ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΗΜΗΤΡΙΟΣ ΚΑΡΝΑΒΑΣ

Διπλωματική εργασία
που υποβλήθηκε στο τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά
ως μέρος των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος

Πειραιάς
Σεπτέμβριος 2012

Το άτομο το οποίο εκπονεί την Διπλωματική Εργασία φέρει ολόκληρη την ευθύνη προσδιορισμού της δίκαιης χρήσης του υλικού, η οποία ορίζεται στην βάση των εξής παραγόντων: του σκοπού και χαρακτήρα της χρήσης (εμπορικός, μη κερδοσκοπικός ή εκπαιδευτικός), της φύσης του υλικού που χρησιμοποιεί (τμήμα του κειμένου, πίνακες, σχήματα, εικόνες), του ποσοστού και της σημαντικότητας του τμήματος, που χρησιμοποιεί σε σχέση με το όλο κείμενο υπό copyright, και των πιθανών συνεπειών της χρήσης αυτής στην αγορά ή στη γενικότερη αξία του υπό copyright κειμένου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1^{Ο} ΕΙΣΑΓΩΓΗ

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.

Πολλές εταιρίες ανεξάρτητα από το μέγεθος ή τα χρήματα τα οποία επενδύθηκαν από τους ιδρυτές της στο ξεκίνημα της κατάφεραν να έχουν μια επιτυχημένη πορεία λόγω της κατανόησης από τη πρώτη στιγμή που ξεκίνησαν σε σχέση με τη σημασία και τη σπουδαιότητα των πληροφοριακών συστημάτων *Slack N.*,(2004). Ως παράδειγμα μπορούμε ν' αναφερθούμε στην αμερικανική εταιρία διανομής αεροπορικών και επίγειων δεμάτων, United Parcel Service, την οποία μπορεί οι ιδρυτές της να έκαναν την έναρξη της σ' ένα υπόγειο γραφείο μεγέθους ντουλάπας και αρχικά να έκαναν τη διανομή των δεμάτων με ποδήλατα, όμως κατάφεραν να τη φτάσουν σήμερα να είναι η μεγαλύτερη εταιρία διανομής στην Αμερική μια και από τη πρώτη στιγμή έδωσαν μεγάλη βαρύτητα στη λειτουργία και σημασία των πληροφορικών συστημάτων επενδύοντας μέσα στα χρόνια οι ίδιοι και οι διάδοχοι τους μεγάλα ποσά στις νέες τεχνολογίες, πετυχαίνοντας έτσι να διαφοροποιούνται συνεχώς αλλά και ν' εξυπηρετούν καλύτερα τους τελικούς πελάτες τους. *Τασόπουλος Α.*(2005),. Το παραπάνω παράδειγμα μας υποδεικνύει τη σημασία των πληροφορικών συστημάτων, των οποίων η χρήση έχουν την ικανότητα ένα μικρό οργανισμό να τον μετατρέψουν σε μεγάλο, αλλά και το αντίθετο μπορεί να συμβεί όταν η χρήση τους είναι ελλιπής ή αόριστη.

1.1 ΣΚΟΠΟΣ ΤΗΣ ΕΡΓΑΣΙΑΣ

Σκοπός της εργασίας είναι η διαχείριση της επικινδυνότητας των πληροφοριακών συστημάτων εστιάζοντας στη διαχείριση ρίσκου και στις δυσλειτουργίες και προτείνοντας τρόπους επίλυσης μέσα από το σωστό σχεδιασμό και την αποτελεσματική διαχείριση.

Οι αντικειμενικοί στόχοι της εργασίας είναι οι κάτωθι :

Α) Να μελετηθεί η βιβλιογραφία σχετικά με τα πληροφοριακά συστήματα και το risk management

Β) Να παρουσιαστεί η μεθοδολογία της διαχείρισης κινδύνου

Γ) Να αναλυθεί ο προγραμματισμός της διαχείρισης κινδύνου

Δ) Να μελετηθεί η σημασία της ασφάλεια των πληροφοριακών συστημάτων

1.2 ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΕΡΓΑΣΙΑΣ

Το αντικείμενο της εργασίας είναι η ασφάλεια των πληροφοριών και ο έλεγχος κινδύνων αναφορικά με τις επιχειρησιακές /επιχειρηματικές διαδικασίες που αποτελούν απαραίτητα συστατικά της εύρυθμης λειτουργίας του οργανισμού, ειδικά μέσα από το πρίσμα των πληροφοριακών συστημάτων. Η λειτουργία της κατάρτισης στρατηγικών κατάλληλων για το χειρισμό κρίσεων στα πληροφοριακά συστήματα, η οποία πρέπει να γίνεται μέσω της δημιουργίας διαδικασιών για την ανάπτυξη και υλοποίηση τεχνικών που μετριάζουν τους κινδύνους που απαντώνται σε ένα πληροφοριακό σύστημα.

Οι διαδικασίες διαχείρισης επιχειρηματικών κινδύνων που αποσκοπούν στην αξιολόγηση των κινδύνων και των πιθανών αρνητικών αντικτύπων που θα έχουν στο πληροφοριακό σύστημα και η αναγνώριση και τεκμηρίωση των πιθανών κινδύνων που μπορεί να παρουσιάσει το πληροφοριακό σύστημα, καθώς επίσης και η δημιουργία Στρατηγικής Διαχείρισης Κινδύνων, η οποία αναφέρεται στα κίνητρα που οδηγούν στην αλλαγή, στην τυχόν αλλαγή της δομής του πληροφοριακού συστήματος, αλλά και στην προσέγγιση που θα ακολουθηθεί.

1.3 ΛΟΓΟΙ ΕΠΙΛΟΓΗ ΤΟΥ ΘΕΜΑΤΟΣ

Βάσει όλων των παραπάνω καθίσταται κατανοητό το ιδιαίτερο ενδιαφέρον που παρουσιάζει το παρόν θέμα της παρούσης εργασίας. Ο γράφων θέλησε να το εξετάσει διεξοδικά, μέσα από μια πλήρη βιβλιογραφική επισκόπηση, προκειμένου να καταστήσει σαφές τον τρόπο με τον οποίο τα πληροφοριακά συστήματα μπορούν να αναδείξουν μια επιχείρηση και να τη βοηθήσουν στην περαιτέρω επέκτασή της, βοηθώντας την να αντιμετωπίσει τα οποιαδήποτε προβλήματα παρουσιαστούν.

Συνοπτικά, οι λόγοι που συνέβαλλαν στην επιλογή του συγκεκριμένου θέματος είναι:

1. Το θέμα είναι αρκετά ενδιαφέρον και επίκαιρο.
2. Η μελέτη του συγκεκριμένου θέματος αφορά άμεσα την ελληνική πραγματικότητα και χρήζει ακαδημαϊκής σπουδής από βιβλιογραφικής ανασκόπησης.
3. Η ανάγκη εφαρμογής των γνώσεων που αποκόμισε ο γράφων στο Πανεπιστήμιο Πειραιά και η εφαρμογή αυτών σ’ ένα σημαντικό ακαδημαϊκό ζήτημα.
4. Η ολοκλήρωση με επιτυχία του παρόντος θέματος αποτελεί αυτοσκοπό για τον φοιτητή, μιας και θα τον βοηθήσει να ολοκληρώσει με επιτυχία τις σπουδές του στο Πανεπιστήμιο Πειραιά.

ΚΕΦΑΛΑΙΟ 2 ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ RISK MANAGEMENT

Οι καλές πληροφορίες πρέπει να είναι κατάλληλες και να σχετίζονται με το πρόβλημα που εξετάζεται *Durbin A.*,(1997). Πρέπει επίσης να είναι έγκυρες. Για παράδειγμα, οι πληροφορίες από την έρευνα για την μπίρα Buckler (χωρίς οινόπνευμα) της ΑΘΗΝΑΪΚΗΣ ΖΥΘΟΠΟΙΙΑΣ Α.Ε. θα ήταν άχρηστες αν δίνονταν δύο χρόνια μετά την απόσυρση του προϊόντος.

Οι καλές πληροφορίες πρέπει, επίσης, να είναι ακριβείς και τελικά οι καλές πληροφορίες μειώνουν την αβεβαιότητα, η οποία δημιουργείται από την έλλειψη πληροφοριών για μια συγκεκριμένη περιοχή ενδιαφέροντος. Στο παράδειγμα της ΑΘΗΝΑΪΚΗΣ ΖΥΘΟΠΟΙΙΑΣ, για να εκπληρώνει αυτά τα κριτήρια η έρευνα πληροφοριών, θα πρέπει να βοηθά το διευθυντή του μάρκετινγκ να απαντήσει στο ερώτημα: "Γιατί οι άνθρωποι δεν αγοράζουν την Buckler με τον τρόπο που νομίζαμε ότι θα το έκαναν;"

Εντούτοις, ακόμη και οι καλές πληροφορίες είναι σχετικά άχρηστες, χωρίς τις γνώσεις που προέρχονται από την ανάλυση και την ερμηνεία τους. Σήμερα, τα στελέχη των επιχειρήσεων κατακλύζονται, αν μη τι άλλο, από πληροφορίες για τις πρακτικές των ανταγωνιστών, για τις αγοραστικές συνήθειες των καταναλωτών, για τη λεπτομερειακή ανάλυση των μηχανών και για πολλά άλλα σχετικά θέματα. Έτσι, ο ρόλος της τεχνολογίας πληροφοριών οργάνωσης δεν είναι μόνο να συλλέγει και να μεταβιβάζει περισσότερες (ή ακόμη καλύτερης ποιότητας) πληροφορίες, αλλά να εφοδιάσει τα στελέχη με τις απαραίτητες γνώσεις, μέσα από την ανάλυση και την ερμηνεία για το τι ακριβώς συμβαίνει στην επιχείρησή τους.

2.1 ΟΡΙΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Σύμφωνα με τον Φωλίνα Δ το (2006) «*ένα πληροφοριακό σύστημα αποτελεί ένα οργανωμένο σύνολο δράσεων, το οποίο αναφέρεται σε πέντε συγκεκριμένα στοιχεία»*. Αναλυτικά αυτά είναι τα ακόλουθα:

1. Το ανθρώπινο στοιχείο, το οποίο αναφέρεται στο σύνολο των ανθρώπων που εργάζονται με το πληροφοριακό σύστημα σε διάφορους ρόλους όπως χρήστες ,διαχειριστές κ.τ.λ.).
2. Οι διαδικασίες, οι οποίες αναφέρονται στο σύνολο των οδηγιών για τη χρήση και συνδυασμό όλων των στοιχείων υποδομής ενός ΠΣ.
3. Η βάση δεδομένων, η οποία σχετίζεται με το σύνολο των πληροφοριών και των στοιχείων τα οποία συσωρεύονται και αναπτύσσονται μέσα από ένα πληροφοριακό σύστημα.
4. Το λογισμικό (software- τα προγράμματα) και ο υλικός εξοπλισμός(hardware).
5. Τέλος το δίκτυο βάση του οποίου οι υπολογιστές επικοινωνούν μεταξύ τους και βοηθούν στην επικοινωνία των χρηστών.

Σύμφωνα με τον Τασοπουλο Α. το (2005) ένα Πληροφοριακό σύστημα βοηθάει στον έλεγχο, στο συντονισμό, στην ανάλυση προβλημάτων, στη λήψη αποφάσεων και στην ανάπτυξη νέων προϊόντων. Προκειμένου να επιτύχει τους στόχους του ένα πληροφοριακό σύστημα θα πρέπει να προσδιορίζει, αποδοτικά και αποτελεσματικά, τις ανθρώπινες ανάγκες αυτών που χρησιμοποιούν ενώ συγχρόνως θα πρέπει να επεξεργάζεται όλες τις πληροφορίες με αποτέλεσμα την ικανοποίηση των αναγκών αυτών.

Προκειμένου ένα πληροφοριακό σύστημα να επιτύχει τους στόχους του θα πρέπει να εστιάζει στην πιο αποτελεσματική ανάκτηση, αποθήκευση, επεξεργασία, παρουσίαση και διάδοση των πληροφοριών. Συγχρόνως θα πρέπει να παρέχει τα απαραίτητα μέσα και το κατάλληλο περιβάλλον μάθησης στους εμπλεκόμενους χρήστες ώστε να βελτιωθεί η αποτελεσματικότητα της διαδικασίας λήψης απόφασης. Τέλος θα πρέπει

να συμβάλει στην υποστήριξη των διαδικασιών λειτουργίας, ελέγχου και στρατηγικού σχεδιασμού την επιχείρησης ή του οργανισμού.

Ο κύκλος ζωής ενός πληροφοριακού συστήματος σύμφωνα με τον Οικονόμου Σ.Γ το 1995 αναφέρεται σε τέσσερα συγκεκριμένα στάδια, αυτά είναι το στάδιο της δημιουργίας, το στάδιο της ανάπτυξης, το στάδιο της εξέλιξης και τέλος της απόσυρσης *Οικονόμου Σ.*(2000).

Η γέννηση ενός πληροφοριακού συστήματος ξεκινά τη στιγμή που μια επιχείρηση ή οργανισμός αποφασίζει να το δημιουργήσει. Μετά από το στάδιο αυτό έχουμε τη περίοδο κατά την οποία προσδιορίζονται οι βασικές απαιτήσεις των λειτουργιών του, οι λειτουργίες αυτές σχεδιάζονται ώστε να καλύπτουν τις ανάγκες μιας επιχείρησης.

Στη συνέχεια έχουμε το στάδιο της ανάπτυξης όπου και το πληροφοριακό σύστημα, αναβαθμίζεται συνεχώς, προκειμένου να είναι επίκαιρο με βάση και την ευρύτερη ανάπτυξη μιας επιχείρησης. Τέλος όταν η επιχείρηση ή ο οργανισμός αποφασίσει ότι είναι πια αναποτελεσματικό και μη αποδοτικό, οπότε και το αποσύρει

Όπως ήδη αναφέραμε τα πληροφοριακά συστήματα συλλέγουν, αποθηκεύουν, μεταδίδουν και επεξεργάζονται δεδομένα για την παροχή χρήσιμων, ολοκληρωμένων και έγκαιρων πληροφοριών όπου και όποτε αυτές χρειάζονται *Βασιλακόπουλος Γ* (2004). Οι λόγοι χρήσεις τους από τις επιχειρήσεις αναφέρονται στα ακόλουθα :

1. Ταχύτατη και ακριβή επεξεργασία των δεδομένων
2. Μεγάλη αποθηκευτική ικανότητα.
3. Ταχύτατη επικοινωνία μεταξύ τοποθεσιών
4. Άμεση πρόσβαση σε πληροφορίες που πρέπει να αντλήσει η επιχείρηση για την δραστηριότητά της
5. Δυνατότητα συντονισμού ατόμων, ομάδων και οργανισμών.
6. Υποστήριξη των αποφάσεων που θα ληφθούν από την επιχείρηση.
7. Αυτοματοποίηση και βελτίωση των διαδικασιών και των ροών

εργασιών.

8. Αξιοποίηση πολύτιμων δεδομένων της επιχείρησης
9. Αύξηση της αποτελεσματικότητας της επιχείρησης

Σε μια επιχείρηση υπάρχουν αρκετοί παράγοντες και εμπλεκόμενοι φορείς με τα πληροφοριακά συστήματα, όπως οι χρήστες αυτών, οι υπεύθυνοι λειτουργίας και ανάπτυξής τους, το απαραίτητο υλικό για την ύπαρξη και υποστήριξη των συστημάτων αυτών, όπως επίσης και διάφοροι εξωτερικοί παράγοντες που μπορούν να επηρεάσουν τα συστήματα αυτά. Η χρήση πληροφοριακών συστημάτων βοήθησε στη δημιουργία νέων θέσεων εργασίας στις επιχειρήσεις, όπως του διευθυντή Πληροφορικής, του διευθυντή Μηχανογράφηση, του προϊστάμενου Τμήματος Μηχανογράφησης, του υπεύθυνου Λογαριασμών & Εφαρμογών, του υπεύθυνου Εξυπηρετητών , του υπεύθυνου Δικτύου, του υπεύθυνου Τεχνικής Υποστήριξης, των διάφορων Αναλυτών, Σχεδιαστών και Προγραμματιστών.

Όλες αυτές οι θέσεις εργασίας, βοήθησαν στη καλύτερη ανάπτυξη και οργάνωση μιας επιχείρησης ενώ συγχρόνως ανέπτυξαν πολλά είδη συστημάτων που μπορούν να χρησιμοποιηθούν ανάλογα με τις ανάγκες και τις οικονομικές δυνατότητες της επιχείρησης *Λαοπόδης Γ.*,(2006),. Τα σημαντικότερα συστήματα είναι τα ακόλουθα:

1. SCMS (Supplier and Contract Management System-Συστήματα Διαχείρισης Αλυσίδας Εφοδιασμού).
2. KMS (Knowledge Management Systems / Συστήματα Διαχείρισης Γνώσης)
3. OAS (Office Automation Systems / Συστήματα Αυτοματοποίησης Γραφείου)
4. TPS (Transaction Processing Systems / Συστήματα Επεξεργασίας Συναλλαγών)
5. ERP (Enterprise resource planning / Συστήματα Ενδοεπιχειρησιακού Σχεδιασμού)

6. ESS (Executive Support Systems / Συστήματα Υποστήριξης Διοίκησης)
7. DSS (Decision Support Systems / Συστήματα Υποστήριξης Απόφασης)
8. MIS (Management Information Systems / Διοικητικά Συστήματα Πληροφόρησης)

Το ποιο ή ποια από τα παραπάνω πληροφοριακά συστήματα θα επιλέξει η επιχείρηση εξαρτάται από αρκετούς παράγοντες. Υπάρχουν θετικά αλλά και αρνητικά για το καθένα σύστημα, ανάλογα βέβαια την επιχείρηση. Το καθένα από τα συστήματα έχει τα δικά του πλεονεκτήματα και μειονεκτήματα, παρακάτω θα δούμε γενικά τα πλεονεκτήματα και τα μειονεκτήματα των πληροφοριακών συστημάτων.

2.2 ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Ένα πληροφοριακό σύστημα μπορεί να οριστεί ως ένα σύνολο ανθρώπων, δεδομένων, τεχνολογίας και οργανωτικών μεθόδων που δουλεύουν μαζί για να συλλέξουν. να επεξεργαστούν. να αποθηκεύσουν και να μεταβιβάσουν πληροφορίες για να στηρίξουν τη λήψη αποφάσεων και τον έλεγχο: Ειδικά, θα εστιάσουμε την ανάλυση στα πληροφοριακά συστήματα διοίκησης, τα οποία είναι συστήματα που στηρίζουν τη λήψη αποφάσεων και τον έλεγχο από τη διεύθυνση των επιχειρήσεων.

Τα πληροφοριακά συστήματα δεν είναι απλώς οι ηλεκτρονικοί υπολογιστές. Συνήθως, το πληροφοριακό σύστημα περιλαμβάνει και την επιχείρηση ή σημαντικά μέρη της, όπως τους εργαζομένους που εισάγουν δεδομένα στο σύστημα και παίρνουν πίσω την εκροή του. Τα στελέχη επιχειρήσεων είναι (ή θα έπρεπε να είναι) μέρος του πληροφοριακού συστήματος, αφού το πληροφοριακό σύστημα είναι σχεδιασμένο για να υπηρετεί τις ειδικές ανάγκες τους για πληροφορίες *Βασιλακόπουλος Γ*, (2004).

2.3 ΔΙΑΚΡΙΣΕΙΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα πληροφοριακά συστήματα διακρίνονται στα εξής βασικά είδη *Δημητριάδης Α.,(*1996), :

Α) Συστήματα Επεξεργασίας Δοσοληψιών (Transaction Processing Systems – T.P.S)

Μια δοσοληψία είναι ένα συμβάν που επηρεάζει την επιχείρηση. Η πρόσληψη ενός εργαζομένου, η πώληση εμπορεύματος, η πληρωμή ενός εργαζομένου και η παραγγελία προμηθειών είναι δοσοληψίες. Στην ουσία, τα συστήματα επεξεργασίας δοσοληψιών συλλέγουν και διατηρούν λεπτομερειακά αρχεία για τις δοσοληψίες της επιχείρησης.

Στις επιχειρήσεις η συλλογή και η διατήρηση αρχείων για τις καθημερινές δοσοληψίες ήταν δύο από τις πρώτες διαδικασίες που άρχισαν να γίνονται μέσω ηλεκτρονικών υπολογιστών. Έτσι, με τα συστήματα επεξεργασίας δοσοληψιών αυτοματοποιήθηκαν οι διαδικασίες εκείνες που επαναλαμβάνονται. Ως παραδείγματα μπορεί να αναφερθούν η χρήση των Η/Υ για τους παρακρατούμενους φόρους (Φ.Π.Α., Ο.Γ.Α., κ.ά.), για την επεξεργασία επιταγών πληρωτέων λογαριασμών, κ.ά. Τα συστήματα επεξεργασίας δοσοληψιών μπορεί να έχουν πέντε χρήσεις. Έτσι αυτά χρησιμοποιούνται:

1. Για την ταξινόμηση δεδομένων που βασίζονται στα κοινά χαρακτηριστικά μιας ομάδας (όπως, π.χ., να βρουν τους εργαζομένους στο τμήμα πωλήσεων, με πενταετή υπηρεσία).

2. Για υπολογισμούς ρουτίνας (όπως το να περνούν στον Η/Υ τις καθαρές αμοιβές μετά από τους φόρους και τις κρατήσεις για κάθε εργαζόμενο).

3. Για την ταξινόμηση σε ομάδες (για παράδειγμα, συγκέντρωση τιμολογίων κατά ομάδες ανάλογα με τον ταχυδρομικό τομέα, ώστε να γίνεται πιο αποδοτικά η διανομή τους).

4. Για συνοπτικούς λογαριασμούς (για παράδειγμα, συνοπτικό λογαριασμό για κάθε προϊστάμενο τμήματος, που δείχνει τις μέσες

μισθολογικές δαπάνες του τμήματός του σε σύγκριση με τα άλλα τμήματα).

5. Τέλος, τα συστήματα επεξεργασίας δοσοληψιών μπορεί να χρησιμοποιηθούν για αποθήκευση (για παράδειγμα, αποθήκευση πληροφοριών για τις μισθολογικές καταστάσεις τα τελευταία πέντε χρόνια).

Β. Πληροφοριακά Συστήματα Διοίκησης (Management Information Systems - M.I.S.):

Ένα πληροφοριακό σύστημα διοίκησης στηρίζει τη λήψη αποφάσεων των στελεχών των επιχειρήσεων, παράγοντας πρότυπες, συνοπτικές εκθέσεις σε τακτική βάση. Τα συστήματα αυτά παράγουν εκθέσεις για μακροπρόθεσμους στόχους, σε σύγκριση με τα συστήματα επεξεργασίας δοσοληψιών που ασχολούνται με διαδικασίες ρουτίνας.

Γ. Συστήματα Υποστήριξης Αποφάσεων (Decision Support systems - D.S.S.):

Τα συστήματα υποστήριξης αποφάσεων βοηθούν τα στελέχη των επιχειρήσεων στη λήψη των αποφάσεων. Τα συστήματα αυτά συνδυάζουν δεδομένα, επεξεργασμένα αναλυτικά πρότυπα και ένα φιλικό για το χρήστη λογισμικό σε ένα ενιαίο ισχυρό σύστημα, που μπορεί να υποστηρίξει ημιδομημένα ή μη δομημένα προβλήματα. Με άλλα λόγια, αυτά τα συστήματα μπορεί να βοηθήσουν τα στελέχη επιχειρήσεων να πάρουν αποφάσεις για μη δομημένα προβλήματα. Ένα σύστημα υποστήριξης αποφάσεων (O.S.S.) διαφέρει από ένα πληροφοριακό σύστημα διοίκησης (M.I.S.) σε πολλά σημεία. Ένα σύστημα υποστήριξης αποφάσεων είναι πιο ικανό να αναλύει ποικίλες εναλλακτικές λύσεις, επειδή τα συστήματα υποστήριξης αποφάσεων επιτρέπουν στο χρήστη να περιλαμβάνει διάφορα υποπρογράμματα, τα οποία δείχνουν πώς σχετίζονται μεταξύ τους τα διάφορα συστατικά μέρη των

υποπρογραμμάτων αυτών.

Έτσι, τα συστήματα υποστήριξης αποφάσεων ασχολούνται με προβλήματα που δεν είναι προγραμματισμένα, τα οποία όμως χρειάζονται την κριτική παρέμβαση του στελέχους, ενώ τα πληροφοριακά συστήματα διοίκησης ασχολούνται βασικά με προβλήματα που είναι προγραμματισμένα και με αποφάσεις ρουτίνας. Επιπλέον, ένα σύστημα υποστήριξης αποφάσεων δεν στηρίζεται μόνο στις εσωτερικές πληροφορίες από το σύστημα επεξεργασίας δοσοληψιών, όπως στηρίζεται τυπικά το πληροφοριακό σύστημα διοίκησης. Αντίθετα, ένα σύστημα υποστήριξης αποφάσεων είναι έτσι δομημένο ώστε να απορροφά στην ανάλυση νέες εξωτερικές πληροφορίες.

Δ. Συστήματα Υποστήριξης της Εκτελεστικής Εξουσίας (Executive Support systems - E.S.S.):

Τα συστήματα υποστήριξης της εκτελεστικής εξουσίας είναι πληροφοριακά συστήματα σχεδιασμένα για να βοηθούν την εκτελεστική εξουσία ανώτερου επιπέδου να αποκτά, να χειρίζεται και να χρησιμοποιεί τις πληροφορίες που χρειάζεται, προκειμένου να διατηρεί τη συνολική αποτελεσματικότητα της επιχείρησης. Αυτά τα συστήματα εστιάζονται συχνά στο να παρέχουν στην ανώτερη διεύθυνση πληροφορίες για τη λήψη στρατηγικών αποφάσεων. Βοηθούν την ανώτερη διεύθυνση να αντιμετωπίζει τις αλλαγές του περιβάλλοντος, λαμβάνοντας υπόψη της τα δυνατά και τα αδύνατα σημεία της επιχείρησης.

Οι εκτελεστικοί μάνατζερ χρησιμοποιούν, επίσης, τα συστήματα υποστήριξης της εκτελεστικής εξουσίας για να ανιχνεύσουν το περιβάλλον της επιχείρησης. Για παράδειγμα, πολλές πληροφορίες είναι διαθέσιμες σε ηλεκτρονικές τράπεζες δεδομένων, στις οποίες περιλαμβάνονται πληροφορίες για πολλές επιχειρήσεις της χώρας μας. Οι εκτελεστικοί μάνατζερ μπορούν να χρησιμοποιούν ένα τέτοιο σύστημα υποστήριξης της εκτελεστικής εξουσίας για να μπαίνουν σε αυτές τις τράπεζες δεδομένων, ώστε να σταχυολογούν δεδομένα σχετικά με την

ανταγωνιστικότητα των άλλων επιχειρήσεων του κλάδου τους.

Τέλος, ένα σύστημα υποστήριξης της εκτελεστικής εξουσίας επιτρέπει στους εκτελεστικούς μάνατζερ να έχουν άμεση πρόσβαση στα δεδομένα. Χρησιμοποιώντας τα τερματικά τους και τις τηλεφωνικές γραμμές τους, οι εκτελεστικοί μάνατζερ μπορούν να χρησιμοποιήσουν ένα σύστημα υποστήριξης της εκτελεστικής εξουσίας για να μπαίνουν άμεσα στα αρχεία δεδομένων της εταιρείας, ώστε να παίρνουν ειδικές πληροφορίες για τις οποίες μπορεί να ενδιαφέρονται, χωρίς να περιμένουν να τους τις συγκεντρώσουν άλλοι.

Ε. Έμπειρα Συστήματα (Expert Systems - E.S):

Ένα έμπειρο σύστημα είναι ένα πληροφοριακό σύστημα, στο οποίο τα προγράμματα ηλεκτρονικού υπολογιστή αποθηκεύουν γεγονότα και κανόνες (αποκαλούνται συχνά βάση γνώσεων), ώστε να αντιγράφουν τις ικανότητες και τις αποφάσεις ανθρώπων που είναι έμπειροι.

Για παράδειγμα, μια πρώιμη εφαρμογή εντόπιζε τα κριτήρια ενός συμβούλου επενδύσεων με βάση τα οποία σύστηνε επενδύσεις σε πελάτες που ήταν σε διάφορες δημογραφικές κατηγορίες και σε ποικίλες κατηγορίες ως προς την τάση ανάληψης κινδύνων.

Κατόπιν αυτές οι παρατηρήσεις χρησιμοποιούνταν για να αναπτυχθεί ένα πρόγραμμα ηλεκτρονικού υπολογιστή, το οποίο αναπαρήγαγε τις περισσότερες από τις αποφάσεις επενδύσεων τις οποίες θα είχε κάνει ο (έμπειρος) σύμβουλος επενδύσεων.

Τα έμπειρα συστήματα χρησιμοποιούνται σε όλους τους τομείς επιχειρήσεων, από την παραγωγή μέχρι το μάρκετινγκ και το χρηματοοικονομικό τομέα . Ωστόσο όλο και περισσότερο ,μια από τις πιο προσβεβλημένες χρήσεις, είναι στο χρηματοοικονομικό τομέα και στις επενδύσεις *Δημητριάδης Α.,(*1996)

2.4 ΕΝΝΟΙΟΛΟΓΙΚΕΣ ΑΠΟΣΑΦΗΝΙΣΕΙΣ ΤΟΥ RISK MANAGEMENT

Ο κίνδυνος σημαίνει «το αρνητικό ενδεχόμενο, η πιθανότητα να συμβεί ένα γεγονός που θα μπορούσε να έχει έναν ανεπιθύμητο ή αρνητικό αντίκτυπο, οτιδήποτε (πράξη, κατάσταση, συμπεριφορά κτλ.) μπορεί να προκαλέσει καταστροφή, να επιφέρει απώλειες και φθορές ή μπορεί να φέρει σε επικίνδυνη θέση κάποιον / κάτι. Ο κίνδυνος χαρακτηρίζεται από την πιθανότητα να συμβεί το γεγονός και το αποτέλεσμα (τις επιπτώσεις), εάν και εφόσον συμβεί» *Κάτσικας, Σ.Κ.*(2010),.

Επιπλέον, οι κίνδυνοι – ή σωστότερα οι παράγοντες κινδύνου – και οι ευκαιρίες μπορούν μερικές φορές να αντιμετωπιστούν ξεχωριστά, αλλά σπανίως είναι ανεξάρτητοι (όπως οι δύο όψεις ενός νομίσματος, οι οποίες μπορούν να εξεταστούν μία κάθε φορά, αλλά δεν είναι ανεξάρτητες όταν ρίχνουμε το νόμισμα). Με βάση αυτόν τον αναθεωρημένο ορισμό, τελικά, ο κίνδυνος μπορεί να διαχωριστεί σε «ανεπιθύμητο ρίσκο» (down-side risk), το οποίο αναφέρεται στην εμφάνιση σημαντικών απειλών ή ανεπιθύμητων συνεπειών, και σε «επιθυμητό ρίσκο» (up-side risk), το οποίο αναφέρεται στην εμφάνιση σημαντικών ευκαιριών ή επιθυμητών συνεπειών.

Με βάση τα παραπάνω, στη παρούσα μελέτη, αν και γίνεται εκτενής αναφορά στο «ανεπιθύμητο ρίσκο», παράλληλα γίνεται προσπάθεια ενσωμάτωσης της διττής σημασίας του όρου ‘κίνδυνος’, όπως ξεκαθαρίστηκε εδώ, δηλαδή, τόσο του «ανεπιθύμητου ρίσκου», όσο και του «επιθυμητού ρίσκου» *Meritt, J.W.*(2010),.

Η Ανάλυση Κινδύνου είναι η διαδικασία του προσδιορισμού και της αποτίμησης του κινδύνου. Σε αυτήν περιλαμβάνεται η κατανόηση της σχετικής σπουδαιότητας των διαφορετικών πηγών κινδύνου και η εκτενής εξέταση των αλληλεπιδράσεων μεταξύ των δραστηριοτήτων του έργου, αλλά και των παραγόντων κινδύνου *Fairley, R.*(1994),.

Οι Παράγοντες Κινδύνου είναι οι παράγοντες εκείνοι που είναι πιθανόν να προκαλέσουν την πιθανότητα εκδήλωσης κάποιων

επικίνδυνων συνεπειών, καθώς η πιθανότητα αυτή εξαρτάται από την ύπαρξη αυτών των παραγόντων (π.χ. πολυπλοκότητα, ταχύτητα, καινοτομία, απαιτήσεις τεχνολογίας, απαιτήσεις προσπάθειας).

Η Έκθεση σε κίνδυνο είναι ένα μέτρο που προσδιορίζει σε ποιο βαθμό ένα έργο ή πρόγραμμα είναι τρωτό σε αρνητικές επιπτώσεις όταν εκτίθεται σε ένα συγκεκριμένο παράγοντα κινδύνου. Ουσιαστικά, η έκθεση σε κίνδυνο προσδιορίζεται με βάση τη σοβαρότητα του κάθε παράγοντα κινδύνου που εμφανίζεται στο έργο ή πρόγραμμα *Meritt, J.W.*(2010),.

2.5 ΜΕΘΟΔΟΛΟΓΙΑ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ

Η μεθοδολογία ανάλυση του κινδύνου εμπεριέχει τρία βασικά στάδια: την αναγνώριση του κινδύνου, την εκτίμηση του και τέλος την αποτίμηση του κινδύνου. Πιο αναλυτικά Baker, K and Baker S.(2000):

2.5.1 ΑΝΑΓΝΩΡΙΣΗ ΚΙΝΔΥΝΟΥ

Η αναγνώριση κινδύνου, αφορά στην ετοιμασία ενός καταλόγου με όλους τους πιθανούς παράγοντες κινδύνου που θα μπορούσε να αντιμετωπίσει ένα πρόγραμμα. Η Αναγνώριση Κινδύνου είναι η διαδικασία προσδιορισμού των επικίνδυνων γεγονότων, των συνθηκών κάτω από τις οποίες ενδεχομένως παράγονται οι δυσμενείς επιδράσεις και της φύσης αυτών.

Ο προσδιορισμός των παραγόντων κινδύνου για μια σειρά από παρόμοια προγράμματα είναι μία επαναληπτική διαδικασία και για αυτόν τον λόγο η εμπειρία και τα ιστορικά αρχεία αποτελούν σημαντικές πηγές πληροφόρησης. Επιπλέον, επειδή είναι το αρχικό και ίσως το πιο βασικό στάδιο της όλης διαδικασίας, υπάρχει μια πληθώρα μεθόδων και εργαλείων για την όσο το δυνατόν πληρέστερη και μεθοδική καταγραφή των επιμέρους παραγόντων κινδύνου *Baker, K and Baker S.*(2000),.

Τα εργαλεία που χρησιμοποιούνται στην αναγνώριση των κινδύνων είναι: τα ερωτηματολόγια, τα οποία περιλαμβάνουν μία πρότυπη λίστα ερωτήσεων για την αρχική καταγραφή ενός αριθμού παραγόντων κινδύνου και χρησιμοποιούνται για την συγκέντρωση ιδεών σχετικά με τους σημαντικότερους παράγοντες κινδύνου που αφορούν το πρόγραμμα. Τα αποτελέσματα αξιολογούνται και καταγράφονται στο Μητρώο Παραγόντων Κινδύνου *Elky, S.*(2006).

Η λίστα Ελέγχου είναι μια λίστα όλων των πιθανών περιοχών, όπου ενδέχεται να παρουσιαστούν προβλήματα. Αποτελεί ένα από τα πιο ευρέως χρησιμοποιούμενα μέσα προσδιορισμού των παραγόντων κινδύνου. Απαραίτητη προϋπόθεση για την κατάρτισή της για κάθε οργανισμό είναι η ύπαρξη πλούσιου ιστορικού όσον αφορά στην Διαχείριση Κινδύνου.

Οι συνεντεύξεις. Το πρόσωπο που διεξάγει τις ερωτήσεις θα πρέπει κατά προτίμηση να είναι εκτός της Υπηρεσίας, ώστε να εξασφαλίζεται η ουδετερότητα. Οι συνεντευξιαζόμενοι θα πρέπει κατά προτίμηση να είναι άτομα από όλα τα επίπεδα της Υπηρεσίας. Οι ερωτήσεις είναι επιθυμητό να είναι προκαθορισμένες και να συζητηθούν λεπτομερώς με τους συνεντευξιαζόμενους.

Τέλος οι συσκέψεις για την ανταλλαγή και την ανάπτυξη ιδεών (Brainstorming), αφορούν μία τεχνική διασκέψεων, από την οποία μία ομάδα ατόμων προσπαθεί να αναπτύξει και να καταγράψει αυθόρμητα όσο το δυνατόν περισσότερες ιδέες σε μια συγκεκριμένη περιοχή ενδιαφέροντος. Στο πρώτο στάδιο της διαδικασίας δεν επιτρέπεται καμία συζήτηση, αξιολόγηση ή κριτική των ιδεών, οι οποίες σκόπιμα αναπτύσσονται γρήγορα και αφορούν ευρύ πεδίο θεμάτων.

Στόχος της απουσίας της ανάλυσης και της κρίσης σε αυτήν την φάση είναι η ενθάρρυνση της δημιουργικότητας των εμπλεκομένων. Οι ιδέες μπορούν να αξιολογηθούν συμβατικά σε επόμενο στάδιο των συσκέψεων. Βασικός σκοπός είναι να αναπτυχθεί ένας περιεκτικός κατάλογος επικίνδυνων ενδεχομένων. Μπορεί να είναι χρήσιμες στην

περίπτωση προγραμμάτων που περιλαμβάνουν νέους / σπάνιους παράγοντες κινδύνου ή καινοτόμες διοικητικές ρυθμίσεις ή για την ανάπτυξη των πινάκων ελέγχου *Elky, S.*(2006).

Άλλα εργαλεία είναι το μητρώο Παραγόντων Κινδύνου (Risk Register/ Risk Log), το οποίο αναφέρεται σε ένα συγκεκριμένο πίνακα, όπου καταγράφονται όλοι οι παράγοντες κινδύνου που έχουν προσδιοριστεί. Επιπρόσθετα, γίνεται καταγραφή στοιχείων σχετικά με την εκτίμηση και την αξιολόγηση των επιμέρους παραγόντων κινδύνου. Η χρήση του διευκολύνεται με την ανάπτυξη μίας εφαρμογής υπολογιστών για την ταχύτερη και πληρέστερη εισαγωγή των στοιχείων στα πεδία και την δημιουργία μίας συνοπτικής κατανομής παραγόντων κινδύνου (Summary Risk Profile, SRP).

Η ανάλυση Δυνατών και Αδύνατων Σημείων, Ευκαιριών και Παραγόντων Κινδύνου (SWOT), η οποία αποτελεί ένα μοντελοποιημένο τρόπο καταγραφής των κυριοτέρων συμπερασμάτων που προκύπτουν από την ανάλυση και την καταγραφή του εσωτερικού και εξωτερικού περιβάλλοντος του εξεταζόμενου οργανισμού.

Απώτερος στόχος της είναι η συμβολή στον καθορισμό των στρατηγικών κατευθύνσεων του οργανισμού. Συνίσταται από τις εξής τέσσερις εξίσου σημαντικές παραμέτρους: Δυνατά Σημεία, Αδύνατα Σημεία, Ευκαιρίες και Απειλές. Οι δύο πρώτες παράμετροι, Δυνατά και Αδύνατα Σημεία, καθορίζονται από την ανάλυση του εσωτερικού περιβάλλοντος και αφορούν αποκλειστικά στον προσδιορισμό των πλεονεκτημάτων ή μειονεκτημάτων που πηγάζουν από την υφιστάμενη δομή και λειτουργική ευρωστία του οργανισμού.

Αντίθετα, οι δύο τελευταίες παράμετροι, Ευκαιρίες και Απειλές, αφορούν στην αξιολόγηση των εξωτερικών παραγόντων, οι οποίοι συνιστούν το εξωτερικό περιβάλλον στο οποίο δραστηριοποιείται ο οργανισμός *Yazar,Z.*(2002). Οι πρώτες μεταβλητές του μοντέλου καθορίζονται και επηρεάζονται από το εσωτερικό περιβάλλον του οργανισμού από την άλλη οι μεταβλητές ευκαιρίες και απειλές

καθορίζονται και επηρεάζονται από το εξωτερικό περιβάλλον.

Ο χάρτης αντίληψης παραγόντων κινδύνου, είναι μια γραφική παρουσίαση των πιθανών κινδύνων, η οποία συνδέει τα αίτια με τα επικίνδυνα γεγονότα. Τέλος βαθμολογεί και αξιολογεί τους παραγοντικούς κινδύνους με βάση τη σοβαρότητα την οποία έχουν για το όποιο πληροφοριακό σύστημα είναι υπό ανάλυση και μελέτη.

Το διάγραμμα αιτίας στοχεύει στη γραφική απεικόνιση της σχέσης μεταξύ αιτιών και επιδράσεων. Δεν χρησιμοποιεί μέσα τα οποία ποσοτικοποιούν τη σχέση αιτίας και επιδράσεων.

Για τη καλύτερη διαχείριση του κινδύνου στα πληροφοριακά συστήματα με βάση την ανάπτυξη των παραδοχών, καλό είναι ένας οργανισμός να αναπτύσσει σενάρια τα οποία να βοηθούν στην πρόβλεψη και πρόληψη έναντι των κινδύνων. Η μελέτη αυτή μπορεί να βοηθήσει στην αποφυγή ανακριβειών, ασυνεπειών αλλά και ατελειών. Η διαδικασία ταξινόμησης των κινδύνων μπορεί να εφαρμοστεί με βάση τις ακόλουθες δράσεις:

1. Αρχικά θα πρέπει να οριστεί η αιτία ανάπτυξης του κινδύνου.
2. Τη συσχέτιση των εσωτερικών με τους εξωτερικούς παραγόντων.
3. Στάδιο υλοποίησης του προγράμματος και η επίπτωση των κινδύνων.
4. Η μελέτη των κινδύνων και η σύγκριση τους.
5. Το μέγεθος των επιπτώσεων ή της σοβαρότητας.
6. Το επίπεδο που μπορούν να ελεγχθούν και να αντιμετωπιστούν.

Τέλος σημαντικό είναι να ληφθούν υπόψη οι ακόλουθοι παράμετροι: Χρόνος, Κόστος, Επίτευξη / εκτέλεση / ποιότητα, Υγιεινή και ασφάλεια, Περιβάλλον, Πολιτική *Yazar, Z.*(2002)

2.5.2 ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΟΥ

Η εκτίμηση κινδύνου αφορά στον προσδιορισμό της έκθεσης σε κάθε παράγοντα κινδύνου, βασισμένος στην εκτίμηση της πιθανότητας να συμβεί και της πιθανής επίπτωσής του, ή του βάρους του σε σχέση με τους υπολοίπους και της σοβαρότητάς του. Η Εκτίμηση Κινδύνου πραγματοποιείται γενικά με τη χρήση δύο μεθόδων. Η μία μέθοδος, συνίσταται στη διαδικασία εκτίμησης του βάρους των παραγόντων κινδύνου σε σχέση με τους υπολοίπους και της σοβαρότητας τους σε περίπτωση που εμφανιστούν.

Η άλλη μέθοδος, συνίσταται στη διαδικασία εκτίμησης της πιθανότητας εμφάνισης των επικίνδυνων γεγονότων και της δριμύτητας των επιδράσεών τους. Αυτό οδηγεί σε μια εκτίμηση του βαθμού έκθεσης του προγράμματος σε κίνδυνο *Elky, S.*(2006) (Βλέπε Πίνακα 2).

Πιθανότητα εμφάνισης παράγοντα κινδύνου	• Εκτίμηση της πιθανότητας κάθε παράγοντα κινδύνου να συμβεί (ποιοτικά ή ποσοτικά).
Επίπτωση παράγοντα κινδύνου	• Εκτίμηση του μεγέθους της κάθε επίπτωσης (ποιοτικά ή ποσοτικά).
Έκθεση στον κίνδυνο	• Εκτίμηση της συνολικής έκθεσης σε κίνδυνο (ποιοτικά ή ποσοτικά). • Ταξινόμηση των παραγόντων κινδύνου ανάλογα με το βαθμό έκθεσης.
Τεκμηρίωση παραγόντων κινδύνου	• Καταγραφή των πιθανοτήτων εμφάνισης, επιπτώσεων και έκθεσης στον κίνδυνο.

Πίνακας 2 - Εκτίμηση Κινδύνου με τη μέθοδο Πιθανότητας-Επίπτωσης

Η πιθανότητα εμφάνισης ενός παράγοντα κινδύνου (probability), αναφέρεται στο ενδεχόμενο ένας συγκεκριμένος παράγοντας να εμφανιστεί πραγματικά κατά τη διάρκεια του προγράμματος. Σε λίγες σχετικά περιπτώσεις είναι δυνατό να υπολογιστεί αριθμητικά η πιθανότητα εμφάνισης ενός παράγοντα κινδύνου. Τις περισσότερες φορές,

όμως, υπολογίζεται και εκφράζεται ποιοτικά σύμφωνα με την εμπειρία ή τη διαίσθηση.

Οι επιπτώσεις (impacts) μπορούν επίσης, σε μερικές περιπτώσεις, να υπολογιστούν χρησιμοποιώντας τις ποσοτικές τεχνικές. Όμως, συχνά και αυτές προκύπτουν από υποκειμενική ποιοτική εκτίμηση βασισμένη στη γνώση τόσο της κατηγορίας του παράγοντα κινδύνου όσο και των λεπτομερειών του ίδιου του προγράμματος *Baker, K and Baker S.*(2000).

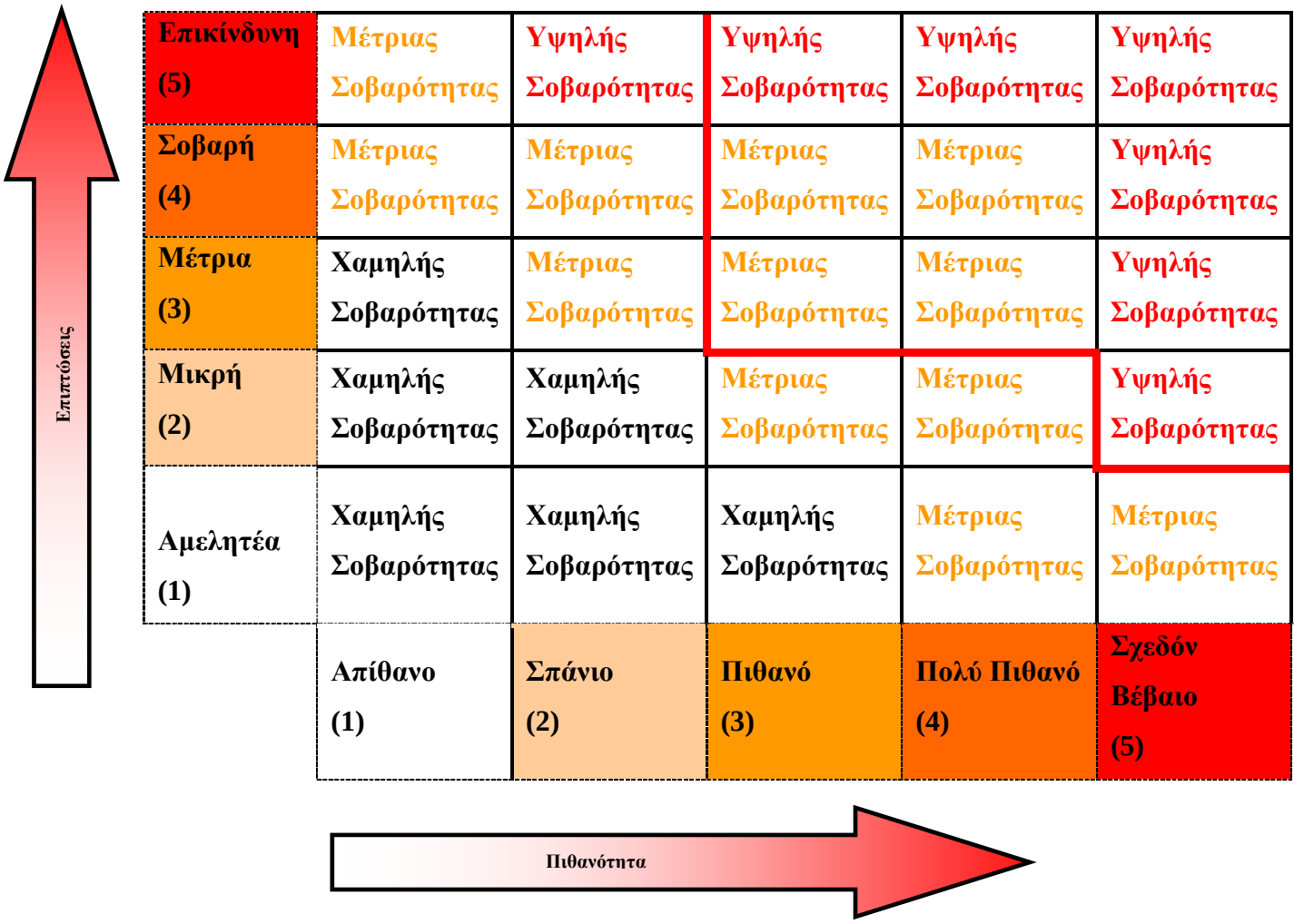
Η έκθεση σε κίνδυνο ορίστηκε με βάση τον συνδυασμό της πιθανότητας ενός ενδεχομένου να συμβεί και των επιπτώσεων που θα έχει σε περίπτωση που συμβεί. Εάν οι πιθανότητες και οι επιπτώσεις του παράγοντα κινδύνου έχουν ποσοτικοποιηθεί, η έκθεση σε κίνδυνο, η οποία μετράτε με τη σοβαρότητα (severity) του εκάστοτε παράγοντα κινδύνου, μπορεί να υπολογιστεί ως το γινόμενο της πιθανότητας και των επιπτώσεων (Βλέπε Πίνακα 3).

	Απεικόνιση		**Ορισμός**
5	Σχεδόν Βέβαιο	>80%	Αναμένεται να συμβεί στις περισσότερες περιπτώσεις.
4	Πολύ Πιθανό	51-80%	Ενδεχομένως να συμβεί στις περισσότερες περιπτώσεις.
3	Πιθανό	21-50%	Πιθανώς να συμβεί κάποια στιγμή.
2	Σπάνιο	6-20%	Μπορεί να συμβεί σε μερικές περιπτώσεις.
1	Απίθανο	0-5%	Μπορεί να συμβεί μόνο σε εξαιρετικές περιπτώσεις.

Πίνακας 3-Εκτίμηση Πιθανότητας

	Απεικόνιση	**Ορισμός**
5	Επικίνδυνη	Εάν συμβεί θα προκαλέσει αποτυχία του προγράμματος.
4	Σοβαρή	Εάν συμβεί θα προκαλέσει σημαντικές επιπτώσεις.
3	Μέτρια	Εάν συμβεί θα προκαλέσει σοβαρές επιπτώσεις, αλλά οι σημαντικοί στόχοι θα επιτευχθούν.
2	Μικρή	Εάν συμβεί θα προκαλέσει κάποιες επιπτώσεις, αλλά σχεδόν όλοι οι στόχοι θα επιτευχθούν.
1	Αμελητέα	Εάν συμβεί δεν θα προκαλέσει επιπτώσεις στο πρόγραμμα.

Πίνακας 4 - Εκτίμηση επιπτώσεων



Σχήμα 1 - Μήτρα Πιθανότητας / Επιπτώσεων

Εάν ο προσδιορισμός του μεγέθους των πιθανοτήτων και των επιδράσεων δεν είναι δυνατός, τότε τα δύο μεγέθη μπορούν μόνο να συνδυαστούν για να δείξουν την έκθεση σε κίνδυνο χρησιμοποιώντας μια μέθοδο ισοδυναμίας. Οι διαφορετικοί παράγοντες κινδύνου που προσδιορίζονται μπορούν να ταξινομηθούν από την άποψη της πιθανότητας εμφάνισής τους και του μεγέθους των επιπτώσεών τους εάν εμφανιστούν χρησιμοποιώντας μια μήτρα Πιθανότητας / Επιπτώσεων. *Elky, S.*(2006)

Από αυτόν τον συνδυασμό της πιθανότητας και των επιπτώσεων ενός παράγοντα κινδύνου προκύπτει η σοβαρότητα (severity) του

εκάστοτε παράγοντα. Τέλος, η συνολική έκθεση σε κίνδυνο μπορεί να προσδιοριστεί σαν το πηλίκο του αθροίσματος της σοβαρότητας όλων των παραγόντων κινδύνου δια του πλήθους τους *Teeples, J.*(2009).

Οι τεχνικές και τα εργαλεία που χρησιμοποιούνται στο βήμα αυτό είναι οι υπολογισμοί της αναμενόμενης αξίας (expected value calculations). Εάν η πιθανότητα του να συμβεί ένα γεγονός είναι pB_{1B}, pB_{2B}, …, pB_{nB}, και μία αντίστοιχη επίπτωση κόστους εκφράζεται ως cB_{1B}, cB_{2B}, …, cB_{nB}, τότε η συνολική αναμενόμενη αξία του κινδύνου είναι το άθροισμα των επιμέρους γινομένων. Δηλαδή, ο συνολικός αναμενόμενος κίνδυνος ισούται με $pB_{1B}cB_{1B}+pB_{2B}cB_{2B}+….+pB_{nB}cB_{nB}$.

Τα δένδρα πιθανοτήτων, τα οποία είναι γραφικές αναπαραστάσεις του συνόλου των πιθανών στρατηγικών και μπορούν να είναι χρήσιμα για προγράμματα που απαιτούν διαδοχικές αποφάσεις. Οι διαφορετικές στρατηγικές οδηγούν σε διαφορετικά αποτελέσματα, ανάλογα με τις συνθήκες και τα γεγονότα που λαμβάνουν χώρα. Τέλος ο συνδυασμός κατανομών (Combination of Distributions), όπου

Σε μερικές περιπτώσεις είναι χρησιμότερο να παρουσιάζονται οι πιθανότητες των επιπτώσεων με τη μορφή στατιστικής κατανομής. Έτσι, αντί η πιθανότητα κινδύνου να έχει μία τιμή μονοσήμαντη, παρουσιάζεται με τη μορφή μιας κατανομής. Αυτό είναι ιδιαίτερα χρήσιμο για τις αβεβαιότητες που έχουν να κάνουν με το κόστος και τα χρονοδιαγράμματα *Elky, S.*(2006).

Η διαδικασία εκτίμησης του ποσοτικού κινδύνου γίνεται με τη βοήθεια των ακόλουθων εργαλείων:

1. **Υπολογισμοί αναμενόμενης αξίας:** Η πιθανότητα να συμβεί ένα γεγονός είναι p και μια αντίστοιχη επίπτωση κόστους είναι ψ, τότε η συνολική αξία του κινδύνου είναι το άθροισμα των γινομένων που δημιουργούνται.
2. **Δένδρα πιθανοτήτων:** Τα δένδρα πιθανοτήτων είναι σημαίνουσας σημασίας αναπαραστάσεις που βασίζονται σε γραφήματα και βοηθούν στην ανάπτυξη διαδοχικών αποφάσεων. Οι διαφορετικές εκδοχές

οδηγούν σε άλλα αποτελέσματα ανάλογα με το εσωτερικό και εξωτερικό περιβάλλον.

3. **Συνδυασμός κατανομών:** Είναι χρήσιμο να αναπτύσσονται οι πιθανές επιπτώσεις του κινδύνου μέσα από στατιστικά στοιχεία . Αυτό σημαίνει ότι αντί η πιθανότητα κινδύνου να έχει μια μονοσήμαντη τιμή εμφανίζεται με τη μορφή κατανομής.
4. **Ανάλυση ευαισθησίας:** Βοηθά στην εκτίμηση του κινδύνου μέσα από την ανάπτυξη διαφορετικών σεναρίων αλλά και τη χρήση πιθανοτήτων σε σχέση με την ανάπτυξη ενός κινδύνου. *Elky, S.*(2006)

2.5.3 ΑΠΟΤΙΜΗΣΗ ΚΙΝΔΥΝΟΥ

Τέλος η αποτίμηση του κινδύνου αφορά στην εκτίμηση της αποδοχής κάθε παράγοντα κινδύνου, με σκοπό να αποφασιστεί τι ενέργειες πρέπει να γίνουν. Η Αποτίμηση Κινδύνου είναι ένας ζωτικής σημασίας προαπαιτούμενο βήμα για τη Διαχείριση Κινδύνου. Χωρίς αυτή, η αποτελεσματική διαχείριση δεν μπορεί να πραγματοποιηθεί, δεδομένου ότι οι υπεύθυνοι δεν θα έχουν γνώση και άποψη για τους σημαντικότερους παράγοντες κινδύνου που θα οδηγήσουν το πρόγραμμα σε αστοχίες.

Υπάρχει επομένως ο γενικότερος κίνδυνος να διαχειριστούν πρώτα τα προβλήματα με τα οποία αισθάνονται πιο οικείοι, ή με τα οποία έχουν προγενέστερη εμπειρία και να καθυστερήσουν ή να μην προσπαθήσουν να ελέγξουν άλλες σημαντικές δραστηριότητες. Όποια κι αν είναι η περίπτωση, η επιτυχής επίτευξη των στόχων του προγράμματος γίνεται πολύ λιγότερο πιθανή *Baker, K and Baker S.(*2000).

Εάν η ανάλυση κινδύνου έχει εκτελεσθεί σε ποσοτική βάση, κατόπιν είναι σχετικά εύκολο να συγκριθούν τα αριθμητικά επίπεδα έκθεσης με τα αποδεκτά όρια που εκφράζονται στις ίδιες μονάδες.

Το όριο ανοχής κινδύνου (γραμμή ανοχής), είναι η μέγιστη πιθανή έκθεση σε κίνδυνο, που μπορεί να γίνει αποδεκτή, με βάση τις πιθανές συνέπειες αλλά και τα εμπλεκόμενα οφέλη που σχετίζονται με τις αιτίες

των επικίνδυνων ενδεχομένων. Το όριο ανοχής αφορά κάθε επιμέρους παράγοντα κινδύνου, αλλά και τη συνολική έκθεση σε κίνδυνο.

Για να προσδιοριστεί το όριο ανοχής για κάθε πρόγραμμα, θα πρέπει να εξεταστεί ιδιαίτερα προσεκτικά για κάθε σημαντικό παράγοντα κινδύνου ο οποίος ενδέχεται να βρίσκεται έξω από το όριο ανοχής και άρα να αποτελεί αιτία διακοπής του προγράμματος, το βάρος του και η σοβαρότητά του ή η πιθανότητα εμφάνισής του και οι επιπτώσεις από ενδεχόμενη εμφάνισή του, ανάλογα με ποια μέθοδο εκτίμησης χρησιμοποιούμε, οι εναλλακτικές δυνατότητες αντίδρασης για την αντιμετώπισή του, καθώς και το μέγεθος των επιπτώσεων που διακινδυνεύετε να προκύψουν από τις αντιδράσεις αυτές. Η ανοχή απέναντι σε έναν παράγοντα κινδύνου μπορεί να ποικίλει ανάλογα με την σοβαρότητα του, αλλά και τον χρόνο, όπως και την περιοχή, που ενδέχεται να προκύψει *Elky, S.*(2006).

2.6 ΜΕΘΟΔΟΛΟΓΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΟΥ

Η Διαχείριση Κινδύνου είναι ο προγραμματισμός και η εφαρμογή ενεργειών για να μειωθεί η σοβαρότητα των παραγόντων κινδύνου που έχουν προσδιοριστεί κατά τη διάρκεια της Ανάλυσης Κινδύνου. Η Διαχείριση Κινδύνου αποτελείται από τέσσερις κύριες δραστηριότητες.

Τον προγραμματισμός (planning), δηλαδή την ανάπτυξη των κατάλληλων ενεργειών για κάθε παράγοντα κινδύνου και προετοιμασία ενός σχεδίου διαχείρισης κινδύνου. Τη διαχείριση πόρων (resourcing) , την κατανομή δηλαδή των πόρων και των ευθυνών για την υλοποίηση του σχεδίου. Τον έλεγχο (controlling) της ορθότητας των σχεδιαζόμενων ενεργειών και της κατανομής πόρων του σχεδίου. Τέλος την παρακολούθηση (monitoring) της αποτελεσματικότητας της εφαρμογής του σχεδίου *Teeples, J.*(2009).

Στόχος της Διαδικασίας Διαχείρισης Κινδύνου αποτελεί η χρησιμοποίηση των συμπερασμάτων των προηγούμενων σταδίων της

Ανάλυσης Κινδύνου για την παραγωγή ενός Βασικού Σχεδίου Δράσης. Εκτός του Βασικού Σχεδίου, παράγωγα της Διαδικασίας Διαχείρισης Κινδύνου αποτελούν και τα Εναλλακτικά Σχέδια Έκτακτης Ανάγκης (Ε.Σ.Ε.Α.).

Τα σχέδια αυτά θα πρέπει να περιλαμβάνουν τις ενέργειες αντιμετώπισης ενός σημαντικού παράγοντα κινδύνου, μετά την εκδήλωσή του. Οι ενέργειες αυτές, όπως ακριβώς και οι Δράσεις του Βασικού Σχεδίου, θα πρέπει να περιγράφονται όσο πιο αναλυτικά είναι εφικτό, σε όρους κόστους, χρονοδιαγράμματος και πόρων. Η κύρια διαφοροποίηση των Ε.Σ.Ε.Α. από το Βασικό Σχέδιο είναι ότι περιέχουν όλες τις «κατασταλτικές» ενέργειες, μετά την εκδήλωση του παράγοντα κινδύνου, ενώ το Βασικό Σχέδιο ενσωματώνει όλες τις προληπτικές ενέργειες Διαχείρισης Κινδύνου.

2.7 ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΟΥ

Το επίπεδο του Προγραμματισμού (planning stage) στη Διαχείριση Κινδύνου παρουσιάζει ομοιότητες με το επίπεδο της Αποτίμησης (risk evaluation stage) στην ανάλυση κινδύνου και στην πραγματικότητα μπορεί να πραγματοποιηθεί παράλληλα με αυτό. *Baker, K and Baker S.*(2000)

Εντούτοις, ενώ στην ανάλυση κινδύνου το κύριο μέλημα είναι να προσδιορισθούν τα μέσα και οι τρόποι για να μειωθεί ο κίνδυνος του προγράμματος, στη Διαχείριση του Κινδύνου έμφαση δίνεται στην ανάπτυξη αυτών των ενεργειών, μέσα από μία πιο αναλυτική και λεπτομερή έρευνα της εφικτότητας των μεθόδων για να επιτευχθεί το προσδοκώμενο αποτέλεσμα, χωρίς να υπάρξουν ανεπιθύμητες επιπτώσεις. Στο τέλος αυτού του σταδίου ετοιμάζεται ένα Σχέδιο Διαχείρισης Κινδύνου σε πρωτόλεια μορφή *Gabel P.E.*(2010).

Οι δυνατότητες που παρέχονται στην Διαχείριση Κινδύνου ταξινομούνται σε τέσσερις μεγάλες κατηγορίες: την αποφυγή του κινδύνου, τη μεταφορά του, τη δράση, για τον έλεγχο / περιορισμό του κινδύνου και την αποδοχή του κινδύνου. Πιο αναλυτικά η αποφυγή κινδύνου, πρόκειται για τη χρησιμοποίηση εναλλακτικών προσεγγίσεων,

οι οποίες δεν περιέχουν καθόλου κίνδυνο. Αυτή η δυνατότητα, αν και είναι η πιο αποτελεσματική από τις τεχνικές Διαχείρισης Κινδύνου, δεν είναι πάντα διαθέσιμη, καθώς σε πάρα πολλές περιπτώσεις είναι πρακτικά αδύνατη η υιοθέτηση μιας στρατηγικής χωρίς καθόλου κίνδυνο. Τέλος, δεν θα πρέπει να παραβλέπεται το γεγονός ότι ο κίνδυνος εμπλέκεται σε πάρα πολλά έργα και προγράμματα, με την προοπτική του κέρδους, καθώς σχεδόν πάντοτε η πορεία προς την υλοποίηση σημαντικών στόχων δεν μπορεί να γίνει χωρίς κίνδυνο.

Η μεταφορά κινδύνου, αφορά στην μεταφορά του κινδύνου σε κάποιο άλλο εμπλεκόμενο μέρος. Πρακτικά, η υλοποίηση αυτής της τακτικής γίνεται με την μεταφορά του κινδύνου μέσα σε μια σύμβαση και άρα με την ανάληψη του κινδύνου από το έτερο συμβαλλόμενο μέρος.

Η δράση για τον έλεγχο / περιορισμό του κινδύνου, αφορά στην τακτική, στην οποία υπάγονται οι περισσότεροι παράγοντες κινδύνου. Σε αυτήν εντάσσονται όλες οι δράσεις που στοχεύουν στον περιορισμό, είτε της πιθανότητας εμφάνισης ενός παράγοντα κινδύνου, είτε των συνεπειών από την εμφάνιση ενός παράγοντα κινδύνου. Οι δράσεις περιορισμού του κινδύνου δεν είναι δυνατόν να εξειδικευθούν περαιτέρω σε αυτό το επίπεδο, καθώς εξαρτώνται από την φύση και το είδος του υπό εξέταση παράγοντα κάθε φορά.

Τέλος, η αποδοχή κινδύνου, αφορά στην αποδοχή του κινδύνου, με τον προγραμματισμό καμιάς απολύτως ενέργειας διαχείρισης του. Αυτό είναι δυνατό να συμβεί σε αρκετές περιπτώσεις, που αφορούν βεβαίως μη κρίσιμους για την επιτυχία του προγράμματος παράγοντες κινδύνου, στις οποίες, είτε η οποιαδήποτε προγραμματιζόμενη αντίδραση θα έχει μεγαλύτερο κόστος από τις συνέπειες της ενδεχόμενης εμφάνισης του παράγοντα κινδύνου, είτε ο κίνδυνος ελέγχεται εξ' ολοκλήρου από εξωτερικούς παράγοντες στους οποίους υπάρχει αδυναμία παρέμβασης.

Οι διαδικασίες Διαχείρισης Κινδύνου εφαρμόζονται σε όλες τις φάσεις του προγράμματος. Όσο πιο νωρίς όμως ενταχθούν στην διαδικασία διαχείρισης του προγράμματος, τόσο μεγαλύτερα θα είναι τα

οφέλη, καθώς είναι φανερό ότι άλλες δυνατότητες παρέχονται για αποτελεσματική Διαχείριση του Κινδύνου, όταν το πρόγραμμα είναι στην φάση της σύλληψης και του σχεδιασμού του και άλλες δυνατότητες παρέχονται όταν πια βρίσκεται στην διαδικασία εφαρμογής του. Χαρακτηριστικά αναφέρεται ότι η τακτική της «Αποφυγής του Κινδύνου» είναι ουσιαστικά ανέφικτη σε προχωρημένα στάδια της εφαρμογής του προγράμματος, στα οποία είναι εξαιρετικά δύσκολο να γίνουν αλλαγές στον σχεδιασμό, ώστε να αποφευχθεί κάποιος συγκεκριμένος παράγοντας κινδύνου *Meritt, J.W.*(2010).

ΚΕΦΑΛΑΙΟ 3^{Ο} Η ΣΗΜΑΣΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.1 ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ

Στο παρελθόν το πληροφοριακό σύστημα ενός οργανισμού βρισκόταν συγκεντρωμένο κεντρικά σε ένα σημείο λόγω τις χρήσης mainframe συστημάτων. Η ασφάλεια του ήταν πολύ πιο απλή και εύκολα εφαρμόσιμη. Σήμερα όμως το περιβάλλον των πληροφοριακών συστημάτων είναι πολύ διαφορετικό. Τα δεδομένα και οι πληροφορίες είναι διασκορπισμένες σε τοπικά δίκτυα και διαφορετικά συστήματα τμημάτων, που ήρθαν να αντικαταστήσουν την συγκεντρωμένη λογική των mainframe. Τα κατανεμημένα συστήματα και η εκτεταμένη δικτύωση δημιουργούν πολύ πιο πολύπλοκες συνθήκες διαχείρισης και ασφάλειας.

Για να μπορέσει να υπολογιστεί ικανοποιητικά η πιθανότητα να συμβεί ένα ανεπιθύμητο γεγονός και το μέγεθος του, πρέπει να υπάρχει μια γνώση των στοιχείων που απαρτίζουν τον κίνδυνο καθώς και των συσχετίσεων μεταξύ τους. Με καλή γνώση του κινδύνου μπορεί κάποιος να αποφασίσει ευκολότερα και σωστότερα για το αν θα αποδεχτεί τον κίνδυνο έτσι όπως έχει αποτιμηθεί ή αν θα προβεί σε ενέργειες που θα τον αποτρέψουν ή θα τον μειώσουν σε αποδεκτά επίπεδα. Αυτός με λίγα λόγια είναι ο σκοπός της ανάλυσης κινδύνων (risk analysis) *CISSP*.(2010) (Βλέπε Πίνακα 1- Στάδια Ανάλυση Κινδύνων).

Στάδια Ανάλυσης Κινδύνου

Αναγνώριση Κινδύνου Ετοιμασία μιας λίστας όλων των πιθανών παραγόντων κινδύνου που θα μπορούσε να αντιμετωπίσει ένα πρόγραμμα.
Εκτίμηση Κινδύνου Προσδιορισμός της έκθεσης σε κάθε παράγοντα κινδύνου, βασισμένος σε μια αξιολόγηση της πιθανότητας εμφάνισής του και του πιθανού αντίκτυπού του, ή του βάρους του σε σχέση με τους υπολοίπους και της σοβαρότητάς του.

Στάδια Διαχείρισης Κινδύνου

Αποτίμηση Κινδύνου Αξιολόγηση της αποδοχής κάθε παράγοντα κινδύνου, προκειμένου να αποφασιστεί ποιες ενέργειες θα ληφθούν.	**Προγραμματισμός** Ανάπτυξη των κατάλληλων ενεργειών για την αντιμετώπιση κάθε παράγοντα κινδύνου και προετοιμασία ενός πλάνου διαχείρισής του.
Διαχείριση πόρων Ανάθεση των πόρων και των ευθυνών.	
Έλεγχος Έλεγχος συμβατότητας του πλάνου Διαχείρισης Κινδύνου σε σχέση με τους διαθέσιμους πόρους και τις ισχύουσες διαδικασίες διαχείρισης του έργου / προγράμματος.	
Παρακολούθηση Παρακολούθηση της αποτελεσματικότητας της εφαρμογής του πλάνου Διαχείρισης Κινδύνου. Εξέταση της ανάγκης τυχόν αναθεώρησής του.	

3.1.1 Η ΕΝΝΟΙΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Αναφορικά με την ασφάλεια του ηλεκτρονικού εμπορίου υπάρχουν διάφορα επίπεδα με μεγάλο βαθμό δυσκολίας για το καθένα από αυτά και μόνο ένας ειδικός μπορεί να κρίνει την ασφάλεια του εκάστοτε συστήματος

Η ασφάλεια είναι σκόπιμο να περιέχει αποτίμηση της παραβίασης πράγμα που είναι σχετικά αληθές στις εμπορικές συνθήκες. Μεγάλη αδυναμία πολλές φορές εμφανίζεται στην κακή χρήση (όπως για παράδειγμα την αναγραφή του PIN της κάρτας τραπέζης στο πίσω μέρος της).

Ο πιο ισχυρός αλγόριθμος δεν ωφελεί εαν το κλειδί προσημειώνεται στο τερματικό της συναλλαγής. Σημαντική αρχή για τα μέτρα ασφάλειας στο ηλ. εμπόριο ωφείλει να αποτελεί η διαδικασία η οποία είναι αρκετά απλή για να χρησιμοποιηθεί από τη σχέση πελάτη / καταναλωτή - προμηθευτή, χωρίς να προϋποθέτεται επιμόρφωση ή ασυνήθισ η προσπάθεια από μέρους του πελάτη / καταναλωτή.

"Πολιτική ασφάλειας (security policy) θεωρείται το σύνολο κανόνων που καθορίζονται για να συναντήσουν έναν ιδιαίτερο στόχο, για να εξασφαλιστεί σε αυτή τη περίπτωση η ασφάλεια σε ένα υπολογιστή ή τις πληροφορίες που επεξεργάζεται. Ένα υπολογιστικό σύστημα έχει 3 δομικά συστατικά:

το **υλικό** (hardware)**,**

το **λογισμικό** (software) και τα

δεδομένα (data). " *Turn R.,* (1986).

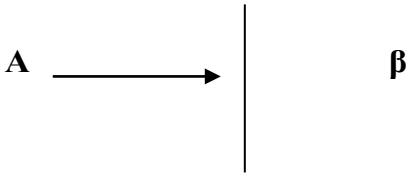
Ο έλεγχος χρησιμοποιείται ως προστατευτικό μέτρο και είναι μια δράση, μια διαδικασία ή μια τεχνική που απομακρύνει ή μειώνει σε επίπεδο διαβαθμίσεων την ευπάθεια. Ο Baker (2000) *Baker, K and Baker S.*(2000) περιγράφει τη σχέση μεταξύ των **απειλών**, των **ελέγχων** και των **ευπαθειών** με τον εξής τρόπο:

"Μια απειλή εμποδίζεται από τον έλεγχο μιας ευπάθειας."

Παρακάτω ακολουθούν οι τέσσερις κοινοί τύποι πιθανών επιθέσεων που είναι:

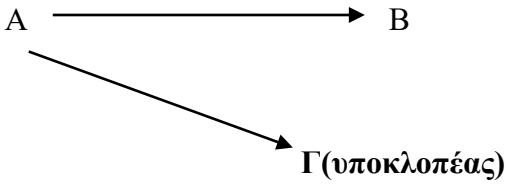
1. Διακοπή (Interruption)

Καμία ενέργεια στον αποδέκτη

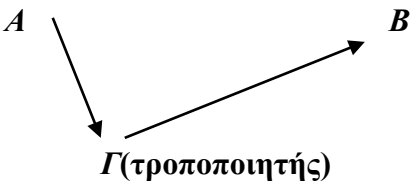


Όταν ένα μήνυμα ταξιδεύει από το Α στο Β δεν φθάνει ποτέ στον προορισμό του λόγω προβλημάτων στο δρομολογητή (router). Κάτι τέτοιο αφορά, που αποτρέπει το μήνυμα να φθάσει στον προορισμό

2. Υποκλοπή (Interception)



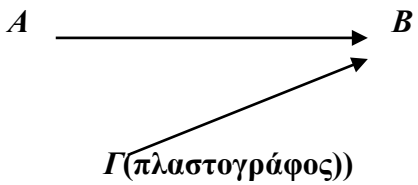
3. Τροποποίηση ***(Modification)***



Ένα μήνυμα που στέλνεται από τον Α στον Β παρεμποδίζεται αρχικά από τον Γ, ο οποίος τροποποιεί το μήνυμα και στέλνει το νέο τροποποιημένο μήνυμα στον Β.

Τροποποίηση σημαίνει ότι αλλάζει το μήνυμα με κάποιο τρόπο (χειρισμό - μεθόδευση).

4. Πλαστογράφηση ***(Fabrication)***



Ένας αγγελιοφόρος πχ. Γ μπορεί να φτιάξει μηνύματα και να τα προωθήσει στον Β, κάνοντάς τα να φαίνονται ότι έχουν αποσταλεί από τον Α. Πλαστογράφηση σημαίνει να δημιουργηθεί ένα όμοιο με το αυθεντικό μήνυμα (συμπεριλαμβανομένης της επανάληψης).

3.2.ΓΙΑΤΙ Η ΕΠΙΤΕΥΞΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΕΙΝΑΙ ΔΥΣΚΟΛΗ

Όταν μιλάμε για ασφάλεια ενός Η/Υ αφορά τις τεχνικές που χρησιμοποιούνται για την διασφάλιση των όποιων κεφαλαίων (assets) και κυρίως των πληροφοριακών. *Turn R.,* (1986).

Η προστασία υπολογιστών ορίζεται συνήθως ως η προστασία του συστήματος και των στοιχείων που αποθηκεύονται εκεί ενάντια στην αναρμόδια πρόσβαση, τροποποίηση, καταστροφή ή χρήση και ενάντια στις ενέργειες ή τις καταστάσεις που αρνούνται την εξουσιοδοτημένη χρήση ή πρόσβαση του συστήματος. Είναι σπάνιο να διαπιστωθεί ότι ένας ενιαίος μηχανισμός ή μια διαδικασία ασφάλειας χρησιμοποιείται μεμονωμένα. Άντ' αυτού, διαφορετικά στοιχεία που λειτουργούν συνήθως μαζί, συνθέτουν ένα σύστημα ασφάλειας για να προστατεύσουν κάτι. Οι άνθρωποι αποτελούν ένα αναπόσπαστο τμήμα των μηχανισμών προστασίας σε ένα σύστημα ασφάλειας. Υπάρχει μια κατηγορία ευπαθειών που συνδέονται με τους ανθρώπους, υπόκεινται στη φυσική επίθεση από τον παραβάτη (violator) και μπορούν να υπονομευθούν ή να εξαπατηθούν. Αυτό που μπορεί να αποτελεί μια

λύση για ένα ιδιαίτερο σύνολο περιστάσεων, δεν απευθύνεται απαραίτητα στο σύνολο των αξιώσεων συναφών αλλά διαφορετικών περιστάσεων

Θεωρία (theory). υπάρχουν μέρη της ασφάλειας υπολογιστών που αποτελούν θεωρητική προσέγγιση. Αυτά είναι:

• **Κρυπτογραφία**, όπου ςε κάθε κατανεμημένο σύστημα πρέπει να υπάρχει κάτι που διακρίνει το νόμιμο παραλήπτη από όλους τους άλλους συμμετέχοντες. Τα **Πρωτόκολλα ασφάλειας δικτύων** που είναι από τα κρισιμότερα στοιχεία που καθιστούν εφικτή την ασφαλή επικοινωνία και την επεξεργασία των πληροφοριών και διασφαλίζουν την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity), την αυθεντικότητα (authenticity) και τη διαθεσιμότητά (availability). Επίσης είναι η **Διαδικασία** ασφάλειας, που έχει ως σκοπό να προσδιορίσει, να καταμετρήσει, να διαχειριστεί και να ελέγξει τους κινδύνους για τη διαθεσιμότητα συστημάτων και στοιχείων, την ακεραιότητα, την εμπιστευτικότητα και να εξασφαλίσει αποδοτικότητα για τις ενέργειες συστημάτων. Τέλος, η **Διαχείριση** όπου όταν ένα σύστημα ασφαλείας υπολογιστών αναπτυχθεί πρέπει να διαχειρίζεται προκειμένου να διασφαλίσει ότι λειτουργεί σωστά. *Turn R.,* (1986).

3.3. ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SECURITY MEASURES)

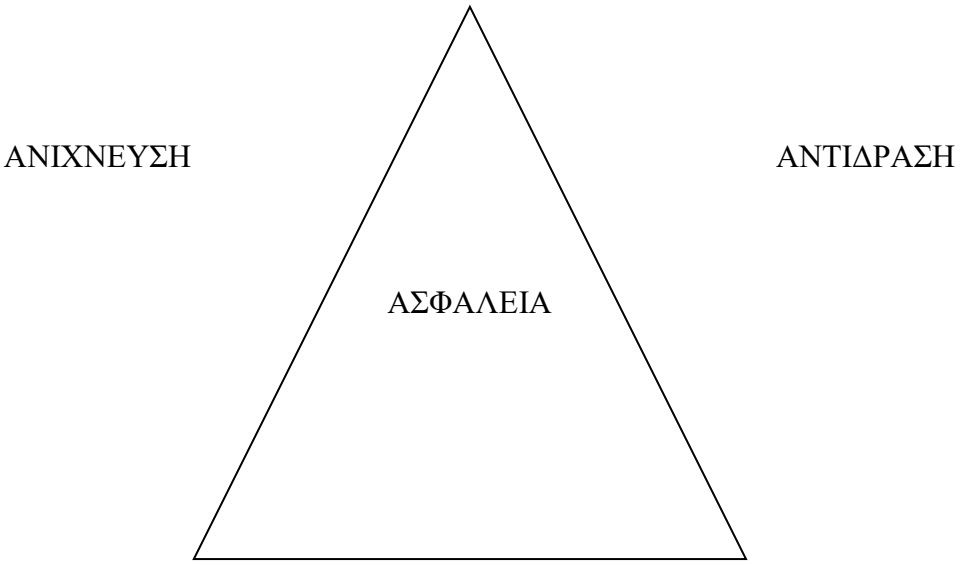
Η τεχνολογία, ειδικά στην περιοχή των υπολογιστών κινείται θεαματικά γρήγορα. ακολουθώντας ,κατά κάποιο τρόπο τον κανόνα της φύσης που διέπει τον άνθρωπο, ότι όλα έχουν μία αρχή και ένα τέλος.

Τα μέτρα προστασίας κατηγοριοποιούνται ενδεικτικά:

• **Πρόληψη (prevention): η προσφυγή σε μέτρα που προλαμβάνουν τα κεφάλαια που βρίσκονται σε ένα υπολογιστικό μέσο από ενδεχόμενη «ζημία»**

Ανίχνευση (detection)**:** η προσφυγή σε μέτρα που επιτρέπουν να ανιχνευθεί ένα κεφάλαιο όταν έχει καταστραφεί, πώς συνέβη η καταστροφή αυτή και ποιος ευθύνεται για τη πρόκληση της καταστροφής.

• **Αντίδραση** (reaction)**:** η προσφυγή σε μέτρα για την επαναφορά ή την ανάληψη μέρους των κεφαλαίων από την όποια πρόκληση καταστροφής. Δηλαδή έχουμε μία τριάδα μέτρων όπου η πρόληψη αποτελεί το θεμέλιο λίθο, καθώς χρησιμεύει ως μονάδα ποσοτικής μέτρησης έναντι της ανίχνευσης και αντίδρασης, η ανίχνευση συνεπικουρεί στην ανίχνευση τυχόν κενών και προβλημάτων ασφάλειας μόλις τα προληπτικά μέτρα τεθούν σε εφαρμογή και τέλος η αντίδραση ανταποκρίνεται με τους κατάλληλους μηχανισμούς στιςδιαρροές ασφάλειας (security breach) *Canavan, J*., (2001).



Η τριάδα ασφάλειας

3.4.ΟΡΙΣΜΟΙ

Για καλύτερη κατανόηση δίνονται παρακάτω οι βασικοί ορισμοί που χρησιμοποιούνται ευρέως στην ανάλυση κινδύνων *CISSP*.(2010),:

Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση

μετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.

Ευπάθεια: Μια αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, εφαρμογή ή υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος.

Κίνδυνος: Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Εναλλακτικά ο κίνδυνος, ο οποίος εκφράζει το ενδεχόμενο για απώλεια, μπορεί να εκφραστεί καλύτερα με την απάντηση των 4 παρακάτω ερωτήσεων:

1. Τι θα μπορούσε να συμβεί; (Απειλή)

2. Πόσο κακό θα μπορούσε να είναι; (Συνέπειες)

3. Πόσο συχνά μπορεί να συμβαίνει; (Συχνότητα)

4. Τι σιγουριά υπάρχει για τις απαντήσεις στις 3 παραπάνω ερωτήσεις; (Βαθμός αβεβαιότητας)

Αντίμετρο: Μέτρο που λαμβάνεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών. Το μέτρο μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή κατηγορίας απειλών.

Ανάλυση κινδύνων: Ανάλυση κινδύνων ενός πληροφοριακού συστήματος είναι η διαδικασία αναγνώρισης και αξιολόγησης των κινδύνων ασφαλείας που εισάγει το σύστημα στην λειτουργία ενός οργανισμού, καθώς και το κόστος των απωλειών που θα προκληθούν σε περίπτωση που δημιουργηθεί πρόβλημα ασφαλείας. Έτσι προσδιορίζεται ο βαθμός κινδύνου του πληροφοριακού συστήματος και οι απαιτήσεις ασφαλείας που υπάρχουν. Υπολογίζεται επιπλέον και το κόστος πρόληψης κάθε απώλειας ώστε να είναι δυνατή μια σωστή αντιμετώπιση των κινδύνων με ορθολογιστικά κριτήρια. *CISSP*.(2010)

3.5 Ο ΤΥΠΟΣ BPL

Ένας βασικός τύπος που αποτελεί την καρδιά της ανάλυσης κινδύνων είναι ο τύπος **B>P*L**

Τα τρία στοιχεία του τύπου BPL είναι:

B = Το κόστος για την πρόληψη μιας απώλειας

P = Η πιθανότητα να συμβεί μια απώλεια

L = Το συνολικό κόστος μιας απώλειας

Το νόημα του τύπου είναι ότι όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή τότε η υλοποίηση του μέτρο πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί. Συνήθως τα μεγέθη υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Ο τύπος αυτός αντικατοπτρίζει την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων, όχι μόνο για πληροφοριακά συστήματα. Την ιδέα του υπολογισμού της πιο συμφέρουσας λύσης *Longstaff, T.A* et al.(2000).

Ωστόσο ο υπολογισμός του τύπου και η πρακτική του εφαρμογή βρίσκει σημαντικές δυσκολίες. Συγκεκριμένα, ο ακριβής υπολογισμός των τιμών των πιθανοτήτων και του κόστους πρόληψης ή απώλειας δεν είναι πάντα εύκολος ή δυνατός. Για παράδειγμα η αντιστοίχηση των απωλειών με οικονομικά νούμερα δεν είναι πάντα δυνατή διότι πολλές φορές στην ανάλυση κινδύνων αξιολογούνται απώλειες απροσδιόριστες όπως η εικόνα ενός οργανισμού και η εμπιστοσύνη που έχουν οι «πελάτες» του σε αυτόν. Ακόμα και αν δεν χρησιμοποιείται όμως άμεσα, όλες οι μέθοδοι της ανάλυσης κινδύνων βασίζονται πάνω στην λογική του τύπου BPL.

3.6 ΒΑΣΙΚΗ ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ

Προκειμένου οι διαχειριστές να πάρουν σωστές αποφάσεις για την αποδοχή, αποτροπή ή μείωση των κινδύνων και την υλοποίηση

αποδοτικών οικονομικά (cost effective) λύσεων ασφαλείας, είναι αναγκαία η υιοθέτηση μιας μεθοδολογίας που θα αντιμετωπίζει τα θέματα με βάση το κόστος και το όφελος. Με τον καιρό έχει δημιουργηθεί μια πληθώρα διαδικασιών που ήρθαν να καλύψουν διαφορετικές ανάγκες για ανάλυση κινδύνων. Αν και υπάρχουν πολλές διαφορετικές διαδικασίες, η βασική μέθοδος παραμένει η ίδια.

Ο κίνδυνος στον οποίο εκτίθεται ένα πληροφοριακό σύστημα είναι συνάρτηση *Longstaff, T.A* et al.(2000):

• Της αξίας των περιουσιακών στοιχείων

• Των ευπαθειών του

• Των πιθανών απειλών και της φύσης τους

• Των επιπτώσεων που μπορεί να προκύψουν

Στο παρακάτω σχήμα φαίνονται οι σχέσεις μεταξύ των παραπάνω καθώς και η σχέση του κινδύνου με τα αντίμετρα που τελικά επιλέγονται.

Σχήμα 2 - Μέθοδοι και Εργαλεία Αναγνώρισης Κινδύνου

Η βασική μεθοδολογία της ανάλυσης κινδύνων περιλαμβάνει τα παρακάτω βήματα:

1. Καθορισμός του σκοπού και της εμβέλειας της ανάλυσης: Στο βήμα αυτό καθορίζεται τι ακριβώς θα περιληφθεί στην ανάλυση κινδύνων και ποια αποτελέσματα αναμένεται να παραχθούν από αυτήν.

2. Αναγνώριση και αξιολόγηση των περιουσιακών στοιχείων του πληροφοριακού συστήματος: Υπάρχουν πολλά περιουσιακά στοιχεία σε έναν οργανισμό, πολλά από τα οποία δεν είναι εύκολα αναγνωρίσιμα. Σε

αυτό το βήμα γίνεται προσπάθεια αναγνώρισης τους και προσδιορισμός της αξίας τους προς τον οργανισμό. *Longstaff, T.A* et al.(2000)

3. Ανάλυση των απειλών προς τα περιουσιακά στοιχεία και των επιπτώσεων που μπορεί να έχουν: Για κάθε κατηγορία περιουσιακών στοιχείων υπάρχουν και μια σειρά από απειλές. Στο βήμα αυτό αναγνωρίζονται οι απειλές για κάθε περιουσιακό στοιχείο, ο τρόπος με τον οποίο το απειλούν και οι επιπτώσεις που θα επιφέρει η κάθε απειλή.

4. Ανάλυση των ευπαθειών: Ένα περιουσιακό στοιχείο μπορεί να είναι λιγότερο ευπαθής προς μια απειλή και περισσότερο προς μια άλλη. Στο βήμα αυτό διευκρινίζεται η ευπάθεια του κάθε περιουσιακού στοιχείου προς κάθε απειλή ξεχωριστά. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή **x** Πιθανότητα να είναι επιτυχής

5. Υπολογισμός του κινδύνου: Ο βαθμός του κινδύνου υπολογίζεται ξεχωριστά για κάθε απειλή προς κάθε περιουσιακό στοιχείο. Είναι συνάρτηση όλων των παραπάνω, δηλαδή:

- Των επιπτώσεων μιας απειλής (που έχουν σχέση με την αξία του περιουσιακού στοιχείου)

- Της ευπάθειας του περιουσιακού στοιχείου ως προς την απειλή

6. Επιλογή τρόπων αντιμετώπισης των κινδύνων: Υπάρχουν 3 τρόποι αντιμετώπισης του κινδύνου:

α) **Αποφυγή** του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη δραστηριότητα

β) **Αποδοχή** του κινδύνου

γ) **Μείωση** του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας)

Με τα αντίμετρα μπορούν να επιτευχθούν τα εξής:

- Μεταφορά κινδύνου, πχ. αγορά ασφάλειας

- Μείωση ευπάθειας:

- Μείωση πιθανότητας να συμβεί μια απειλή

- πχ. απαγορεύοντας το κάπνισμα σε μια ευαίσθητη περιοχή

- Μείωση πιθανότητας μια απειλή να είναι επιτυχής

- πχ. χρήση κρυπτογράφησης, χρήση firewall

- Μείωση αντίκτυπου, πχ. σύστημα πυρόσβεσης

- Μέτρα ανάνηψης (επαναφοράς), πχ. backup

Κατά το βήμα αυτό αναγνωρίζονται τα πιθανά αντίμετρα που μπορούν να εφαρμοστούν και επιλέγονται αυτά που συμφέρουν περισσότερο στον οργανισμό.

7. Τα επόμενα βήματα: Η ανάλυση κινδύνων και η ασφάλεια των πληροφοριακών συστημάτων γενικότερα είναι μια συνεχόμενη διαδικασία. Μετά την επιλογή των τρόπων αντιμετώπισης και την εφαρμογή τους στον οργανισμό πρέπει να υπάρχει μια συνεχής παρακολούθηση των κινδύνων. Τα δεδομένα σε ένα πληροφοριακό σύστημα αλλάζουν συνεχώς, εισάγονται νέες απειλές, νέες ευπάθειες, νέες επιπτώσεις κτλ. Τα αντίμετρα που έχουν επιλεχθεί ελέγχονται συνεχώς για την αποτελεσματικότητα τους. Πολλά από αυτά με τον καιρό σταματούν να

συμφέρουν στον οργανισμό και πρέπει να καταργηθούν ή να αντικατασταθούν από νέα αντίμετρα. *Longstaff, T.A* et al.(2000)

3.7 ΟΦΕΛΗ ΑΠΟ ΤΗΝ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ

Παρακάτω αναφέρονται τα πιο σημαντικά οφέλη που αποκομίζονται από την ανάλυση κινδύνων πληροφοριακών συστημάτων *Wallmuller, E.*(2010),.

Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος

Η ανάλυση κινδύνων βοηθάει στην γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος αναγνωρίζοντας και αντιμετωπίζοντας τους σημαντικότερους κινδύνους που το απειλούν.

Στόχευση της ασφάλειας

Η ασφάλεια πρέπει να στοχεύει κατάλληλα και άμεσα στις πιθανές επιπτώσεις, απειλές και υπάρχουσες ευπάθειες. Η αποτυχία να γίνει αυτό μπορεί να οδηγήσει σε υπερβολικές και μη αναγκαίες δαπάνες. Η ανάλυση κινδύνων προάγει πολύ καλύτερη στόχευση που βοηθά στην εξάλειψη των άσκοπων δαπανών και στην πιο αποτελεσματική αντιμετώπιση των πραγματικών προβλημάτων ασφαλείας.

Βελτίωση της κατανόησης του συστήματος

Κατά την διαδικασία της ανάλυσης κινδύνων βελτιώνεται η γνώση και η κατανόηση του συστήματος ως προς θέματα ασφαλείας. Καταρχάς αναγνωρίζονται οι διάφορες απειλές και φανερώνονται οι ευπάθειες του. Επίσης κατανοείται η πραγματική αξία των επιμέρους συστημάτων που αποτελούν το πληροφοριακό σύστημα.

Κατανόηση της αναγκαιότητας της ασφάλειας

Η συμμετοχή στην διαδικασία της ανάλυσης κινδύνων διαμορφώνει μια καλύτερη κατανόηση των προβλημάτων ασφαλείας καθώς και των επιπτώσεων που μπορεί να έχουν αυτά. Με αυτό τον τρόπο επιτυγχάνεται καλύτερη επιλογή αντιμέτρων αλλά και μεγαλύτερη αποδοχή των αντιμέτρων που προτείνονται από τους χρήστες. Η κατανόηση της αναγκαιότητας της ασφάλειας έχει ως αποτέλεσμα την αντιμετώπιση των θεμάτων ασφαλείας με την σοβαρότητα που τους αρμόζει.

Δικαιολόγηση δαπανών για την ασφάλεια

Η εισαγωγή ασφάλειας σε ένα πληροφοριακό σύστημα σχεδόν πάντα σημαίνει επιπλέον κόστος. Επειδή όμως δεν οδηγεί άμεσα σε αύξηση των κερδών μιας επιχείρησης, πρέπει να δικαιολογείται οικονομικά. Η ανάλυση κινδύνων δημιουργεί την κατάλληλη δικαιολόγηση για την αναγκαιότητα της ασφάλειας που προτείνεται και του κόστους που αυτή προσθέτει. *Wallmuller, E.*(2010)

3.8 ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ

Υπάρχει ένας πολύ μεγάλος αριθμός από τεχνικές ανάλυσης κινδύνων. Αυτό οφείλεται στις διαφορετικές ανάγκες που χρειάζεται να καλύψουν. Γενικά όμως υπάρχουν δύο μεγάλες κατηγορίες για ανάλυση κινδύνων: Η ποσοτική(quantitative) και η ποιοτική (qualitative) *Yazar, Z.*(2002),.

Ποσοτική ανάλυση: Η ποσοτική ανάλυση προσπαθεί να προσδιορίσει αντικειμενικές αριθμητικές τιμές (πχ. χρηματικά ποσά) για κάθε συνιστώσα της ανάλυσης κινδύνων. Για παράδειγμα προσπαθεί να υπολογίσει την χρηματική αξία των απωλειών ή την πιθανότητα (σε νούμερο) να συμβεί ένα περιστατικό. Στην περίπτωση που «ποσοτικοποιηθούν» όλες οι συνιστώσες (αξία περιουσιακών στοιχείων, συχνότητα απειλών, αποτελεσματικότητα αντίμετρων, κόστος αντίμετρων, αβεβαιότητα και πιθανότητα) τότε η ανάλυση ονομάζεται πλήρως ποσοτική.

Πλεονεκτήματα:

• Τα αποτελέσματα έχουν το κύρος της μαθηματικής απόδειξης

• Τα αποτελέσματα μπορούν να εκφραστούν σε γλώσσα κατανοητή από τους

διαχειριστές (managers) του οργανισμού

• Η ανάλυση κόστους/όφελους (cost/benefit) είναι πιο εύκολη και άμεση.

• Η αξία των περιουσιακών στοιχείων του πληροφοριακού συστήματος (όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) γίνεται καλύτερα κατανοητή όταν εκφράζεται σε χρηματικά ποσά. Αυτό βοηθάει στην μεγαλύτερη αποδοχή της ασφάλειας.

Μειονεκτήματα:

• Οι υπολογισμοί μπορεί να είναι πολύπλοκοι

• Η ανάλυση χρειάζεται πολύ χρόνο για να ολοκληρωθεί

• Χρειάζεται μεγάλη ποσότητα προκαταρτικής εργασίας

• Η καθοδήγηση των συμμετεχόντων στην ανάλυση δεν μπορεί να γίνει εύκολα. Έτσι συνήθως χρειάζεται η συμμετοχή έμπειρων στην ποσοτική ανάλυση ατόμων.

• Ιστορικά, η ποσοτική ανάλυση λειτουργεί καλά μόνο με την χρήση κάποιου

αυτοματοποιημένου εργαλείου συνδεδεμένου με μια γνωστική βάση (knowledge base).

Ιστορικά, η ποσοτική ανάλυση ήταν η πρώτη που χρησιμοποιήθηκε για την ανάλυση κινδύνων πληροφοριακών συστημάτων. Οι πρώτες προσπάθειες όμως συνάντησαν σημαντικές δυσκολίες λόγω της μεγάλης ποσότητας των δεδομένων και τις πολυπλοκότητας των υπολογισμών. Έτσι, ενώ πολλοί σχεδίασαν εργαλεία και αυτόματες διαδικασίες για την υποβοήθηση της ποσοτικής ανάλυσης, άλλοι κατέφυγαν στην δημιουργία πιο ποιοτικών μεθόδων ανάλυσης οι οποίες τελικά έγιναν και οι πιο διαδεδομένες.

Ποιοτική ανάλυση. Η ποιοτική ανάλυση δεν προσπαθεί να δώσει ακριβείς αριθμητικές τιμές στις συνιστώσες της ανάλυσης κινδύνου. Αντιθέτως αρκείται να τις χαρακτηρίζει με εκφράσεις όπως πχ. μεγάλο, μέτριο, μικρό ή να δίνει τιμές από μια προαποφασισμένη κλίμακα. Με την λογική αυτή παρακάμπτονται οι πολύπλοκοι υπολογισμοί. Αν και οι κίνδυνοι δεν υπολογίζονται επακριβώς, επιτυγχάνεται η ταξινόμηση τους και επομένως η προτεραιότητα για την αντιμετώπιση τους. Η ποιοτική ανάλυση

βασίζεται στην εμπειρία των ανθρώπων που συμμετέχουν για τον προσδιορισμό των κινδύνων. Πρόκειται προφανώς για μια υποκειμενική μέθοδος. Προσπαθεί να εκμεταλλευτεί την γνώση των ατόμων που συμμετέχουν ώστε να φτάσει σε αποδεκτά προσεγγιστικά αποτελέσματα στον ελάχιστο δυνατό χρόνο και με την ελάχιστη προσπάθεια, παρακάμπτοντας το πολύπλοκο μαθηματικό κομμάτι της ανάλυσης. Έχει αποδειχτεί με τον καιρό ότι η ποιοτική ανάλυση παράγει ικανοποιητικά αποτελέσματα όταν τα άτομα που συμμετέχουν έχουν την απαιτούμενη γνώση και εμπειρία για το πληροφοριακό σύστημα που εξετάζεται *Yazar, Z.*(2002)

Πλεονεκτήματα:

• Αποφεύγονται πολύπλοκοι υπολογισμοί

• Δεν είναι απαραίτητος ο αριθμητικός υπολογισμός της αξίας των περιουσιακών στοιχείων

• Είναι ευκολότερη η συμμετοχή ατόμων που δεν έχουν σχέση με την ασφάλεια και την πληροφορική.

• Η ποιοτική ανάλυση χρειάζεται λιγότερο χρόνο και λιγότερους πόρους σε σχέση με την ποσοτική

• Η διαδικασία της ανάλυσης είναι πιο ευέλικτη

Μειονεκτήματα:

• Είναι υποκειμενικής φύσεως

• Δεν γίνεται μεγάλη προσπάθεια για την αναγνώριση της αντικειμενικής αξίας των περιουσιακών στοιχείων. Έτσι, η αντίληψη της αξίας μπορεί να μην αντικατοπτρίζει την πραγματική αξία κατά τον υπολογισμό του κινδύνου. *Wallmuller, E.*(2010)

• Η ποιότητα των αποτελεσμάτων βασίζεται εξ' ολοκλήρου στην γνώση και την εμπειρία των ατόμων που συμμετέχουν στην ανάλυση

• Η ανάλυση κόστους/οφέλους (cost/benefit) δεν βασίζεται σε μαθηματική απόδειξη Στην πραγματικότητα οι περισσότερες τεχνικές που

χρησιμοποιούνται σήμερα είναι μια μίξη ποσοτικής και ποιοτικής ανάλυσης. Τον χαρακτηρισμό ποιοτική ή ποσοτική ανάλυση την παίρνουν ανάλογα με ποια ανάλυση προσεγγίζουν καλύτερα.

3.9 ΠΛΑΝΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ

Το πλάνο διαχείρισης κινδύνου εστιάζει σε συγκεκριμένες ενέργειες που πρέπει να πραγματοποιηθούν στο γενικό πλαίσιο διαχείρισης κινδύνων. Πιο συγκεκριμένα ορίζει πώς οι κίνδυνοι που συνδέονται με ένα σύστημα θα προσδιοριστούν, αναλυθούν και διαχειριστούν. Περιγράφει πώς οι δραστηριότητες διαχείρισης κινδύνου θα πρέπει να εκτελούνται, καταχωρούνται και παρακολουθούνται ενώ παρέχει πρότυπα και πρακτικές για την καταγραφή και ιεράρχηση των συγκεκριμένων κινδύνων.

Το πλάνο δημιουργείτε από το υπεύθυνο του έργου (project manager) στη φάση σχεδιασμού και απευθύνεται στην ομάδα ανάπτυξης του έργου , στη διεύθυνση του οργανισμού (management) όπως και στη οικονομική διεύθυνση και παρακολουθείται και ενημερώνεται καθ' όλη τη διάρκεια του έργου.

Ένα πλάνο διαχείρισης κινδύνου αποτελείτε από τα εξής μέρη :

Α) <u>Προσδιορισμός των κινδύνων</u>

Η αναγνώριση των κίνδυνων πραγματοποιείται από την ομάδα ανάπτυξης του έργου καθώς και από τους εμπλεκόμενους φορείς και περιλαμβάνει την αξιολόγηση περιβαλλοντικών παραγόντων, την οργανωτική κουλτούρα και τη διαχείριση του έργου συμπεριλαμβανομένου του πεδίου εφαρμογής του έργου. Ιδιαίτερή προσοχή στον προσδιορισμό κινδύνου θα δοθεί στο ίδιο το έργο, πιθανές παραδοχές και περιορισμούς αυτού, σε εκτιμήσεις κόστους και δυσκολίας όπως και τη διαχείριση πόρων. Θα πρέπει να δημιουργηθεί ένα αρχείο διαχείρισης κινδύνου το οποίο θα αποθηκεύεται σε ηλεκτρονική μορφή και θα ανανεώνεται σε τακτά χρονικά διαστήματα.

Β) <u>Ανάλυση κινδύνων</u>.

Όλοι οι κίνδυνοι που έχουν προσδιοριστεί θα πρέπει να αξιολογηθούν για να προσδιοριστεί ο βαθμός με τον οποίο επηρεάζουν το σύστημα. Οι κίνδυνοι αυτοί θα βαθμονομηθούν για να αποφασιστεί ποιοι από αυτούς είναι πιο σημαντικοί και πρέπει να αντιμετωπιστούν άμεσα και ποιοι μπορούν να αγνοηθούν. Όπως ήδη έχουμε αναφέρει οι τεχνικές ανάλυσης κίνδυνου είναι : ποιοτική και ποσοτική και οι δυο καταγράφονται στο πλάνο διαχείρισης κινδύνου. Πιο συγκεκριμένα :

1) Ποιοτική ανάλυση. Η πιθανότητα και τις επιπτώσεις της εμφάνισης για κάθε προσδιορισμένο κίνδυνο και θα πρέπει να αξιολογούνται με τον ακόλουθο τρόπο.

Πιθανότητα

- Υψηλή - Πιθανότητα εμφάνισης μεγαλύτερη από πχ 70%
- Medium - πιθανότητα εμφάνισης μεταξύ πχ 30% και 70%
- Χαμηλή - Πιθανότητα εμφάνισης κάτω από πχ 30%

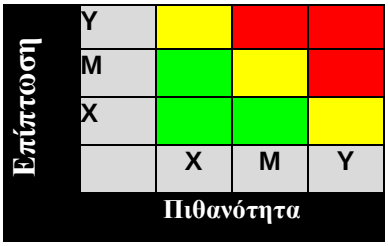
(Τα πιο πάνω ποσοστά παρουσιάζονται ως παράδειγμα)

Επιπτώσεις

• Υψηλές - Κίνδυνος που έχει τη δυνατότητα να επηρεάσει σε μεγάλο βαθμό το κόστος του έργου, το χρονοδιάγραμμα του έργου ή την απόδοση

• Μέτριες - Κίνδυνος που έχει τη δυνατότητα να επηρεάσει ελαφρώς το κόστος του έργου, το χρονοδιάγραμμα του έργου ή την απόδοση

• Χαμηλές - Κίνδυνος που έχει σχετικά μικρή επίπτωση στο κόστος, το χρονοδιάγραμμα ή την απόδοση.



Οι κίνδυνοι που εμπίπτουν στις κόκκινες και κίτρινες περιοχές πρέπει να αντιμετωπιστούν μέσω του σχεδιασμού αντιμετώπισης κινδύνων.

2) Ποσοτική Ανάλυση. Οι κίνδυνοι οι οποίοι έχουν προτεραιότητα βάση της ποιοτικής ανάλυσης, θα αναλυθούνε ως προς τις επιπτώσεις στη λειτουργία του συστήματος, θα τεκμηριώνονται ,θα βαθμολογούνται και θα καταγράφονται σε αυτό το τμήμα το πλάνου.

Γ) Σχεδιασμός αντιμετώπισης κινδύνων.

Οι προσεγγίσεις αντιμετώπισης για κάθε σημαντικό κίνδυνο (που εμπίπτει στις κόκκινες και κίτρινες περιοχές του παραπάνω σχήματος) είναι οι :

- Αποφυγή : εξάλειψη του κίνδυνού από την εξάλειψη της αιτίας.
- Μετριασμός : Χρησιμοποιώντας τρόπους που θα μειώσουν την πιθανότητα εμφάνισης και την επίδραση του κινδύνου
- Αποδοχή : Τίποτα δε θα γίνει
- Μεταφορά : Μεταφορά του κινδύνου σε τρίτο φορέα(πχ ασφαλιστικό φορέα, ανάθεση αντιμετώπισης σε άλλο οργανισμό)

Για κάθε σημαντικό κίνδυνο που πρόκειται να μετριαστεί ή γίνει αποδεκτός, θα πρέπει να καταγραφεί στο πλάνο μια σειρά ενεργειών που θα πρέπει να πραγματοποιηθούν προκειμένου να ελαχιστοποιηθούν οι επιπτώσεις του.

Δ) Παρακολούθηση , έλεγχος και αναφορά κινδύνων

Η διαχείριση κινδύνων είναι μια δραστηριότητα που συνεχίζεται καθ 'όλη τη διάρκεια της ζωής του πληροφοριακού συστήματος. Η διαδικασία αυτή περιλαμβάνει τη συνέχιση δραστηριοτήτων ταυτοποίησης των κινδύνων, την εκτίμηση του κινδύνου, τον προγραμματισμό αντιμετώπισης πρόσφατων κινδύνων, και τα σχέδια έκτακτης ανάγκης, και υποβολή αναφορών σχετικά με τον κίνδυνο ανά τακτά χρονικά διαστήματα . Μερικά χαρακτηριστικά του κινδύνου, όπως η πιθανότητα και οι επιπτώσεις, θα μπορούσαν να αλλάξουν κατά

τη διάρκεια της ζωής ενός συστήματος κάτι το οποίο θα πρέπει να αναφερθεί στο πλάνο.

ΚΕΦΑΛΑΙΟ 4^{Ο} ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ

Η ανάλυση κινδύνων αποτελεί δύσκολη και πολύπλοκη με μεγάλο αριθμό δεδομένων επεξεργασίας και όσο πιο μεγάλο το εύρος της ανάλυσης, τόσο πιο δύσκολη είναι η διαχείριση των συλεγόμενων πληροφοριών .

Λόγω αυτής της δυσκολίας πολλές εταιρίες έχουν αναπτύξει λογισμικό για την διευκόλυνση της ανάλυσης κινδύνων. Στις περισσότερες περιπτώσεις οι εταιρίες έχουν αναπτύξει τις δικές τους παραλλαγές μεθόδων ανάλυσης κινδύνων που υποβοηθούνται από το λογισμικό. Η εξέλιξη αυτή βοήθησε την απλοποίηση της ανάλυσης κινδύνων ώστε να μπορεί πλέον να γίνεται στο εσωτερικό ενός οργανισμού με ελάχιστη ή καθόλου παρέμβαση από εξωτερικούς ειδικούς.

Τα πακέτα λογισμικού ανάλυσης κινδύνων που υπάρχουν αυτή τη στιγμή στην αγορά είναι αρκετά και καλύπτουν πολλές και διαφορετικές ανάγκες και απαιτήσεις.

4.1. ΤΕΧΝΟΛΟΓΙΑ ΛΟΓΙΣΜΙΚΟΥ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΩΝ

Η ανάπτυξη λογισμικού ξεκίνησε από την δεκαετία του ’80 και τα προγράμματα που σχεδιάστηκαν τα πρώτα χρόνια ήταν απλά με απλούς υπολογισμούς αλλά αργότερα τα προγράμματα για ανάλυση κινδύνων έλαβαν πιο ενεργό ρόλο αναλαμβάνοντας την διευκόλυνση του συνόλου της ανάλυσης κινδύνων με πολλά διαφορετικά εργαλεία.

Γύρω στο 1990 που τέτοιου είδους προγράμματα κυκλοφόρησαν ελεύθερα, ο ανταγωνισμός οδήγησε τις εταιρίες ανάπτυξης τους να προσθέσουν νέα χαρακτηριστικά ώστε τελικά να καταλήξουν σε μεγάλα πακέτα εφαρμογών.

Στη συνέχεια περιγράφονται οι δυνατότητες, τα χαρακτηριστικά και τα εργαλεία που έχουν αναπτυχθεί όλα αυτά τα χρόνια για το λογισμικό ανάλυσης κινδύνων.

Ποιοτική και ποσοτική ανάλυση:

Κυκλοφορούν λογισμικά πακέτα και για τις 2 διαφορετικές μεθόδους ανάλυσης κινδύνων. Τα πακέτα που χρησιμοποιούν την ποσοτική μέθοδο συνήθως χρησιμοποιούν μεγάλες γνωσιακές βάσεις (knowledge bases) με δεδομένα από ποσοτικές αναλύσεις, τα οποία χρησιμοποιούν για τον υπολογισμό των απειλών και των κινδύνων. Τα τελευταία χρόνια όμως άρχισε να γίνεται φανερό ότι ο κάθε

οργανισμός έχει τις δικές του ειδικές ανάγκες και παραμέτρους ασφαλείας, με αποτέλεσμα να προτιμάται η ποιοτική ανάλυση, η οποία απαιτεί και πολύ λιγότερο χρόνο και προσπάθεια για υλοποίηση.

Καταγραφή και αποτίμηση περιουσιακών στοιχείων:

Υπάρχουν εργαλεία για την εύκολη καταγραφή, κατηγοριοποίηση και αποτίμηση των περιουσιακών στοιχείων και στον πληροφοριακό τομέα τα περιουσιακά στοιχεία δεν είναι εύκολο να αποτιμηθούν λόγο της αφηρημένης έννοιας τους.

Λίστες απειλών:

Επειδή τα περισσότερα πακέτα λογισμικού ανάλυσης κινδύνων δεν απευθύνονται αποκλειστικά σε ειδικούς με την ασφάλεια πληροφοριακών συστημάτων, έχουν δημιουργηθεί λίστες με τις πιθανές απειλές που υπάρχουν.

Αποτίμηση απειλών:

Υπάρχουν πολλοί τρόποι που χρησιμοποιούνται από τα προγράμματα για την αποτίμηση των απειλών αλλά ο δημοφιλέστερος είναι τα ερωτηματολόγια. Σε αντίθεση με τους ανθρώπους, το λογισμικό δεν μπορεί να κατανοήσει από μόνο του την δομή του πληροφοριακού συστήματος του οργανισμού και τις συσχετίσεις μεταξύ των διαφόρων περιουσιακών στοιχείων. Για να επιτευχθεί αυτό έχουν δημιουργηθεί εργαλεία για την δημιουργία μοντέλου. Το μοντέλο αυτό απαρτίζεται κυρίως από τις διάφορες συσχετίσεις που υπάρχουν μεταξύ των περιουσιακών στοιχείων. Έτσι, το πρόγραμμα μπορεί να υπολογίσει την μεταφορά κινδύνου από το ένα περιουσιακό στοιχείο στο άλλο και τελικά να καθορίσει τον τελικό βαθμό του κινδύνου για καθένα από αυτά.

Υπολογισμός βαθμού κινδύνου:

Με την κατεργασία των περιουσιακών στοιχείων, των απειλών και των ευπαθειών του πληροφοριακού συστήματος υπολογίζονται οι βαθμοί κινδύνου. Ο υπολογισμός γίνεται αυτόματα από το πρόγραμμα από την στιγμή που εισαχθούν όλα τα απαραίτητα δεδομένα.

Λίστες αντιμέτρων:

Όλα τα πακέτα λογισμικού για ανάλυση κινδύνων περιέχουν βάση δεδομένων με αντίμετρα κάθε κατηγορίας, καθώς και πληροφορίες για το ποιες απειλές αντιμετωπίζουν, πόσο αποτελεσματικά είναι και τι κόστος έχουν. Τα αντίμετρα αυτά έχουν επιλεγεί από ειδικούς και καλύπτουν όλο το φάσμα των απειλών.

Αυτόματη επιλογή αντιμέτρων:

Υπάρχουν αλγόριθμοι για την αυτόματη επιλογή των κατάλληλων αντιμέτρων βάση των στοιχείων που έχουν συλλεχθεί κατά την διάρκεια της ανάλυσης. Η επεξεργασία του τύπου των απειλών, του βαθμού των κινδύνων, του κόστους των αντιμέτρων, τις αποτελεσματικότητας των αντιμέτρων, της ύπαρξης άλλων αντιμέτρων και πολλών άλλων παραμέτρων οδηγεί στην επιλογή αντιμέτρων που έχουν βέλτιστο λόγο απόδοσης/κόστους.

Ανάλυση What If:

Η χρήση των Η/Υ στην ανάλυση κινδύνων προσθέτει νέες δυνατότητες όπως η ανάλυση what if. Η ανάλυση what if ελέγχει υποθετικά σενάρια ώστε να δει τι επιδράσεις θα έχουν οι διάφορες αλλαγές στους βαθμούς των κινδύνων. Με αυτό τον τρόπο μπορούν να ελεγχθούν και να προταθούν διαφορετικές προσεγγίσεις για την λύση των προβλημάτων. **Δημιουργία αναφορών:**

Τα περισσότερα πακέτα ανάλυσης κινδύνων δεν περιορίζονται στα τυπικά μέρη της ανάλυσης κινδύνων αλλά περιέχουν και εργαλεία για την γενικότερη διευκόλυνση των ανθρώπων που εργάζονται για αυτήν. Ένα από αυτά είναι και η δημιουργία αναφορών. Υπάρχουν πακέτα που προσφέρουν σύγχρονα εργαλεία για την υποβοήθηση της δημιουργίας πολιτικών ασφαλείας.

Διαχείριση εγγράφων:

Ένα χαρακτηριστικό που δεν προσφέρουν πολλά πακέτα ανάλυσης κινδύνων αλλά είναι πολύ σημαντικό είναι η διαχείριση εγγράφων. Διατηρείται βάση δεδομένων με τις πολιτικές ασφαλείας, τις διαδικασίες που πρέπει να ακολουθούνται και άλλα έγγραφα σχετικά με την ασφάλεια του πληροφοριακού συστήματος. Η βάση δεδομένων δίνει την κατάλληλη πρόσβαση σε κάθε χρήστη, δίνοντας του μόνο τα στοιχεία που χρειάζεται έτσι ώστε να μην χάνει χρόνο στην αναζήτηση. Η βάση δεδομένων βρίσκεται μέσα στο τοπικό δίκτυο έτσι ώστε η πρόσβαση στα αρχεία αυτά να είναι εύκολη και γρήγορη από όλα τα μέλη του οργανισμού. Συμμετοχή στην ανάλυση κινδύνων μέσω δικτύου:

1 από τις πιο σύγχρονες λειτουργίες του λογισμικού ανάλυσης κινδύνων είναι η χρήση του δικτύου για την συμμετοχή στην ανάλυση κινδύνων. Δίνεται η δυνατότητα στους χρήστες να συνδέονται στο περιβάλλον του προγράμματος μέσω ενός απλού web browser και να απαντούν σε ερωτηματολόγια. Ο κάθε

χρήστης βλέπει μόνο τα ερωτηματολόγια που του αντιστοιχούν. Με αυτό τον τρόπο απλοποιείται η διαδικασία, καθώς οι χρήστες μπορούν να συμμετέχουν από οπουδήποτε. Δίνεται επίσης η δυνατότητα διαχείρισης του προγράμματος από τους χειριστές του εξ αποστάσεως.

Έλεγχος συμμόρφωσης με στάνταρ:

Τα πιο πολλά από τα προγράμματα ανάλυσης κινδύνων που υπάρχουν στο εμπόριο δίνουν την δυνατότητα ελέγχου της συμμόρφωσης ενός οργανισμού με τα διεθνή στάνταρ. Σε περίπτωση μη συμμόρφωσης τα προγράμματα μπορούν να αναλύσουν το σύστημα και να κάνουν προτάσεις για την επίτευξη συμμόρφωσης.

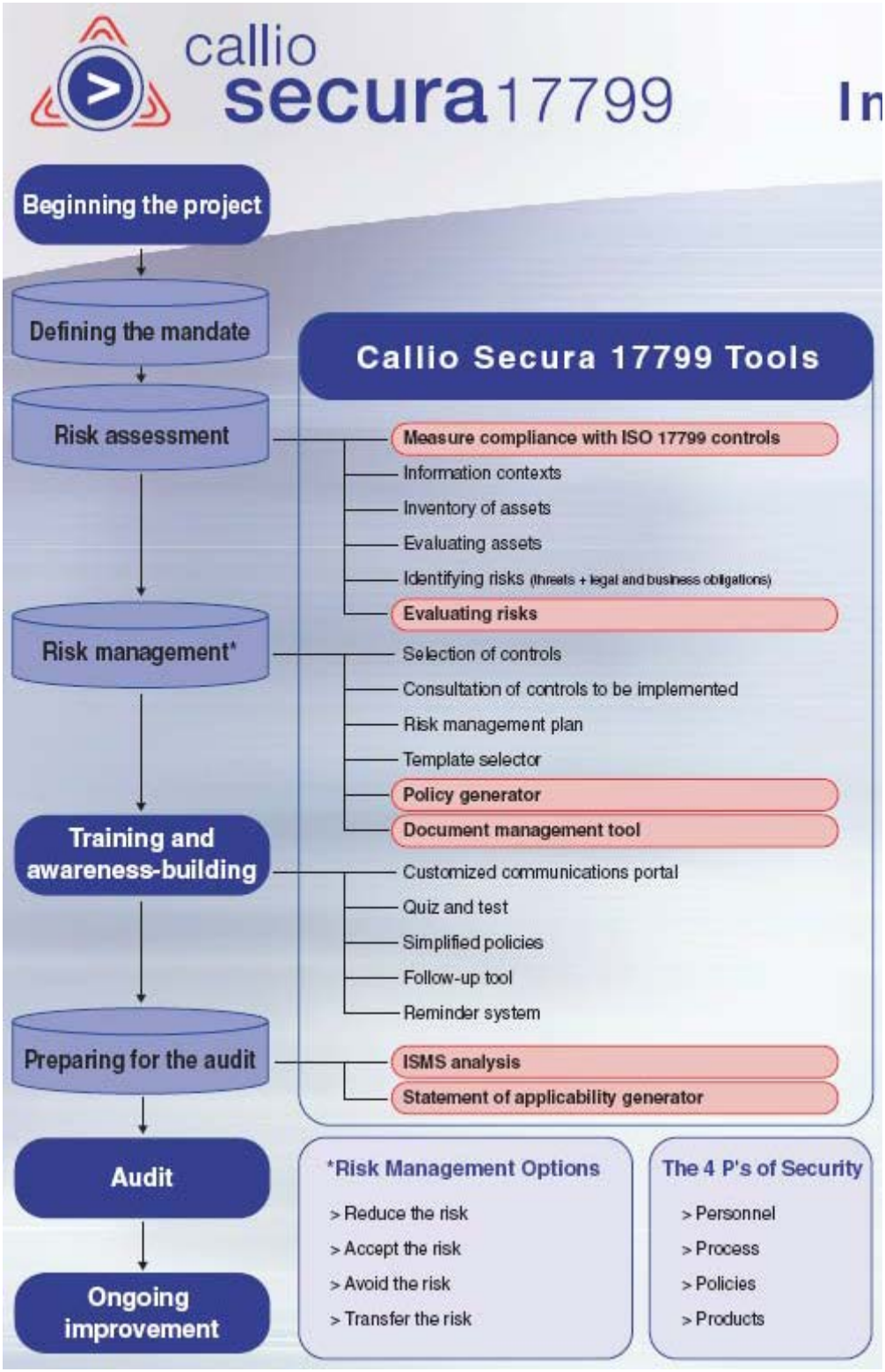
Δυνατότητα εξαγωγής σε βάσεις δεδομένων:

Πολλά λογισμικά πακέτα ανάλυσης κινδύνων συνήθως αποθηκεύουν τα δεδομένα της ανάλυσης σε εσωτερική βάση δεδομένων που έχουν. Σε πολλά από αυτά υπάρχει δυνατότητα εξαγωγής των αποτελεσμάτων σε μορφή που μπορεί να επεξεργαστεί από άλλες βάσεις δεδομένων. *Wallmuller, E.*(2010)

4.2.CALLIO SECURA 17799

"Το Callio Secura 17799 αφορά το προϊόν μιας σχετικά καινούργιας εταιρίας που ειδικεύεται στην ασφάλεια πληροφοριακών συστημάτων, της Callio Technologies που ιδρύθηκε το 2001 στον Καναδά. Το εν λόγω πρόγραμμα δίνει έμφαση την συμμόρφωση με το διεθνές στάνταρ BS7799 / ISO 17799 ενώ επίσης βασίζεται σε μια δική του μέθοδο για την ανάλυση κινδύνων που είναι σχετικά απλή, βήμα προς βήμα, ώστε να γίνεται εύκολα κατανοητή και να μην απαιτεί ειδικευμένο προσωπικό για την χρήση του. Ανήκει δε στην κατηγορία των ποιοτικών μεθόδων. Περιλαμβάνει ολοκληρωμένα εργαλεία για: Την αποτίμηση των κινδύνων, Την αντιμετώπιση τους, Την δημιουργία πολιτικών ασφαλείας,Την διαχείριση εγγράφων, Την δημιουργία αναφορών, Και τέλος αυτό που το κάνει να ξεχωρίζει, την εκπαίδευση του προσωπικού.Περιέχει επίσης όλα εκείνα τα εργαλεία που χρειάζονται για την συνεχή διαχείριση και βελτίωση όλων των εγγράφων ασφαλείας του οργανισμού (πχ. version control). Το interface του προγράμματος είναι πολύ εύκολο και χρηστικό και δεν χρειάζεται ειδική εκπαίδευση για την χρησιμοποίηση του. Στη συνέχεια δίνεται ένα διάγραμμα που δείχνει τα εργαλεία που προσφέρει το Callio Secura 17799 για κάθε βήμα της

ανάλυσης κινδύνων (και γενικότερα της διαχείρισης της ασφάλειας)." *Wallmuller, E.(2010)*



Απόκομμα από το φυλλάδιο του Callio Secura 17799

4.3.COBRA

Όταν μιλάμε για το πρόγραμμα COBRA αναφερόμαστε σε ένα από τα πιο παλιά που κυκλοφορούν στην αγορά το οποίο σχεδιάστηκε από την εταιρία C&A Systems Security Ltd και έχει φτάσει σήμερα στην έκδοση 3. Το εν λόγω πρόγραμμα χρησιμοποιεί την δική του μέθοδο για ανάλυση κινδύνων, η οποία βοηθάει στην επίτευξη συμμόρφωσης με το διεθνές στάνταρ ISO17799/BS7799. Ένα από τα σημαντικότερα πλεονεκτήματα του είναι η αυτόματη προσαρμογή της ανάλυσης στις συγκεκριμένες ανάγκες του κάθε οργανισμού. Επίσης, για πιο απαιτητικές αναλύσεις επιτρέπεται η πλήρη παραμετροποίηση των γνωσιακών βάσεων που περιέχει (knowledge bases). Περιλαμβάνεται επιπλέον και η λεγόμενη «What if» ανάλυση, κατά την οποία ελέγχονται υποθετικά σενάρια ώστε να διαπιστωθεί δυναμικά η επίδραση που θα έχουν συγκεκριμένα αντίμετρα στους βαθμούς κινδύνου. Τέλος, το πρόγραμμα έχει την δυνατότητα δημιουργίας αναφορών επαγγελματικού επιπέδου που δεν μοιάζουν με τυπικές αναφορές που παράγονται από υπολογιστή. Μάλιστα υπάρχει η δυνατότητα αναφορών που αναφέρονται είτε σε τεχνικό προσωπικό (άρα με γνώσεις σε τεχνικούς όρους) είτε στην διοίκηση του οργανισμού.

Το πρόγραμμα τρέχει σε πλατφόρμα MS Windows με ελάχιστες απαιτήσεις αλλά και με interface που παραπέμπει σε λίγο παλαιότερες εποχές." Πάγκαλος Γ.

4.4.CRAMM

"Το CRAMM είναι ένα εργαλείο ποιοτικής ανάλυσης κινδύνων που αναπτύχθηκε από το CCTA (Central Computer and Telecommunications Agency) της βρετανικής κυβέρνησης το 1985 ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων πληροφοριακών συστημάτων. Το πρόγραμμα, το οποίο έχει υποστεί σημαντικές αναθεωρήσεις και βρίσκεται σήμερα στην έκδοση 5, συνεχίζει να αναπτύσσεται
πλέον από την εμπορική εταιρία Insight Consulting που έχει έδρα στην Αγγλία. Το CRAMM έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε παραπάνω από 500 οργανισμούς σε 23 χώρες, συμπεριλαμβανομένου και του NATO. Το πρόγραμμα

ακολουθεί την δική του μέθοδο, η οποία αποτιμά και βοηθάει τους οργανισμούς να επιτύχουν συμμόρφωση με το διεθνές στάνταρ ISO17799/BS7799. Τα βασικά χαρακτηριστικά του προγράμματος είναι:

- Τεράστια βάση αντιμέτρων (3000 αντίμετρα) που καλύπτει όλες τις πτυχές της ασφάλειας πληροφοριακών συστημάτων.

Η βάση ανανεώνεται συνεχώς. - «What if» ανάλυση

- Εργαλεία για την δημιουργία σχεδίων «Business Continuity»
- Οδηγούς για την δημιουργία πολιτικών ασφαλείας
- Οδηγούς για την δημιουργία αναφορών με δυνατότητες χάραξης πινάκων και γραφημάτων και εξαγωγής σε διάφορες μορφές αρχείων
- Σχετικά σύγχρονο περιβάλλον σε πλατφόρμα MS Windows
- Δυνατότητα προσαρμογής του προγράμματος στις ανάγκες του κάθε οργανισμού (σε συνεννόηση με την εταιρία)

Ένα από τα μειονεκτήματα του CRAMM είναι η όχι και τόσο απλή χρήση του, με αποτέλεσμα να απαιτείται εκπαίδευση και εξοικείωση για να επιτευχθούν τα βέλτιστα αποτελέσματα. Τέλος, υπάρχει και η έκδοση CRAMM Express η οποία δεν περιλαμβάνει όλα τα εργαλεία σαν την κανονική έκδοση αλλά είναι πιο απλή στην χρήση και οδηγεί σε πιο γρήγορα αλλά λιγότερο αναλυτικά αποτελέσματα."
*Κατσίκας Σ (*Risk Analysis and Risk Management)

4.5.EZRISK

"Το Ezrisk είναι ένα σχετικά νέο προϊόν σχεδιασμένο από την εταιρία Ezrisk Limited και στοχεύει κυρίως στις μικρές και μεσαίες επιχειρήσεις. Οι επιχειρήσεις αυτές συνήθως δεν έχουν ειδικούς για να διεξάγουν τις δικές τους αναλύσεις κινδύνων και ούτε έχουν τους πόρους για να αγοράσουν ανάλογες υπηρεσίες. Το πρόγραμμα αυτό είναι φθηνό και πολύ απλό, ώστε να μην χρειάζεται ειδική εκπαίδευση για την χρήση του. Περιέχει αλγορίθμους που ελέγχουν τα δεδομένα που εισάγει ο χρήστης, αναγνωρίζουν τυχόν σφάλματα ή αντιφάσεις και βοηθούν στην επίλυση τους. Είναι συμβατό με το διεθνές στάνταρ ISO17799/BS7799 και βοηθάει στην επίτευξη συμμόρφωσης με αυτό. Μπορεί να

παράγει αναφορές σε απλή και κατανοητή μορφή, εξηγώντας τους κινδύνους και τα αντίμετρα που προτείνονται σε κάθε περίπτωση. Τέλος, δημιουργεί σχέδιο δράσης που δείχνει τα βήματα που πρέπει να ακολουθηθούν μέχρι την επίτευξη συμμόρφωσης με το διεθνές στάνταρ ISO17799/BS7799, βάση της προτεραιότητας τους. Το Ezrisk μπορεί να μην έχει τις δυνατότητες και το κύρος άλλων προγραμμάτων αλλά αποτελεί μια ικανοποιητική λύση για μικρές επιχειρήσεις και σφιχτούς προϋπολογισμούς." *Κατσίκας Σ (*Risk Analysis and Risk Management)

4.6.RISKWATCH FOR INFORMATION SYSTEMS & ISO 17799

"Η εταιρία RiskWatch ειδικεύεται στην δημιουργία προγραμμάτων ανάλυσης κινδύνων για πολλούς τομείς, μεταξύ των οποίων και ο τομέας της ασφάλειας πληροφοριακών συστημάτων. Η κύρια διαφορά του σε σχέση με τα περισσότερα προγράμματα του ανταγωνισμού είναι η χρήση ποσοτικής μεθόδου ανάλυσης κινδύνων. Το πρόγραμμα περιέχει χρόνια δεδομένων ποσοτικής ανάλυσης που χρησιμοποιούνται έτοιμα για την εξοικονόμηση χρόνου και προσπάθειας. Τα κύρια χαρακτηριστικά του είναι τα εξής:

- Βοήθεια για επίτευξη συμμόρφωσης με το διεθνές πρότυπο ISO 17799
- Πλήρης παραμετροποίηση από τον χρήστη, με δυνατότητες δημιουργίας καινούργιων κατηγοριών περιουσιακών στοιχείων, απειλών, ευπαθειών, αντιμέτρων, ερωτηματολογίων κτλ.
- Δυνατότητα εισαγωγής δεδομένων και ερωτηματολογίων που έχουν δημιουργηθεί από άλλους χρήστες
- Δυνατότητα δημιουργίας ξεχωριστών σετ ερωτήσεων για τα διαφορετικά τμήματα του οργανισμού, τα οποία μπορούν να διανεμηθούν μέσω δισκετών ή δικτύου
- Ανάλυση ROI (Return on Investment). Λόγω της ποσοτικής του φύσης, το πρόγραμμα μπορεί εύκολα να επιδεικνύει τα αντίμετρα με τον καλύτερο λόγω απόδοσης/κόστους.
- Ανάλυση «What if»

- Δυνατότητα δημιουργίας ποικίλων αναφορών σε κατανοητή μορφή και με χρήση πινάκων και γραφημάτων. Υποστηρίζεται επίσης και η εξαγωγή τους σε διάφορες μορφές αρχείων.
- Σύγχρονο περιβάλλον (interface) σε πλατφόρμα windows με ελάχιστες απαιτήσεις Το RiskWatch είναι ιδιαίτερα δημοφιλής στις ΗΠΑ και έχει μεγάλο κύρος καθώς χρησιμοποιείται σε πολλές κυβερνητικές υπηρεσίες και μεγάλους ιδιωτικούς οργανισμούς. Μερικοί από αυτούς είναι: Υπουργείο Αμύνης των ΗΠΑ, Πεντάγωνο, NSA (National Security Agency), AT&T και Vodafone" *Alberts C* (2003)

ΚΕΦΑΛΑΙΟ 5^{Ο} ΠΑΡΑΔΕΙΓΜΑ ΕΦΑΡΜΟΓΗΣ

5.1 Το Σύστημα TradeNet

Το σύστημα TradeNet είναι ένα ηλεκτρονικό σύστημα συναλλαγών που διευκολύνει την επεξεργασία εμπορικών εγγράφων στην Σιγκαπούρη.

Το διεθνές εμπόριο δεν χαρακτηρίζεται μόνο από την μετακίνηση αγαθών μεταξύ συνόρων, αλλά και από τον μεγάλο αριθμό εγγράφων που τα συνοδεύει. Αυτά τα έγγραφα περιέχουν στοιχεία ιδιοκτησίας, λεπτομέρειες που σχετίζονται με τα αγαθά, διευθύνσεις, κτλ και επιτρέπουν στο κράτος τον έλεγχο του εμπορίου. Το TradeNet επιτρέπει την ηλεκτρονική υποβολή και έγκριση των εγγράφων, αντικαθιστώντας την χέρι με χέρι υποβολή χάρτινων εγγράφων, της χειροκίνητης εκείνης διαδικασίας δηλαδή που υπήρχε πριν.

Με τη λειτουργία του TradeNet οι έμποροι είχαν τη δυνατότητα επεξεργασίας των εγγράφων αυτών από το κράτος πριν τα προϊόντα φτάσουν στον προορισμό τους, εξαλείφοντας την διαδικασία προσωρινής αποθήκευσης σε τελωνεία. Εταιρείες με μηχανογραφικό υλικό μπορούσαν να περάσουν τα απαραίτητα δεδομένα απευθείας στο σύστημα TradeNet γλιτώνοντας διπλές καταχωρήσεις .

Η ανάπτυξη του συστήματος TradeNet εγκρίθηκε από την κυβέρνηση της Σιγκαπούρης στα τέλη του 1986 και ανακοινώθηκε επίσημα από τον υπουργό εμπορίου το Δεκέμβριο του 1986. Δυο δημόσιες υπηρεσίες ανέλαβαν την από κοινού ανάπτυξη του συστήματος : η Επιτροπή Εμπορικής Ανάπτυξης (ΕΕΑ) και η Εθνική Επιτροπή Πληροφοριακών Συστημάτων (ΕΕΠΣ). Η ΕΕΠΣ συγκρότησε την ομάδα έργου που συνεργάστηκε με τους χρήστες για την δημιουργία των απαιτήσεων. Μετά από διαγωνισμό η ανάπτυξη του τεχνικού μέρους του συστήματος ανατέθηκε στην IBM τον Απρίλιο του 1988 ενώ το ίδιο χρονικό διάστημα ιδρύθηκε μια ιδιωτική εταιρεία η Singapore Network Services SNS που θα αναλάμβανε την εγκατάσταση και το χειρισμό του TradeNet.

Στη συνέχει αναλύεται η επικινδυνότητα ως προς τους παράγοντες υλοποίησης, οργανωτικούς παράγοντες, τεχνολογικούς παράγοντες και παράγοντες αγοράς (market)

5.2 Επικινδυνότητα

Παράγοντες υλοποίησης. Το TradeNet ήταν μέχρι εκείνη τη στιγμή το μεγαλύτερο πληροφοριακό σύστημα που υλοποιήθηκε στη Σιγκαπούρη με κόστος 20 εκ. δολαρίων. Επηρέαζε αρκετούς κυβερνητικούς οργανισμούς και εμπορικές εταιρείες και υπήρχε κίνδυνος μη τήρησης του χρονοδιαγράμματος υλοποίησης των 2 χρόνων .

Οργανωτικοί παράγοντες. Κανένας κυβερνητικός οργανισμός δεν είχε την γνώση τους πόρους και την κατάρτιση για την υλοποίηση του TradeNet. Το ΕΕΠΣ δεν γνώριζε τους κανόνες του εμπορίου, ενώ το ΕΕΑ δεν είχε κατάρτιση σε θέματα μηχανογράφησης. Επίσης πολλές εμπορικές εταιρίες δεν είχαν εμπειρία σε θέματα ηλεκτρονικού εμπορίου.

Τεχνολογικοί παράγοντες. Η ηλεκτρονική διακίνηση εγγράφων ήταν καινούργια τεχνολογία για τη Σιγκαπούρη και απαιτούσε μια κοινή πλατφόρμα δεδομένων και τυποποίηση εγγράφων. Άλλοι τεχνολογικοί παράγοντες είχαν σχέση με τον προμηθευτή του συστήματος. Η ομάδα ανάπτυξης λογισμικού της IBM στη Σιγκαπούρη δεν είχε εμπειρία με συστήματα ηλεκτρονικής διακίνησης εγγράφων, επίσης το TradeNet αποτελείτο από πολλές εφαρμογές η ανάπτυξη των οποίων ανατέθηκε από την IBM σε τρίτες εταιρείες οι οποίες δεν είχαν εμπειρία με τα εργαλεία ανάπτυξης λογισμικού της IBM και το απαραίτητο ανθρώπινο δυναμικό για την υλοποίηση μέσα στο χρονοδιάγραμμα των 2 χρόνων.

Παράγοντες αγοράς. Δεν υπήρχε νομικό πλαίσιο για της ηλεκτρονικές συναλλαγές και υπήρχε κίνδυνος να μη γίνει αποδεκτό από την αγορά. Επίσης πολυεθνικές εταιρείες όπως η General Electric ήδη πρόσφεραν υπηρεσίες διακίνησης ηλεκτρονικών εγγράφων

παγκοσμίως , το TradeNet θα αντιμετώπιζε μεγάλο ανταγωνισμό σε περίπτωση που αυτές οι εταιρείες προωθούσαν τις υπηρεσίες τους στη Σιγκαπούρη.

5.3 Στρατηγικές διαχείρισης κινδύνου.

Θα κατηγοριοποιήσουμε τις αποφάσεις που πάρθηκαν και τις ενέργειες που εκτελέστηκαν σε 4 κατηγορίες : Προετοιμασία για την αποφυγή κινδύνου, Μετρίαση του κινδύνου, Απομόνωση του κινδύνου, Διαμερισμός του κινδύνου.

5.3.1 Προετοιμασία.

Η προετοιμασία είναι το σύνολο των αρχικών ενεργειών που πρέπει να εκτελεστούν έτσι ώστε ο οργανισμός να αποκτήσει πλεονεκτική θέση έναντι του ανταγωνισμού MacMillan(1983). Στη περίπτωση το πληροφοριακού συστήματος TradeNet μας ενδιαφέρουν οι πρώτες ενέργειες που πρέπει να ακολουθηθούν έτσι ώστε να αποκτήσει νωρίς πλεονεκτήματα έναντι του ανταγωνισμού. τα όποιο θα γίνονται αντιληπτά τόσο από τους χρήστες όσο και από τον ανταγωνισμό.

Οι ενέργειες αυτές είναι 1) η ανάδειξη του συστήματος TradeNet στο πλαίσιο της αγοράς και σε σχέση με τον ανταγωνισμό 2) Παροχή κινήτρων για την υιοθέτηση του συστήματος.

1) **Ανάδειξη του συστήματος.** Η ανάδειξη του συστήματος, έχει σαν σκοπό τη διαφοροποίηση του από άλλα διαθέσιμα παρόμοια πληροφοριακά συστήματα. αποφεύγοντας κινδύνους που προκύπτουν από οργανωτικούς παράγοντες. Αυτό επιτυγχάνεται διαμορφώνοντας τη στάση των ενδιαφερομένων ομάδων απέναντι στο σύστημα, επιτυγχάνοντας τη συμμετοχή και την πολιτική στήριξη. Αυτό επιτευχθεί ως εξής :

α) Προώθηση του συστήματος : Η SNS παρουσίασε το TradeNet σαν εθνικό έργο στρατηγικής σημασίας για τα συμφέροντα της Σιγκαπούρης, καθιερώνοντας έτσι τη σημασία του και εξασφαλίζοντας την υποστήριξη και συμμετοχή της κυβέρνησης και επιχειρηματιών

β) Κυβερνητική υποστήριξη και εξουσιοδότηση : Η αποδοχή και υποστήριξή από την κυβέρνηση παρείχε στο TradeNet την αξιοπιστία και την νομιμότητα, πείθοντας τους σκεπτικιστές για τη νομιμότητα.

γ) Καταδεικνύοντας την προσήλωση στην επιτυχή ολοκλήρωση της υλοποίησης.

2) **Παροχή κινήτρων.**

α) Διευκόλυνση της μετάβασης. Ο μεγαλύτερος κίνδυνος του TradeNet ήταν η τάση κάποιων εμπόρων να βασίζονται στις υπάρχουσες χειροκίνητες διαδικασίες. Για να ενθαρρύνουν τους εμπόρους ως προς τη χρήση του συστήματος TradeNet αυξήθηκε το κόστος επεξεργασίας εγγραφών με τον παλαιό τρόπο κατά 60% ενώ το κόστος επεξεργασίας μέσω TradeNet παρέμεινε στα ίδια επίπεδα, ο χρόνος επεξεργασίας μέσω TradeNet έπεσε στα 15 λεπτά και διεξάχθηκαν σεμινάρια εκπαιδεύοντας τους χρήστες στη χρήση το συστήματος.

β) Υιοθέτηση διεθνών προτύπων. Η υιοθέτηση του παγκόσμιου προτύπου EDIFACT παρείχε νομιμοποίηση και άνοιγε το δρόμο σε παγκόσμιες αγορές

γ) Παροχή μεγάλου εύρους υπηρεσιών για την προσέλκυση χρηστών με διαφορετικές ανάγκες και απαιτήσεις.

5.3.2 Μετρίαση του ρίσκου

Η μείωση του ρίσκου ορίζεται ως η μείωση της αβεβαιότητας που για την περίπτωση του TradeNet προκύπτει από την έλλειψη τεχνογνωσίας και πληροφοριών σε σχέση με το σύστημα. Για να

αντιμετωπιστούν τα παραπάνω υπήρξε σχέδιο αναζήτησης πληροφορίων και πρόσληψη ατόμων με τεχνογνωσία.

Επίσης για τη μείωση του ρίσκου δημιουργήθηκαν διαδικασίες ελέγχου και επιρροής των ατόμων που αποτελούσαν την ομάδα ανάπτυξης. Οι διαδικασίες αυτές είναι μέρος της Διαχείρισης ανάπτυξης έργου που θα αναλύσουμε παρακάτω.

1. **Σχέδιο αναζήτησης πληροφοριών.** Οι πληροφορίες σχετικά με τα συστήματα ηλεκτρονικής διακίνησης εγγράφων αναζητήθηκαν σε τρίτους οργανισμούς. Για αυτό το λόγο πραγματοποιήθηκε ένας μεγάλος αριθμός ταξιδιών στο εξωτερικό σε πάροχους υπηρεσιών που ήδη χρησιμοποιούσαν παρόμοια συστήματα, από μέλη της ομάδας ανάπτυξης έργου. Αυτό είχε σαν αποτέλεσμα την αντιμετώπιση των κινδύνων που προέκυπταν από την έλλειψη εμπειρίας και τεχνογνωσίας.
2. **Προσλήψεις ατόμων με τεχνογνωσία.** Η πρόσληψη ατόμων με εμπειρία σε συστήματα ηλεκτρονικής διακίνησης εγγράφων ήταν μια άλλη κίνηση αντιμετώπισης της έλλειψης τεχνογνωσίας. Η IBM έστειλε πολλούς από τους μηχανικούς της για εκπαίδευση στην Ιαπωνία ενώ προσέλαβε άτομα με διεθνή εμπειρία σε παρόμοια συστήματα για να συμπληρώσουν διευθυντικές θέσεις.
3. **Διαχείριση ανάπτυξης έργου**

   α) Επιλογή προμηθευτών. Καθώς το χρονοδιάγραμμα ανάπτυξης του συστήματος ήταν δύο χρόνια, αποφασίστηκε ο πυρήνας/κύριο μέρος της εφαρμογής να αγοραστεί έτοιμός και μόνο τα τμήματα που είχαν σχέση με το εμπορικό πλαίσιο της Σιγκαπούρης να αναπτυχθούν από την αρχή. Ο προμηθευτής του πυρήνα του συστήματος ηλεκτρονικής διακίνησης εγγράφων ήταν η IBM, ενώ για την ανάπτυξη των περιφερειακών ως προς τον πυρήνα εφαρμογών επιλέχτηκαν 4 εταιρείες λογισμικού με εμπειρία σε παρόμοια έργα. Η SNS παρείχε τις απαιτήσεις και την τεχνική βοήθεια σε αυτές τις εταιρείες καθ' όλη τη διάρκεια ανάπτυξης των εφαρμογών.

β)Διαδικασίες ελέγχου. Για να εξασφαλιστεί πως το σύστημα θα υλοποιηθεί εγκαίρως και μέσα στις προδιαγραφές, ακολουθήθηκαν πιστά συγκεκριμένες διαδικασίες ελέγχου σε τομείς όπως προϋπολογισμός έργου, διαδικασίες που σχετίζονταν με τις αλλαγές στις απαιτήσεις οι οποίες αξιολογούνταν ως προς το κόστος και τον επιπλέον χρόνο και διαδικασίες ελέγχου ποιότητας. Ειδικά για τις τελευταίες η SNS υιοθέτησε τις διαδικασίες ελέγχου ποιότητας της IBM εξοικονομώντας χρόνο άλλα και μειώνοντας το ρίσκο που προέκυπτε από τη χρήση ακατάλληλων διαδικασιών.

5.3.3 Απομόνωση του κινδύνου

Η απομόνωση του κινδύνου αποσκοπεί στον περιορισμό των επιπτώσεων μιας πιθανής αποτυχίας σε ένα συγκεκριμένο μέρος του συστήματος, μειώνοντας έτσι τις επιπτώσεις στην γενική απόδοση αυτού.

Στο σύστημα TradeNet η απομόνωση του κινδύνου επιτεύχθει με την οριοθέτηση και την εκχώρηση των τμημάτων του έργου σε συγκεκριμένα άτομα ή ομάδες. Αυτό είχε σαν αποτέλεσμα τον καλύτερο έλεγχο , διαμερισμό ευθυνών και γρήγορη επίλυση προβλημάτων.

1. **Διαχωρισμός έργου.** Το χρονοδιάγραμμα υλοποίησης του TradeNet διαχωρίστηκε σε 4 φάσεις με διαφορετικές ημερομηνίες υλοποίησης η κάθε μία. Ο διαχωρισμός του έργου σε φάσεις είναι μια τακτική που ακολουθείται σε μεγάλα έργα με πολλούς εμπλεκόμενους και πολύπλοκες διαδικασίες, και σαν σκοπό έχει την καλύτερη διαχείριση και ανάθεση του έργου.

   Με το διαχωρισμό σε φάσεις κάθε ομάδα είχε να πετύχει πιο σαφείς στόχους, σε πιο τακτά διαστήματα και μπορούσε να επικεντρωθεί στην αναγνώριση και επίλυση προβλημάτων στο πλαίσιο της εκάστοτε φάσης.
2. **Αναλογισμός ευθυνών.** Αμέσως μετά τον διαχωρισμό σε φάσεις ομάδες όπως η IBM ανέλαβαν την ευθύνη για την υλοποίηση των κομματιών που αντιστοιχούσαν σε κάθε φάση.

3. **Εμφάνιση προβλημάτων.** Μια άλλη τακτική απομόνωσης κινδύνου είχε στόχο τα προβλήματα που εμφανίζονταν και την επίλυση τους πριν αυτά επιδράσουν άλλα μέρη του συστήματος. Με το που εμφανιζόντουσαν προβλήματα και περιοριζόντουσαν οι ομάδες επικεντρωνόντουσαν στη επίλυση και έλεγχο της αρνητικής επίδρασης. Σε συναντήσεις που πραγματοποιούταν ανά εβδομάδα μεταξύ των εταιρειών κατά τη φάση της ανάπτυξης, υπήρχε αξιολόγηση των προβλημάτων σε σχέση με το εύρος της επίδρασης, το κόστος, το χρόνο επίλυσης αυτών και αποφασίζανε τους τρόπους επίλυσης αυτών.

   Τέλος τα δοκιμαστικά τεστ είχαν σαν σκοπό την έγκαιρη ανάδειξη προβλημάτων προς επίλυση.

5.3.4 Διαμερισμός του κινδύνου

Ο διαμερισμός του κινδύνου πραγματοποιήθηκε μεταξύ ομάδων και οργανισμών που είχαν συμφέρον ως προς τη σωστή λειτουργία του TradeNet επιτυγχάνοντας πρόσβαση στους πόρους αυτών αλλά και την άμεση υποστήριξη. Τα παραπάνω επιτεύχθηκαν με τη συνεργασία άλλων οργανισμών , διορισμός και συνεργασία ατόμων με επιρροή , και σύνδεση με άλλα συστήματα.

1. **Συνεργασία με άλλους οργανισμούς**. Στρατηγικές συνεργασίες επιτεύχθηκαν μεταξύ κυβερνητικών οργανισμών όπως της Επιτροπής Εμπορικής Ανάπτυξης (ΕΕΑ) και της Εθνικής Επιτροπή Πληροφοριακών Συστημάτων (ΕΕΠΣ) που ανέλαβαν από κοινού ευθύνη για το TradeNet . Επίσης το SNS άνηκε σε 4 επιτροπές όπως επιτροπή τηλεπικοινωνιών και επιτροπή εμπορίου.
2. **Διορισμός ατόμων με επιρροή** . Ο διορισμός ατόμων επιρροής από τον επιχειρηματικό αλλά και τον κυβερνητικό τομέα ως μέλη επιτροπής ή διευθυντικά στελέχη.
3. **Σύνδεση με άλλα συστήματα**. Η σύνδεση με άλλα συστήματα παρείχε στο TradeNet τη δυνατότητα πρόσβασης από χρήστες άλλων

συστημάτων ηλεκτρονικής διακίνησης εγγράφων μειώνοντας έτσι τον κίνδυνο από τον ανταγωνισμό. Και αυτό επειδή πλέον χρήστες του TradeNet δεν είχαν λόγο η κίνητρο να χρησιμοποιούν ανταγωνιστικά συστήματα.

5.4 Αξιολόγηση : Ήταν το TradeNet επιτυχές ;

Η αξιολόγηση θα γίνει ως προς της εξής κατηγορίες :

1. Διαχείριση έργου : Τηρήθηκαν τα χρονοδιαγράμματα και ο προϋπολογισμός ;
2. Επιδόσεις συστήματος : Πέτυχε τους αντικειμενικούς στόχους της ταχείας επεξεργασίας εγγράφων. Ήταν επικερδές ;
3. Υιοθέτηση από χρήστες : Πόσο γρήγορα υιοθετήθηκε το TradeNet από τους χρήστες ;
4. Οργανισμοί : Επωφελήθηκαν οι χρήστες από τη χρήση το TradeNet ;
5. Διάδοση : Πως το TradeNet επηρέασε την έλευση άλλων συστημάτων ηλεκτρονικής διακίνησης εγγράφων ;

1. Διαχείριση έργου

Η SNS επεξεργάστηκε το πρώτο έγγραφο μέσω TradeNet τον Ιανουάριο του 1989 και τηρώντας το χρονοδιάγραμμα. Οι χρήστες είχαν πρόσβαση στο σύστημα τον Φεβρουάριο του ίδιου έτους. Μπορούμε να θεωρήσουμε ότι έστω και πιλοτικά λειτούργησε μέσα στο χρονοδιάγραμμα.

Δεν υπήρξαν μεταβολές στον προϋπολογισμό που ουσιαστικά ήταν το κόστος του συμβολαίου με την IBM. Βέβαια κάποιες αλλαγές στις απαιτήσεις που προτάθηκαν από τους πιλοτικούς χρήστες η υλοποίηση των οποίων επηρέαζε αυξητικά το κόστος, δεν υλοποιήθηκαν

2. Επιδόσεις συστήματος

Το 97% των εγγράφων που επεξεργάστηκαν μεσώ TradeNet εγκρίθηκαν μέσα σε 15’ από τη στιγμή της υποβολής. Αναλογικά ο χρόνος επεξεργασίας με τον προηγούμενο τρόπο των χάρτινων εγγράφων ήταν 2 ημέρες. Το κόστος επεξεργασίας των εμπορικών εγγράφων μέσω TradeNet ήταν 6$/έγγραφο. Τα κέρδη της SNS αυξανόντουσαν 50% ανά έτος και το σύστημα είχε απόσβεση το 2ό χρόνο 3 χρόνια πιο νωρίς από ότι αναμενόταν

3. Υιοθέτηση από χρήστες

Η υιοθέτηση του TradeNet από χρήστες εμπορικών εταιρειών ξεπέρασε της υψηλές προσδοκίες της SNS. Ο στόχος για το πρώτο έτος ήταν 15% των χρηστών να μεταβούν στο TradeNet και το πραγματικό ήταν 45%, ενώ για το δεύτερό έτος ο στόχος ήταν 40% και το πραγματικό ποσοστό 92%

4. Οργανισμοί

Κάποιες εμπορικές εταιρείες ανέφεραν 20% έως 30% μείωση εργατικού δυναμικού και κόστους αποθήκευσης. Άλλες εταιρείες παραπονέθηκαν την αύξηση κόστους λόγο αγοράς υλικού μηχανογράφησης απαραίτητου για την υιοθέτηση του TradeNet . Οι περισσότερες εταιρείες αναγνώρισαν τα οφέλη του TradeNet, αλλά τα οφέλη σε κερδοφορία ήταν αμελητέα.

Οι επιδράσεις που είχε το TradeNet στην Επιτροπή Εμπορικής Ανάπτυξης (ΕΕΑ) ήταν πιο δραματικές. Μέχρι το τέλος του 1992 το προσωπικό στα τμήματα που σχετίζονταν με τα έγγραφα μειώθηκε από 134 σε 88 και ο χώρος μειώθηκε από 1390 τ.μ. σε 985 τ.μ.

5. **Διάδοση**

Η SNS συνέχισε με την υλοποίηση νέων υπηρεσιών που βασίζονταν στον πυρήνα ηλεκτρονικής διακίνησης εγγράφων ανταποκρινόμενη στις ποίκιλες ανάγκες άλλων βιομηχανικών τομέων. Παραδείγματα τέτοιων υπηρεσιών είναι το MediNet για τον τομέα υγείας, το LawNet για τον τομέα της δικαιοσύνης και ένα σύνολο υπηρεσιών που επιτρέπουν τη διασύνδεση κατασκευαστών , προμηθευτών , πωλητών και οικονομικών οργανισμών. Για παράδειγμα τα νοσοκομεία μπορούσαν να στείλουν τους λογαριασμούς των ασφαλισμένων ασθενών ηλεκτρονικά στο κράτος μέσω MediNet προς πληρωμή. Κατασκευαστές και πωλητές μπορούσαν να συναλλάσσονται ηλεκτρονικά αποστέλλοντας παραγγελίες , παραστατικά , τιμολόγια ακόμα και πληρωμές ηλεκτρόνια μέσω τραπεζών,

Μπορούμε να συμπεράνουμε με βάση την αξιολόγηση στις παραπάνω 5 κατηγορίες πως η ανάπτυξη και η υλοποίηση του συστήματος TradeNet ήταν επιτυχής. Στη Σιγκαπούρη η ηλεκτρονική διακίνηση εγγράφων δεν είναι αποκλειστικά συνδεδεμένη με εμπορικά έγγραφα. Είναι μια τεχνολογία που χρησιμοποιείται σε όλους τους τομείς συναλλαγών και είναι εναρμονισμένη με την επιχειρηματική δραστηριότητα στη Σιγκαπούρη.

5.5 Συμπεράσματα

Εξετάζοντας τα αίτια των κινδύνων του έργου και τα βήματα που πρέπει να ακολουθηθούν για να αποφευχθούν οι κίνδυνοι μπορούν να εξαχθούν συμπεράσματα ως προς τη βιωσιμότητα του έργου πριν γίνουν οι χρηματικές επενδύσεις. Οι στρατηγικές διαχείρισης ρίσκου που παρουσιάστηκαν σε αυτό το κεφάλαιο μπορούν να επιφέρουν μείωση του κινδύνου αποτυχίας. Η διαχείριση κινδύνου θα πρέπει να λαμβάνει υπόψιν περιβαντολογικούς και οργανωτικούς παράγοντες. Επίσης στρατηγικές διαχείρισης κινδύνων που σχετίζονται με πολιτικούς παράγοντες μπορούν να αποφέρουν υποστήριξη από την πολιτική ηγεσία και συνεπώς

αναγνωρισιμότητα ενώ ανάλυση κινδύνων που προκύπτουν από την κατάσταση της αγοράς αποφέρουν κρίσιμα συμπεράσματα σε σχέση με τον ανταγωνισμο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Alberts C., Dorofee A., Stevens J. and Woody C., Introduction to the OCTAVE Approach (pdf), CERT, August 2003 βhttp://www.cert.org/octave/approach_intro.pdf
2. Artech House Publishers; 1st edition
3. Baker, K and Baker S.(2000), *Project Management*, Alfa Books
4. Canavan, J., (2001). The Fundamentals of Network Security, Publisher:
5. CISSP.(2010), *Information Security and Risk Management*, Course Technology
6. Durbin A., Essentials of Marketing , 14th edition , South – Western College Publishing 1997 , pp., 411-437.
7. Elky, S.(2006),An Introduction to Information System Risk Management,SANS
8. Fairley, R.(1994), Risk Management For Software Projects, IEEE
9. Gabel P.E.(2010), *Project Risk Management Guide Comment*, WSDOT
10. Lientz P.B and Larsen L.(2006), *Risk Management for IT Projects How to Deal with Over 150 Issues and Risks*, Elsevier
11. Longstaff, T.A et al.(2000), *Are We Forgetting the Risks of Information Technology?*, University of Virginia
12. Meritt, J.W.(2010), *Risk management*, Wang Global
13. MacMillan, I.C.(Fall of 1983) *Preemtive Strategies*, Journal of Business Strategies
14. Slack N., Chambers S., and Johnston R., (2004). *Operations. Management*, (4th edition), FT Prentice Hall, Harlow
15. Slack N., Chambers S., and Johnston R., (2004). *Operations. Management*, (4th edition), FT Prentice Hall, Harlow
16. Teeples, J.(2009), *Risk Management*, Renton Washington.The Journal of Computing in Small Colleges (JCSC), Vol.18, No.6, pp.57-66

17. Turn R., (1986). Security and Privacy requirements in computing, Proceedings of 1986 ACM Fall joint computer conference, pp. 1106 – 1114.
18. Wallmuller, E.(2010), *Risk Management for IT and Software Projects,* Zürich Qualität und Informatik
19. Wallmuller, E.(2010), *Risk Management for IT and Software Projects,* Zürich Qualität und Informatik
20. Whitson G., (2003). Computer security: theory, process and management,
21. Yazar, Z.(2002), A qualitative risk analysis and management tool – CRAMM, SANS.
22. Yazar, Z.(2002), *A qualitative risk analysis and management tool – CRAMM*, SANS.
23. Yazar, Z.(2002), *A qualitative risk analysis and management tool – CRAMM*, SANS.
24. Βασιλακόπουλος Γ. – Χρυσικόπουλος Β.,(2004),Πληροφοριακά συστήματα διοίκησης. Ανάλυση και σχεδιασμός, Σταμούλης
25. Δημητριάδης Α.,(1996),Διοίκηση-διαχείριση πληροφοριακών συστημάτων», Εκδόσεις Νέων Τεχνολογιών
26. Κατσίκας Σ., Risk Analysis and Risk Management: Capabilities and Limitations
27. Κάτσικας, Σ.Κ.(2010), *Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων*, Πανεπιστήμιο Πειραιώς.
28. Λαοπόδης Γ.,(2006),Ανάλυση και σχεδιασμός συστημάτων. Ανάπτυξη πληροφοριακών συστημάτων», Εκδόσεις Νέων Τεχνολογιών
29. Οικονόμου Σ. Γ.– Γεωργόπουλος Β. Ν.,(2000),Πληροφοριακά συστήματα για τη διοίκηση επιχειρήσεων. Διοίκηση, πληροφορία, σύστημα, Μπένος
30. Πάγκαλος Γ. και Μαυρίδης Ι., Ασφάλεια Πληροφοριακών συστημάτων, ΑΝΙΚΟΥΛΑ
31. Τασόπουλος Α.(2005),Πληροφοριακά συστήματα. Οργάνωση, μεθοδολογία, εφαρμογές, Σταμούλης
32. Τασόπουλος Α.(2005),Πληροφοριακά συστήματα. Οργάνωση, μεθοδολογία, εφαρμογές, Σταμούλης

33. Φωλίνας Δ.,(2006),Ολοκληρωμένα πληροφοριακά συστήματα διαχείρισης επιχειρηματικών πόρων, Εκδόσεις Ανίκουλα, Αθήνα 2006

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Α

ΠΡΟΒΛΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Στην δεκαετία του ’80, όταν τα πληροφοριακά συστήματα άρχισαν σιγά σιγά να διεισδύουν στις μεσαίες και μεγάλες επιχειρήσεις, οι άνθρωποι που ήξεραν να τα χειρίζονται ήταν λίγοι και εξειδικευμένοι. Τα φαινόμενα παραβίασης της ασφάλειας ήταν σχεδόν ανύπαρκτα. Κατά την διάρκεια της δεκαετίας του ’90 και μέχρι σήμερα, οι νέες τεχνολογίες οδήγησαν σε ευρεία χρήση των ηλεκτρονικών υπολογιστών με αποτέλεσμα ο αριθμός των παραβιάσεων ασφαλείας να ακολουθεί μια συνεχή εκθετική αύξηση.

Παρακάτω φαίνονται τα κρούσματα παραβίασης ασφάλειας που καταγράφηκαν από τον διεθνή οργανισμό CERT κατά την διάρκεια των ετών 1988-2003:

Παράλληλα, η ταχύτητα ανάπτυξης της επιστήμης της πληροφορικής αναγκάζει τις εταιρίες ανάπτυξης λογισμικού και προϊόντων πληροφορικής να βγάζουν προϊόντα στην αγορά στον ελάχιστο δυνατό χρόνο ώστε να προλαβαίνουν τις τελευταίες εξελίξεις στον χώρο. Λόγω της πίεσης χρόνου, τα προϊόντα αυτά περιέχουν πολλά σφάλματα στην υλοποίηση τους (bugs).

Επίσης, τις περισσότερες φορές οι εταιρίες δεν υπολογίζουν καν τα θέματα ασφαλείας με αποτέλεσμα τα προϊόντα που παράγουν να μην παρέχουν καμία απολύτως λειτουργία ασφάλειας[1].

Παρόμοια σφάλματα όμως κάνουν και οι εταιρίες που χρησιμοποιούν τα υπολογιστικά συστήματα για την εσωτερική τους λειτουργία. Για λόγους κόστους, χρόνου αλλά και άγνοιας σε θέματα ασφαλείας, παραβλέπουν την ασφάλεια κατά την εγκατάσταση νέων

[1] Lientz P.B and Larsen L.(2006), *Risk Management for IT Projects How to Deal with Over 150 Issues and Risks*, Elsevier

υπολογιστικών συστημάτων και κατά την λειτουργία τους. Έτσι αφήνουν τα συστήματα τους ευπαθή σε διάφορους τύπους επιθέσεων.

Παρακάτω φαίνονται οι ευπάθειες που αναφέρθηκαν σε συστήματα και καταγράφηκαν από τον διεθνή οργανισμό CERT κατά την διάρκεια των ετών 1995-2003:

Σημείωση: Τα νούμερα από τις δύο παραπάνω καταγραφές δεν είναι παρά μόνο δείγμα των συνολικών κρουσμάτων και θα πρέπει να χρησιμοποιούνται για να δούμε τις τάσεις και όχι σαν απόλυτα νούμερα.

ΟΙΚΟΝΟΜΙΚΕΣ ΑΠΩΛΕΙΕΣ

Οι οικονομικές απώλειες που οφείλονται σε προβλήματα ασφαλείας πληροφοριακών συστημάτων είναι πολύ μεγάλες και σημειώνουν αυξητικό χαρακτήρα κατά τα τελευταία χρόνια. Οι απώλειες μπορεί να οφείλονται σε απάτη με σκοπό το κέρδος, σε κακόβουλες πράξεις που αποσκοπούν την ζημίωση ή και σε τυχαία γεγονότα όπως για παράδειγμα η καταστροφή δεδομένων από ιούς. Τα αποτελέσματα μπορεί να είναι καταστροφικά και στις

τρεις περιπτώσεις.

Σε έρευνα που έγινε στις ΗΠΑ το 2002 από το Computer Security Institute (CSI) με την συνεργασία του FBI και με συμμετοχή 503 ειδικών ασφαλείας από εταιρίες, κρατικούς οργανισμούς, οικονομικούς οργανισμούς, νοσοκομεία και πανεπιστήμια, το 80% των ερωτηθέντων αναγνώρισαν οικονομικές απώλειες λόγω προβλημάτων ασφαλείας. Οι 223 από αυτούς μπόρεσαν να υπολογίσουν τις απώλειες που ανήλθαν σε $455,848,000. Οι μεγαλύτερες οικονομικές απώλειες προήλθαν από κλοπή ιδιωτικών δεδομένων ($170,827,000) και από οικονομική απάτη ($115,753,000). Σε παρόμοια έρευνα που έγινε το 2003 παρατηρήθηκε σημαντική μείωση των απωλειών σε $201,797,340, αλλά ο αριθμός των

παραβιάσεων παρέμεινε ο ίδιος[2].

Στις ίδιες έρευνες αποκαλύφθηκε ότι οι επιθέσεις προέρχονται και από το εσωτερικό της επιχείρησης αλλά και από το Internet. Παρ' όλα αυτά, για 4η χρονιά στη σειρά, το μεγαλύτερο μέρος των ερωτηθέντων (73%) αναφέρει το Internet σαν συχνό σημείο επίθεσης παρά τα εσωτερικά τους συστήματα (36%).

Βέβαια όλα τα παραπάνω στοιχεία είναι μόνο ένα μικρό κομμάτι των απωλειών παγκοσμίως. Ειδικοί αναλυτές για θέματα ασφαλείας υπολογίζουν τις απώλειες σε παγκόσμιο επίπεδο σε πολλά δισεκατομμύρια δολάρια ετησίως. Αξίζει να αναφερθεί ότι ο ιός Mydoom που εμφανίστηκε πρόσφατα υπολογίζετε ότι κόστισε συνολικά γύρω στα 38 δισεκατομμύρια δολάρια, συμπεριλαμβάνοντας τις απώλειες από αδυναμία λειτουργίας, μείωση παραγωγικότητας, συμφόρηση δικτύων, κόστος επαναφοράς και αναβαθμίσεις λογισμικού.

Το μέγεθος των απωλειών είναι αρκετά μεγάλο ώστε να καταστρέψει ολόκληρες εταιρίες και οργανισμούς ή να θέσει εκτός ανταγωνισμού όσους αρνούνται να δουν τα θέματα ασφαλείας των υπολογιστικών συστημάτων ως σημαντικό ρίσκο της λειτουργίας ενός οργανισμού.

ΑΝΤΙΜΕΤΩΠΙΣΗ

Η αντιμετώπιση των προβλημάτων ασφαλείας, παρότι δεν είναι απλή υπόθεση, πρέπει να λαμβάνεται σοβαρά υπόψη. Η εισαγωγή πληροφοριακών συστημάτων σε ένα περιβάλλον μπορεί μεν να αυξάνει κατακόρυφα την παραγωγικότητα και το κέρδος, αλλά εισάγει νέους κινδύνους που αυξάνουν σημαντικά το ρίσκο και επομένως πρέπει

[2] Κάτσικας, Σ.Κ.(2010), *Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων*, Πανεπιστήμιο Πειραιώς.

οπωσδήποτε να αναγνωριστούν και να αντιμετωπιστούν ανάλογα[3].

Ο κλάδος της ασφάλειας πληροφοριακών συστημάτων έχει να προσφέρει ευτυχώς μια πληθώρα από αντίμετρα (εργαλεία, μεθόδους, έλεγχους, πολιτικές ασφαλείας) για την αντιμετώπιση κάθε είδους προβλήματος. Η ενσωμάτωση όμως όλων αυτών σε κάθε οργανισμό δεν είναι καθόλου απλή υπόθεση. Αντιθέτως, ο διαφορετικός τρόπος λειτουργίας καθώς και η διαφορετική ανάθεση πόρων για θέματα ασφαλείας δημιουργούν εντελώς διαφορετικές συνθήκες, μοναδικές για κάθε οργανισμό. Η ενσωμάτωση της ασφάλειας λοιπόν δεν πρέπει να θεωρηθεί ως μια απλή διαδικασία, καθώς πρέπει κάθε φορά να λαμβάνονται υπόψη όλοι οι παράγοντες ώστε η ασφάλεια να μην γίνετε εμπόδιο στην λειτουργία του οργανισμού αλλά να τον υπηρετεί.

Λύση στο πρόβλημα αυτό δίνει η ανάλυση κινδύνων (risk analysis). Η ανάλυση κινδύνων έχει ως σκοπό την αξιολόγηση των περιουσιακών στοιχείων του οργανισμού και την αναγνώριση όλων των κινδύνων και των ευπαθειών που τα απειλούν. Θα πρέπει στο σημείο αυτό να αναφερθεί ότι με τον όρο «περιουσιακά στοιχεία» δεν εννοούνται μόνο τα καθαρά οικονομικά μεγέθη. Αντιθέτως, συμπεριλαμβάνονται και αξίες όπως προσωπικά δεδομένα, στοιχεία που η παραβίαση τους μπορεί να οδηγήσει στην απώλεια ανθρώπινης ζωής, η εικόνα ενός οργανισμού προς τα έξω κτλ. Με τα δεδομένα αυτά υπολογίζεται το ρίσκο που εισάγει η χρήση κάθε πληροφοριακού συστήματος στην λειτουργία του οργανισμού. Έτσι, μπορούν να υπολογιστούν με ικανοποιητική ακρίβεια ποια αντίμετρα συμφέρει να εγκατασταθούν και σε ποιες περιπτώσεις είναι προτιμότερη η αποδοχή του ρίσκου.

Επιπρόσθετα, η ανάλυση κινδύνων θέτει προτεραιότητες στα αντίμετρα που μπορούν να εγκατασταθούν, με αποτέλεσμα να μπορεί να γίνει μια πιο ορθή επιλογή στις περιπτώσεις που ο προϋπολογισμός δεν επιτρέπει αρκετούς πόρους ώστε να καλυφθούν όλες οι ανάγκες για

[3] Elky, S.(2006),An Introduction to Information System Risk Management,SANS

θέματα ασφαλείας. Ιδιαίτερα σήμερα που η παγκόσμια οικονομία βρίσκεται σε ύφεση και οι περισσότερες επιχειρήσεις και οργανισμοί αναγκάζονται να κάνουν περικοπές σε όλους τους τομείς, η ανάλυση κινδύνων έρχεται να παίξει ουσιαστικό ρόλο στην σωστή αντιμετώπιση των προβλημάτων ασφαλείας με οργανωμένο και αποτελεσματικό τρόπο.