ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»
ΚΑΤΕΥΘΥΝΣΗ: ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΚΙΝΔΥΝΩΝ ΕΡΓΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ: ΘΕΩΡΙΑ ΚΑΙ ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ

ΠΑΠΟΥΤΣΗ ΑΙΚΑΤΕΡΙΝΗ ΜΤΕ/1023
ΕΠΙΒΛΕΠΟΥΣΑ: ΜΑΛΑΜΑΤΕΝΙΟΥ ΦΛΩΡΑ

ΠΕΙΡΑΙΑΣ, ΔΕΚΕΜΒΡΙΟΣ 2013

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά την καθηγήτριά μου και επιβλέπουσα της παρούσας μεταπτυχιακής διατριβής κ. Φλώρα Μαλαματένιου, όχι μόνο για την εμπιστοσύνη που μου έδειξε, αλλά και για την καθοδήγηση, την υποστήριξη και τη βοήθειά της καθ' όλη τη διάρκεια διεκπεραίωσης της μεταπτυχιακής μου διατριβής.

Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στη μητέρα μου, που όλα αυτά τα χρόνια μου συμπαραστέκεται ηθικά και οικονομικά και διαμορφώνει γύρω μου ένα άνετο περιβάλλον, μέσα στο οποίο μπορώ να εργαστώ και να επεκτείνω τις γνώσεις μου.

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Τα έργα πληροφορικής, κυρίως μεγάλου μεγέθους και πολυπλοκότητας, εμπεριέχουν ποικίλους κινδύνους που απειλούν την επιτυχία της εφαρμογής τους. Καθώς οι περισσότεροι οργανισμοί βασίζουν πλέον ένα μεγάλο μέρος της λειτουργίας τους σε πληροφοριακά συστήματα, η ανάγκη για κατάλληλη ασφάλεια αυξάνεται. Δυστυχώς, είναι δύσκολο να γίνει επιλογή των μέτρων ασφάλειας που χρειάζονται για να επιτευχθεί ικανοποιητική ασφάλεια. Η παρούσα διπλωματική εργασία ασχολείται με την ανάλυση και διαχείριση κινδύνων, μια διαδικασία που αναγνωρίζει τα προβλήματα ασφάλειας, τα ταξινομεί με βάση τη σημαντικότητά τους και, τέλος, προτείνει λύσεις για την αντιμετώπισή τους.

Στόχος της εργασίας είναι η ανάλυση των κινδύνων που υπεισέρχονται στην ανάπτυξη και υλοποίηση ενός πληροφοριακού συστήματος και των μεθόδων προσδιορισμού και διαχείρισης κινδύνων. Σκοπεύει, ουσιαστικά, σε μια συστηματική βιβλιογραφική ανασκόπηση και συγκριτική παρουσίαση των μεθόδων που αναφέρθηκαν προηγουμένως. Θα μπορούσαμε, ακόμα, να πούμε ότι απώτερο στόχο αποτελεί και η σύγκριση της ακαδημαϊκής υπόστασης της ανάλυσης και διαχείρισης κινδύνων σε σχέση με το τι συμβαίνει στην πραγματικότητα στην αγορά.

Επίσης, παρουσιάζεται μια μελέτη περίπτωσης που αφορά την ανάλυση και διαχείριση κινδύνων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) μιας τσέχικης εταιρείας.

Η παρούσα διπλωματική εργασία, λοιπόν, αναπτύχθηκε σε πέντε κεφάλαια ως εξής:

- Το κεφάλαιο 1 ασχολείται με τον εισαγωγικό ορισμό του θέματος.
- Στο κεφάλαιο 2 περιγράφεται το γενικό μεθοδολογικό πλαίσιο για τον προσδιορισμό κινδύνων έργων πληροφοριακών συστημάτων.
- Το κεφάλαιο 3 πραγματεύεται το θεωρητικό υπόβαθρο της ανάλυσης κινδύνων σε έργα πληροφοριακών συστημάτων.
- Στο κεφάλαιο 4 επιδεικνύεται μια θεωρητική προσέγγιση της διαχείρισης κινδύνων σε έργα πληροφοριακών συστημάτων.
- Στο κεφάλαιο 5 αναφέρεται μία πρακτική εφαρμογή ανάλυσης και διαχείρισης κινδύνων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) μιας τσέχικης εταιρείας με τη μέθοδο CRAMM και το ανάλογο λογισμικό.
- Στο κεφάλαιο 6 παρουσιάζονται τα συνολικά συμπεράσματα και προτάσεις για περαιτέρω μελέτη.

ABSTRACT

Information Technology (IT) projects, especially those of large size and complexity, involve a variety of risks that threaten the success of their application. While most organizations now base a large part of their operation on information systems, the need for adequate security increases. Unfortunately, it is difficult to select the security measures needed to achieve satisfactory security. This thesis deals with the analysis and management of risks, a process that recognizes the security problems, sorts them based on their importance and, finally, proposes solutions to confront them.

The aim of this paper is to analyze the risks involved in the development and implementation of an information system and the methods of identification and risk management. It targets, essentially, in a systematic literature review and comparative presentation of the methods mentioned above. It might, even, be said that an ultimate goal is the comparison of the academic status of risk analysis and management in relation to what is actually happening in the market.

In addition, a case study is presented, which relates to the risk analysis and management of Information Security Management System (ISMS) of a czech company.

This master thesis, therefore, developed in five chapters as follows:

- Chapter 1 deals with the introductory definition of the subject.
- In chapter 2 the general methodological framework for identifying risks of information systems projects is described.
- Chapter 3 handles with the theoretical background of the risk analysis in information systems projects.
- In chapter 4 a theoretical approach of risk management in information systems projects is demonstrated.
- Chapter 5 refers to a practical application of risk analysis and management of Information Security Management System (ISMS) of a czech company using the CRAMM method and associated software.
- In Chapter 6 the overall conclusions and recommendations for further study are presented.

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Οι αποτυχίες σε έργα πληροφοριακών συστημάτων είναι ο εφιάλτης της εποχής της πληροφορίας. Τεράστιες ποσότητες πόρων ξοδεύονται σε όλες τις σχετικές βιομηχανίες, με σκοπό την καταπολέμηση αυτού του εφιάλτη. Παρ' όλ' αυτά, τελικά είναι αδύνατο να υπάρξει εγγύηση ότι το έργο θα είναι τέλειο, όπως είναι, επίσης, αδύνατο να προβλεφθεί και να εξαλειφθεί κάθε τι από τον εξωτερικό κόσμο που πιθανόν να απειλήσει το έργο όσο αυτό εκτελείται.

Εκείνο, όμως, που μπορεί να επιτευχθεί είναι η μείωση της πιθανότητας αποτυχίας ενός έργου, η οποία θα επιφέρει και ελάττωση της αβεβαιότητας που υπάρχει σε αυτό. Προϋπόθεση για την επίτευξη αυτής της ελάττωσης αποτελεί η εφαρμογή κατάλληλης ανάλυσης και διαχείρισης κινδύνων καθ' όλη τη διάρκεια ανάπτυξης του έργου.

Άλλωστε, η επικινδυνότητα και η διαχείριση αυτής έχουν αναδειχτεί σε θέματα μεγάλου ενδιαφέροντος, ιδιαίτερα μάλιστα κατά τη διάρκεια των τελευταίων ετών όπου έχουν προκύψει νέες προοπτικές και ευκαιρίες, ενώ παράλληλα έχει οξυνθεί και ο ανταγωνισμός στην αγορά.

Οι διάφορες προσεγγίσεις που έχουν κατά καιρούς αναπτυχθεί και εφαρμόζονται εξετάζουν το θέμα της ανάλυση και διαχείρισης κινδύνων κατά τη διάρκεια όλων των φάσεων του κύκλου ζωής του έργου, χωρίς καμία ιδιαίτερη εστίαση σε κάποια συγκεκριμένη φάση. Αυτή η άποψη περί εφαρμογής της ανάλυσης και διαχείρισης κινδύνων από τη στιγμή που ξεκινά να αναπτύσσεται το έργο έως τη στιγμή που παραδίδεται και συντηρείται είναι απόλυτα ορθή και δικαιολογημένη, διότι σε διαφορετική περίπτωση δε θα μπορούσε να επιτευχθεί επαρκής αναγνώριση και αποτελεσματική αντιμετώπιση των διαφόρων κινδύνων που απειλούν το εκάστοτε έργο πληροφοριακού συστήματος.

Ο βασικός στόχος της ασφάλειας των πληροφοριακών συστημάτων είναι η στήριξη της αποστολής του οργανισμού. Όλοι οι οργανισμοί εκτίθενται σε αβεβαιότητες, μερικές από τις οποίες έχουν αντίκτυπο στην οργάνωση με έναν αρνητικό τρόπο. Για να υποστηρίξουν την οργάνωση οι επαγγελματίες της ασφάλειας, πρέπει να είναι σε θέση να βοηθήσουν τη διαχείριση των οργανισμών τους με το να κατανοήσουν και να διαχειριστούν αυτές τις αβεβαιότητες.

Ο κύριος λόγος για την ανάλυση και διαχείριση κινδύνων σε μια εταιρεία είναι να προστατευτεί η αποστολή και τα περιουσιακά στοιχεία της. Ως εκ τούτου, πρέπει να είναι μια λειτουργία διαχείρισης και όχι τεχνική, καθώς πρόκειται για μια ζωτικής σημασίας λειτουργία για ένα έργο. Είναι γεγονός ότι όλοι οι οργανισμοί έχουν περιορισμένους πόρους και, όπως ήδη έχει αναφερθεί, ο κίνδυνος δε μπορεί ποτέ να μειωθεί στο μηδέν. Έτσι, η κατανόηση των κινδύνων, ιδίως όσον αφορά το μέγεθός τους, επιτρέπει στις εταιρείες να δώσουν προτεραιότητα σε σπάνιους πόρους.

Η διαχείριση των αβεβαιοτήτων δεν είναι εύκολο έργο. Οι περιορισμένοι πόροι και το συνεχώς μεταβαλλόμενο τοπίο των απειλών και των τρωτών σημείων κάνουν αδύνατο το μετριασμό όλων των κινδύνων. Ως εκ τούτου, οι επαγγελματίες για την ασφάλεια των πληροφοριακών συστημάτων πρέπει να έχουν ένα σύνολο εργαλείων, ώστε να μοιράζονται μια κοινώς κατανοητή αντίληψη με τους διευθυντές επιχειρήσεων και πληροφοριακών συστημάτων σχετικά με τις πιθανές επιπτώσεις των διαφόρων απειλών στα έργα πληροφοριακών συστημάτων. Αυτό το σύνολο εργαλείων πρέπει να είναι σταθερό, επαναλαμβανόμενο, συμφέρον από πλευράς κόστους και να μειώνει τους κινδύνους σε ένα λογικό επίπεδο.

Η ανάλυση και διαχείριση κινδύνων δεν είναι κάτι καινούργιο. Υπάρχουν πολλά εργαλεία και τεχνικές που διατίθενται για την οργανωτική ανάλυση και διαχείριση κινδύνων έργων πληροφοριακών συστημάτων.

Η γενική μεθοδολογία ανάλυσης και διαχείρισης κινδύνων αποτελείται από τρία βασικά στάδια η μεν και ακολούθως από τέσσερα η δε. Τα τρία πρώτα στάδια, λοιπόν, είναι η αναγνώριση κινδύνου, όπου συγκροτείται μια λίστα όλων των πιθανών παραγόντων κινδύνου που θα μπορούσε να αντιμετωπίσει ένα έργο, η εκτίμηση κινδύνου, όπου προσδιορίζεται η έκθεση σε κάθε παράγοντα κινδύνου βάσει μιας αξιολόγησης της πιθανότητας εμφάνισής του και του πιθανού αντίκτυπού του ή βάσει του βάρους του σε σχέση με τους υπόλοιπους και της σοβαρότητάς του, και η αποτίμηση κινδύνου, όπου αξιολογείται η αποδοχή κάθε παράγοντα κινδύνου προκειμένου να αποφασιστεί ποιες ενέργειες θα ληφθούν. Τα επόμενα τέσσερα στάδια είναι ο προγραμματισμός διαχείρισης κινδύνου, όπου αναπτύσσονται κατάλληλες ενέργειες για την αντιμετώπιση κάθε παράγοντα κινδύνου και προετοιμάζεται ένα πλάνο διαχείρισής του, η διαχείριση πόρων, όπου γίνεται ανάθεση των πόρων και των ευθυνών, ο έλεγχος διαδικασίας διαχείρισης κινδύνου, όπου γίνεται έλεγχος συμβατότητας του πλάνου διαχείρισης κινδύνου σε σχέση με τους διαθέσιμους πόρους και τις ισχύουσες διαδικασίες διαχείρισης του έργου, και η παρακολούθηση διαδικασίας διαχείρισης κινδύνου, όπου παρακολουθείται η αποτελεσματικότητα της εφαρμογής του πλάνου διαχείρισης κινδύνου και εξετάζεται η ανάγκη τυχόν αναθεώρησής του.

Αντικείμενο αυτής της εργασίας, λοιπόν, είναι ο εντοπισμός των σύγχρονων τεχνικών και μεθοδολογιών ανάλυσης και διαχείρισης κινδύνων που απαιτούνται στην εκτέλεση έργων πληροφορικής και η καταγραφή των κυριότερων βημάτων που ακολουθούνται σε αυτές τις μεθόδους. Στόχο της παρούσας διπλωματικής αποτελεί η παρουσίαση των βασικών κινδύνων που εντοπίζονται στα έργα πληροφοριακών συστημάτων, καθώς και των στρατηγικών και τεχνικών με τις οποίες αυτοί εντοπίζονται και αντιμετωπίζονται. Πέρα από το θεωρητικό μέρος παρατίθεται και μια έρευνα μικρής κλίμακας που πραγματοποιήθηκε για το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) μιας τσέχικης εταιρείας. Η αξιολόγηση των δεδομένων του ΣΔΑΠ, όπως θα δούμε στη συνέχεια, γίνεται με βάση τον αντίκτυπο που έχει η μη διαθεσιμότητα, η μη εξουσιοδοτημένη αποκάλυψη (υποκλοπή) και η μετατροπή με πρόθεση των δεδομένων.

ΚΕΦΑΛΑΙΟ 2

Γενικά

2.1 Το Ζήτημα του Κινδύνου

Ο κίνδυνος είναι παρών σε κάθε πτυχή της ζωής. Ως εκ τούτου, η διαχείριση κινδύνων είναι μία καθολική έννοια, εφαρμόσιμη σε όλο σχεδόν το εύρος της ανθρώπινης δραστηριότητας. Στην πλειοψηφία, βέβαια, των περιπτώσεων αποτελεί μία αδόμητη δραστηριότητα, βασισμένη στην κοινή λογική, την εμπειρία και το ένστικτο. Οι πρώτοι κίνδυνοι παρουσιάζονται καθώς συλλαμβάνεται ως ιδέα το έργο, «χτίζεται» η δομή του και αναπτύσσονται οι στόχοι σχετικά με το κόστος, το χρονοδιάγραμμα και το αντικείμενο του έργου. Αρχικά, αυτοί οι κίνδυνοι μπορούν να κατηγοριοποιηθούν ως υποθέσεις, αλλά όταν γίνεται σαφές ότι αποτελούν αστάθμητους παράγοντες, τότε εμφανίζονται οι πρώτοι τεκμηριωμένοι κίνδυνοι. Ενώ ο λεπτομερής σχεδιασμός των κινδύνων λαμβάνει χώρα μετά τον καθορισμό του έργου, το πιο σημαντικό μέρος της Διαχείρισης Κινδύνων συμβαίνει κατά τη διάρκεια της αρχικής ανάπτυξης της δομής του, επειδή εκείνη τη στιγμή κατανέμονται τα κονδύλια του προϋπολογισμού, ώστε να προσαρμοστούν στους κινδύνους του έργου. Αξίζει, επίσης, να τονιστεί το υψηλό επίπεδο πληροφορίας που απαιτείται κατά τη διάρκεια του Σχεδιασμού Κινδύνων, καθώς ο Σχεδιασμός Κινδύνων είναι πιθανό να προκαλέσει αναθεώρηση των αρχικών υποθέσεων σχετικά με το αντικείμενο του έργου, τις ευθύνες, το κόστος, το χρονοδιάγραμμα και τα κονδύλια του προϋπολογισμού που προορίζονται για τους κινδύνους.

Οι οργανισμοί που διαθέτουν τους κατάλληλους πόρους για την καλύτερη κατανόηση των κινδύνων που αντιμετωπίζουν και την αποτελεσματικότερη διαχείρισή τους μπορούν όχι μόνο να αποφύγουν απρόβλεπτες δυσκολίες, αλλά ταυτόχρονα να απελευθερώσουν πόρους προς άλλες κατευθύνσεις και να επωφεληθούν ευκαιριών (για νέες επενδύσεις), οι οποίες διαφορετικά ενδεχομένως να απορρίπτονταν ως απλά πολύ επικίνδυνες. Γίνεται, λοιπόν, αντιληπτό ότι η οργανωμένη προσπάθεια ανάλυσης και διαχείρισης κινδύνων έχει να προσφέρει σημαντική βοήθεια στους οργανισμούς, όχι μόνο σχετικά με την αποφυγή ή καλύτερα τον έλεγχο επικίνδυνων καταστάσεων, που σε διαφορετική περίπτωση θα θεωρούνταν απρόβλεπτες, αλλά ταυτόχρονα και με τη θεώρηση νέων πρακτικών ή προσπαθειών που προσφέρουν σημαντικές ευκαιρίες. Υπό αυτή την οπτική γωνία, είναι σαφές ότι ο κίνδυνος εμπεριέχει τόσο την έννοια της απειλής, όσο και αυτή της ευκαιρίας. Αφενός, δηλαδή, θεωρείται ως απειλή σε περίπτωση που οι συνέπειες στους στόχους του Έργου είναι αρνητικές και αφετέρου ως ευκαιρία σε περίπτωση που οι συνέπειες στους στόχους του έργου είναι θετικές.

Όσον αφορά τη Διαχείριση Έργων, παρά την ραγδαία εξέλιξή της τα τελευταία έτη, τον εμπλουτισμό της με ισχυρό επιστημονικό υπόβαθρο και τον καθορισμό

συστηματικών διαδικασιών για όλα τα στάδια του κύκλου ζωής ενός Έργου, η Διαχείριση Κινδύνων θεωρούταν μέχρι πολύ πρόσφατα σαν μια επιπλέον διαδικασία. Τελευταία έχει ξεκινήσει η αναθεώρηση αυτής της πρακτικής και η πλήρης ενσωμάτωση της Διαχείρισης Κινδύνων στην αποτελεσματική πρακτική της Διαχείρισης Έργων. Η ενσωμάτωση αυτή προσφέρει τη μεγιστοποίηση του οφέλους από την χρήση των διαδικασιών Ανάλυσης και Διαχείρισης κινδύνου, καθώς μόνο έτσι δίνεται πραγματικά η δυνατότητα για αυτό που περιγράφηκε προηγουμένως, δηλαδή όχι μόνο την αποφυγή των κινδύνων ή τον μετριασμό των επιπτώσεών τους, αλλά και την πλήρη εκμετάλλευση των ευκαιριών που παρουσιάζονται σε όλα τα στάδια ενός έργου πληροφοριακού συστήματος.

Τα περισσότερα αυτοματοποιημένα Πληροφοριακά Συστήματα Διοίκησης χρησιμοποιούν υλικό (hardware) που υπάρχει έτοιμο (off the shelf). Κατά συνέπεια, η σχεδίασή τους -από πλευράς υλικού- δεν περιλαμβάνει υψηλούς τεχνικούς κινδύνους. Μόνη εξαίρεση στη διαπίστωση αυτή είναι, ίσως, τα Πληροφοριακά Συστήματα (Π.Σ.) που ικανοποιούν στρατιωτικές απαιτήσεις. Η φύση των απαιτήσεων αυτών αναγκάζει πολλές φορές το σχεδιαστή να σχεδιάσει υλικό από την αρχή, ειδικά για τις ανάγκες του χρήστη αφού δεν υπάρχει έτοιμο προϊόν στην αγορά.

Από πλευράς λογισμικού τα πράγματα είναι λίγο διαφορετικά. Εδώ η σχεδίαση του λογισμικού (software) είναι ένα τμήμα του όλου έργου, αφού σπάνια είναι δυνατόν να υπάρξει έτοιμο λογισμικό που να ικανοποιεί αυτούσιο, χωρίς δηλαδή μετατροπές, τις απαιτήσεις του χρήστη. Όμως, τις περισσότερες φορές έτοιμο είναι το λογισμικό συστήματος (system's software) και όχι το λογισμικό εφαρμογών (application's software). Ίσως τα Πληροφοριακά Συστήματα που χρησιμοποιούνται για στρατιωτικούς σκοπούς να αποτελούν και εδώ την εξαίρεση: για να ικανοποιηθούν μερικές απαιτήσεις του Συστήματος χρειάζεται πολλές φορές αρχική σχεδίαση, τόσο στο επίπεδο του λογισμικού συστήματος όσο και στο επίπεδο του υλικού.

Γίνεται, λοιπόν, αντιληπτό ότι η ανάπτυξη μεγάλων συστημάτων λογισμικού αποτελεί μια επικίνδυνη διαδικασία. Σύμφωνα με αναφορά του «The Standish Group, "CHAOS: A Recipe for Success"» μόνο το 28% των έργων λογισμικού που έγιναν το 2000 παραδόθηκαν εγκαίρως και στα πλαίσια του αρχικού προϋπολογισμού, πληρώντας παράλληλα και όλες τις απαιτήσεις του αρχικού σχεδιασμού. Αυτό σημαίνει ότι το υπόλοιπο 72% είτε απέτυχε ή δεν κατάφερε να ικανοποιήσει τους αρχικούς στόχους. Αυτά τα ποσοστά είναι τρομακτικά σε μια εποχή που τα πληροφοριακά έργα παίζουν καταλυτικό ρόλο στη λειτουργία ενός οργανισμού. Χαρακτηριστικό παράδειγμα αποτελεί η επιχείρηση e-Bay που πραγματοποιούσε δημοπρασίες στο διαδίκτυο και έχασε εκατομμύρια δολάρια όταν τα συστήματά της δεν ήταν διαθέσιμα για μόλις μερικές ώρες. Εταιρείες παραγωγής λογισμικού, όπως η Microsoft και η Oracle, χάνουν τεράστια ποσά όταν η διάθεση των προϊόντων τους καθυστερεί ή αυτά δε λειτουργούν όπως θα έπρεπε. Ακόμα και μικρού ή μεσαίου μεγέθους έργα επιβαρύνονται οικονομικά από τυχόν καθυστερήσεις. Πέραν από τις καθαρά οικονομικές απώλειες υπάρχει πάντα και το κόστος των χαμένων ευκαιριών, των απολεσθέντων πωλήσεων αλλά και των δυσαρεστημένων πελατών που τελικά θα μπορούσε να αποδειχθεί ακόμα μεγαλύτερο (Murthi, 2002).

Πολλές εταιρείες υιοθετούν λεπτομερείς και αυστηρές μεθοδολογίες ελέγχου της παραγωγής, ελπίζοντας να μειώσουν τις καθυστερήσεις και την πιθανότητα αποτυχίας, ενεργώντας ακριβώς τη στιγμή που θα εμφανιστεί το κάθε πρόβλημα. Δυστυχώς, αυτές οι θεραπευτικές, και όχι προληπτικές, μέθοδοι συμβάλλουν με τη σειρά τους στην αύξηση των καθυστερήσεων, ενώ παράλληλα παρέχουν μικρή εγγύηση επιτυχίας. Επίσης, τα μέτρα εξάλειψης του προβλήματος λαμβάνονται όταν το πρόβλημα έχει πλέον εμφανιστεί και αποδεικνύονται πολλές φορές πιο επιζήμια και από το ίδιο το πρόβλημα. Τα ανώτερα στελέχη ενημερώνονται για το πρόβλημα όταν έχουν ήδη αρχίσει να χάνονται κύριοι στόχοι της πορείας του έργου ή ακόμα και από αναφορές πελατών για προβλήματα λογισμικού. Αποτέλεσμα αυτού είναι η προσπάθεια αντιμετώπισης του προβλήματος με μη ενδεδειγμένους τρόπους, όπως μειώνοντας δραστικά το πεδίο του έργου, αντικαθιστώντας τους υπεύθυνούς του και μισθώνοντας ακριβούς ανάδοχους ή και αντλώντας πόρους από άλλα έργα μεταφέροντας έτσι το πρόβλημα και αλλού. Στο τέλος, η εταιρεία πολλές φορές αναγκάζεται να εγκαταλείψει το έργο, καθώς η διόρθωση του προβλήματος έχει ήδη γίνει πιο δαπανηρή από τα κέρδη που αναμένονταν με την ολοκλήρωσή του.

Μια καλύτερη προσέγγιση αποτελεί η προληπτική διαχείριση κινδύνων. Αυτό σημαίνει πως η μελέτη διαχείρισης κινδύνων γίνεται κατά τη φάση σχεδιασμού του έργου και όχι παράλληλα με την υλοποίησή του, ενώ κατά τη διάρκεια αυτής θα εμπλουτίζεται απλώς με μικρές προσθήκες, που θα την προσαρμόζουν στις εκάστοτε αλλαγές των συνθηκών. Η διαχείριση κινδύνων αποτελεί μια επιστημονική προσέγγιση στο πρόβλημα της αντιμετώπισης των κινδύνων από άτομα και οργανισμούς. Βασίζεται σε μια ευδιάκριτη φιλοσοφία και ακολουθεί μια καλά ορισμένη συνέχεια βημάτων. Καταρχήν έχουμε την εκτίμηση ενός κινδύνου. Εκτίμηση κινδύνου δε σημαίνει απλώς να εντοπίσουμε το πρόβλημα, αλλά να ποσοτικοποιήσουμε και τις επιπτώσεις αυτού (καθώς δεν είναι απαραίτητο οι επιπτώσεις να μεταφράζονται άμεσα σε χρήματα), να εκτιμήσουμε την πιθανότητα εμφάνισής του και κατόπιν να αξιολογήσουμε την όλη κατάσταση ως προς το επίπεδο έκθεσης στο συγκεκριμένο κίνδυνο (Murthi, 2002).

Η διαχείριση κινδύνων, όμως, δε σταματά εκεί. Θα πρέπει να προταθούν λύσεις προστασίας του έργου από τον κίνδυνο, είτε αυτό σημαίνει μηδενισμό ή μείωση της πιθανότητας εμφάνισης του κινδύνου είτε αυτό σημαίνει οργάνωση στρατηγικής για μείωση των επιπτώσεων. Φυσικά, υπάρχει πάντοτε η πιθανότητα μια μελέτη διαχείρισης κινδύνων να καταλήξει στη ματαίωση υλοποίησης ενός έργου, καθώς τα οφέλη από την επιτυχή διεκπεραίωσή του μπορεί να είναι πολύ μικρότερα συγκρινόμενα με τις πιθανές απώλειες από την παρουσία των κινδύνων. Αυτό δεν σημαίνει πως τέτοιες μελέτες έχουν απαισιόδοξο χαρακτήρα και οδηγούν στην απαξίωση της εξέλιξης και της εισαγωγής νέων τεχνολογιών, αλλά αντίθετα αποτελούν ένα ορθολογικό εργαλείο που στοχεύει στην προστασία των συμφερόντων του κάθε οργανισμού που τις υιοθετεί.

Θα πρέπει εδώ να τονίσουμε ότι καμία μελέτη διαχείρισης κινδύνων δε δύναται να φέρει τη σιγουριά πως, πλην των προβλεφθέντων κινδύνων, τίποτα άλλο δε μπορεί να παρενοχλήσει τη διεκπεραίωση του έργου. Ενδεχομένως να υπάρχουν και άλλες ευάλωτες πτυχές του έργου που να μην έχουν προβλεφθεί και να αποφέρουν δυσμενή αποτελέσματα στην εξέλιξή του. Υπάρχει, δηλαδή, ομοφωνία μεταξύ των ειδικών στην

ασφάλεια των Πληροφοριακών Συστημάτων ότι δε μπορεί να υπάρξει 100% ασφάλεια, με άλλα λόγια μηδενικός κίνδυνος. Συνεπώς, η έμφαση σε ό,τι αφορά τους κινδύνους επεκτείνεται από την αποφυγή των κινδύνων έως τη διαχείριση των κινδύνων (risk management). Για το λόγο αυτό, έργα μεγάλου μεγέθους και πολυπλοκότητας απαιτούν τη διαρκή επαγρύπνηση των υπευθύνων για τον έγκαιρο εντοπισμό ανεπιθύμητων καταστάσεων. Φυσικά, η εισαγωγή της διαχείρισης κινδύνων στο σχεδιασμό του έργου μειώνει κατά πολύ τις πιθανότητες εμφάνισης απρόοπτων καταστάσεων.

Η σχεδίαση και η τροποποίηση του λογισμικού εφαρμογών έχει αποδειχθεί ότι δεν περιλαμβάνει τεχνολογικούς κινδύνους αφού σχεδόν πάντα, τουλάχιστον για τις συνήθεις εφαρμογές, είναι μέσα στα πλαίσια της υπάρχουσας σήμερα τεχνογνωσίας (staten of art). Όμως, είναι κοινή διαπίστωση ότι η ανάπτυξη ενός αυτοματοποιημένου Πληροφοριακού Συστήματος, ανεξάρτητα από το μέγεθος και την περιπλοκή του, είναι ένα δύσκολο έργο. Επιβεβαίωση της διαπίστωσης αυτής είναι το γεγονός ότι η ανάπτυξη πάρα πολλών Πληροφοριακών Συστημάτων, όπως έχει ήδη αναφερθεί, έχει καταλήξει σε αποτυχία, ολική ή μερική, με την έννοια ότι είτε δεν ικανοποιήθηκαν οι απαιτήσεις που τέθηκαν είτε έγινε υπέρβαση των οικονομικών ή χρονικών ορίων ολοκλήρωσης του έργου. Η ανάγκη, λοιπόν, για Ανάλυση και Διαχείριση Κινδύνων έχει τονιστεί κυρίως από τις εκ των υστέρων αξιολογήσεις του παρελθόντος. Σε αυτές, επανειλημμένα, έχουν προσδιοριστεί περιπτώσεις όπου το αποτέλεσμα επηρεάστηκε αρνητικά από γεγονότα, των οποίων οι επιδράσεις θα μπορούσαν να έχουν μειωθεί αν είχε διενεργηθεί ουσιαστική Ανάλυση και Διαχείριση Κινδύνων (Visintine, 2003).

2.2 Ο Κίνδυνος στη Ζωή του Ανθρώπου – Ιστορική Αναδρομή

Ο άνθρωπος από την αρχή της ύπαρξής του βρέθηκε αντιμέτωπος με ένα πλήθος κινδύνων. Οι πρώτοι κίνδυνοι που κλίθηκε να αντιμετωπίσει αφορούσαν κυρίως την επιβίωσή του. Τα καιρικά φαινόμενα, η έλλειψη τροφής, τα υπόλοιπα μέλη του ζωικού βασιλείου, ασθένειες είναι μερικοί μόνο από τους κινδύνους που απειλούσαν την ύπαρξή του. Εντούτοις, προσαρμόζοντας τη συμπεριφορά του και ακολουθώντας το ένστικτό του κατόρθωσε να ξεπεράσει τα εμπόδια που του παρουσιάζονταν και να επιζήσει επιδεικνύοντας από τότε τη δεινότητά του στην αντιμετώπιση των κινδύνων. Φυσικά, δε μπορούμε να υποστηρίξουμε πως αυτό συνέβη στη βάση κάποιας οργανωμένης στρατηγικής, σίγουρα όμως αποτελεί μια απόδειξη της πρώτης επιτυχημένης προσπάθειας του ανθρώπου να διαχειριστεί τους κινδύνους που τον απειλούσαν.

Σημαντικό βήμα για την αποτελεσματικότερη αντιμετώπιση των κινδύνων αποτέλεσε η οργάνωση των ανθρώπων σε μικρές κοινωνίες. Η οργάνωση αυτή δημιούργησε, όμως, και νέους κινδύνους, άγνωστους στην έως τότε μοναχική του διαβίωση. Οι νέοι κίνδυνοι, που προήλθαν από τη συνύπαρξη πολλών ανθρώπων στον ίδιο χώρο, έκαναν φανερή την ανάγκη θεσμοθέτησης κανόνων και διαχωρισμού ευθυνών και υποχρεώσεων για την αρμονική τους συμβίωση. Όλα αυτά έδωσαν ώθηση στην εξέλιξη του ανθρώπινου είδους και ο άνθρωπος βρέθηκε εις αναζήτηση τρόπων βελτίωσης της ποιότητας της ζωής του. Κάθε βήμα προόδου, όμως, έφερνε μαζί του και νέους κινδύνους. Η έννοια της ιδιωτικής ιδιοκτησίας εισήχθη στη ζωή των ανθρώπων και μαζί με αυτή και η αγωνία διατήρησης των κεκτημένων αλλά και της διεύρυνσης αυτών.

Ακολούθησαν χρόνια εξέλιξης πριν την εμφάνιση των πρώτων επιχειρησιακών κινδύνων, που συνέπεσαν με την έναρξη των εμπορικών συναλλαγών. Όταν, λοιπόν, τα αγαθά έγιναν αντικείμενο συναλλαγών, τότε ξεκίνησε ουσιαστικά η πρώτη επιχειρηματική δραστηριότητα του ανθρώπου, που συνοδεύτηκε από την εμφάνιση των πρώτων επιχειρησιακών κινδύνων και την ανάγκη αντιμετώπισής τους. Από τα αρχαιολογικά ευρήματα διαπιστώνουμε πως αυτοί οι πρώιμοι επιχειρηματίες είχαν αναπτύξει αξιόλογες τεχνικές για την αντιμετώπιση των κινδύνων που τους παρουσιάζονταν.

Μια καινοτομία που έφερε επανάσταση στο εμπόριο, την ιδιωτική ιδιοκτησία και τη συσσώρευση πλούτου ήταν η χρήση του χρήματος. Μέχρι να αρχίσει ο άνθρωπος να το χρησιμοποιεί για τις συναλλαγές του, το εμπόριο στηριζόταν σε μια βάση ανταλλαγής προϊόντων. Με την εισαγωγή του χρήματος εισήχθησαν επίσης για πρώτη φορά και οι έννοιες της πίστωσης και του δανεισμού. Είναι ολοφάνερο πως το χρήμα μαζί με όλες τις διευκολύνσεις που παρείχε έφερε και μια πληθώρα κινδύνων, καθώς όσο εύκολη ήταν η διακίνησή του, το ίδιο εύκολη ήταν και η απώλεια του. Μια άλλη ανησυχία αποτέλεσε η ακριβής αποτίμηση των αγαθών και των υπηρεσιών στις αναπτυσσόμενες αγορές της εποχής, καθώς οι έμποροι επιδίωκαν τις μεγαλύτερες δυνατές τιμές για τα προϊόντα τους, που να είναι, όμως, παράλληλα ανταγωνιστικές σε σχέση με τις τιμές των προϊόντων των άλλων εμπόρων.

Η σύγχρονη κεφαλαιοκρατία αναδύθηκε μετά από μια μεταβατική περίοδο αρκετών αιώνων, κατά τη διάρκεια των οποίων δημιουργήθηκαν οι όροι που απαιτούνται για μια κοινωνία καπιταλιστικής αγοράς. Προσπερνώντας όλο αυτό το διάστημα φτάνουμε στη βιομηχανική επανάσταση. Είχε πλέον γίνει αντιληπτό πως κάθε καινοτομία, κάθε νέα τεχνολογία, εκτός των πλεονεκτημάτων και των διευκολύνσεων που προσέφερε, δημιουργούσε και νέες πηγές κινδύνων. Η δημιουργία οργανισμών μοίρασε τους κινδύνους σε ένα σύνολο ατόμων και αύξησε την παραγωγή, τη διανομή αλλά και τους πόρους κεφαλαίου. Οι επενδυτές άθροιζαν τα κεφάλαιά τους, συμμετέχοντας με αυτόν τον τρόπο από κοινού στα κέρδη αλλά και στους κινδύνους της επιχείρησης. Το καινοτόμο χαρακτηριστικό γνώρισμα δεν ήταν η συνεργασία ή η από κοινού συγκέντρωση κεφαλαίου, αλλά ότι οι εταιρείες αντιμετώπιζαν τους κινδύνους με ένα διαφορετικό τρόπο, περιορίζοντας και κατανέμοντας τις ευθύνες των επενδυτών με βάση το ποσό που επένδυαν.

Προχωρώντας στην ανθρώπινη εξέλιξη και φτάνοντας στη σημερινή εποχή, στην εποχή της πληροφορίας και του διαδικτύου, ο κάθε οργανισμός έχει να αντιμετωπίσει, ίσως περισσότερο από ποτέ, μαζί με τους κινδύνους του παρελθόντος και αυτούς που γεννιούνται από τις ραγδαίες πλέον τεχνολογικές εξελίξεις. Είναι αυτονόητο πως ένα από τα πιο ευάλωτα σημεία των σύγχρονων επιχειρήσεων σε τέτοιου είδους κινδύνους είναι τα έργα πληροφορικής. Κανενός είδους έργο δε μπορεί να αναπτυχθεί μέσα σε ένα ιδανικό και πλήρως προσδιορισμένο περιβάλλον εργασίας. Όλες οι παράμετροι των έργων, όπως είναι τα χρονοδιαγράμματα, το κόστος, η ποιότητα, το περιεχόμενο, κ.λπ., αντιμετωπίζουν κινδύνους, οι οποίοι μπορούν να επηρεάσουν δραστικά την έκβαση του έργου, είτε θετικά είτε αρνητικά, ανάλογα με το αν πρόκειται για θετικό ή αρνητικό κίνδυνο αντίστοιχα. Καθώς, λοιπόν, τέτοια έργα μπορεί να είναι μεγάλου μεγέθους και πολυπλοκότητας και η όλη λειτουργία ενός οργανισμού, που έχει δαπανήσει υπέρογκα ποσά για την υλοποίησή τους, να βασίζεται στην επιτυχημένη ολοκλήρωσή τους, γίνεται επιτακτική η ανάγκη ύπαρξης διαδικασιών Ανάλυσης και Διαχείρισης Κινδύνων. Τέτοιες διαδικασίες περιλαμβάνουν τις ενέργειες προσδιορισμού, αξιολόγησης και παρακολούθησης των κινδύνων καθώς και την εφαρμογή των απαραίτητων μέτρων και διαδικασιών που θα εγγυηθούν ένα αποδεκτό επίπεδο έκθεσης σε αυτούς (Gallati, 2003).

Κάνοντας, λοιπόν, μια αναδρομή στο παρελθόν και με μια αξιολόγηση των διαρκώς αυξανόμενων κινδύνων της σύγχρονης εποχής, παρατηρούμε πως η ύπαρξη κινδύνων δεν είναι ένα καινούργιο φαινόμενο που παρουσιάστηκε τα τελευταία χρόνια στη ζωή του ανθρώπου, αλλά υπήρχε πάντα και έπαιρνε διαφορετικές μορφές σε όλη τη διάρκεια της ανθρώπινης ιστορίας. Φυσικά, οι κίνδυνοι δεν εντοπίζονται μόνο σε επιχειρηματικές δραστηριότητες, αλλά ελλοχεύουν και σε όλη την καθημερινότητα του σύγχρονου ανθρώπου. Πάντα, όμως, είτε επρόκειτο για μικρούς είτε για μεγάλους κινδύνους, είτε για επιχειρησιακούς είτε για κινδύνους της καθημερινότητας, ο άνθρωπος αναζητούσε τρόπους αποφυγής τους ή μετριασμού των επιπτώσεών τους, όχι απαραίτητα με οργανωμένο τρόπο αλλά ακόμα και με ενστικτώδεις αντιδράσεις. Η ύπαρξη, ωστόσο, επιχειρησιακών κινδύνων και οι απώλειες του πρόσφατου παρελθόντος από κινδύνους, οι οποίοι δεν προβλέφθηκαν και δε σχεδιάστηκε δράση αντιμετώπισής τους, δημιούργησαν την ανάγκη οργανωμένης αντιμετώπισης αυτών. Αυτή η οργανωμένη και επιστημονική αντιμετώπιση ονομάζεται Διαχείριση Κινδύνων κι εμφανίστηκε ως δομημένη διαδικασία διοίκησης των έργων τη δεκαετία του ΄90. Η διαχείριση κινδύνων έργων δεν περιορίζεται στην ασφάλεια της εργασίας, αλλά εκτείνεται σε κινδύνους προγραμματισμού (όπως οι καθυστερήσεις υπεργολάβων), νομικών προβλημάτων (όπως η αδυναμία έκδοσης άδειας) και οτιδήποτε άλλο μπορεί να επηρεάσει τους στόχους ενός έργου (κόστος, χρόνο και ποιότητα). Γίνεται, λοιπόν, αντιληπτό ότι η διαχείριση των κινδύνων αποτελεί μια πολύ σημαντική διαδικασία κατά τη διαχείριση έργων. Όπως, λοιπόν, η διαχείριση έργου διέπεται από αρχές και διαδικασίες, έτσι συμβαίνει και στη διαχείριση κινδύνου, η οποία αποτελεί μια συνεχή διαδικασία σε όλη τη διάρκεια ζωής του έργου.

2.3 Έννοιες – Ορισμοί

Για την καλύτερη κατανόηση της παρούσας εργασίας παρατίθεται το βασικό εννοιολογικό πλαίσιο που χρησιμοποιείται ευρέως στην ανάλυση κινδύνων:

Πληροφοριακό Σύστημα (Information System - IS):

Ένα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός, διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας επιχείρησης ή ενός οργανισμού.

Αγαθά ή Περιουσιακά Στοιχεία (Assets):

Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία (value), άρα σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους πόρους και επομένως, πρέπει να προστατευθούν.

Ασφάλεια Πληροφοριακού Συστήματος (Information System Security):

Το οργανωμένο πλαίσιο από έννοιες, αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τόσο τα στοιχεία του Πληροφοριακού Συστήματος όσο και ολόκληρο το Πληροφοριακό Σύστημα από τυχαία ή σκόπιμη απειλή.

Εγκυρότητα (Validity):

Απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.

Αυθεντικότητα (Authenticity):

Αποφυγή ατελειών και ανακριβειών κατά την εξουσιοδοτημένη τροποποίηση μιας πληροφορίας.

Ακεραιότητα (Integrity):

Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

Εμπιστευτικότητα (Confidentiality):

Αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες.
(Αποτελεί και χαρακτηριστικό ασφάλειας ενός Πληροφοριακού Συστήματος.)

Διαθεσιμότητα (Availability):

Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας ή των υπολογιστικών πόρων σε νόμιμα εξουσιοδοτημένους χρήστες.
(Αποτελεί και χαρακτηριστικό ασφάλειας ενός Πληροφοριακού Συστήματος.)

Παραβίαση (Breach):

Ένα γεγονός το οποίο προσβάλλει μία ή περισσότερες από τις ακόλουθες ιδιότητες: εγκυρότητα, αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα.

Απειλή (Threat):

Μια πιθανή ενέργεια ή ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων χαρακτηριστικών ασφάλειας ενός Πληροφοριακού Συστήματος (όπως τη μη διαθεσιμότητα του συστήματος και των υπηρεσιών, την τυχαία ή με πρόθεση μετατροπή των δεδομένων, την καταστροφή των δεδομένων ή του συστήματος και τέλος τη μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών). κ.λπ.). Όσο το τεχνολογικό περιβάλλον εξελίσσεται διαρκώς και ταχέως, τόσο και οι απειλές μεταβάλλονται και εξελίσσονται.

Ευπάθεια ή Αδυναμία (Vulnerability):

Ένα σημείο ή μια σχεδιαστική ατέλεια ενός Πληροφοριακού Συστήματος που μπορεί να επιτρέψει να συμβεί παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος, δηλαδή να επιτρέψει σε μια απειλή να προκαλέσει ζημιά. Η ευπάθεια μπορεί να οριστεί και με τον εξής τύπο: *Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής η απειλή*.
(Αποτελεί και χαρακτηριστικό ασφάλειας ενός Πληροφοριακού Συστήματος.)

Αβεβαιότητα (Uncertainty):

Το γεγονός που χαρακτηρίζει ότι ο κίνδυνος μπορεί ή δε μπορεί να συμβεί.

Απώλεια ή Ζημία (Loss or Damage / Harm):

Οι ανεπιθύμητες συνέπειες που θα επηρεάσουν αρνητικά τη μερική ή ολική αξίας ενός αγαθού.

Περιστατικό (Incident):

Ένα γεγονός, το οποίο είτε έχει ως συνέπεια μια παραβίαση είτε αποτελεί μια απόπειρα παραβίασης είτε θέτει σε κίνδυνο την ασφάλεια ενός Πληροφοριακού Συστήματος.

Παράγοντες Κινδύνου (Risk Factors):

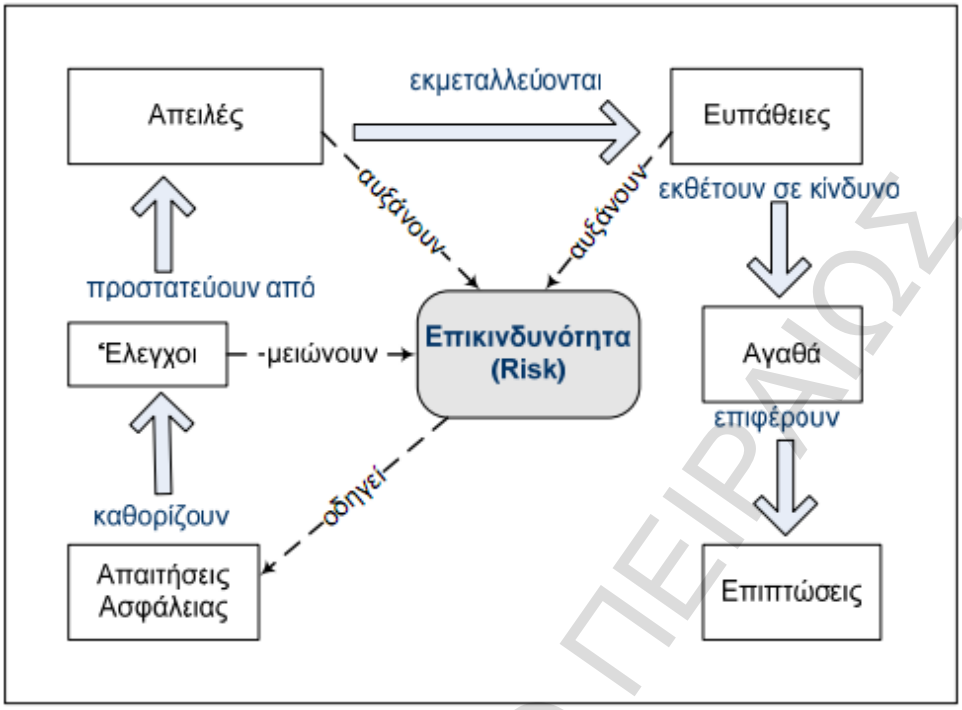
Οι παράγοντες (π.χ. πολυπλοκότητα, ταχύτητα, καινοτομία, απαιτήσεις τεχνολογίας, απαιτήσεις προσπάθειας)που ενδέχεται να προκαλέσουν την πιθανότητα εκδήλωσης επικίνδυνων συνεπειών, καθώς η πιθανότητα αυτή εξαρτάται από την ύπαρξη των εν λόγω παραγόντων.

Επίπτωση ή Αντίκτυπος (Impact):

Οι συνέπειες, βραχυπρόθεσμες ή μακροπρόθεσμες, ενός παράγοντα κινδύνου, όσον αφορά την απώλεια μιας αξίας, την αύξηση του κόστους ή άλλη απώλεια που προκύπτει ως αποτέλεσμα μιας συγκεκριμένης απειλής. Η μελέτη και εξέταση της επίπτωσης δε θα πρέπει να περιορίζεται στα στενά όρια του έργου. Μερικές ενδιάμεσες επιπτώσεις μπορεί να επιφέρουν σημαντικές αλλοιώσεις των στόχων του συστήματος μακροπρόθεσμα, ενώ άλλες μπορεί να επηρεάσουν μη κρίσιμα σημεία και στοιχεία του συστήματος. Ως εκ τούτου, ένας παράγοντας κινδύνου μπορεί να έχει πολλαπλές επιπτώσεις και πολλοί παράγοντες να οδηγούν στην ίδια επίπτωση.

Κίνδυνος ή Επικινδυνότητα (Risk):

Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια, με αποτέλεσμα να υπάρξει μη επιθυμητό αποτέλεσμα στο έργο ή απόκλιση από τους αρχικούς στόχους που έχουν τεθεί. Ο κίνδυνος εκφράζει το ενδεχόμενο για απώλεια. Πρόκειται, λοιπόν, για ένα γεγονός το οποίο, εξ ορισμού, εμπεριέχει την έννοια της αβεβαιότητας εμφάνισης. Αποτελεί συνάρτηση τριών παραγόντων, της έντασης των Απειλών που αντιμετωπίζει το Πληροφοριακό Σύστημα, της σοβαρότητας των αντίστοιχων Ευπαθειών (ή Αδυναμιών) του και των Επιπτώσεων που θα υπάρξουν (ανάλογες με την αξία των αγαθών) από την πραγματοποίηση των Απειλών (σχήμα 2.1). Αποδίδοντας, λοιπόν, τον κίνδυνο με τη μορφή τύπου, θα μπορούσαμε να πούμε ότι: *Κίνδυνος = Απειλή x Ευπάθεια x Επίπτωση*. Για παράδειγμα, η πυρκαγιά είναι μία Απειλή, η οποία για να εξαπλωθεί χρειάζεται να εκμεταλλευτεί μια Αδυναμία, όπως η ύπαρξη εύφλεκτων υλικών, και όταν πραγματοποιηθεί προξενεί βλάβη ή ολική καταστροφή σε ορισμένα Αγαθά του οργανισμού. Το μέγεθος των συνεπειών που θα έχει η πυρκαγιά είναι ίσο με την Επίπτωση που θα έχει η απώλεια των αντίστοιχων Αγαθών. Ο κίνδυνος μπορεί να είναι ενδογενής (αδυναμία) ή εξωγενής (απειλή) σε σχέση με τα αγαθά. Παράλληλα με τον κίνδυνο εντοπίζεται και ο όρος της επικινδυνότητας. Η επικινδυνότητα έχει γενικότερη σημασία από τον κίνδυνο, τον οποίο και περιέχει. Για παράδειγμα, όταν δεν υπάρχει κανένας κίνδυνος, τότε έχουμε και ανυπαρξία επικινδυνότητας. Αντίστοιχα, ένα υψηλό επίπεδο επικινδυνότητας υπονοεί την ύπαρξη σημαντικών κινδύνων, ενώ ένα χαμηλό επίπεδο επικινδυνότητας δηλώνει την ύπαρξη λιγότερο σημαντικών κινδύνων. Σίγουρο είναι, πάντως, ότι η επικινδυνότητα αφορά τις δυσμενείς επιπτώσεις που προκαλούνται στο σύστημα όταν ενεργοποιηθεί μια απειλή.



Σχήμα 2.1: Κίνδυνος ή Επικινδυνότητα

Όπως, όμως, ευρέως αναγνωρίζεται, αυτή η σκοπιά του κινδύνου είναι περιοριστική, γιατί αποτυγχάνει να συμπεριλάβει τη διαχείριση των ευκαιριών, με την έννοια των καλοδεχούμενων επιρροών στην απόδοση του έργου. Ο κίνδυνος, λοιπόν, 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. Στην παρούσα εργασία, αν και γίνεται εκτενής αναφορά στο «ανεπιθύμητο ρίσκο», παράλληλα γίνεται προσπάθεια ενσωμάτωσης της διττής σημασίας του όρου 'κίνδυνος', δηλαδή, τόσο του «ανεπιθύμητου ρίσκου», όσο και του «επιθυμητού ρίσκου».

Μέσο/Μέτρο Προστασίας ή Αντίμετρο (Security Countermeasure):

Ένα μέτρο που λαμβάνεται για την προστασία του Πληροφοριακού Συστήματος και την αντιμετώπιση των απειλών, σχεδιασμένο, δηλαδή, με σκοπό να εμποδίσει μια απειλή να συμβεί ή να μειώσει μια αδυναμία-ευπάθεια ή τις δυνητικές επιπτώσεις τους. Μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή μιας κατηγορίας απειλών. Τα μέσα/μέτρα προστασίας διακρίνονται σε κατηγορίες ανάλογα με τον τρόπο με τον οποίο ενεργούν και το σκοπό της δράσης τους, ο οποίος μπορεί να είναι:

- Πρόληψη (Prevention), όπου αποσκοπούν στην αποτροπή της πραγματοποίησης μιας απειλής.

- Ανίχνευση (Detection), όπου σκοπός είναι η διαπίστωση και ο εντοπισμός της εμφάνισης ενός περιστατικού ή μιας απειλής.
- Ανάκαμψη (Recovery), όπου επιχειρούν την αποκατάσταση της λειτουργίας του συστήματος σε επιθυμητό επίπεδο μετά την εμφάνιση κάποιας απειλή.
- Περιορισμός (Mitigation), όπου αποσκοπούν στη μείωση των επιπτώσεων που είχε μια απειλή.

Πολιτική Ασφάλειας (Security Policy):

Περιγραφή σε γενικό-αφαιρετικό επίπεδο του συνόλου των κανόνων, των μέτρων και των διαδικασιών που ορίζουν τα φυσικά, διαδικαστικά και προσωπικά μέτρα ασφάλειας, που λαμβάνονται κατά τη διαχείριση, τη διανομή και την προστασία των αγαθών.

Ανάδοχος ή Συμβατικός Συνεργάτης (Partner, Contracted Party):

Φορείς, εταιρείες, οργανισμοί ή φυσικά πρόσωπα με τους οποίους υπήρξαν, υπάρχουν ή πρόκειται να υπάρξουν συμβατικές σχέσεις.

Ανάλυση Κινδύνων (Risk Analysis):

Η διαδικασία του προσδιορισμού και της αποτίμησης των κινδύνων που εισάγει το σύστημα στη λειτουργία ενός οργανισμού. Σε αυτή 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. Συγκεκριμένα, προσδιορίζονται τα αγαθά του συστήματος, οι απειλές, οι αδυναμίες καθώς και οι συνέπειες που έχουν οι τελευταίες στα αγαθά. Έπειτα, γίνεται αποτίμηση των αγαθών και εκτίμηση του επιπέδου απειλών, αδυναμιών και συνεπειών προκειμένου να υπολογιστεί η συνολική επικινδυνότητα που υπάρχει στο συγκεκριμένο σύστημα. Υπολογίζεται, επιπλέον, και το κόστος πρόληψης κάθε απώλειας, ώστε να είναι δυνατή μια σωστή αντιμετώπιση των κινδύνων με ορθολογιστικά κριτήρια. Η ανάλυση κινδύνων υιοθετεί την παραδοσιακή (θετικιστική) μέθοδο του ανταγωνισμού.

Διαχείριση Κινδύνων (Risk Management):

Το σύνολο των διαδικασιών που απαιτούνται να αναπτυχθούν σε ένα έργο, προκειμένου να μειωθεί η πιθανότητα εμφάνισης καταστροφικών δυνάμεων σε αυτό και καταστάσεων που έρχονται σε αντίθεση με την αρμοστή λειτουργία του οργανισμού. Ενδέχεται να περιέχει εν μέρει την ανάλυση κινδύνων και, ουσιαστικά, αποτελεί τη συνολική διαδικασία προσδιορισμού, ελέγχου, εξάλειψης ή περιορισμού αβέβαιων γεγονότων (απειλών) που επηρεάζουν δυσμενώς τους πόρους του συστήματος. Παράλληλα, στόχος της διαχείρισης κινδύνων είναι η αποφυγή των αρνητικών συνεπειών που θα έχει η υλοποίηση ενός επικίνδυνου φαινομένου. Αφορά αποφάσεις σχετικά με την αποδοχή έκθεσης στον κίνδυνο ή τη μείωση των αδυναμιών του συστήματος, μετριάζοντας τους κινδύνους ή εφαρμόζοντας αποτελεσματικούς

ελέγχους. Αποτελεί την ευρύτερη διαδικασία, που εκτός από την ανάλυση κινδύνων και την επιλογή των κατάλληλων μέτρων προστασίας, καθορίζει και προβλέπει συνεχή έλεγχο της λειτουργίας του συστήματος, αναθεώρηση, όπου και όταν κρίνεται απαραίτητη, και ανάπτυξη της πολιτικής ασφάλειάς του. Αποτελείται από τον προγραμματισμό, την οργάνωση, την καθοδήγηση, το συντονισμό και τον έλεγχο των δραστηριοτήτων που αναλαμβάνονται με σκοπό την παροχή ενός αποδοτικού σχεδίου. Πολλές φορές, βέβαια, η διαχείριση κινδύνων αντιμετωπίζει σοβαρά διλήμματα, αφού καλείται να υλοποιήσει διαδικασίες αντιμετώπισης κινδύνων με χαμηλή πιθανότητα εμφάνισης, αλλά υψηλή καταστροφική ικανότητα, και κινδύνων με υψηλή πιθανότητα εμφάνισης, αλλά χαμηλή καταστροφική ικανότητα.

Έκθεση σε Κίνδυνο (Risk Exposure):

Ένα μέτρο που προσδιορίζει σε ποιο βαθμό ένα έργο 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.

Αποδοτικότητα Διαχείρισης Κινδύνου (Risk Efficiency):

Θεωρώντας ότι η απόδοση μπορεί να μετρηθεί μόνο σε όρους κόστους, το αποδοτικότερο σχέδιο για το ίδιο αναμενόμενο κόστος θα είναι αυτό που εμπλέκει το μικρότερο δυνατό επίπεδο κινδύνου. Αντίστροφα, το αποδοτικότερο σχέδιο για ένα συγκεκριμένο επίπεδο κινδύνου είναι αυτό που συνεπάγεται το μικρότερο δυνατό κόστος. Στόχος, λοιπόν, κάθε προσπάθειας Διαχείρισης Κινδύνου είναι η επίτευξη της μέγιστης δυνατής αποδοτικότητας, δηλαδή, με δεδομένο το αναμενόμενο κόστος του σχεδίου να εξασφαλιστεί το χαμηλότερο δυνατό επίπεδο έκθεσης σε κίνδυνο, ή αντίστροφα, με δεδομένο το επίπεδο έκθεσης σε κίνδυνο να εξασφαλιστεί το χαμηλότερο δυνατό κόστος.

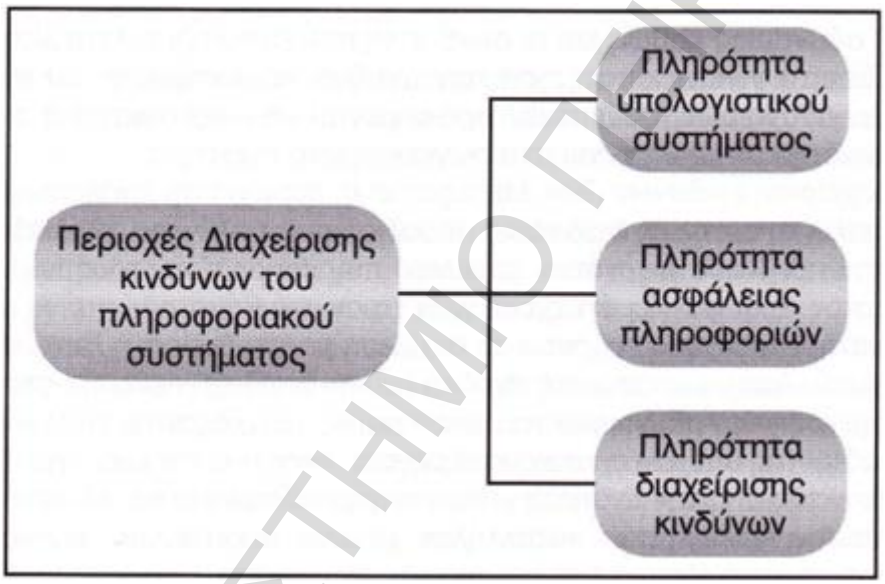
2.4 Γενικό Πλαίσιο Ανάλυσης και Διαχείρισης Κινδύνων

Ενδιαφέρον παρουσιάζει η προσπάθεια ανάπτυξης ενός γενικού πλαισίου ανάλυσης και διαχείρισης κινδύνων που προτάθηκε το 1993 από τους Eloff, Labuschagne και Badenhorst (Eloff, Labuschagne και Badenhorst, 1993) και περιέχει τις περιοχές διαχείρισης κινδύνων σε ένα σύστημα. Τις περιοχές αυτές αποτελούν:

- *η πληρότητα υπολογιστικού συστήματος*: Πρόκειται για έναν τομέα που εξελίσσεται και αναπτύσσεται συνεχώς, παράλληλα με την εξέλιξη της

τεχνολογίας. Οποιαδήποτε, λοιπόν, προσέγγιση ανάλυσης και διαχείρισης κινδύνων θα πρέπει να αναφέρεται στον τομέα αυτό.

- *η πληρότητα ασφάλειας πληροφοριών:* Προσδιορίζονται οι κίνδυνοι που αφορούν τη διαθεσιμότητα, ακεραιότητα, αυθεντικότητα και εγκυρότητα των πληροφοριών που διαχειρίζεται το σύστημα.
- *η πληρότητα διαχείρισης κινδύνων:* Το τμήμα αυτό ουσιαστικά ασχολείται πλήρως με τον προσδιορισμό των κινδύνων και αποτελείται από τέσσερις διαδοχικές φάσεις: προσδιορισμός κινδύνων (risk identification), εκτίμηση κινδύνων (risk assessment), επίλυση κινδύνων (risk resolution), έλεγχος κινδύνων (risk monitoring).



Σχήμα 2.2: Περιοχές ανάλυσης και διαχείρισης κινδύνων του πληροφοριακού συστήματος.

Η ανάλυση και διαχείριση κινδύνων είναι μια πρακτική με τις διαδικασίες, τις μεθόδους, και τα εργαλεία για την αντιμετώπιση των κινδύνων σε ένα έργο. Παρέχει ένα πειθαρχημένο περιβάλλον για τη δυναμική λήψη αποφάσεων, που βασίζονται σε (Κιουντούζης, 2004):

- συνεχή αξιολόγηση του τι θα μπορούσε να πάει στραβά (κίνδυνοι)
- προσδιορισμό των υπό εξέταση κινδύνων
- εφαρμογή στρατηγικών για την αντιμετώπιση αυτών των κινδύνων

Γενικότερα, θα μπορούσε να χαρακτηριστεί ως μια συστηματική διαδικασία χειρισμού των κινδύνων στους οποίους εκτίθεται μια επιχείρηση, ώστε να επιτύχει τους στόχους της κατά τρόπο σύμφωνο με το δημόσιο ενδιαφέρον, την ανθρώπινη ασφάλεια, τους περιβαλλοντικούς παράγοντες, και το νόμο. Αποτελείται από τον προγραμματισμό, την οργάνωση, την καθοδήγηση, το συντονισμό, και τον έλεγχο των

δραστηριοτήτων που αναλαμβάνονται με πρόθεση την παροχή ενός αποδοτικού σχεδίου που ελαχιστοποιεί το δυσμενή αντίκτυπο του κινδύνου στους πόρους της οργάνωσης, τις αποδοχές, και τις ροές μετρητών.

Για να μπορέσει ένας οργανισμός ή μια επιχείρηση να εφαρμόσει σωστή ανάλυση και διαχείριση των κινδύνων των έργων της, θα πρέπει να διέπεται από τρία (3) χαρακτηριστικά (Κιουντούζης, 2004):

1. Να ξεκινάει από την αρχική φάση (σύλληψη ή εννοιολογικός σχεδιασμός) του έργου και να αναπτύσσεται παράλληλα με τον κύκλο ζωής του.
2. Δεν πρέπει να λειτουργεί ως μια ανεξάρτητη διαδικασία, αλλά να είναι ενοποιημένη με τις λοιπές λειτουργίες της διαχείρισης έργου.
3. Μπορεί να συντονίζεται από κάποιους αρμόδιους, αλλά ευθύνη και ενεργό ρόλο έχουν όλοι οι συμμετέχοντες του έργου (stakeholders).

Τέλος, είναι γεγονός ότι η ολική εξάλειψη του κινδύνου είναι αδύνατη. Για αυτό, ο υπεύθυνος έργου οφείλει να διαχειριστεί το υπολειπόμενο ρίσκο όσο το δυνατόν πιο αποτελεσματικά.

2.5 Οι Αρχές της Ανάλυσης και Διαχείρισης Κινδύνων

Οι θεμελιώδεις αρχές της ανάλυσης και διαχείρισης κινδύνων μπορούν να συνοψιστούν στα παρακάτω (Δρυμούσης, 2007):

1. *Ποσοτικοποίηση των απαιτήσεων:* Όλες οι κρίσιμες απαιτήσεις σε πόρους και απόδοση επιβάλλεται να προσδιοριστούν και να ποσοτικοποιηθούν αριθμητικά
2. *Μεγιστοποίηση του κέρδους:* Εστίαση στην επίτευξη των μέγιστων οφελών στα πλαίσια του προϋπολογισμού και των χρονοδιαγραμμάτων, παρά στην προσπάθεια να αποβληθεί όλος ο κίνδυνος.
3. *Ελαχιστοποίηση στο μέγιστο ή ακόμη και εξάλειψη του πλέον ανεπιθύμητου κινδύνου:* Ο “απαράδεκτος κίνδυνος” πρέπει να αποφεύγεται συνειδητά σε όλα τα στάδια, επίπεδα και περιοχές σχεδιασμού του έργου.
4. *Σχεδιασμός στον πλεονασμό:* Κατά τον προγραμματισμό και εκτέλεση ενός έργου, αποτελεί απαραίτητο κόστος η χρήση εφεδρικού πλεονασμού για την αντιμετώπιση των κίνδυνων.
5. *Παρουσία οργάνων ελέγχου:* Στις διαδικασίες ανάπτυξης και συντήρησης πρέπει να προγραμματιστεί ένας συχνός και μετρήσιμος έλεγχος ώστε να

προσδιοριστούν και αξιολογηθούν τυχόν κίνδυνοι εγκαίρως, προτού γίνουν επικίνδυνοι.

6. *Μείωση του επιπέδου κινδύνου:* Το συνολικό επίπεδο κινδύνου σε οποιοδήποτε χρόνο πρέπει να είναι συνειδητά μεταξύ 2% και 5% του συνολικού προϋπολογισμού.
7. *Επαναχρησιμοποίηση όλων των γνώσεων σε σχέση με τον κίνδυνο:* Πρότυπα, κανόνες και καθοδήγηση πρέπει να βοηθήσουν στην ορθή πρακτική και ταυτόχρονα σε μια συνεχή βελτίωση της διαδικασίας.
8. *Προσωπική ευθύνη για τον κίνδυνο:* Κάθε υπεύθυνος πρέπει να έχει την αποκλειστική αρμοδιότητα στον τομέα του, ώστε να μπορεί να αναγνωρίζει και να αντιμετωπίζει τους ενδεχόμενους κινδύνους.
9. *"Ανάθεση" κινδύνου:* Η ύπαρξη, βάση συμφωνιών και συμβολαίων, αρμόδιων για κινδύνους προμηθευτών και συνεργατών, θα οδηγήσει σε καλύτερη παροχή υπηρεσιών.

2.6 Προτερήματα και Περιορισμοί Ανάλυσης και Διαχείρισης Κινδύνων

Στα πλεονεκτήματα της ανάλυσης και διαχείρισης κινδύνων περιλαμβάνονται τα παρακάτω (Νικήτας, 2004):

- Παρέχει τη δυνατότητα αιτιολόγησης του κόστους των αντιμέτρων, βοηθώντας έτσι την εξάλειψη των άσκοπων δαπανών και την πιο αποτελεσματική αντιμετώπιση των πραγματικών προβλημάτων ασφάλειας.
- Αποτελεί ένα εργαλείο επικοινωνίας ανάμεσα στους ειδικούς των πληροφοριακών συστημάτων και στη διοίκηση των οργανισμών, καθώς επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντας την ασφάλεια ως «επένδυση» που αποτιμάται με όρους κόστους/οφέλους.
- Συμβάλλει στην κατανόηση της αναγκαιότητας της ασφάλειας. Η συμμετοχή στη διαδικασία της ανάλυσης και διαχείρισης κινδύνων διαμορφώνει μια καλύτερη κατανόηση των προβλημάτων ασφαλείας, καθώς και των επιπτώσεων που μπορεί να έχουν αυτά. Με τον τρόπο αυτό επιτυγχάνεται καλύτερη επιλογή 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 και ως εκ τούτου την αύξηση της αξιοπιστίας της εκάστοτε εταιρείας.

- Είναι αρκετά ευέλικτη, ώστε να μπορεί να ενταχθεί σε διάφορα επιστημολογικά πλαίσια και να εφαρμόζεται είτε αυτούσια, είτε σε συνδυασμό με άλλες μεθοδολογίες. Η πολιτική ασφάλειας, δηλαδή, ανταποκρίνεται στις ιδιαίτερες ανάγκες του οργανισμού για τον οποίο έχει μελετηθεί η επικινδυνότητα.
- Καλύπτει τις απαιτήσεις της ευρωπαϊκής και ελληνικής νομοθεσίας, που απαιτούν από τα πληροφοριακά συστήματα, τα οποία επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας, έτσι ώστε «να εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων».
- Διευκολύνει την καλύτερη κατανόηση της φύσης και της λειτουργίας του πληροφοριακού συστήματος. Αποτελεί, δηλαδή, ένα μέσο καταγραφής και ανάλυσης αυτού. Καταρχάς αναγνωρίζονται οι διάφορες απειλές και φανερώνονται οι ευπάθειες του. Επίσης, κατανοείται η πραγματική αξία των επιμέρους συστημάτων που αποτελούν το πληροφοριακό σύστημα.
- Αποτελεί την πλέον διαδεδομένη μεθοδολογία σχεδιασμού και διαχείρισης της ασφάλειας πληροφοριακών συστημάτων και έχει εφαρμοστεί με επιτυχία σε ένα μεγάλο πλήθος περιπτώσεων.

Παράλληλα, όμως, η μεθοδολογία ανάλυσης και διαχείρισης κινδύνων παρουσιάζει σημαντικά μειονεκτήματα, όπως τα παρακάτω:

- Στηρίζεται σε ένα απλοϊκό μοντέλο του πληροφοριακού συστήματος και αγνοεί τα ιδιαίτερα χαρακτηριστικά και τις απαιτήσεις του οργανισμού στον οποίο ανήκει το πληροφοριακό σύστημα.
- Εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις τόσο της αξίας των αγαθών, όσο και της αποτίμησης απειλών και ευπαθειών. Τα αποτελέσματα, δηλαδή, μιας μεθόδου ανάλυσης και διαχείρισης κινδύνων εξαρτώνται σε μεγάλο βαθμό από την εμπειρία και τις γνώσεις του αναλυτή. Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών-πιθανοτικών μοντέλων στα οποία στηρίζεται, τη συστηματικότητα των περισσότερων μεθόδων ανάλυσης επικινδυνότητας και την ‘αντικειμενικότητα’ των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.
- Βασίζεται σε απλές στατιστικές μεθόδους για τον υπολογισμό της πιθανότητας εμφάνισης μιας απειλής. Η εγκυρότητα της εφαρμογής των μεθόδων αυτών στον τομέα της ασφάλειας πληροφοριακών συστημάτων έχει αμφισβητηθεί από πολλούς ερευνητές.

2.7 Η Αναγκαιότητα της Ανάλυσης και Διαχείρισης Κινδύνων

Μετά τη δημιουργία ενός ρεαλιστικού προγραμματισμού έργου και ενός λεπτομερούς σχεδίου υλοποίησης, η πρόοδος του έργου αξιολογείται βάση αυτού του σχεδίου. Ο εν λόγω προγραμματισμός αποτελεί τον οδηγό του έργου και οτιδήποτε παρεμβληθεί μπορεί να αποβεί καταστροφικό για την πορεία του έργου και τις πιθανότητες επιτυχίας του. Δυστυχώς, ακόμα και στα καλύτερα σχεδιασμένα πλάνα κάτι μπορεί να πάει στραβά από καιρό σε καιρό. Αυτά τα προβλήματα επηρεάζουν τον προγραμματισμό, με αποτέλεσμα να εκπονείται πλάνο αποκατάστασης, ώστε να ξεπεραστεί το πρόβλημα και να κερδιστεί όσος χρόνος χάθηκε κατά τη διαδικασία επίλυσης του προβλήματος. Η πλέον διαδεδομένη μέθοδος, η οποία στοχεύει στην αντιμετώπιση των παραπάνω ζητημάτων, είναι η μεθοδολογία της ανάλυσης και διαχείρισης κινδύνων πληροφοριακών συστημάτων, ώστε να προβλεφθούν τυχόν προβλήματα και να ληφθούν οι κατάλληλες δράσεις αποφυγής τους. Η μεθοδολογία αυτή, δηλαδή, υιοθετεί την έννοια της επικινδυνότητας, η οποία προέρχεται από το χώρο της χρηματοοικονομικής διοίκησης, υποκαθιστώντας το στόχο της επίτευξης της ασφάλειας με τον εφικτό και μετρήσιμο στόχο του περιορισμού της επικινδυνότητας που ενέχεται στη λειτουργία ενός πληροφοριακού συστήματος εντός αποδεκτών ορίων (Κάτσικας, 2001).

Συγκεκριμένα, μερικοί λόγοι για τους οποίους η αποτελεσματική ανάλυση και διαχείριση κινδύνων είναι σημαντική και ευεργετική έχουν να κάνουν με:

- *το περιβάλλον:* Ένα εναλλασσόμενο περιορισμένο περιβάλλον έργου, συμπεριλαμβανομένων της συρρίκνωσης, των «σφιχτότερων» προϋπολογισμών, και της επιθυμίας να αναπτυχθούν και να παραδοθούν τα συστήματα γρηγορότερα, έχει ως συνέπεια η ανάπτυξη και η παράδοση πολλών συστημάτων να ενέχει υψηλότερο κίνδυνο από τον συνηθισμένο. Για τη λειτουργία των συστημάτων, η απαίτηση να ολοκληρωθεί το ίδιο (ή μεγαλύτερο) επίπεδο διαδικασιών με λιγότερο προσωπικό και λιγότερη συντήρηση σημαίνει ότι αυτές οι διαδικασίες εμπεριέχουν υψηλότερο κίνδυνο από τον αναμενόμενο.
- *την επίσημη μεθοδολογία:* Η ανάλυση και διαχείριση κινδύνου είναι ένα δομημένο εργαλείο για τις καθημερινές αποφάσεις.
- *τις επίσημες διαδικασίες:* Κατά την εμφάνιση απρόβλεπτων προβλημάτων (όπως τα εξωτερικά γεγονότα που δεν ήταν προβλέψιμα), η ανάλυση και διαχείριση κινδύνων μπορεί να συμβάλει στην αποτελεσματική λύση τους.
- *τη γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος:* Περιλαμβάνει και τη δικαιολόγηση των δαπανών για την ασφάλεια.
- *την καλύτερη κατανόηση του πληροφοριακού συστήματος*.

Η ανάλυση και διαχείριση κινδύνων ενδιαφέρεται για τα μελλοντικά γεγονότα, η ακριβής έκβαση των οποίων είναι άγνωστη, και για το πώς να εξετάσει αυτές τις αβεβαιότητες (π.χ., μια σειρά πιθανών εκβάσεων) εκ των προτέρων. Γενικά, οι εκβάσεις είναι ταξινομημένες ως έκταση από ευνοϊκές σε δυσμενείς και η διαχείριση

κινδύνων είναι η τέχνη και η επιστήμη του προγραμματισμού, αξιολογώντας, αντιμετωπίζοντας και ελέγχοντας ενέργειες που οδηγούν σε μελλοντικά γεγονότα, ώστε να εξασφαλιστούν ευνοϊκές εκβάσεις. Κατά συνέπεια, μια σωστή διαδικασία διαχείρισης κινδύνου είναι δυναμικής φύσης και πλήρως διαφορετική από τη διαχείριση κρίσης (ή την επίλυση προβλήματος), η οποία είναι αντιδραστική. Επιπλέον, η διαχείριση κρίσης είναι μια εντατική διαδικασία που περιορίζεται από ένα πεπερασμένο σύνολο διαθέσιμων επιλογών. Αυτό συμβαίνει εν μέρει επειδή οι επιλογές επίλυσης ενός προβλήματος μειώνονται χαρακτηριστικά, καθώς ο χρόνος για την επίλυση των προβλημάτων αυξάνεται. Οι δυσμενείς επιδράσεις δαπανών, σχεδιασμού και απόδοσης που συνδέονται με τις συγκεκριμένες επιλογές είναι πιθανό να είναι ουσιαστικά μεγαλύτερες εάν τα ζητήματα δεν είχαν ήδη προσδιοριστεί.

Θα μπορούσαμε να πούμε ότι η ανάλυση και διαχείριση κινδύνων είναι η διαδικασία που επιτρέπει στους υπεύθυνους των πληροφοριακών έργων να εξισορροπούν τις λειτουργικές και οικονομικές δαπάνες για τα μέτρα προστασίας με το επίπεδο ασφαλείας του εκάστοτε έργου. Οι δαπάνες αυτές κρίνεται απαραίτητο να μην είναι υπερβολικές, γιατί τότε ενδεχομένως να μην είναι καν συμφέρουσα η ανάληψη του έργου, αλλά δε θα πρέπει να αντιμετωπίζονται και σαν περιττά έξοδα και να περικόπτονται ασύστολα, γιατί η ενδεχόμενη εμφάνιση ενός κινδύνου, και μάλιστα ήδη προβλεφθέντος που δε μεριμνήθηκε η αντιμετώπιση του, θα μπορούσε να μεταβάλλει την όλη υλοποίηση του έργου σε μια ζημιογόνο διαδικασία. Στη σημερινή εποχή, που ο ανταγωνισμός μεταξύ των εταιρειών είναι μεγάλος, η ανάληψη ενός έργου προϋποθέτει τη μείωση του κέρδους για να μπορέσει η κάθε υποψήφια ανάδοχος εταιρεία να παρουσιάσει μια ανταγωνιστική πρόταση. Όταν, λοιπόν, τα κέρδη έχουν ήδη μειωθεί σε τόσο μεγάλο βαθμό, γίνεται επιτακτική η ανάγκη εξασφάλισης ότι τίποτα απρόοπτο δε θα συμβεί που θα επιβαρύνει οικονομικά το έργο, αλλά και ότι θα επιβαρυνθεί κατά το ελάχιστο δυνατό το κόστος υλοποίησης του έργου από τα μέτρα προστασίας κατά των πάσης φύσεως κινδύνων που το απειλούν.

Ο υπεύθυνος, λοιπόν, του σχεδιασμού ενός τέτοιου έργου θα πρέπει να είναι σε θέση να ισορροπήσει τις παραπάνω καταστάσεις, ή ακόμα και στη χειρότερη των περιπτώσεων να μπορεί να αναγνωρίσει και να αποδεχτεί αν τελικά η υλοποίηση κάποιου έργου από την εταιρεία θα αποδειχθεί επιζήμια και δε θα πρέπει να γίνει η ανάληψή του. Για να μπορέσει, όμως, να φτάσει σε ένα ασφαλές συμπέρασμα για το τι πρέπει να πράξει είναι αναγκαίο να ακολουθήσει μια καλά δομημένη και επιστημονική διαδικασία, όπως είναι η ανάλυση και διαχείριση κινδύνων. Μάλιστα, μια τέτοια μελέτη πρέπει να ετοιμαστεί με ακόμα μεγαλύτερη υπευθυνότητα όταν πρόκειται για μεγάλα πληροφοριακά έργα, εξαιτίας του μεγάλου τους κόστους, της μεγάλης αξίας των χρονικών καθυστερήσεων, της πληθώρας κινδύνων που τα απειλούν λόγω της πολυπλοκότητας τους αλλά και της ευαισθησίας τους λόγω των τεχνολογικών καινοτομιών που τα συνοδεύουν.

Μια τέτοια μελέτη, φυσικά, πέρα από τον κύριο σκοπό που έχει να επιτελέσει, θα μπορούσε να προσφέρει χρήσιμες πληροφορίες και για τον όλο σχεδιασμό του έργου. Θα παράσχει πληροφορίες και για τις δυνατότητες της εταιρείας στην οποία ανήκει, αλλά και τεχνογνωσία για ακόμα πιο ολοκληρωμένες και πετυχημένες προτάσεις ανάληψης ενός έργου στο μέλλον.

Η ανάλυση και διαχείριση κινδύνων ενός πληροφοριακού συστήματος, αντιμετωπιζόμενη ως επιστημονική μέθοδος, θεωρείται μη αυστηρά τεκμηριωμένη και για αυτό το λόγο έχει υποστεί αυστηρή κριτική. Παρόλα αυτά, πρακτικά είναι η μοναδική ακολουθητέα μεθοδολογία μέχρι σήμερα σε διεθνή κλίμακα. Ο κυριότερος λόγος είναι ότι λειτουργεί ως επιτυχής δίαυλος επικοινωνίας μεταξύ των τεχνικών εμπειρογνωμόνων σε θέματα ασφάλειας και της διοίκησης ενός οργανισμού. Το γεγονός αυτό εκτιμάται ως εξαιρετικά σημαντικό, δεδομένου ότι τα απαιτούμενα μέτρα προστασίας και εξασφάλισης των πληροφοριακών συστημάτων ενός οργανισμού πρέπει να ληφθούν με συνεργασία αμφοτέρων των μερών. Η ανάλυση και η διαχείριση κινδύνων επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση και έτσι δεν απαιτείται αυτή να διαθέτει εξειδικευμένες τεχνικές γνώσεις (Chapman και Ward, 1996).

Κάθε βήμα της ανάλυσης και διαχείρισης κινδύνων προσφέρει ένα κατάλληλο κύριο σημείο για αναφορά, αναθεώρηση και δράση. Κάθε επόμενο βήμα εξαρτάται και χτίζεται πάνω στη δουλειά που έγινε στο προηγούμενο, παρέχοντας μια εξελισσόμενη κατανόηση των ζητημάτων και την ανάπτυξη περισσότερο θεμελιωμένων ενεργειών.

Τέλος, πρέπει να σημειώσουμε ότι τόσο η ισχύουσα (ν. 2472/97) όσο και η υπό ψήφιση (νόμος για την ασφάλεια των επικοινωνιών) ελληνική νομοθεσία αποδίδει ιδιαίτερη σημασία στον εντοπισμό των κατάλληλων (σε σχέση με το κόστος και με τους κινδύνους που καλούνται να αντιμετωπίσουν) μέτρων ασφάλειας. Πράγματι, σύμφωνα με το άρθρο 10, παρ. 3 του ν. 2472/97, «Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας». Είναι φανερό, λοιπόν, ότι η ανάλυση και διαχείριση κινδύνων αποκτά βαρύνουσα σημασία, αφού στην ουσία αποτελεί υποχρέωση του υπεύθυνου επεξεργασίας, όπως απορρέει από το νόμο.

2.8 Τομείς της Παραγωγικής Διαδικασίας στους Οποίους Εμπλέκεται η Ανάλυση και Διαχείριση Κινδύνων

Η ελαχιστοποίηση των αρνητικών επιπτώσεων σε έναν οργανισμό και η ανάγκη για υγιείς βάσεις στη διαδικασία λήψης αποφάσεων είναι οι θεμελιώδεις λόγοι για τους οποίους ένας οργανισμός εφαρμόζει τη διαδικασία ανάλυσης και διαχείρισης κινδύνων για τα πληροφοριακά του συστήματα. Η αποτελεσματική διαχείριση κινδύνου πρέπει να

ενσωματωθεί συνολικά σε όλο τον κύκλο ζωής ενός πληροφοριακού έργου, ο οποίος αποτελείται από πέντε φάσεις: εκκίνηση, ανάπτυξη ή απόκτηση, εφαρμογή, έναρξη λειτουργίας/συντήρηση και διάθεση. Σε μερικές περιπτώσεις, ένα έργο πληροφορικής μπορεί να βρίσκεται σε περισσότερες από μία φάσεις συγχρόνως, δηλαδή είναι πιθανό αυτές να αλληλεπικαλύπτονται. Εντούτοις, η μεθοδολογία ανάλυσης και διαχείρισης κινδύνου είναι η ίδια ανεξάρτητα από τη φάση του κύκλου ζωής για την οποία πραγματοποιείται η εκτίμηση, ενώ αποτελεί και μια επαναληπτική διαδικασία που μπορεί να εκτελεστεί κατά τη διάρκεια κάθε σημαντικής φάσης. Στον πίνακα 2.1 που ακολουθεί παρουσιάζεται η εμπλοκή που έχει η διαδικασία ανάλυσης και διαχείρισης κινδύνων σε όλες τις φάσεις του κύκλου ζωής του έργου (Stoneburner, Goguen και Feringa, 2001).

Φάση του Κύκλου Ζωής του Έργου	Χαρακτηριστικά κάθε Φάσης	Υποστήριξη από τις Δραστηριότητες Ανάλυσης και Διαχείρισης Κινδύνων
1η Φάση **Εκκίνηση**	Εκφράζεται η ανάγκη υλοποίησης ενός έργου πληροφορικής και καθορίζεται πλήρως το πεδίο και ο σκοπός του.	Οι αναγνωρισμένοι κίνδυνοι χρησιμοποιούνται κατά την αναζήτηση των απαιτήσεων του έργου, και ειδικότερα των απαιτήσεων ασφάλειας, αλλά και κατά τον καθορισμό των διαδικασιών ασφάλειας.
2η Φάση **Ανάπτυξη ή απόκτηση**	Το πληροφοριακό σύστημα σχεδιάζεται, αγοράζεται, προγραμματίζεται, αναπτύσσεται ή κατασκευάζεται.	Οι κίνδυνοι που προσδιορίζονται κατά τη διάρκεια αυτής της φάσης μπορούν να χρησιμοποιηθούν για να υποστηρίξουν τις αναλύσεις ασφάλειας του συστήματος, που είναι πιθανό να οδηγήσουν σε αλλαγές αρχιτεκτονικής και σχεδίου κατά τη διάρκεια της ανάπτυξης των συστημάτων.

3η Φάση **Εφαρμογή**	Τα χαρακτηριστικά των συστημάτων ασφαλείας διαμορφώνονται, ενεργοποιούνται, εξετάζονται και ελέγχονται.	Αξιολογείται η εφαρμογή των συστημάτων έναντι των απαιτήσεών τους σε ένα μοντελοποιημένο λειτουργικό περιβάλλον. Οι αποφάσεις σχετικά με τους προσδιορισμένους κινδύνους πρέπει να ληφθούν προτού τα συστήματα τεθούν σε λειτουργία.
4η Φάση **Έναρξη Λειτουργίας/Συντήρηση**	Το σύστημα εκτελεί τις λειτουργίες του. Ουσιαστικά, το σύστημα τροποποιείται σε μια τρέχουσα βάση μέσω της προσθήκης υλικού (hardware) και λογισμικού (software) καθώς και από αλλαγές στις διαδικασίες και πολιτικές του οργανισμού.	Οι δραστηριότητες της ανάλυσης και διαχείρισης κινδύνων πραγματοποιούνται για την περιοδική εξουσιοδότηση των συστημάτων ή όποτε γίνονται σημαντικές αλλαγές στο λειτουργικό ή στο περιβάλλον παραγωγής του λειτουργικού συστήματος.
5η Φάση **Διάθεση**	Μπορεί να περιλαμβάνονται οι δραστηριότητες διάθεσης των πληροφοριών, του υλικού (hardware) και του λογισμικού (software). Οι δραστηριότητες αυτές ενδέχεται να εμπεριέχουν τη μετακίνηση, την αρχειοθέτηση, την απόρριψη ή την καταστροφή των πληροφοριών και την αποστείρωση του υλικού και του λογισμικού.	Οι δραστηριότητες ανάλυσης και διαχείρισης κινδύνων εκτελούνται για τα τμήματα των συστημάτων που θα διατεθούν ή θα αντικατασταθούν, με σκοπό να εξασφαλιστεί ότι το υλικό (hardware) και το λογισμικό (software) διατίθενται κατάλληλα, ότι τα υπόλοιπα δεδομένα χρησιμοποιούνται ορθά και ότι η μετακίνηση των συστημάτων διευθύνεται με ασφαλή και συστηματικό τρόπο.

Πίνακας 2.1: Συμμετοχή ανάλυσης και διαχείρισης κινδύνων στη διαδικασία παραγωγής.

2.9 Συμμετοχή Στελεχών στην Ανάλυση και Διαχείριση Κινδύνων

Στην παράγραφο αυτή περιγράφονται οι βασικοί ρόλοι των στελεχών του οργανισμού που πρέπει να υποστηρίξουν και να συμμετάσχουν στη διαδικασία ανάλυσης και διαχείρισης κινδύνων (Stoneburner, Goguen και Feringa, 2001):

Ανώτερη διοίκηση (Senior Management):

Η ανώτερη διοίκηση φέρει τη μεγαλύτερη ευθύνη για τη διεκπεραίωση του έργου και πρέπει να εξασφαλίσει ότι οι απαραίτητοι πόροι διατίθενται αποτελεσματικά για την ικανοποίηση των αναγκών που απαιτούνται με σκοπό την ολοκλήρωση του έργου. Πρέπει να αξιολογήσει και να ενσωματώσει τα αποτελέσματα της εκτίμησης κινδύνου στη διαδικασία λήψης απόφασης. Η κατάρτιση ενός αποτελεσματικού προγράμματος διαχείρισης κινδύνων που να αξιολογεί και να μετριάζει τους σχετικούς με το πληροφοριακό έργο κινδύνους, απαιτεί την υποστήριξη και τη συμμετοχή της ανώτερης διοίκησης.

Κύριο ανώτερο στέλεχος πληροφοριών (Chief Information Officer - CIO):

Το στέλεχος αυτό είναι αρμόδιο για το σχεδιασμό του πληροφοριακού έργου, τη σύνταξη του προϋπολογισμού και την απόδοσή του, συμπεριλαμβανομένων και των τμημάτων που αφορούν την ασφάλεια των πληροφοριών. Οι αποφάσεις που λαμβάνονται για αυτά τα θέματα πρέπει να βασιστούν σε ένα αποτελεσματικό πρόγραμμα ανάλυσης και διαχείρισης κινδύνου.

Κάτοχοι συστημάτων και πληροφοριών (System and Information Owners):

Οι κάτοχοι συστημάτων και πληροφοριών είναι αρμόδιοι να εξασφαλίσουν ότι οι κατάλληλοι έλεγχοι θα πραγματοποιηθούν με σκοπό την εξέταση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των συστημάτων και των στοιχείων του έργου λογισμικού, του οποίου έχουν την κυριότητα. Ουσιαστικά, είναι υπεύθυνοι για τις αλλαγές στα πληροφοριακά τους συστήματα, δηλαδή αυτοί που θα εγκρίνουν τις όποιες αλλαγές, όπως για παράδειγμα προσθήκη νέων συστημάτων ή αλλαγές στο υλικό (hardware) και στο λογισμικό (software). Επιβάλλεται, λοιπόν, να καταλάβουν το ρόλο τους στη διαδικασία ανάλυσης και διαχείρισης κινδύνων και να την υποστηρίξουν πλήρως.

Επιχειρησιακοί και λειτουργικοί διευθυντές (Business and Functional Managers):

Οι αρμόδιοι διευθυντές για τις επιχειρησιακές διαδικασίες και τη διαδικασία προμήθειας πληροφοριακών συστημάτων πρέπει να πάρουν ενεργό ρόλο στη διαδικασία ανάλυσης και διαχείρισης κινδύνου. Οι διευθυντές αυτοί είναι τα πρόσωπα που φέρουν την ευθύνη για αποφάσεις αλλαγών, ουσιαστικών για την ολοκλήρωση του εκάστοτε έργου. Η συμμετοχή τους στη διαχείριση κινδύνων παρέχει την κατάλληλη ασφάλεια των πληροφοριακών συστημάτων, η οποία, εάν χρησιμοποιηθεί σωστά, θα

προσφέρει την αποτελεσματική ολοκλήρωση της αποστολής με τις ελάχιστες δυνατές δαπάνες πόρων.

Διευθυντές Προγράμματος Ασφάλειας (Information System Security Officer):

Οι διευθυντές προγράμματος ασφάλειας πληροφοριακών συστημάτων και τα ανώτερα στελέχη ασφάλειας υπολογιστών είναι αρμόδιοι για τα προγράμματα ασφάλειας του οργανισμού, συμπεριλαμβανομένης και της ανάλυσης και διαχείρισης κινδύνου. Επομένως, διαδραματίζουν κύριο ρόλο στην εισαγωγή μιας κατάλληλης, δομημένης μεθοδολογίας για να βοηθήσουν στον προσδιορισμό, την αξιολόγηση και την ελαχιστοποίηση των κινδύνων των πληροφοριακών συστημάτων που υποστηρίζουν τις λειτουργίες του οργανισμού. Ενεργούν, επίσης, και ως σύμβουλοι της ανώτερης διοίκησης και εξασφαλίζουν ότι αυτή η δραστηριότητα πραγματοποιείται σε διαρκή βάση.

Χειριστές συστημάτων ασφάλειας πληροφοριακών έργων (Information Technology Security Practitioners):

Τα στελέχη αυτά (για παράδειγμα διοικητές βάσεων δεδομένων, ειδικοί υπολογιστών, αναλυτές ασφάλειας, σύμβουλοι ασφάλειας) είναι αρμόδια για τη σωστή εφαρμογή των απαιτήσεων ασφάλειας των πληροφοριακών συστημάτων. Καθώς οι αλλαγές εμφανίζονται στο υπάρχον λογισμικό περιβάλλον (π.χ. επέκταση στη συνδεσιμότητα δικτύων, αλλαγές στην υπάρχουσα υποδομή και στην πολιτική του οργανισμού, εισαγωγή νέων τεχνολογιών), οφείλουν να υποστηρίξουν ή να χρησιμοποιήσουν τη διαχείριση κινδύνων για να προσδιορίσουν και να αξιολογήσουν τους νέους πιθανούς κινδύνους και να εφαρμόσουν τους νέους ελέγχους ασφάλειας, όπως απαιτούνται για την προστασία των συστημάτων.

Εκπαιδευτές χρήσης συστημάτων ασφάλειας (Security Awareness Trainers):

Η χρήση των συστημάτων και των στοιχείων πληροφορικής, σύμφωνα με την πολιτική, τις οδηγίες και τους κανόνες συμπεριφοράς του οργανισμού, είναι κρίσιμη για τον μετριασμό του κινδύνου και την προστασία των πληροφοριακών συστημάτων. Είναι ουσιαστικό, λοιπόν, οι χρήστες να έχουν συνείδηση της αξίας των συστημάτων και μηχανισμών ασφάλειας τους. Επομένως, οι εκπαιδευτές ασφάλειας πρέπει να κατανοήσουν τη διαδικασία ανάλυσης και διαχείρισης κινδύνου, έτσι ώστε να μπορούν να αναπτύξουν τα κατάλληλα μέσα κατάρτισης του προσωπικού και να ενσωματώσουν την αξιολόγηση κινδύνου στα επιμορφωτικά προγράμματα εκπαίδευσης των τελικών χρηστών.

Ένα σύστημα ανάλυσης και διαχείρισης κινδύνων απαιτεί κόστος και προσπάθεια για την ενεργοποίηση των ανθρώπων μέσα σε έναν οργανισμό. Αυτά τα στελέχη που επωμίζονται το ρόλο και την ευθύνη της ανάλυσης και διαχείρισης κινδύνων θα πρέπει να έχουν ικανότητες και επιδεξιότητες τέτοιες, ώστε να οδηγήσουν την ομάδα έργου

στην υλοποίηση των στόχων, διαχειριζόμενοι με επιτυχία τους κινδύνους που εμφανίζονται. Χωρίς αυτές τις ικανότητες, η ανάλυση και διαχείριση κινδύνων παραμένει απλά μια ευχή. Ένας ικανός διαχειριστής κινδύνων θα πρέπει να έχει όλες ή τις περισσότερες από τις παρακάτω ιδιότητες (Θωμά - Τσοπουρίδου, 2011):

- προληπτική συμπεριφορά αντιμετώπισης των κινδύνων και ικανότητα ανάληψης συνετών αποφάσεων με λογικό ρίσκο
- προσαρμοστικότητα στις αλλαγές
- ικανότητα παραδοχής λαθών και εκμάθησης μέσω αυτών
- γνώση της διεργασίας λήψης αποφάσεων που αφορούν την ανάλυση και διαχείριση κινδύνων
- ικανότητα να αντιμετωπίζει την αβεβαιότητα και να λειτουργεί υπό πίεση εξίσου καλά
- ικανότητα επικοινωνίας με τους μετόχους του έργου, ειλικρίνεια και ακεραιότητα
- ικανότητα επίλυσης πολυδιάστατων προβλημάτων και υψηλή συναισθηματική νοημοσύνη
- διορατικότητα και ικανότητα δημιουργίας εναλλακτικών σεναρίων
- ευκολία συνεργασίας με άλλα τμήματα και ομάδες, επαγγελματισμό και διοικητικές ικανότητες

ΚΕΦΑΛΑΙΟ 3

Ανάλυση Κινδύνων σε Έργα Πληροφοριακών Συστημάτων

3.1 Γενική Μεθοδολογία Ανάλυσης Κινδύνων

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 αποτρέψουν ή θα μειώσουν τον κίνδυνο σε αποδεκτά επίπεδα. Αυτός, με λίγα λόγια, είναι ο σκοπός της ανάλυσης κινδύνων. Μια ουσιαστική αφετηρία για την ανάλυση κινδύνων είναι η δήλωση των στόχων του κάθε έργου, οι οποίοι μπορούν να χωριστούν σε αποτελέσματα, ενέργειες ή χαμηλότερου επιπέδου δραστηριότητες (Λέρα, 2012).

Ο βασικός τύπος που αποτελεί την καρδιά της ανάλυσης κινδύνων είναι: $B > P \times L$,

όπου B = το κόστος για την πρόληψη μιας απώλειας,

P = η πιθανότητα να συμβεί μια απώλεια,

L = το συνολικό κόστος μιας απώλειας.

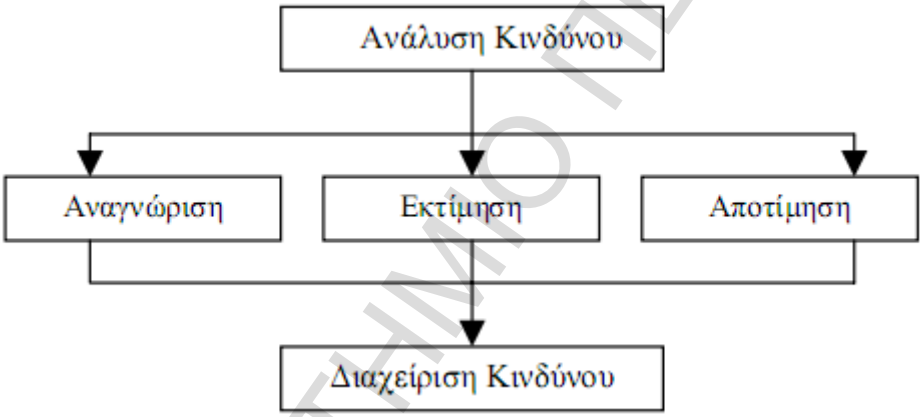
Ο τύπος αυτός αποτελεί την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων, την ιδέα, δηλαδή, του υπολογισμού της πιο συμφέρουσας λύσης, όχι μόνο για πληροφοριακά συστήματα. Το νόημα του τύπου είναι ότι όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή, τότε η υλοποίηση του μέτρου πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση, το μέτρο πρόληψης συμφέρει να υλοποιηθεί.

Ωστόσο, ο υπολογισμός του τύπου και η πρακτική του εφαρμογή βρίσκουν 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 αντιστοίχιση των απωλειών με οικονομικά νούμερα δεν είναι πάντα δυνατή, διότι πολλές φορές στην ανάλυση κινδύνων αξιολογούνται απροσδιόριστες απώλειες, όπως η εικόνα ενός οργανισμού και η εμπιστοσύνη που έχουν οι πελάτες του σε αυτόν. Όμως, ακόμα και αν δε χρησιμοποιείται άμεσα, όλες οι μέθοδοι της ανάλυσης κινδύνων βασίζονται πάνω στην λογική του τύπου BPL.

Γενικά, λοιπόν, είναι σημαντικό να γίνει η επιλογή της μεθοδολογίας ανάλυσης κινδύνων που θα εφαρμοστεί. Οι υπάρχουσες διαφορετικές μεθοδολογίες είναι πολυποίκιλες, αν και οι περισσότερες είναι απλά παραλλαγές μιας γενικής

μεθοδολογίας. Αυτή η γενική μεθοδολογία αποτελείται από τρία στάδια (Gerber και Solms, 2005) (σχήμα 3.1):

1. ***Αναγνώριση Κινδύνου (Risk Identification):*** Δημιουργία ενός καταλόγου με όλους τους πιθανούς παράγοντες κινδύνου που θα μπορούσε να αντιμετωπίσει ένα έργο.
2. ***Εκτίμηση Κινδύνου (Risk Estimation):*** Προσδιορισμός της έκθεσης σε κάθε παράγοντα κινδύνου, λαμβάνοντας υπόψη είτε την εκτιμώμενη πιθανότητα να εμφανιστεί ο κίνδυνος και την πιθανή επίπτωσή του, είτε το βάρος του κινδύνου σε σχέση με τους υπολοίπους και τη σοβαρότητά του.
3. ***Αποτίμηση Κινδύνου (Risk Evaluation):*** Εκτίμηση της αποδοχής κάθε παράγοντα κινδύνου, προκειμένου να αποφασιστούν οι ενέργειες που πρέπει να γίνουν.



Σχήμα 3.1: Η μετάβαση από την οργάνωση στην ανάλυση κινδύνου.

3.1.1 Αναγνώριση Κινδύνου

Η αναγνώριση κινδύνου είναι η διαδικασία προσδιορισμού των επικίνδυνων γεγονότων και της φύσης τους, των συνθηκών, δηλαδή, κάτω από τις οποίες ενδεχομένως να παράγονται δυσμενείς επιδράσεις (πίνακας 3.1). Συγκεκριμένα, πρόκειται για τη διαδικασία συλλογής στοιχείων και κατασκευής ενός αφηρημένου μοντέλου του πληροφοριακού συστήματος και του περιβάλλοντός του (οριοθέτησή του). Προσδιορίζονται τα περιουσιακά του στοιχεία (αγαθά) που θα προστατευθούν, οι πιθανές απειλές και οι αδυναμίες που υπάρχουν. Βασικός στόχος είναι ο προσδιορισμός και η ανάλυση των συνεπειών από μια απειλή σε ένα συγκεκριμένο αγαθό. Στο στάδιο αυτό, ουσιαστικά, γίνεται προσπάθεια εντοπισμού όλων των δυνατών και πιθανών συνδυασμών «αγαθού - απειλής - αδυναμίας» που μπορεί να υπάρχουν και επομένως οι πιθανοί κίνδυνοι (Ξανθόπουλος, 2004).

Ποιοι είναι οι παράγοντες κινδύνου και ποιες οι επιπτώσεις τους;	
Προετοιμασία	• Συγκέντρωση των στόχων του έργου. • Δήλωση όλων των παραδοχών του έργου. • Καθορισμός των κριτηρίων για την επιτυχία του έργου. • Αξιολόγηση πρότερης πείρας.
Προσδιορισμός πιθανών παραγόντων κινδύνου	• Προβληματισμός για το τι μπορεί να οδηγήσει σε αρνητικές εξελίξεις. • Εξέταση των επακόλουθων παραγόντων κινδύνου. • Ονομασία κάθε παράγοντα κινδύνου. • Ταξινόμηση των παραγόντων κινδύνου, χρησιμοποιώντας κατάλληλες κατηγοριοποιήσεις.
Προσδιορισμός επιπτώσεων	• Χρησιμοποίηση της λογικής συνάρτησης: ΑΝ (παράγοντας κινδύνου) … ΤΟΤΕ (επίπτωση). • Εξέταση των επακόλουθων επιπτώσεων. • Ταξινόμηση των επιπτώσεων, χρησιμοποιώντας τις σχετικές κατηγοριοποιήσεις.
Τεκμηρίωση παραγόντων κινδύνων – Σύνταξη αναφοράς	• Δημιουργία καταλόγου των παραγόντων κινδύνου (ανά κλάση) και των επιπτώσεων (ανά κατηγορία).

Πίνακας 3.1: Φάσεις αναγνώρισης κινδύνου (Στάδιο 1).

Προετοιμασία

Το πρώτο βήμα της διαδικασίας αναγνώρισης κινδύνου είναι η προετοιμασία, δηλαδή η συλλογή πληροφοριών σχετικά με τον οργανισμό για τον οποίο προορίζεται

το έργο, τις ανάγκες που καλείται να καλύψει το έργο αυτό, αλλά και πληροφορίες για τυχόν παρόμοια έργα που έχουν υλοποιηθεί στο παρελθόν. Η συλλογή αυτών των πληροφοριών θα βοηθήσει στην αναζήτηση των κινδύνων, στους οποίους είναι δυνατόν να εκτεθεί το έργο, αλλά και των τρόπων μετριασμού της πιθανότητας εμφάνισης αυτών ή των επιπτώσεών τους. Απαιτείται, λοιπόν, η πλήρης κατανόηση του περιβάλλοντος του πληροφοριακού έργου. Οι πληροφορίες που πρέπει να συλλεχθούν μπορούν να ταξινομηθούν στις εξής κατηγορίες (Stoneburner, Goguen και Feringa, 2001):

Υλικό (hardware) πληροφοριακού συστήματος

Πληροφορίες για τον ήδη υπάρχοντα εξοπλισμό, αλλά και για τον εξοπλισμό που πρόκειται να χρησιμοποιηθεί για το νέο πληροφοριακό έργο. Τέτοιες είναι οι εξής:

- Λειτουργικές απαιτήσεις του πληροφοριακού συστήματος.
- Πολιτικές ασφαλείας συστημάτων, δηλαδή πολιτική του οργανισμού και νομοθετικά πλαίσια.
- Αρχιτεκτονική των συστημάτων ασφαλείας.
- Τρέχουσα δικτυακή τοπολογία.
- Προστασία αποθηκευμένων πληροφοριών.
- Ροή πληροφοριών σχετικών με το πληροφοριακό σύστημα (διεπαφές συστήματος, διάγραμμα ροής εισόδων εξόδων του συστήματος, κ.α.).
- Τεχνικοί έλεγχοι που χρησιμοποιούνται για το πληροφοριακό έργο, όπως ενσωματωμένο ή πρόσθετο υλικό ασφαλείας που υποστηρίζει την αναγνώριση και την επικύρωση πρόσβασης και πληροφοριών, διακριτικοί ή αυστηροί έλεγχοι πρόσβασης, μέθοδοι κρυπτογράφησης κ.α..
- Διοικητικοί έλεγχοι για την προστασία του πληροφοριακού συστήματος, όπως κανόνες συμπεριφοράς, σχεδιασμός ασφάλειας κ.α..
- Λειτουργικοί έλεγχοι, όπως ασφάλεια προσωπικού, διαδικασίες αποκατάστασης και συντήρησης συστημάτων, έλεγχος χρήσης συστημάτων, προσθήκης και διαγραφής δεδομένων, έλεγχος πρόσβασης χρηστών και ιδιαιτέρως αυτών που έχουν πρόσβαση σε αρχεία και λειτουργίες πέραν των τυποποιημένων κ.α..
- Ασφάλεια των εγκαταστάσεων του οργανισμού.
- Ασφάλεια σε σχέση με το φυσικό περιβάλλον του έργου, όπως έλεγχοι για υγρασία, θερμοκρασία, μόλυνση, διαχείριση ενέργειας, βαθμός έκθεσης σε φυσικές καταστροφές κ.α..

Λογισμικό (software) πληροφοριακού συστήματος

Πληροφορίες για παλαιό και νέο λογισμικό.

Διεπαφές συστημάτων

Πρέπει να αναγνωριστούν οι εσωτερικές και εξωτερικές διασυνδέσεις του συστήματος που θα εγκατασταθεί.

Βάσεις δεδομένων

Το είδος, η ποιότητα και η ποσότητα των πληροφοριών και δεδομένων που θα κληθεί να διαχειριστεί το νέο λογισμικό.

Στελέχη που θα υποστηρίξουν και θα χρησιμοποιήσουν το νέο πληροφοριακό σύστημα

Αναζήτηση στελεχών που να διαθέτουν τις κατάλληλες γνώσεις για να χειριστούν το νέο λογισμικό, τι απαιτήσεις για επιπλέον εκπαίδευση υπάρχουν, αν τα στελέχη κατανοούν την αξία, τη χρησιμότητα και την ευαισθησία του νέου πληροφοριακού συστήματος.

Στόχος του νέου έργου πληροφοριακού συστήματος

Ποιες λειτουργίες καλείται να επιτελέσει το νέο πληροφοριακό σύστημα.

Αξία του νέου έργου πληροφοριακού συστήματος

Πόσο σημαντική είναι η εγκατάσταση του νέου πληροφοριακού συστήματος για τη λειτουργία του οργανισμού.

Ευαισθησία του πληροφοριακού συστήματος

Το επίπεδο προστασίας που απαιτείται για τη διατήρηση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των συστημάτων και πληροφοριών.

Για ένα πληροφοριακό σύστημα που είναι στη φάση της έναρξης ή του σχεδιασμού, οι πληροφορίες μπορούν να προέλθουν από το ίδιο το σχέδιο ή από την κατάσταση με τις απαιτήσεις του έργου. Όταν το έργο είναι υπό ανάπτυξη, χρήσιμες πληροφορίες μπορούν να προέλθουν από τον καθορισμό των βασικών κανόνων και των στοιχείων ασφαλείας που προγραμματίζονται για το σύστημα. Για ένα έργο λογισμικού οι πληροφορίες συλλέγονται από το περιβάλλον παραγωγής του έργου, συμπεριλαμβανομένων στοιχείων που αφορούν τη διαμόρφωση των συστημάτων, τη συνδεσιμότητά τους και τις προκαθορισμένες ή ακαθόριστες διαδικασίες και πρακτικές. Επομένως, η περιγραφή των συστημάτων μπορεί να βασιστεί στην ασφάλεια που παρέχεται από την υπάρχουσα υποδομή ή τα μελλοντικά σχέδια ασφαλείας.

Φυσικά, η συλλογή όλων αυτών των πληροφοριών δεν είναι μια απλή διαδικασία, αλλά απαιτεί προσεκτική, επιστημονική και αυστηρά καθορισμένη ενασχόληση από τα άτομα που θα κληθούν να συλλέξουν αυτές τις πληροφορίες, ούτως ώστε τα αποτελέσματα της έρευνας να έχουν ουσιαστική αξία, να είναι αξιόπιστα και τεκμηριωμένα και να μπορούν να προσφέρουν στη διαδικασία αναγνώρισης κινδύνων και όχι να οδηγήσουν σε λάθος συμπεράσματα ή να αποτελέσουν μια άχρηστη βάση δεδομένων. Οποιοιδήποτε τεχνική ή ένας συνδυασμός των τεχνικών που παρουσιάζονται στο σχήμα 3.2, και περιγράφονται σύντομα στη συνέχεια, μπορούν να χρησιμοποιηθούν για τη συγκέντρωση των πληροφοριών που απαιτούνται. Πρέπει να τονιστεί ότι η συλλογή πληροφοριών είναι απαραίτητο να συνεχίσει να πραγματοποιείται καθ' όλη τη διάρκεια υλοποίησης του έργου.

Σχήμα 3.2: Μέθοδοι συλλογής πληροφοριών.

Ερωτηματολόγια

Το προσωπικό αξιολόγησης των κινδύνων, για να συλλέξει τις σχετικές πληροφορίες, μπορεί να αναπτύξει ένα ή περισσότερα ερωτηματολόγια σχετικά με τη διαχείριση και τους λειτουργικούς ελέγχους που προγραμματίζονται για το νέο πληροφοριακό σύστημα ή που ήδη χρησιμοποιούνται για τα υπάρχοντα συστήματα. Τα ερωτηματολόγια αυτά πρέπει να διανεμηθούν στο προσωπικό που σχεδιάζει ή υποστηρίζει το σύστημα.

Συνεντεύξεις

Οι συνεντεύξεις του προσωπικού υποστήριξης του συστήματος και του διοικητικού προσωπικού του οργανισμού μπορούν να παράσχουν στα άτομα που πραγματοποιούν την αξιολόγηση των κινδύνων χρήσιμες πληροφορίες για την αξία και την αποστολή του νέου πληροφοριακού συστήματος, καθώς και για τις αντιδράσεις των στελεχών στην εισαγωγή νέων τεχνολογιών. Οι συνεντεύξεις αυτές σε ομάδες αλλά και σε μεμονωμένα άτομα θα βοηθήσουν, επίσης, στην κατανόηση των λειτουργικών χαρακτηριστικών του οργανισμού και στην αξιολόγηση του φυσικού περιβάλλοντος όπου θα εγκατασταθεί το νέο πληροφοριακό σύστημα.

Χρήση αυτοματοποιημένου ανιχνευτικού εξοπλισμού

Δυναμικές τεχνικές μέθοδοι μπορούν να χρησιμοποιηθούν για τη συλλογή πληροφοριών. Για παράδειγμα, ένα σύστημα χαρτογράφησης δικτύων μπορεί να προσδιορίσει τις υπηρεσίες που τρέχουν σε μια μεγάλη ομάδα τερματικών και να παρουσιάσει με γρήγορο τρόπο το προφίλ του εν λόγω πληροφοριακού συστήματος

Πληροφορίες για παρόμοια έργα πληροφορικής που έχουν ήδη υλοποιηθεί

Μέσω αυτών των πληροφοριών μπορεί να χρησιμοποιηθεί η πρότερη πείρα σε παρόμοια έργα, ώστε να αποφευχθούν λάθη και παραλήψεις του παρελθόντος και να σχηματιστεί μια πιο ρεαλιστική εικόνα των τρόπων αντιμετώπισης των επιπτώσεων. Πρόκειται, δηλαδή, για έρευνα των συγκριτικών μετρήσεων επιδόσεων από παρόμοιες διαδικασίες.

Αναθεώρηση εγγράφων

Έχει να κάνει με πολιτικά έγγραφα (νομοθεσία, κρατικές οδηγίες), έγγραφα σχετικά με το πληροφοριακό σύστημα (οδηγός χρήσης, διοικητικό εγχειρίδιο συστημάτων, σχέδιο του συστήματος και κατάλογος απαιτήσεων, τίτλοι ιδιοκτησίας) και έγγραφα σχετικά με την ασφάλεια (προηγούμενη έκθεση λογιστικού ελέγχου και αξιολόγησης κινδύνου, αποτελέσματα δοκιμής συστημάτων, σχεδιασμός ασφάλειας συστημάτων, διαδικασίες ασφάλειας) που μας παρέχουν αρκετές και σημαντικές πληροφορίες για το σχηματισμό μιας άρτιας εικόνας του οργανισμού και της αξίας και λειτουργικότητας του νέου έργου για αυτόν.

Πόρισμα εμπειρογνωμόνων

Πρόκειται για την παρακολούθηση και τη συγκέντρωση πληροφοριών σχετικά με το λειτουργικό και φυσικό περιβάλλον του έργου από το προσωπικό αξιολόγησης κινδύνων, ύστερα από δική τους προσωπική παρατήρηση στο περιβάλλον του οργανισμού. Η αξία αυτού του πορίσματος είναι πολύ μεγάλη, καθώς δεν περιλαμβάνει την προσωπική άποψη των στελεχών του οργανισμού, που μπορεί να μην είναι απόλυτα αντικειμενική, αλλά μόνο την καταγραφή γεγονότων με βάση την αμεροληψία και τη διορατικότητα των εμπειρογνωμόνων.

Προσδιορισμός πιθανών παραγόντων κινδύνου

Αφού έχουν συλλεχθεί όλες οι απαραίτητες πληροφορίες, λοιπόν, προχωράμε στη διαδικασία εκτίμησης κινδύνων, που δεν είναι άλλο από τον προσδιορισμό των ίδιων των κινδύνων. Τα πρόσωπα που θα κληθούν να συμπληρώσουν τον κατάλογο των πιθανών κινδύνων θα πρέπει, εκτός από τις αναγκαίες γνώσεις και την εμπειρία, να διαθέτουν και πλούσια φαντασία και διορατικότητα ώστε να μπορέσουν να διακρίνουν και κινδύνους πέραν των τυποποιημένων. Φυσικά, καθώς η εκτίμηση κινδύνων είναι μια επιστημονική διαδικασία, δε μπορεί να βασιστεί μόνο στη φαντασία αυτών που την πραγματοποιούν, αλλά απαιτεί ένα συνδυασμό όλων των παραπάνω για να επέλθει το επιθυμητό αποτέλεσμα. Για το λόγο αυτό, είναι χρήσιμο να στελεχωθεί μια ομάδα κατάλληλων προσώπων που θα επιτελέσουν αυτή τη διαδικασία και όχι να ανατεθεί ως ευθύνη ενός μόνο προσώπου.

Οι κίνδυνοι που μπορεί να υπάρξουν σε ένα πληροφοριακό σύστημα οφείλονται, συνήθως, στη φύση ή στον άνθρωπο. Έτσι, διακρίνονται σε δύο κατηγορίες, ανάλογα με την πηγή πρόκλησής τους (Κιουντούζης, 2004):

- Προκαλούνται από φυσικά φαινόμενα, τα οποία από την πλευρά τους οφείλονται στις καιρικές συνθήκες και, επομένως, πρόκειται για τυχαία γεγονότα (πίνακας 3.2).
- Προκαλούνται από τον ανθρώπινο παράγοντα και μπορεί να πρόκειται για τυχαία (accidental) ή σκόπιμα (intentional) γεγονότα. Τα τυχαία γεγονότα προκύπτουν από ενέργειες που δεν προϋποθέτουν κακή πρόθεση, ενώ τα σκόπιμα γεγονότα προϋποθέτουν κακή πρόθεση και την ύπαρξη κάποιου κινήτρου από την πλευρά του επιτιθέμενου (πίνακας 3.2).

Φυσικής Προέλευσης	Ανθρώπινης Προέλευσης	
	Τυχαία γεγονότα	Σκόπιμα γεγονότα
Σεισμός	Περιέργεια	Τρομοκρατική ενέργεια
Πλημμύρα	Αμέλεια	Κατασκοπία
Πυρκαγιά	Ανικανότητα	Κλοπή
Τυφώνας	Άγνοια	Απεργία
Καταιγίδα	Έλλειψη πείρας	Βανδαλισμός
Κεραυνός	Κόπωση	Κατάχρηση
Έκρηξη ηφαιστείου	Διαδηλώσεις	Απάτη
Λαίλαπα	Ταραχές	Προσωπικό όφελος
	Πολιτικές ενέργειες	Εκδίκηση

Πίνακας 3.2: Είδη κινδύνων σε ένα πληροφοριακό σύστημα ανάλογα με την πηγή πρόκλησής τους.

Μια άλλη διάκριση των κινδύνων που μπορεί να εφαρμοστεί είναι ανάλογα με τις επιπτώσεις, τις οποίες συνεπάγονται:

- *Διακοπή λειτουργίας του συστήματος*, που μπορεί να οφείλεται σε φυσικά φαινόμενα ή σε γεγονότα, όπως διαδηλώσεις, ταραχές, πολιτικές ενέργειες, τρομοκρατικές ενέργειες, κλοπή, απεργίες, βανδαλισμούς, κ.α..
- *Καταστροφή*, η οποία μπορεί να συμβεί και να επεκταθεί σε όλες τις συνιστώσες του πληροφοριακού συστήματος. Προέρχεται από φυσικά φαινόμενα, που περιγράφηκαν προηγουμένως, ή από ανθρώπινες ενέργειες, όπως τρομοκρατική ενέργεια, κλοπή, απεργία, βανδαλισμός, διαδηλώσεις, ταραχές κ.α..
- *Τροποποίηση ή αλλοίωση*, την οποία υφίστανται συνήθως τα δεδομένα, το λογισμικό και οι επικοινωνίες του συστήματος. Οι μεταβολές αυτές είναι τυχαίες (π.χ. οφείλονται σε αμέλεια, άγνοια, ανικανότητα κ.α.) ή σκόπιμες (π.χ. προσωπικό όφελος, απάτη, κατασκοπεία, εκδίκηση κ.α.).
- *Αποκάλυψη πληροφοριών*, η οποία μπορεί να είναι τυχαία (π.χ. περιέργεια, αμέλεια κ.α.) ή σκόπιμη (π.χ. κατασκοπία, προσωπικό όφελος κ.α.).

Οι πιθανοί κίνδυνοι μπορούν, τέλος, να κατηγοριοποιηθούν ανάλογα με την προέλευσή τους. Στο σχήμα 3.3 φαίνονται οι έξι κατηγορίες κινδύνων, στα πλαίσια των οποίων θα αναζητηθούν παρακάτω οι πιθανές απειλές ενός πληροφοριακού έργου.

Σχήμα 3.3: Κατηγορίες πιθανών κινδύνων ανάλογα με την προέλευσή τους.

Φυσικές καταστροφές

Η πρώτη κατηγορία κινδύνων στους οποίους μπορεί να εκτεθεί ένα πληροφοριακό έργο είναι οι φυσικές καταστροφές. Τέτοιου είδους καταστροφές θα μπορούσαν να προσβάλλουν το οποιοδήποτε έργο και όχι μόνο κάποιο πληροφοριακό, καθώς ουσιαστικά προσβάλλουν τις κτιριακές εγκαταστάσεις του οργανισμού και εμμέσως και τα πληροφοριακά συστήματα που στεγάζονται σε αυτές.

Στην κατηγορία αυτή ανήκουν οι σεισμοί, οι πλημμύρες, οι καθιζήσεις του εδάφους, οι χιονοθύελλες και άλλα τέτοιου είδους φυσικά φαινόμενα. Η κατηγορία αυτή είναι, βέβαια, κάπως πιο ιδιόμορφη, καθώς εξαρτάται και από τη γεωγραφική θέση της εκάστοτε εγκατάστασης. Για παράδειγμα δε θα περίμενε κανείς να χτυπηθεί από χιονοθύελλα ένας οργανισμός που εδρεύει κοντά στον Ισημερινό. Τέτοιες φυσικές καταστροφές θα μπορούσαν να καταστρέψουν μια ολόκληρη εγκατάσταση και μαζί με αυτή και το έργο λογισμικού που είναι υπό ανάπτυξη ή να προκαλέσουν μεμονωμένες ζημιές που θα αυξήσουν το χρόνο και το κόστος υλοποίησης του έργου.

Μια πιο λεπτομερής περιγραφή των εν λόγω κινδύνων δε κρίνεται αναγκαία καθώς είναι προφανής ο τρόπος με τον οποίο μπορούν να προσβάλλουν την άρτια εξέλιξη του έργου.

Φυσικό και θεσμικό περιβάλλον του έργου

Η δεύτερη κατηγορία αναφέρεται στο περιβάλλον του έργου. Με τον όρο περιβάλλον αναφερόμαστε στις εγκαταστάσεις του οργανισμού, στις γειτονικές προς αυτόν εγκαταστάσεις και στις κρατικές παροχές.

Όσον αφορά τις εγκαταστάσεις του οργανισμού, ένας πρώτος εχθρός του πληροφοριακού έργου είναι η παλαιότητα των εγκαταστάσεων. Τα προβλήματα που μπορούν να προέλθουν από αυτή επικεντρώνονται κυρίως στο δίκτυο υδροδότησης και ηλεκτροδότησης. Ένας παλιός σωλήνας, που θα μπορούσε να χρησιμοποιείται ακόμα και για τη θέρμανση του χώρου, ο οποίος δεν έχει συντηρηθεί σωστά, μπορεί να

καταστρέψει τον εξοπλισμό του υπό ανάπτυξη συστήματος εάν σπάσει και τα νερά βρουν πρόσβαση προς το δωμάτιο όπου αυτός φυλάσσεται ή έχει ήδη εγκατασταθεί. Η ηλεκτροδότηση παίζει εξίσου σημαντικό ρόλο, καθώς οι ατέλειες σε αυτή μπορούν να προκαλέσουν ένα βραχυκύκλωμα με καταστροφικές συνέπειες, όπως μία πυρκαγιά ή να τεθεί το σύστημα εκτός λειτουργίας για κάποιο χρονικό διάστημα. Η απρόβλεπτη πτώση του συστήματος ενδέχεται να επιφέρει απώλεια σημαντικών δεδομένων, καταστροφή μέρους του hardware και του software, αλλά και χρηματικές απώλειες από τη μη λειτουργία του συστήματος, έστω και για λίγες ώρες. Επίσης, θα ήταν απογοητευτικό να ολοκληρωθεί ένα μέρος του συστήματος και να μη μπορεί να τεθεί σε λειτουργία λόγω έλλειψης ισχύος.

Οι γειτονικές εγκαταστάσεις και γενικά ο περιβάλλον χώρος του οργανισμού θα μπορούσαν εμμέσως να αποτελέσουν απειλή για το νέο πληροφοριακό έργο. Ένα προφανές παράδειγμα αποτελεί η εκδήλωση πυρκαγιάς σε γειτονικό κτίσμα που θα μπορούσε να επεκταθεί και στις εγκαταστάσεις του οργανισμού. Για το λόγο αυτό, σημαντική είναι και η επιλογή της θέσης μέσα στην εγκατάσταση όπου θα τοποθετηθεί το νέο σύστημα.

Με τον όρο κρατικές παροχές αναφερόμαστε σε όλες εκείνες τις διαδικασίες του οργανισμού τις οποίες επηρεάζει ο κρατικός παράγοντας. Πρώτα από όλα είναι το νομικό πλαίσιο που καθορίζει τις διαδικασίες του οργανισμού, την τήρηση βάσεων δεδομένων και τη ροή πληροφοριών. Το αναπτυσσόμενο έργο πληροφορικής θα πρέπει να υπακούει στις νομοθετικές ρυθμίσεις, έτσι ώστε να μπορεί να χρησιμοποιηθεί και να μην επιβληθούν κυρώσεις στον οργανισμό από τη μη εξουσιοδοτημένη χρήση συστημάτων, ούτε να καθυστερήσει η ολοκλήρωση του έργου από αλλαγές που θα το συμμορφώνουν με την υπάρχουσα νομοθεσία. Στις κρατικές παροχές περιλαμβάνονται, επίσης, οι τεχνολογίες οι οποίες μπορεί να υποστηριχθούν, αλλά και τα σχέδια του κράτους για εκσυγχρονισμό, για παράδειγμα, των δικτύων ροής πληροφορίας. Μια νέα τεχνολογία που έχει εξαιρετικές δυνατότητες αλλά δε μπορεί ουσιαστικά να τεθεί σε εφαρμογή λόγω έλλειψης κρατικής υποδομής, όπως η ύπαρξη και χρήση παλαιών δικτύων μικρής χωρητικότητας, θα ήταν ουσιαστικά άχρηστη και η εισαγωγή της στο νέο σύστημα μόνο επιζήμια θα μπορούσε να χαρακτηριστεί. Στην αντίπερα όχθη, εάν τα κρατικά σχέδια για εισαγωγή νέων τεχνολογιών δε ληφθούν υπόψη, υπάρχει ο κίνδυνος να μη χρησιμοποιηθούν τελικά τα βέλτιστα συστήματα στην υλοποίηση του νέου έργου, με αποτέλεσμα αυτό να θεωρηθεί απαρχαιωμένο, ακόμα και από την έναρξη της λειτουργίας του.

Ανθρώπινος παράγοντας

Αυτή η πηγή κινδύνων αναφέρεται σε άτομα που σκόπιμα θα προσπαθήσουν να βλάψουν τη λειτουργία του συστήματος ή να την εκμεταλλευτούν για προσωπικό τους όφελος, ζημιώνοντας τον οργανισμό στον οποίο ανήκουν. Τέτοια πρόσωπα μπορεί να προέρχονται από το προσωπικό του οργανισμού ή να είναι πρόσωπα που δεν ανήκουν σε αυτόν, αλλά μπορούν να αποκτήσουν πρόσβαση στα πληροφοριακά του συστήματα.

Τα πρόσωπα που δεν ανήκουν στον οργανισμό και επιθυμούν τη ζημίωση αυτού είναι κυρίως οι ανταγωνιστές του. Αυτοί, ενδεχομένως, να προσπαθήσουν να αποκτήσουν πρόσβαση στις βάσεις δεδομένων του νέου συστήματος και να αντλήσουν πληροφορίες για το προσωπικό, για μελλοντικές στρατηγικές, για καινοτομίες του οργανισμού ή για άλλου είδους αποθηκευμένες πληροφορίες, προσβάλλοντας με αυτόν τον τρόπο την αξιοπιστία, την ακεραιότητα και την εμπιστευτικότητα του έργου. Έτσι, η εταιρεία μπορεί να απολέσει ευκαιρίες αιφνιδιασμού της αγοράς, ενδεχομένως το μονοπώλιο της, να χαλάσουν μελλοντικές συνεργασίες που βρίσκονταν υπό συζήτηση ή ακόμα και να χάσει στελέχη πολύτιμα για αυτή που θα δελεαστούν από προτάσεις ανταγωνιστών, οι οποίοι γνωρίζουν το βιογραφικό τους αλλά και την αξία τους για την ευδοκίμηση της εταιρείας. Επιπρόσθετα, οι εισβολείς θα μπορούσαν ακόμα και να εκβιάσουν τον οργανισμό για τη μη κοινοποίηση των στοιχείων που καπηλεύτηκαν.

Πέραν της διαρροής πληροφοριών, οι ανταγωνιστές που θα αποκτήσουν πρόσβαση στο λογισμικό του οργανισμού μπορούν ακόμα και να το καταστρέψουν. Δολιοφθορές θα μπορούσαν να προκληθούν και στον τεχνικό εξοπλισμό του έργου, όμως, αυτή είναι μία ακραία κατάσταση και αναφέρεται πιο πολύ σε ειδικές περιπτώσεις, όπως στον κίνδυνο από επιθέσεις τρομοκρατών και αναρχικών προς το λογισμικό και το υλικό του οργανισμού. Όλα αυτά, φυσικά, είναι πιθανόν να συμβούν με την προϋπόθεση ότι δεν υπάρχει η απαραίτητη ασφάλεια των δικτύων αλλά και των εγκαταστάσεων και ότι υπάρχει κίνητρο για τη διενέργεια τέτοιων επιθέσεων.

Μία άλλη μερίδα προσώπων που θα μπορούσαν να πλήξουν το κύρος και την αξιοπιστία που αποπνέει το έργο είναι οι hackers, οι οποίοι μπορούν να φέρουν αναστάτωση και να προκαλέσουν καταστροφές στο νέο σύστημα μόνο και μόνο για την προσωπική τους ικανοποίηση.

Εκτός, όμως, από τις παραπάνω περιπτώσεις, υπάρχουν και πρόσωπα που ανήκουν στο δυναμικό του οργανισμού, τα οποία θα μπορούσαν να θέσουν σε κίνδυνο την ακεραιότητα και την αξιοπιστία του έργου. Κίνητρο αυτών, η ικανοποίηση προσωπικών φιλοδοξιών, χρηματικά οφέλη ή ακόμα και η έκφραση της δυσαρέσκειάς τους προς τους διοικούντες του οργανισμού. Τέτοια πρόσωπα είναι στελέχη που είτε είναι εξουσιοδοτημένα να έχουν πρόσβαση σε ευαίσθητα δεδομένα και λογισμικό μεγάλης αξίας, είτε μπορούν να αποκτήσουν τέτοια πρόσβαση σε τέτοια δεδομένα λόγω ελλιπούς ασφάλειας αυτών.

Τα στελέχη αυτά θα μπορούσαν να αποκρύψουν πληροφορίες ή να παραποιήσουν δεδομένα, ώστε να παρουσιάζονται ως ιδιαίτερα ικανά για να εξελιχθούν στην ιεραρχία του οργανισμού, δημιουργώντας προβλήματα στην τήρηση βάσης δεδομένων. Επίσης, μπορούν να αποκαλύψουν πληροφορίες ή να καταστρέψουν δεδομένα και λογισμικό, παρακινούμενοι και, φυσικά, πληρωμένοι από εξωτερικούς παράγοντες, όπως είναι οι ανταγωνιστές του οργανισμού. Τέλος, δυσαρεστημένοι υπάλληλοι από την εξέλιξή τους, τις αποδοχές τους ή τη συμπεριφορά των ανωτέρων τους προς αυτούς, ενδεχομένως, να επιχειρήσουν να βλάψουν τη λειτουργία του οργανισμού, προσβάλλοντας τη λειτουργία και την ανάπτυξη ενός τόσο ζωτικής σημασίας έργου.

Τέλος, τα πρόσωπα που, είτε ανήκουν είτε όχι στο δυναμικό του οργανισμού, θα προσπαθήσουν να εκμεταλλευτούν τα ευαίσθητα δεδομένα αυτού, στα οποία θα έχουν τη δυνατότητα να αποκτήσουν πρόσβαση, όπως για παράδειγμα την πρόσβαση σε υλικό δικογραφιών, ιστορικό ασθενών ή περιουσιακά στοιχεία προσώπων (για περιπτώσεις που το νέο πληροφοριακό σύστημα ανήκει σε κάποιον από τους αντίστοιχους οργανισμούς της κρατικής μηχανής).

Κίνδυνοι τεχνολογίας

Η πρώιμη υιοθέτηση νέων τεχνολογιών προσφέρει ένα δυνατό πλεονέκτημα σε σχέση με τους ανταγωνιστές ενός οργανισμού, καθώς παρέχει μεγαλύτερη ταχύτητα, ασφάλεια και αξιοπιστία στις διαδικασίες του οργανισμού, καλύτερη λειτουργικότητα των συστημάτων, αλλά και ανοίγει το δρόμο για περαιτέρω ανάπτυξη. Αποτελεί, όμως, και τη σημαντικότερη, ίσως, εστία κινδύνων που μπορούν να προσβάλλουν ένα πληροφοριακό έργο. Οι κίνδυνοι αυτοί χαρακτηρίζονται ως κίνδυνοι τεχνολογίας και αφορούν τις νέες τεχνολογίες που πρόκειται να εισαχθούν με την ολοκλήρωση του έργου και την προσαρμογή αυτών στα ήδη υπάρχοντα συστήματα του οργανισμού.

Η χρήση νέων τεχνολογιών που δεν έχουν δοκιμαστεί και αξιολογηθεί σε πραγματικές συνθήκες συνοδεύονται από τον κίνδυνο να αποδειχθούν, σε βάθος χρόνου, μη λειτουργικές, χωρίς σημαντικό επιχειρησιακό όφελος και, ενδεχομένως, επιζήμιες για το κύρος του οργανισμού. Τα νέα συστήματα που θα εισαχθούν είναι πιθανό να μη μπορούν να ανταποκριθούν στις ανάγκες του οργανισμού, να αδυνατούν να παρακολουθήσουν τις λειτουργίες της αγοράς, ή απλά να αποδειχθούν ελαττωματικά. Οι κίνδυνοι αυτοί, φυσικά, συνοδεύουν κάθε καινοτομία που εισάγεται στη λειτουργία ενός οργανισμού. Όταν, όμως, αναφερόμαστε σε ένα πληροφοριακό έργο μεγάλης κλίμακας, γίνεται αντιληπτό ότι η αποτυχία αυτού θα προκαλέσει τεράστια ζημιά στον οργανισμό εξαιτίας των κονδυλίων που θα χαθούν. Παράλληλα, ένας οργανισμός μπορεί να έχει στηρίξει όλες τις προοπτικές ανάπτυξής του σε ένα τέτοιο έργο και με την αποτυχία αυτού να χάσει κάθε δυνατότητα να παρουσιαστεί ανταγωνιστικός στον τομέα που ειδικεύεται.

Προσπαθώντας οι υπεύθυνοι σχεδιασμού του έργου να ελαχιστοποιήσουν τον παραπάνω κίνδυνο, μπορεί να προτιμήσουν τεχνολογίες που έχουν ήδη χρησιμοποιηθεί και έχει αποδειχθεί η λειτουργικότητά τους και οι υπηρεσίες που μπορεί να προσφέρει η υιοθέτησή τους. Εδώ, όμως, υπάρχει ο κίνδυνος αυτές οι τεχνολογίες, βραχυχρόνια, να θεωρηθούν απαρχαιωμένες και να μη μπορούν να παρακολουθήσουν τους ρυθμούς ανάπτυξης που απαιτούνται για να είναι η εταιρεία ανταγωνιστική. Με την αντίθεση αυτών των δύο κινδύνων, γίνεται φανερή η αναγκαιότητα της μελέτης διαχείρισης κινδύνων, ώστε να προβλεφθεί, όσο αυτό είναι εφικτό, το επίπεδο τεχνολογίας που πρέπει να χρησιμοποιηθεί για να μεγιστοποιηθούν τα οφέλη του οργανισμού. Η διαχείριση κινδύνων θα πρέπει να προβλέψει ακόμα και αν η χρονική περίοδος είναι η κατάλληλη για την υλοποίηση ενός τέτοιου έργου, βάση των τεχνολογικών εξελίξεων που αναμένονται.

Ένας άλλος κίνδυνος που απειλεί ένα έργο πληροφορικής, εξαιτίας της χρήσης νέων τεχνολογιών, είναι η μη συμβατότητα των νέων συστημάτων με τον ήδη υπάρχον

εξοπλισμό. Δηλαδή, θα πρέπει να μελετηθεί αν τα νέα συστήματα μπορούν να συνδεθούν και να εναρμονιστούν με τα υπάρχοντα συστήματα, να εκτιμηθεί το κόστος και ο χρόνος που απαιτείται για αυτήν τη σύνδεση, αλλά και να προσδιοριστούν οι τυχόν αντικαταστάσεις και αλλαγές που πρέπει να πραγματοποιηθούν στον υπάρχον εξοπλισμό. Η εκτίμηση αυτή είναι ιδιαίτερα σημαντική, καθώς είναι σαφές ότι το νέο υλικό και λογισμικό δε θα πρέπει να καθιστά άχρηστη την τρέχουσα υποδομή, αλλά να "συνεργάζεται" με αυτή αρμονικά, για να εξασφαλιστεί η ορθή και η όσο το δυνατόν αποδοτικότερη λειτουργία του οργανισμού.

Πέραν, όμως, των συνδέσεων με τα άλλα συστήματα του οργανισμού, θα πρέπει να προβλεφθεί και ο κίνδυνος μη συμβατότητας του εξοπλισμού του ίδιου του έργου. Καθώς θα πρόκειται για εντελώς νέες τεχνολογίες, υπάρχει ο κίνδυνος τα διάφορα μέρη υλικού και λογισμικού να μη μπορούν να συνδεθούν απευθείας μεταξύ τους, αλλά να απαιτούνται ιδιόμορφες συνδεσμολογίες, που αν δεν έχουν προβλεφθεί και εισαχθεί στον αρχικό σχεδιασμό του έργου θα μπορούσαν να το θέσουν εκτός χρονοδιαγράμματος, αλλά και να αυξήσουν το κόστος υλοποίησης του. Παράλληλα, όλες αυτές οι συνδεσμολογίες θα πρέπει να παρουσιάζουν ευελιξία σε τροποποιήσεις που ενδεχομένως να χρειαστεί να πραγματοποιηθούν στο μέλλον.

Επιχειρησιακοί κίνδυνοι

Οι κίνδυνοι αυτοί απορρέουν από τη διαδικασία επιχειρησιακής ένταξης των νέων τεχνολογιών στον τρόπο λειτουργίας του οργανισμού. Υπάρχει ο κίνδυνος οι νέες τεχνολογίες να μη μπορούν να αφομοιωθούν άμεσα από τη λειτουργία του οργανισμού, με αποτέλεσμα το κάθε τμήμα του έργου που θα ολοκληρώνεται να καθυστερεί να τεθεί σε λειτουργία και να προκαλεί έτσι καθυστερήσεις και στην περαιτέρω εξέλιξη του έργου. Επίσης, θα πρέπει να υπάρχει εξ αρχής σαφές πλάνο των διαδικασιών στις οποίες θα συμμετάσχουν τα νέα συστήματα, έτσι ώστε η χρονική στιγμή της παράδοσης κάθε τμήματος του έργου να ταυτίζεται με τη στιγμή έναρξης της λειτουργίας του και της αξιοποίησης των δυνατοτήτων του. Ο κίνδυνος εύρεσης διαρκώς νέων αναγκών που θα μπορούσαν να καλυφθούν από το νέο λογισμικό, λόγω πρόχειρου αρχικού σχεδιασμού, μπορεί να οδηγήσει σε καθυστερήσεις λόγω τροποποιήσεων της τελευταίας στιγμής αλλά και λόγω της αναζήτησης πλήρους τρόπου αξιοποίησης του έργου, όταν ήδη έχουν αρχίσει να ολοκληρώνονται τμήματα αυτού.

Κίνδυνος, όμως, στην επιχειρησιακή ένταξη των νέων τεχνολογιών μπορεί να προέλθει και από το επίπεδο εκπαίδευσης του προσωπικού. Είναι πολύ πιθανό το μεγαλύτερο μέρος του προσωπικού να μη μπορεί να χρησιμοποιήσει τα νέα συστήματα, δημιουργώντας έτσι καθυστερήσεις, καθώς θα απαιτηθεί επιπλέον χρόνος για την εκπαίδευση αυτού, έτσι ώστε να είναι σε θέση να χειριστεί τα νέα συστήματα. Η εκπαίδευση του προσωπικού θα πρέπει να πραγματοποιηθεί πριν την ολοκλήρωση του έργου για να αποφευχθούν οι επιπλέον καθυστερήσεις. Επιπλέον, η διοίκηση του οργανισμού οφείλει να ελέγξει το επίπεδο εκπαίδευσης του προσωπικού της για να προλάβει λάθος χειρισμούς που θα μπορούσαν να δημιουργήσουν προβλήματα στη λειτουργία του πληροφοριακού έργου, αλλά και να βλάψουν το κύρος του οργανισμού.

Παράλληλα, με αυτό τον έλεγχο και γνωρίζοντας τις δυνατότητες του προσωπικού της, ο οργανισμός θα μπορεί να το τοποθετήσει στις κατάλληλες θέσεις για την καλύτερη δυνατή αξιοποίηση των δυνατοτήτων του έργου.

Πέραν όμως της εκπαίδευσης του προσωπικού σε θέματα τεχνολογίας, τα διάφορα στελέχη θα πρέπει να ενημερωθούν και να κατανοήσουν την αξία και την ευαισθησία του νέου συστήματος, ώστε να σεβαστούν και τη διαδικασία εκπαίδευσής τους αλλά και τις διαδικασίες ασφάλειας που συνοδεύουν το έργο. Η απείθαρχη συμπεριφορά του προσωπικού και η άρνηση προσαρμογής στις νέες συνθήκες θα μπορούσε να προκαλέσει σοβαρά προβλήματα στην ανάπτυξη και τη βιωσιμότητα του έργου.

Κίνδυνοι οργάνωσης του έργου

Η τελευταία κατηγορία κινδύνων πηγάζει από την οργάνωση του έργου. Το είδος και το πλήθος των κινδύνων αυτών είναι άμεσα συνυφασμένο με την εμπειρία των προσώπων που λαμβάνουν τις αποφάσεις για το σχεδιασμό και την υλοποίηση του έργου.

Πρώτη και κύρια μέριμνα των προσώπων αυτών είναι οι διαδικασίες λήψης αποφάσεων και διοίκησης του έργου. Τα προβλήματα ξεκινούν όταν δεν υπάρχει η απαραίτητη εμπειρία και τεχνογνωσία για λήψη αποφάσεων, για προβλήματα που ανακύπτουν κατά την πορεία εκτέλεσης του έργου και που απαιτούν την άμεση αντίδραση των υπευθύνων. Η αδράνεια αυτών αλλά και η χρονοτριβή έως ότου φτάσουν στη λήψη της σωστής απόφασης επιβαρύνουν, σαφώς, τη διάρκεια ολοκλήρωσης του έργου. Φυσικά, ακόμα μεγαλύτερη επιβάρυνση θα επιφέρει η λήψη μιας βεβιασμένης απόφασης από πρόσωπα χωρίς την απαιτούμενη κατάρτιση, που σε βάθος χρόνου θα αποδειχθεί λανθασμένη. Ο χρόνος υλοποίησης του έργου θα επιβαρυνθεί και από τη σύγχυση δικαιοδοσιών και αρμοδιοτήτων μεταξύ στελεχών που καλούνται να λάβουν τις αποφάσεις. Ο τομέας ευθύνης του καθενός θα πρέπει να είναι αυστηρά καθορισμένος και οι αποφάσεις του να γίνονται σεβαστές από το υπόλοιπο περιβάλλον του έργου.

Είναι σαφές πως η παραπάνω σύγχυση είναι πιθανότερο να εμφανιστεί στην περίπτωση κοινοπραξίας για την εκτέλεση του έργου, όπου πέραν του διαχωρισμού των ευθυνών απαιτείται και η αρμονική συνεργασία μεταξύ των εμπλεκομένων.

Ευθύνη των διοικούντων του έργου είναι και σύναψη σαφών και ασφαλών συμφωνιών με τους προμηθευτές εξοπλισμού. Η αναξιοπιστία ενός προμηθευτή και η αθέτηση των αρχικών συμφωνιών μπορεί να προκαλέσει καθυστερήσεις στην προμήθεια του εξοπλισμού που απαιτείται. Θα πρέπει, επίσης, να έχει προβλεφθεί η περίπτωση προβληματικών προμηθειών ή η καταστροφή υλικού κατά τη διαδικασία εγκατάστασής του, έτσι ώστε να είναι άμεση η αντικατάστασή του.

Τέλος, η υλοποίηση του πληροφοριακού έργου μπορεί να απειληθεί από κακή οργάνωση στον τομέα της χρηματοδότησής του. Ο κίνδυνος μπορεί να προέλθει από τον ασαφή καθορισμό του τρόπου και του χρόνου (είτε βάση χρονοδιαγράμματος είτε βάση της προόδου του έργου) διάθεσης των κονδυλίων και είναι ακόμα πιο πιθανός στην περίπτωση που οι χρηματοδότες είναι περισσότεροι του ενός. Καθυστερήσεις

στην κάλυψη των δαπανών για οποιοδήποτε λόγο θα καθυστερήσουν και το χρόνο ολοκλήρωσης του έργου, ενώ η ασάφεια στις υποχρεώσεις κάθε χρηματοδότη μπορεί να οδηγήσει ακόμα και στην περικοπή κονδυλίων, με αποτέλεσμα να μειωθούν τόσο η ποιότητα όσο και οι δυνατότητες του υλοποιούμενου πληροφοριακού συστήματος. Επίσης, για ένα τέτοιο έργο, με τόσο υψηλό προϋπολογισμό, θα πρέπει να ληφθεί υπόψη και η πιθανότητα αδυναμίας κάλυψης των δαπανών από το χρηματοδότη, γεγονός που θα επέφερε τεράστιες απώλειες στην ανάδοχο εταιρεία.

Ο προσδιορισμός των πιθανών παραγόντων κινδύνου για μια σειρά από παρόμοια έργα είναι μία επαναληπτική διαδικασία και για αυτόν τον λόγο η εμπειρία και τα ιστορικά αρχεία αποτελούν σημαντικές πηγές πληροφόρησης (Nichols, 2002). 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. Οι περισσότερες από αυτές παρουσιάζονται στο σχήμα 3.4 και περιγράφονται σύντομα παρακάτω:

Σχήμα 3.4: Μέθοδοι και εργαλεία αναγνώρισης κινδύνου.

Συνεντεύξεις

- Το πρόσωπο που διεξάγει τις ερωτήσεις καλό είναι να μην ανήκει στην Υπηρεσία, 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.

Διάγραμμα Αιτίας - Επίδρασης (Cause - Effect Diagram)

- Παρουσιάζει γραφικά τις σχέσεις μεταξύ των αιτιών και των επιδράσεων.
- Δεν εμπεριέχει μεγέθη που να ποσοτικοποιούν τα αίτια και τις επιδράσεις.

Ερωτηματολόγια

- Περιλαμβάνουν μία πρότυπη λίστα ερωτήσεων για την αρχική καταγραφή ενός αριθμού παραγόντων κινδύνου.
- Χρησιμοποιούνται για τη συγκέντρωση ιδεών σχετικά με τους σημαντικότερους παράγοντες κινδύνου που αφορούν το έργο.
- Τα αποτελέσματα αξιολογούνται και καταγράφονται στο Μητρώο Παραγόντων Κινδύνου.

Λίστες (Πίνακες) Ελέγχου (Checklists)

- Πρόκειται για λίστες όλων των πιθανών περιοχών όπου ενδέχεται να παρουσιαστούν προβλήματα.
- Αποτελούν ένα από τα πιο ευρέως χρησιμοποιούμενα μέσα προσδιορισμού των παραγόντων κινδύνου.
- Είναι διαφορετικές για κάθε οργάνωση και δραστηριότητα και για αυτό δεν πρέπει να χρησιμοποιούνται ως το μόνο εργαλείο στην Αναγνώριση Κινδύνου.
- Απαραίτητη προϋπόθεση για την κατάρτισή τους για κάθε οργανισμό είναι η ύπαρξη πλούσιου ιστορικού όσον αφορά τη Διαχείριση Κινδύνου, που θα αναφερθεί παρακάτω.

Συσκέψεις για την Ανταλλαγή και Ανάπτυξη Ιδεών (Brainstorming)

- Είναι 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 αυτή την φάση είναι η ενθάρρυνση της δημιουργικότητας των εμπλεκομένων. Οι ιδέες μπορούν να αξιολογηθούν σε επόμενο στάδιο των συσκέψεων.
- Βασικός σκοπός είναι να αναπτυχθεί ένας περιεκτικός κατάλογος επικίνδυνων ενδεχομένων.

- Μπορεί να είναι χρήσιμες για έργα που περιλαμβάνουν νέους / σπάνιους παράγοντες κινδύνου ή καινοτόμες διοικητικές ρυθμίσεις ή για την ανάπτυξη των λιστών (πινάκων) ελέγχου.

Μητρώο Παραγόντων Κινδύνου (Risk Register / Risk Log)

- 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.
- Είναι ίσως μαζί με το μητρώο διαχείρισης κινδύνου, το οποίο περιγράφεται σε επόμενη παράγραφο, το βασικό εργαλείο της διαδικασίας Διαχείρισης Κινδύνου, που όπως είπαμε θα αναφερθεί παρακάτω.
- Απαιτεί τον καθορισμό του πιθανού Υπεύθυνου Παράγοντα Κινδύνου (Risk Owner) για κάθε παράγοντα κινδύνου.
- Η χρήση του διευκολύνεται με την ανάπτυξη μιας εφαρμογής υπολογιστών για την ταχύτερη και πληρέστερη εισαγωγή των στοιχείων στα πεδία και την δημιουργία μίας συνοπτικής κατανομής παραγόντων κινδύνου (Summary Risk Profile - SRP).

Δομή Αναλυτικής Παράθεσης Παραγόντων Κινδύνου, Δ.Α.Π.Π.Κ. (Risk Breakdown Structure, RBS)

- Ταξινόμηση των παραγόντων κινδύνου, προσανατολισμένη στην προέλευση τους, όπου κάθε επόμενο επίπεδο παρουσιάζει πιο λεπτομερή καταγραφή των αιτίων.
- Βοηθάει στην αντίληψη της κατανομής και του τύπου των παραγόντων κινδύνου σε ένα έργο.
- Παρέχει μια τυποποιημένη παρουσίαση των παραγόντων κινδύνου του έργου, διευκολύνοντας την κατανόηση, την επικοινωνία και τη διαχείριση.
- Τα πρώτα επίπεδα μπορούν να χρησιμοποιηθούν σα μια άμεση λίστα για την εξασφάλιση της πληρέστερης καταγραφής των ενδεχόμενων παραγόντων κινδύνου.

Ανάλυση Δυνατών και Αδύνατων Σημείων, Ευκαιριών και Κινδύνων (SWOT)

- Αποτελεί ένα μοντελοποιημένο τρόπο καταγραφής των κυριότερων 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 τον 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 την αξιολόγηση των εξωτερικών παραγόντων, οι οποίοι συνιστούν το εξωτερικό περιβάλλον στο οποίο δραστηριοποιείται ο οργανισμός.

Χάρτης Αντίληψης Παραγόντων Κινδύνου (Risk Concept Map)

- Αποτελεί μια γραφική απεικόνιση των πιθανών παραγόντων κινδύνου.
- Αλληλοσυσχετίζει τα αίτια με τα αντίστοιχα επικίνδυνα γεγονότα και αποτελέσματα.
- Παρουσιάζει τους παράγοντες κινδύνου με κριτήριο την αύξηση της σοβαρότητας τους.

Ανάλυση Παραδοχών

- Κάθε πρόγραμμα συλλαμβάνεται και αναπτύσσεται βασιζόμενο σε ένα σύνολο σεναρίων και παραδοχών.
- Πρόκειται για μια τεχνική που εξερευνά την ακρίβεια των παραδοχών και προσδιορίζει τους παράγοντες κινδύνου για το έργο από την ανακρίβεια, την ασυνέπεια ή την ατέλεια των παραδοχών αυτών.

Η ταξινόμηση των παραγόντων κινδύνου παρέχει τη δυνατότητα παρακολούθησης και ένταξής τους στις ίδιες στρατηγικές αντιμετώπισης, ανάλογα με τις κατηγορίες στις οποίες ανήκουν. Αυτή η ταξινόμηση μπορεί να γίνει με βάση:

- την αιτία,
- το αν απορρέουν από την εσωτερική λειτουργία του έργου ή από εξωτερικούς παράγοντες,
- το στάδιο υλοποίησης του έργου στο οποίο ενδέχεται να εμφανιστούν,
- την πιθανότητα να συμβούν ή το βάρος τους σε σχέση με τους υπολοίπους,
- το μέγεθος των επιπτώσεων ή της σοβαρότητας τους εάν εμφανιστούν και
- το αν χαρακτηρίζονται ως ελέγξιμοι ή όχι.

Για την ολοκλήρωση της διαδικασίας προσδιορισμού των πιθανών παραγόντων κινδύνου, οι υπεύθυνοι σχεδιασμού του έργου καλούνται να αξιολογήσουν τους υπάρχοντες μηχανισμούς ελέγχου των πληροφοριακών συστημάτων του οργανισμού. Οι μηχανισμοί αυτοί έχουν να κάνουν με την ασφάλεια του έργου και δεν αφορούν όλες τις κατηγορίες κινδύνων που μπορούν να το προσβάλλουν. Η εν λόγω αξιολόγηση έχει σκοπό να εντοπιστούν τυχόν ελλείψεις και αδυναμίες στα συστήματα ασφαλείας, ούτως ώστε να είναι πιο εύκολος αργότερα ο σχεδιασμός των διαδικασιών ασφαλείας του νέου πληροφοριακού συστήματος. Στο βήμα αυτό θα φανεί αρκετά χρήσιμη η συλλογή πληροφοριών που προηγήθηκε.

Μπορούμε να διακρίνουμε τους ελέγχους σε αποτρεπτικούς και σε ελέγχους εντοπισμού σφαλμάτων. Αποτρεπτικοί είναι οι έλεγχοι που στοχεύουν στο να εμποδίσουν τη δημιουργία επικίνδυνων καταστάσεων για τον οργανισμό, ενώ οι έλεγχοι εντοπισμού έχουν την ευθύνη να εντοπίζουν τις όποιες ανεπιθύμητες καταστάσεις εμφανίζονται στη λειτουργία των συστημάτων. Οι έλεγχοι ασφαλείας πραγματοποιούνται είτε από προσωπικό ασφαλείας είτε από διάφορα ηλεκτρονικά συστήματα είτε από πληροφοριακά συστήματα.

Το προσωπικό ασφαλείας οφείλει να ελέγχει τα πρόσωπα που εισέρχονται στους χώρους όπου διενεργούνται οι εργασίες εγκατάστασης του συστήματος, τα πρόσωπα που εισέρχονται στους χώρους αποθήκευσης του εξοπλισμού, αλλά και τα μέλη του προσωπικού που χρησιμοποιούν τα ήδη παραδοθέντα τμήματα του έργου και αποκτούν πρόσβαση σε ευαίσθητο λογισμικό και βάσεις δεδομένων. Επίσης, το προσωπικό ασφαλείας έχει την ευθύνη φύλαξης των εγκαταστάσεων κατά τις ώρες μη λειτουργίας του οργανισμού.

Εκτός, όμως, από το προσωπικό φύλαξης των εγκαταστάσεων του οργανισμού, υπάρχει και το προσωπικό φύλαξης του λογισμικού του έργου. Τα στελέχη αυτά παρακολουθούν τη λειτουργία των συστημάτων, έτσι ώστε να μπορούν να επέμβουν άμεσα σε περίπτωση κάποιας δυσλειτουργίας του συστήματος και να προλάβουν δυσμενέστερες επιπτώσεις αυτής. Επιπλέον, παρακολουθούν τα τερματικά που αποκτούν πρόσβαση στα διάφορα τμήματα του πληροφοριακού συστήματος (χρήση software, βάσεων δεδομένων) για τον εντοπισμό τυχόν μη εξουσιοδοτημένων χρηστών. Για το σκοπό αυτό, φυσικά, χρησιμοποιούν το κατάλληλο λογισμικό που τους επιτρέπει την πρόσβαση για έλεγχο σε κάθε ευαίσθητο κομμάτι του συστήματος.

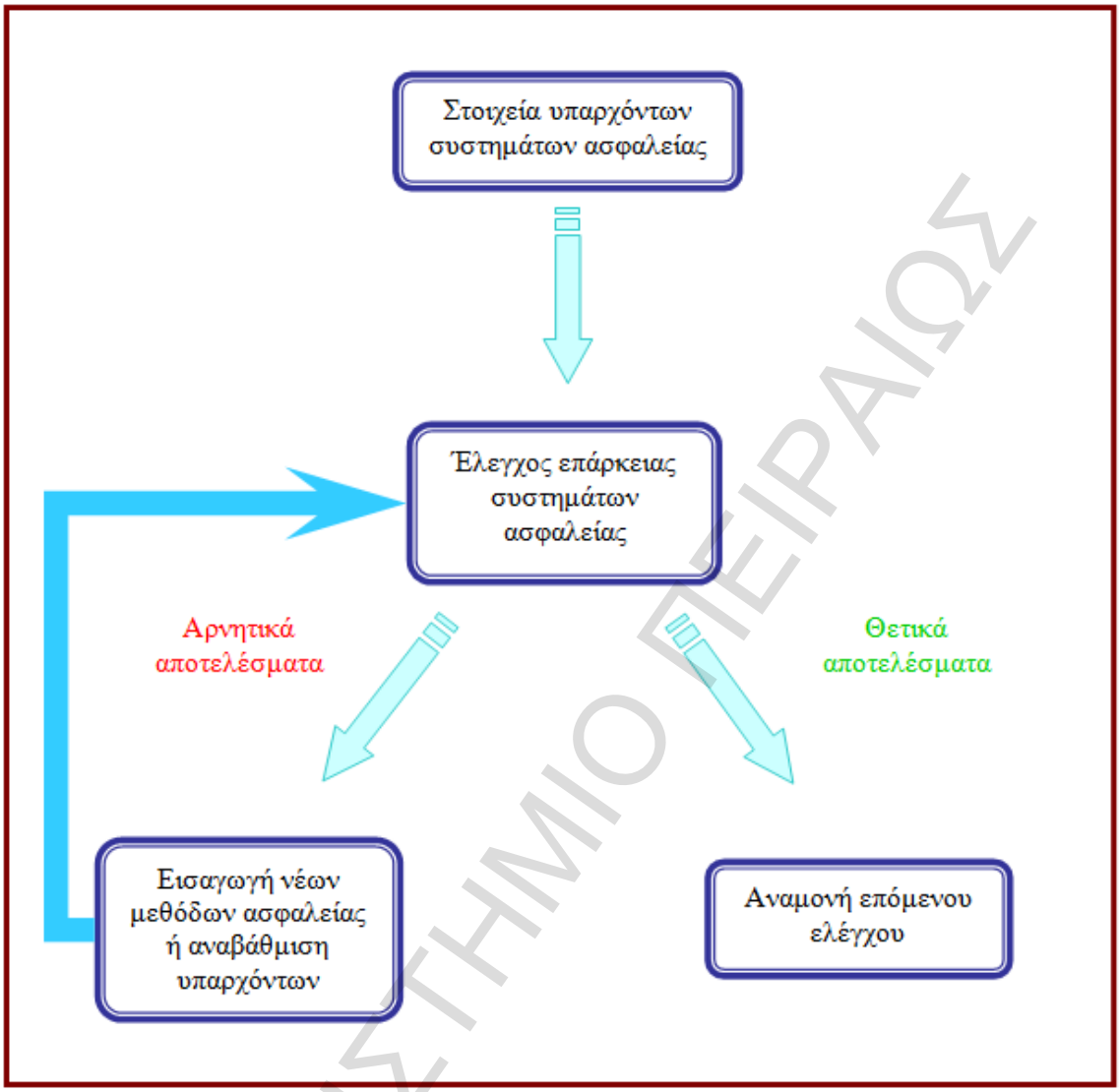
Παράλληλα, θα πρέπει να υπάρχουν και συστήματα που προστατεύουν το σύστημα από ανεπιθύμητους εισβολείς.

Ο εξοπλισμός (σε hardware και software) θα πρέπει να ελεγχθεί και να αξιολογηθεί ως προς την επάρκεια και την αποτελεσματικότητά του. Παράλληλα, θα πρέπει να αξιολογηθεί και το ίδιο το προσωπικό για τις τεχνικές γνώσεις του και τις δυνατότητές του να παρακολουθεί και να ελέγχει τη λειτουργία του συστήματος, να επoπτεύει τους χρήστες των συστημάτων και να εντοπίζει τις όποιες παράτυπες καταστάσεις εμφανίζονται στη λειτουργία του συστήματος. Το προσωπικό θα πρέπει να ελεγχθεί και για την αντίληψη που έχει για τη σημαντικότητα των καθηκόντων του όσον αφορά την ορθή λειτουργία και την ασφάλεια του έργου λογισμικού.

Υπάρχουν και τα ηλεκτρονικά συστήματα που ελέγχουν την τήρηση των συνθηκών ασφαλείας στους χώρους όπου βρίσκεται εγκατεστημένο το υλικό του πληροφοριακού έργου. Τέτοια είναι τα συστήματα πυρασφαλείας, τα συστήματα ελέγχου θερμοκρασίας και υγρασίας στο δωμάτιο εγκατάστασης του υλικού, θερμοστάτες στα διάφορα τμήματα του συστήματος, μετρητές τάσης και άλλα τέτοιου είδους μέσα ελέγχου της ασφαλούς λειτουργίας των συστημάτων.

Όλες οι παραπάνω διαδικασίες θα πρέπει να ελεγχθούν ως προς την ύπαρξή τους πρώτα από όλα, την αρτιότητα της λειτουργίας τους, την αποτελεσματικότητά τους, αλλά και τη συμβατότητά τους με το νέο λογισμικό και υλικό. Εκτός αυτών, όμως, θα πρέπει να αξιολογηθεί και η κρισιμότητα της χρήσης τους, καθώς τέτοιοι έλεγχοι καθυστερούν τη λειτουργία των συστημάτων και αυξάνουν την πολυπλοκότητά τους, με αποτέλεσμα να είναι πιθανόν επιζήμια, τελικά, η εισαγωγή τους σε τομείς του έργου που δεν εκτίθενται ιδιαίτερα σε κίνδυνο.

Στο παρακάτω διάγραμμα περιγράφονται σχηματικά οι διεργασίες ελέγχου και προσθήκης των συστημάτων ασφαλείας.



Σχήμα 3.5: Διαδικασία ελέγχου συστημάτων ασφαλείας.

Προσδιορισμός επιπτώσεων

Επιπρόσθετα, ενδέχεται να κριθεί χρήσιμη και η κατηγοριοποίηση των επιπτώσεων που παρουσιάζονται αν συμβεί το αρνητικό ενδεχόμενο. Αυτή μπορεί να γίνει με βάση τα ακόλουθα χαρακτηριστικά:

- χρόνος
- κόστος
- επίτευξη / εκτέλεση / ποιότητα
- υγιεινή και ασφάλεια

- περιβάλλον
- πολιτική

Τεκμηρίωση παραγόντων κινδύνων – Σύνταξη αναφοράς

Η πληροφορίες κατά τη διαδικασία αναγνώρισης κινδύνου σε συνδυασμό με την αναφορά επιπτώσεων θα αποτελέσουν ένα πολύ χρήσιμο εργαλείο για την κατάρτιση σχεδίου δράσης, με σκοπό τη μείωση ή την εξάλειψη της πιθανότητας εμφάνισης των διαφόρων κινδύνων. Οι ελλείψεις ή αδυναμίες θα πρέπει να καλυφθούν και οι διαδικασίες ασφαλείας να περάσουν ξανά από έλεγχο επάρκειας των δυνατοτήτων τους. Ο έλεγχος αυτός, φυσικά, θα πρέπει να επαναλαμβάνεται σε όλη τη διάρκεια υλοποίησης του έργου και τα συστήματα συνεχώς να αναβαθμίζονται για διατήρηση ικανοποιητικών επιπέδων ασφαλείας.

Μια σημαντική εκτίμηση κατά την αναγνώριση κινδύνου είναι να διασφαλιστεί ότι τα αποτελέσματα της διεργασίας δεν θα περιοριστούν από έλλειψη χρόνου, χρηματοοικονομικών πόρων ή διαπραγματευτικών δυσκολιών. Σε πολλές περιπτώσεις, τα διάφορα θέματα δεν τίθενται εγκαίρως, με αποτέλεσμα οι επιχειρήσεις να αντιμετωπίζουν κινδύνους που δεν θα αντιμετώπιζαν αν είχαν μια καλύτερη εκτίμηση των πιθανών συνεπειών.

3.1.2 Εκτίμηση Κινδύνου

Η εκτίμηση κινδύνου πραγματοποιείται γενικά με τη χρήση δύο μεθόδων, κάθε μία από τις οποίες οδηγεί σε μια εκτίμηση του βαθμού έκθεσης του έργου σε κίνδυνο. Η μία μέθοδος, συνίσταται στη διαδικασία εκτίμησης της πιθανότητας εμφάνισης των επικίνδυνων γεγονότων και της σοβαρότητας των επιδράσεών τους (πίνακας 3.3), ενώ όσον αφορά την άλλη μέθοδο, πρόκειται για μια διαδικασία εκτίμησης του βάρους των παραγόντων κινδύνου σε σχέση με τους υπολοίπους και της σοβαρότητας τους σε περίπτωση που εμφανιστούν (πίνακας 3.11). Συγκεκριμένα, συγκεντρώνονται τα στοιχεία από το προηγούμενο στάδιο προκειμένου να γίνει αποτίμηση των αγαθών και εκτίμηση των απειλών και αδυναμιών. Χρησιμοποιώντας τις προηγούμενες εκτιμήσεις, στη συνέχεια προσδιορίζεται το επίπεδο επικινδυνότητας για κάθε τμήμα του συστήματος. Για τις εκτιμήσεις αυτές μπορεί να γίνει χρήση ποσοτικών τεχνικών μέτρησης, ποιοτικών τεχνικών μέτρησης ή και των δύο. Τα πορίσματα της εκτίμησης κινδύνου βοηθούν στον προσδιορισμό των κατάλληλων ελέγχων για τη μείωση ή την εξάλειψη των κινδύνων κατά τη διαδικασία μετριασμού τους (Ξανθόπουλος, 2004).

Εκτίμηση Κινδύνου με τη Μέθοδο Πιθανότητας – Επίπτωσης

Ποια η πιθανότητα εμφάνισης των παραγόντων κινδύνου; ***Πόσο σοβαρές είναι οι επιπτώσεις τους;***	
Εκτίμηση πιθανότητας εμφάνισης παράγοντα κινδύνου	• Εκτίμηση της πιθανότητας να συμβεί κάθε παράγοντας κινδύνου (ποιοτικά ή ποσοτικά).
Προσδιορισμός επιπτώσεων κάθε παράγοντα κινδύνου	• Εκτίμηση του μεγέθους κάθε επίπτωσης κινδύνου (ποιοτικά ή ποσοτικά).
Εκτίμηση της έκθεσης στον κίνδυνο	• Εκτίμηση της συνολικής έκθεσης σε κίνδυνο (ποιοτικά ή ποσοτικά). • Ταξινόμηση των παραγόντων κινδύνου, ανάλογα με το βαθμό έκθεσης.
Τεκμηρίωση παραγόντων κινδύνου – Σύνταξη αναφοράς	➢ Καταγραφή πορίσματος σχετικά με την πιθανότητα εμφάνισης κινδύνου, την πιθανότητα ύπαρξης επιπτώσεων και την πιθανότητα έκθεσης σε κίνδυνο.

Πίνακας 3.3: Φάσεις εκτίμησης κινδύνου με τη μέθοδο πιθανότητας - επίπτωσης (Στάδιο 2).

Ποιοτικός προσδιορισμός του κινδύνου

Εκτίμηση πιθανότητας εμφάνισης παράγοντα κινδύνου

Η πιθανότητα (probability) εμφάνισης ενός παράγοντα κινδύνου αναφέρεται στο ενδεχόμενο ένας συγκεκριμένος παράγοντας να εμφανιστεί πραγματικά κατά τη διάρκεια του έργου. Σε σχετικά λίγες περιπτώσεις, όμως, είναι δυνατό να υπολογιστεί αριθμητικά η πιθανότητα εμφάνισης ενός παράγοντα κινδύνου. Τις περισσότερες φορές υπολογίζεται και εκφράζεται ποιοτικά σύμφωνα με την εμπειρία ή τη διαίσθηση.

Κατά τη διαδικασία εκτίμησης της πιθανότητας εμφάνισης κινδύνων, πρέπει να ληφθούν υπόψη τα εξής (Stoneburner, Goguen και Feringa, 2001):

- Το κίνητρο και οι δυνατότητες της κάθε πηγής κινδύνων.
- Η φύση των ευπαθειών.
- Η παρουσία και η αποτελεσματικότητα των υπαρχόντων ελέγχων.

Η διαδικασία εκτίμησης της πιθανότητας εμφάνισης ενός παράγοντα κινδύνου δεν είναι απλή. Καταρχήν, τα πρόσωπα που θα προβούν σε αυτή την εκτίμηση θα πρέπει να έχουν κατάλληλη κατάρτιση, σωστή ενημέρωση και την απαιτούμενη πείρα, ούτως ώστε να μπορέσουν να εκτιμήσουν ορθολογικά την πιθανότητα παρουσίας κάθε ανεπιθύμητου γεγονότος. Μια λανθασμένη εκτίμηση μπορεί να έχει καταστροφικές συνέπειες για την αξιοπιστία και τη χρησιμότητα της όλης διαδικασίας διαχείρισης κινδύνων. Όμοια, μια αισιόδοξη εκτίμηση για την πιθανότητα εμφάνισης κάποιων απειλών μπορεί να οδηγήσει στην υποτίμησή τους και τη μη λήψη των κατάλληλων μέτρων για την αντιμετώπισή τους. Από την άλλη, απαισιόδοξες εκτιμήσεις θα έχουν ως αποτέλεσμα την άσκοπη διάθεση κονδυλίων και την αύξηση της πολυπλοκότητας και των καθυστερήσεων στη λειτουργία των συστημάτων, για αντιμετώπιση κινδύνων που δεν αποτελούν ουσιαστική απειλή για την υλοποίηση του έργου λογισμικού.

Η έκθεση σε κίνδυνο ορίστηκε με βάση το 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 μετριέται με τη σοβαρότητα (severity) του εκάστοτε παράγοντα κινδύνου, μπορεί να υπολογιστεί ως το γινόμενο της πιθανότητας και των 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 έναν πίνακα πιθανότητας / επιπτώσεων. Από αυτόν τον συνδυασμό της πιθανότητας και των επιπτώσεων ενός παράγοντα κινδύνου προκύπτει η σοβαρότητα (severity) κάθε παράγοντα. Τέλος, η συνολική έκθεση σε κίνδυνο μπορεί να προσδιοριστεί ως το πηλίκο του αθροίσματος της σοβαρότητας όλων των παραγόντων κινδύνου δια του πλήθους τους.

Παρακάτω παρουσιάζονται οι κλίμακες βαθμολόγησης που χρησιμοποιούνται για την εκτίμηση της πιθανότητας εμφάνισης κινδύνου (πίνακας 3.4), των επιπτώσεων των παραγόντων κινδύνου (πίνακας 3.5), καθώς και ο πίνακας πιθανότητας-επιπτώσεων (πίνακας 3.8):

Απεικόνιση		Ορισμός
Σχεδόν Βέβαιο	>80%	Αναμένεται να συμβεί στις περισσότερες περιπτώσεις και/ή οι αρμόδιες διαδικασίες ελέγχου αποδεικνύονται αναποτελεσματικές για την αντιμετώπισή του.
Πολύ Πιθανό	51-80%	Ενδεχομένως να συμβεί στις περισσότερες περιπτώσεις και/ή οι απαιτούμενες διαδικασίες ελέγχου παρουσιάζουν μεγάλες αδυναμίες και ελλείψεις.
Πιθανό	21-50%	Πιθανώς να συμβεί κάποια στιγμή και/ή οι διαδικασίες ελέγχου ενδεχομένως να τον αντιμετωπίσουν αποτελεσματικά.
Σπάνιο	6-20%	Μπορεί να συμβεί σε μερικές περιπτώσεις και/ή οι διαδικασίες ελέγχου δύνανται να τον αντιμετωπίσουν με επιτυχία.
Απίθανο	0-5%	Μπορεί να συμβεί μόνο σε εξαιρετικές περιπτώσεις και/ή οι διαδικασίες ελέγχου είναι ουσιαστικά “αδιαπέραστες”.

Πίνακας 3.4: Εκτίμηση πιθανότητας εμφάνισης κινδύνου.

Η κλίμακα πιθανότητας εμφάνισης κινδύνου βρίσκεται μεταξύ 0 ή 0% (καμία πιθανότητα) και 1 ή 100% (βεβαιότητα). Ο ακριβής υπολογισμός της πιθανότητας εμφάνισης ενός κινδύνου είναι μια πολύ δύσκολη διαδικασία και τα αποτελέσματά της είναι δύσκολο να ελεγχθούν για την ακρίβεια και την ορθότητά τους. Για αυτό, συχνά χρησιμοποιείται μια γενική κλίμακα τυποποιημένων πιθανοτήτων, ανάλογα με τα επίπεδα πιθανότητας του παραπάνω πίνακα. Οι τυποποιημένες τιμές της κλίμακας αυτής, ανάλογα με το πόσο πιθανή είναι η εμφάνιση ενός γεγονότος, είναι 0.1, 1.3, 0.5, 0.7 και 0.9 αντίστοιχα.

Είδαμε παραπάνω πώς μπορούμε να κατατάξουμε τους κινδύνους ανάλογα με την πιθανότητα εμφάνισής τους. Το πιο δύσκολο, όμως, κομμάτι αυτής της διαδικασίας είναι το πώς θα καθοριστεί η πιθανότητα εμφάνισης της κάθε απειλής. Για το σκοπό αυτό, θα φανούν εξαιρετικά χρήσιμες οι πληροφορίες που συλλέχθηκαν κατά τη φάση της αναγνώρισης κινδύνου (στάδιο 1) σχετικά με τον οργανισμό και τους στόχους που θα έχει να επιτελέσει το νέο πληροφοριακό έργο, καθώς και με τους υπάρχοντες ελέγχους ασφαλείας. Για παράδειγμα, η χρήση τεχνολογιών που εφαρμόζονται για πρώτη φορά εμφανίζουν υψηλή επικινδυνότητα να παρουσιάσουν δυσλειτουργίες στη χρήση τους και να μη μπορέσουν τελικά να ανταποκριθούν στις απαιτήσεις του οργανισμού, ενώ η χρήση δοκιμασμένων συστημάτων δεν προβληματίζει τόσο για τη

λειτουργικότητα της χρησιμοποίησής τους. Αυτές οι δοκιμασμένες, όμως, τεχνολογίες αντιμετωπίζουν με τη σειρά τους τον κίνδυνο να καταστούν απαρχαιωμένες σε μικρό χρονικό διάστημα από την εκκίνηση της λειτουργίας τους, κάτι που έχει πολύ μικρές πιθανότητες να συμβεί με τη χρήση νέων και σύγχρονων τεχνολογιών.

Ένα δεύτερο παράδειγμα αποτελούν οι απειλές από ανταγωνιστές. Ένα έργο με κοινωφελείς προεκτάσεις, όπως η διαδικτυακή σύνδεση νοσοκομείων για την μεταφορά αρχείων με το ιστορικό των ασθενών, φαντάζει αδύνατο να έχει να αντιμετωπίσει τον κίνδυνο δολιοφθορών από ανταγωνιστές ή τρομοκρατικών επιθέσεων, αλλά κινδυνεύει από τη χρήση των στοιχείων των ασθενών από πρόσωπα που επιδιώκουν να τα εκμεταλλευτούν για προσωπικό όφελος. Ενδεικτικά αναφέρονται οι λίστες των δωρητών οργάνων, η κοινοποίηση των οποίων μπορεί να θέσει σε κίνδυνο τις ζωές των δωρητών από επιτήδειους που αναζητούν απεγνωσμένα κάποιο όργανο και διαθέτουν τα χρήματα και τα μέσα για να το αποκτήσουν με κάθε τρόπο. Τέλος, ένα ακόμα παράδειγμα που κάνει σαφή τη διαφορετικότητα του κάθε υπό υλοποίηση έργου είναι τα καιρικά φαινόμενα που μπορούν να απειλήσουν τις εγκαταστάσεις του οργανισμού και που διαφοροποιούνται ανάλογα με τη γεωγραφική θέση του οργανισμού και γενικότερα το περιβάλλον όπου βρίσκονται οι εγκαταστάσεις.

Προσδιορισμός επιπτώσεων κάθε παράγοντα κινδύνου

Σημαντικό βήμα για την εκτίμηση κινδύνου με τη μέθοδο πιθανότητας-επίπτωσης αποτελεί η αξιολόγηση των επιπτώσεων από την εμφάνιση κάποιας εκ των απειλών στην πορεία υλοποίησης του έργου. Σκοπός της εκτίμησης κινδύνου είναι να χωρίσει τους κινδύνους σε ομάδες με συγκεκριμένη προτεραιότητα, οι οποίες βοηθούν στην ανάπτυξη της στρατηγικής αντιμετώπισης κάθε κινδύνου. Η διαδικασία εκτίμησης κινδύνων, η οποία αποτελεί μια συστηματική διαδικασία με σκοπό τον καθορισμό της συχνότητας και το μέγεθος των πιθανών συνεπειών τους, παράγει ένα σύνολο παραγόντων και επιπέδων κινδύνου που χρησιμοποιούνται για να θέσουν προτεραιότητες ως προς την αντιμετώπισή τους. Οι προτεραιότητες αυτές τίθενται με βάση τα οριοθετημένα επίπεδα κινδύνου και άλλα κριτήρια που έχουν οριστεί κατά την ανάλυση του στρατηγικού και οργανωτικού πλαισίου του έργου. Για την επιτυχημένη ολοκλήρωση του βήματος αυτού είναι απαραίτητη η γνώση κάποιων πληροφοριών σχετικά με το έργο πληροφορικής, όπως:

- η αποστολή του συστήματος (οι διαδικασίες που θα επιτελούνται από το πληροφοριακό σύστημα),
- η κρισιμότητα του συστήματος και της βάσης δεδομένων που διατηρεί (η αξία και η σημασία του συστήματος για τη λειτουργία και την ανάπτυξη του οργανισμού) και
- η ευαισθησία του συστήματος και της βάσης δεδομένων.

Οι πληροφορίες αυτές μπορούν να συλλεχθούν από υπάρχουσες εκθέσεις της λειτουργίας του οργανισμού, όπως η έκθεση ανάλυσης αντίκτυπου ενός στόχου ή η έκθεση αξιολόγησης κρισιμότητας μιας διαδικασίας. Η έκθεση ανάλυσης αντίκτυπου ενός στόχου παρουσιάζει το επίπεδο των κινδύνων που συνοδεύουν την εφαρμογή μιας διαδικασίας μαζί με τα προτερήματα αυτής, βασισμένη σε μια ποιοτική ή ποσοτική αξιολόγηση της ευαισθησίας και της κρισιμότητας αυτών των προτερημάτων. Η έκθεση αξιολόγησης κρισιμότητας μιας διαδικασίας αναγνωρίζει και δίνει προτεραιότητα στα ευπαθή και κρίσιμα προτερήματα του οργανισμού που παίζουν σημαντικό ρόλο στην επίτευξη των στόχων του.

Εάν τέτοιου είδους εκθέσεις δεν υπάρχουν, τότε η ευαισθησία συστημάτων και πληροφοριών μπορεί να καθοριστεί με βάση το επίπεδο προστασίας που απαιτείται για τη διατήρηση της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας αυτών. Ανεξάρτητα από τη μέθοδο που θα χρησιμοποιηθεί για τον καθορισμό της ευαισθησίας του πληροφοριακού συστήματος και της βάσης δεδομένων του, οι υπεύθυνοι υλοποίησης του έργου, σε συνεργασία με τη διοίκηση του οργανισμού για τον οποίο υλοποιείται το έργο, οφείλουν να είναι σε θέση να καθορίσουν το επίπεδο των επιπτώσεων από την ενδεχόμενη δυσλειτουργία ή προσβολή από εξωτερικούς παράγοντες του συστήματος. Για την αξιολόγηση των επιπτώσεων, λοιπόν, θα ήταν χρήσιμες οι πληροφορίες από τις συναντήσεις με τους διοικούντες του οργανισμού, οι οποίοι αποφάσισαν την προσθήκη ενός τέτοιου συστήματος στο δυναμικό του οργανισμού. Ακολουθεί μια συνοπτική περιγραφή των στόχων ασφαλείας που πρέπει να επιτευχθούν και των συνεπειών από τη μη επιτυχημένη προστασία τους (Stoneburner, Goguen και Feringa, 2001):

Απώλεια ακεραιότητας

Η ακεραιότητα συστημάτων και πληροφοριών αναφέρεται στην απαίτηση αυτά να προστατεύονται από την ανάρμοστη τροποποίηση ή καταστροφή, αλλά και την απαίτηση άμεσης αποκατάστασης της λειτουργίας τους, σε περίπτωση που αυτή παρουσιάσει προβλήματα. Η ακεραιότητα χάνεται εάν πραγματοποιούνται μη προγραμματισμένες αλλαγές, είτε σκόπιμα είτε τυχαία, ή όταν τμήματα του εξοπλισμού παρουσιάζουν ελαττωματική λειτουργία ή ακόμα και όταν έχουν γίνει σφάλματα στο σχεδιασμό του έργου. Η απώλεια ακεραιότητας στη βάση δεδομένων του συστήματος ή στο λογισμικό του και ο μη έγκαιρος εντοπισμός των σφαλμάτων μπορεί να οδηγήσει σε ανακρίβειες, απάτες σε βάρος του οργανισμού και σε λανθασμένες αποφάσεις από τη διοίκηση εξαιτίας της χρήσης αλλοιωμένων πληροφοριών. Επίσης, η παραβίαση της ακεραιότητας μπορεί να αποτελέσει το πρώτο βήμα σε μια επιτυχή επίθεση ενάντια στη διαθεσιμότητα ή την εμπιστευτικότητα των συστημάτων. Η δυσλειτουργία λογισμικού και υλικού από αίτια, όπως αυτά που αναφέρθηκαν στην παράγραφο 3.1.1, θα επιβαρύνουν τον αρχικό προϋπολογισμό για την υλοποίηση του έργου αλλά και θα προκαλέσουν μεγάλες καθυστερήσεις στην ολοκλήρωσή του. Και πάλι, με αυτόν τον τρόπο προσβάλλεται η διαθεσιμότητα των συστημάτων.

Απώλεια διαθεσιμότητας

Τμήματα του πληροφοριακού συστήματος ή και ολόκληρο το σύστημα δεν είναι διαθέσιμο, είτε διότι δεν έχουν ολοκληρωθεί οι εργασίες εγκατάστασής του βάση των χρονοδιαγραμμάτων, είτε διότι παρουσίασε σφάλματα κατά τη χρήση του και τέθηκε εκτός λειτουργίας έως ότου διορθωθεί το πρόβλημα. Η απώλεια της διαθεσιμότητας μπορεί να είναι, όπως είδαμε παραπάνω, απόρροια της απώλειας της ακεραιότητας του συστήματος. Όποια κι αν είναι η αιτία, όμως, η ζημιά για τον οργανισμό είναι πολύ μεγάλη, καθώς χάνονται τα χρηματικά οφέλη που ενδεχομένως να αποκομίζονται από τη λειτουργία του συστήματος (π.χ. διακοπή παραγωγικής διαδικασίας, αδυναμία διάθεσης υπηρεσιών ή προϊόντων μέσω του διαδικτύου), αποδιοργανώνονται οι διαδικασίες του οργανισμού, χάνονται ευκαιρίες που θα βοηθούσαν στην ανάπτυξη και στην αύξηση των κερδών του, ενώ παράλληλα πλήττεται και το κύρος και η αξιοπιστία του οργανισμού. Το είδος και το επίπεδο των απωλειών εξαρτάται από το είδος του οργανισμού και τους σκοπούς που εξυπηρετεί το πληροφοριακό σύστημα. Γίνεται, όμως, φανερό πόσο σημαντική είναι η τήρηση των χρονοδιαγραμμάτων για την ολοκλήρωση του έργου, η πρόληψη για την αποφυγή σφαλμάτων και παραλήψεων που θα θέσουν το σύστημα εκτός λειτουργίας, αλλά και η πρόβλεψη για την άμεση αποκατάσταση της διαθεσιμότητας του συστήματος σε περίπτωση που τελικά δεν αποφευχθεί η διακοπή της λειτουργίας του.

Απώλεια εμπιστευτικότητας

Η εμπιστευτικότητα συστημάτων και δεδομένων αναφέρεται στην προστασία των πληροφοριών από μη εξουσιοδοτημένη κοινοποίηση. Οι επιπτώσεις μιας τέτοιας κοινοποίησης μπορούν να κυμανθούν από τη διακινδύνευση της εθνικής ασφάλειας έως την απώλεια αιφνιδιασμού της αγοράς από την εισαγωγή ενός νέου προϊόντος ή τη μείωση των τιμών και γενικά οποιαδήποτε ενέργεια που δεν αναμένουν οι ανταγωνιστές. Μπορούν, ακόμα, να διαρρεύσουν τα μελλοντικά σχέδια του οργανισμού, επιτρέποντας στους ανταγωνιστές να προετοιμάσουν τα δικά τους σχέδια ή ακόμα και να γνωστοποιηθούν ευαίσθητα προσωπικά δεδομένα στελεχών του οργανισμού ή άλλων προσώπων, στοιχεία των οποίων υπάρχουν στις βάσεις δεδομένων του συστήματος. Πέραν όλων των άλλων, η μη εξουσιοδοτημένη, παράνομη ή ακούσια δημοσιοποίηση τέτοιων πληροφοριών θα μπορούσε να οδηγήσει στην απώλεια της δημόσιας εμπιστοσύνης, στην αμηχανία της διοίκησης ή ακόμα και στη λήψη νομικής δράσης ενάντια στον οργανισμό για κοινοποίηση ευαίσθητων προσωπικών δεδομένων που διατηρούσε στη βάση δεδομένων του και που αφορούν τρίτα πρόσωπα, είτε αυτά ανήκουν στον οργανισμό είτε όχι. Ένα παράδειγμα αποτελεί η διαρροή του ιστορικού ασθενών που νοσηλεύθηκαν σε κάποιο ιδιωτικό νοσοκομείο, το οποίο βρισκόταν στη βάση δεδομένων του.

Οι επιπτώσεις (impacts) που απορρέουν από την εμφάνιση των κινδύνων δε μπορούν πάντα να μετρηθούν και να αποτιμηθούν. Οι επιπτώσεις από την καταστροφή υλικού ή λογισμικού μπορούν να αποτιμηθούν από το κόστος αγοράς και εγκατάστασης νέου εξοπλισμού και από την καθυστέρηση εξέλιξης του έργου. Γενικά,

οι επιπτώσεις που επιφέρουν επιπλέον κόστος ή καθυστερήσεις είναι εύκολο να ποσοτικοποιηθούν και να εκτιμηθεί η σοβαρότητά τους. Επιπτώσεις, όμως, όπως η απώλεια ευκαιριών σε μια ανταγωνιστική αγορά, η απώλεια μονοπωλίου, η καθυστέρηση στην παράδοση προϊόντων ή στην παροχή υπηρεσιών και η επικείμενη δυσαρέσκεια των πελατών, η προσβολή του κύρους και της αξιοπιστίας του οργανισμού, η δημιουργία τριβών στη σχέση της διοίκησης με το προσωπικό κ.α. δε μπορούν να ποσοτικοποιηθούν. Αυτές θα πρέπει να αξιολογηθούν ποιοτικά με βάση τη γνώση τόσο της κατηγορίας του παράγοντα κινδύνου όσο και των λεπτομερειών του ίδιου του έργου. Για το σκοπό αυτό, μπορούμε να κατατάξουμε τις επιπτώσεις από τον κάθε κίνδυνο σε κάποιον από τους παρακάτω πέντε χαρακτηρισμούς όπως κάναμε και για την πιθανότητα εμφάνισής τους:

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

Πίνακας 3.5: Εκτίμηση επιπτώσεων παραγόντων κινδύνου.

Καθένα από τα παραπάνω επίπεδα περιγράφει τη σοβαρότητα των επιπτώσεων που επιφέρει η εμφάνιση ενός κινδύνου για τον οργανισμό. Μπορούμε να αντιστοιχίσουμε την κλίμακα που χρησιμοποιήσαμε για την πιθανότητα εμφάνισης ενός κινδύνου στις πέντε αυτές διαβαθμίσεις. Αντί αυτής, όμως, θα χρησιμοποιήσουμε μια μη γραμμική κλίμακα, η οποία τονίζει περισσότερο την επιθυμία των διοικούντων του οργανισμού να αποφύγουν κινδύνους με πολύ σοβαρές συνέπειες. Η νέα κλίμακα είναι 0.05, 0.1, 0.2, 0.4 και 0.8. Η κλίμακα αυτή θα μπορούσε να διαφοροποιηθεί και να προσαρμοστεί στα ζητούμενα του κάθε οργανισμού.

Ο πίνακας 3.6 που ακολουθεί δίνει μια περιγραφή της σημασίας του κάθε επιπέδου κινδύνου:

Αξιολόγηση επιπτώσεων κινδύνων στους ευπαθείς τομείς ενός έργου					
Ευπαθείς τομείς	**Αμελητέες 0.05**	**Μικρές 0.1**	**Μέτριες 0.2**	**Σοβαρές 0.4**	**Επικίνδυνες 0.8**
Κόστος	Αμελητέα αύξηση του κόστους	Αύξηση κόστους <5%	Αύξηση κόστους 5-10%	Αύξηση κόστους 10-20%	Αύξηση κόστους >20%
Χρονοδιά-γραμμα	Αμελητέα ολίσθηση χρονοδιαγράμ-ματος	Ολίσθηση χρονοδιαγράμ-ματος <5%	Ολίσθηση χρονοδιαγράμ-ματος 5-10%	Ολίσθηση χρονοδιαγράμ-ματος 10-20%	Ολίσθηση χρονοδιαγράμ-ματος >20%
Σκοπός	Μικρή παρέκκλιση από το στόχο ελάχιστα παρατηρήσιμη	Μικρά τμήματα του στόχου έχουν επηρεαστεί	Μεγάλα τμήματα του στόχου έχουν επηρεαστεί	Παρέκκλιση από το στόχο σε μη αποδεκτά επίπεδα για τον αγοραστή	Το έργο που παρήχθη είναι λειτουργικά άχρηστο
Ποιότητα	Υποβιβασμός της ποιότητας ελάχιστα παρατηρήσιμος	Μόνο πολύ απαιτητικές εφαρμογές επηρεάζονται	Μείωση της ποιότητας απαιτείται έγκριση από τον αγοραστή	Μείωση της ποιότητας σε μη αποδεκτά επίπεδα για τον αγοραστή	Το έργο που παρήχθη δεν μπορεί να χρησιμοποιηθεί

Πίνακας 3.6: Επίπεδο επιπτώσεων ανά ευπαθή τομέα ενός έργου.

Στον παραπάνω πίνακα παρουσιάζονται οι επιπτώσεις των κινδύνων σε βάρος της πορείας υλοποίησης του πληροφοριακού έργου. Πέραν αυτών, όμως, θα πρέπει να εκτιμώνται και οι επιπτώσεις στη λειτουργία του οργανισμού από την ενδεχόμενη εμφάνιση κάποιων κινδύνων. Οι επιπτώσεις αυτές, βέβαια, πηγάζουν από την προσβολή κάποιου από τους παραπάνω τέσσερις ευπαθείς τομείς. Το επιπλέον κόστος, ανάλογα με την αρχική συμφωνία, μπορεί να επιβαρύνει είτε την ανάδοχο εταιρεία είτε τον ίδιο τον οργανισμό. Η μη τήρηση των χρονοδιαγραμμάτων σημαίνει ότι πλήττεται η διαθεσιμότητα του έργου. Η παρέκκλιση από τους αρχικούς στόχους που θα πρέπει να εκπληρώνει το νέο λογισμικό πλήττει, ουσιαστικά, εξαρχής την ακεραιότητα του έργου, ενώ η υποβάθμιση της ποιότητάς του δημιουργεί αμφιβολίες για την ασφαλή (ακεραιότητα – εμπιστευτικότητα) και εποικοδομητική λειτουργία του συστήματος.

Παράλληλα, ιδιαίτερη σημασία έχει και η πρόβλεψη μιας αλυσίδας επιπτώσεων. Δηλαδή, η εμφάνιση ενός κινδύνου μπορεί να προκαλεί προβλήματα σε περισσότερους του ενός τομείς του έργου. Για παράδειγμα, μπορεί η δυσλειτουργία ενός τμήματος του έργου να απαιτεί την αντικατάσταση ή την επιπλέον επεξεργασία του εξοπλισμού, γεγονός, όμως, που θα επηρεάσει το κόστος και το χρόνο υλοποίησης του έργου αλλά πιθανώς και την ποιότητα αυτού.

Συνεπώς, γίνεται φανερό ότι για την ορθή αξιολόγηση των επιπτώσεων θα πρέπει να συνυπολογίζονται και οι ιδιαίτερες συνθήκες που διέπουν τη λειτουργία του κάθε έργου πληροφορικής. Για παράδειγμα, για έναν οργανισμό που εκτελεί δημοπρασίες μέσω διαδικτύου, η καθυστέρηση παράδοσης του έργου ή η αναγκαστική διακοπή της λειτουργίας τμημάτων, που έχουν ήδη παραδοθεί, για επιδιορθώσεις λόγω εσφαλμένης λειτουργίας ή λόγω δυσκολίας διασύνδεσης με τα υπόλοιπα τμήματα του έργου που είναι υπό παράδοση μπορεί να επιφέρει τεράστιες οικονομικές απώλειες για τον οργανισμό από την αδυναμία διάθεσης των προϊόντων του, ενώ κάποιες προσαυξήσεις στο κόστος παραγωγής ή κάποιες παραχωρήσεις στην ποιότητα του έργου, ενδεχομένως, να μην αποτελούσαν σημαντικά πλήγματα. Αντίστοιχα, η δικτυακή οργάνωση της μισθοδοσίας ενός τομέα του δημοσίου δε θα είχε ιδιαίτερη επιβάρυνση από κάποια ολιγοήμερη καθυστέρηση στην ολοκλήρωση των εργασιών, καθώς απλώς θα καθυστερούσε ο εκσυγχρονισμός των διαδικασιών, ενώ οι μισθοδοσίες θα πραγματοποιούνταν και θα καταγράφονταν με τις ήδη υπάρχουσες μεθόδους.

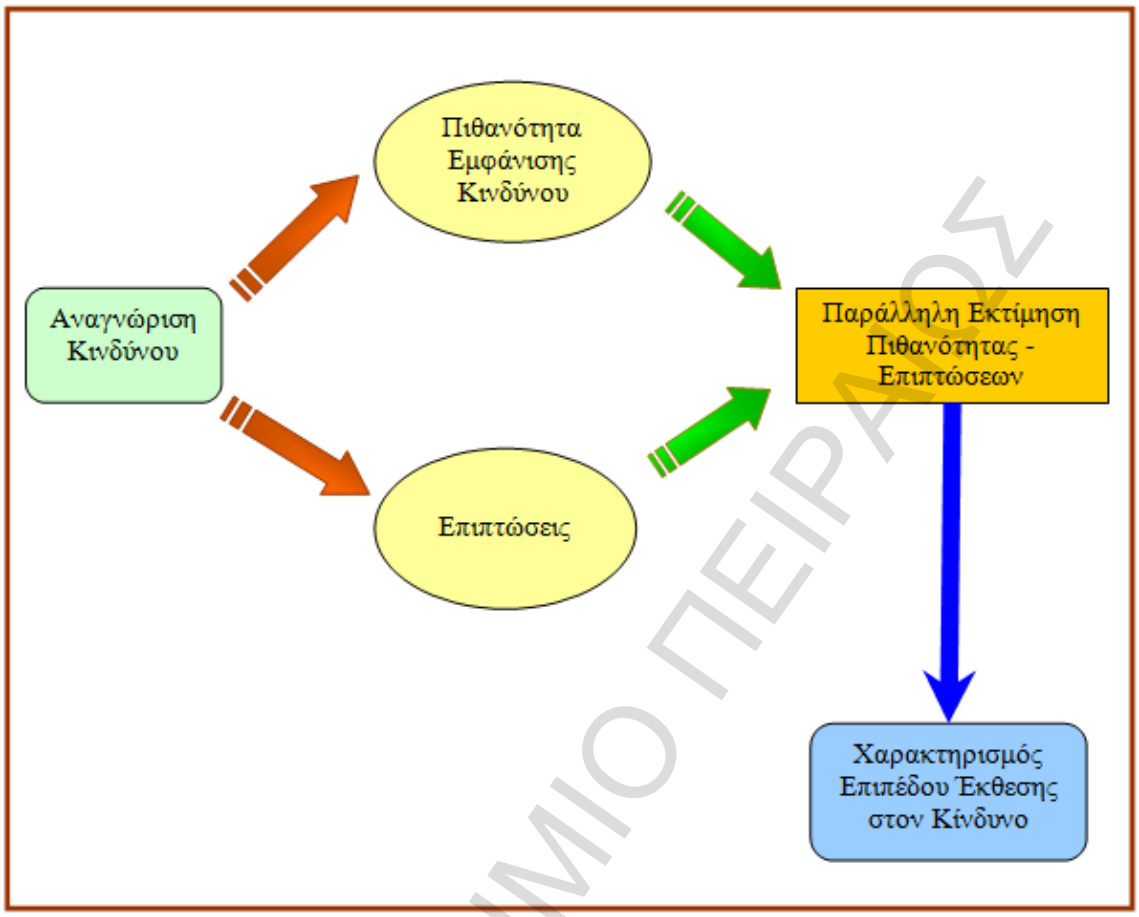
Ιδιαίτερη αντιμετώπιση θα πρέπει να έχουν και τα αντίστοιχα τμήματα του ίδιου του έργου. Διαφορετική βαρύτητα έχουν οι παραχωρήσεις στην ασφάλεια οικονομικών συναλλαγών και διαφορετική στην ασφάλεια παρουσίασης διαφημιστικού υλικού. Επίσης, διαφορετικές είναι οι επιπτώσεις από την πτώση ενός server και διαφορετικές από τη δυσλειτουργία ενός τερματικού.

Από όλα τα παραπάνω αντιλαμβάνεται κανείς την ανάγκη συνεργασίας με τη διοίκηση του οργανισμού για την ορθή κατηγοριοποίηση των επιπτώσεων από την εμφάνιση ενός κινδύνου, καθώς η κάθε περίπτωση απαιτεί τη δική της ιδιαίτερη αντιμετώπιση. Εξίσου απαραίτητη είναι και η αίτηση της συμβολής ειδικών σε τεχνικά θέματα για την κατανόηση της σημασίας και της δυσκολίας αντιμετώπισης των προβλημάτων που μπορεί να αντιμετωπίζει το κάθε τμήμα του έργου.

Εκτίμηση της έκθεσης στον κίνδυνο

Η αξιολόγηση του επιπέδου κινδύνου για το υπό κατασκευή πληροφοριακό σύστημα θα πραγματοποιηθεί μέσω της παράλληλης εξέτασης της πιθανότητας εμφάνισης ενός κινδύνου και των επιπτώσεών του και μπορεί να εκφραστεί από (σχήμα 3.6):

- Την πιθανότητα μια δεδομένη πηγή κινδύνου να επιδιώξει να επιφέρει κάποια δυσμενή επίπτωση.
- Το μέγεθος των επιπτώσεων από μια τέτοια επιτυχημένη προσπάθεια.
- Η επάρκεια των προγραμματιζόμενων ή υπαρχόντων ελέγχων ασφαλείας για τη μείωση ή την εξάλειψη του κινδύνου.



Σχήμα 3.6: Διαδικασία εκτίμησης επιπέδου έκθεσης σε κίνδυνο.

Για την εκτίμηση της σοβαρότητας ενός κινδύνου συνυπολογίζεται η πιθανότητα εμφάνισης με το επίπεδο των επιπτώσεων. Για να επιτευχθεί αυτό, όπως έχει ήδη αναφερθεί, πολλαπλασιάζουμε τις τυποποιημένες τιμές που υπολογίσαμε προηγουμένως για κάθε πιθανότητα και επίπτωση και ανάλογα με το αριθμητικό αποτέλεσμα χαρακτηρίζουμε τον κίνδυνο υψηλής, μέτριας ή χαμηλής σοβαρότητας. Στον πίνακα που ακολουθεί παρουσιάζονται τα αποτελέσματα από το συνδυασμό όλων των επιπέδων πιθανότητας εμφάνισης και επιπτώσεων:

Αριθμητικά αποτελέσματα συνυπολογισμού των διαφόρων επιπέδων πιθανότητας και επιπτώσεων σε ένα συγκεκριμένο τομέα π.χ. κόστος, χρόνος, ποιότητα (μη γραμμική κλίμακα)						
Βαθμολογία επιπέδου έκθεσης σε κίνδυνο	0.80	0.08	0.24	0.40	0.56	0.72
	0.40	0.04	0.12	0.20	0.28	0.36
	0.20	0.02	0.06	0.10	0.14	0.18
	0.10	0.01	0.03	0.05	0.07	0.09
	0.05	0.01	0.02	0.03	0.04	0.05
		0.1	0.3	0.5	0.7	0.9
		Πιθανότητα				

Πίνακας 3.7: Αριθμητικά αποτελέσματα συνυπολογισμού των διαφόρων επιπέδων πιθανότητας και επιπτώσεων.

Ο χαρακτηρισμός των κινδύνων ως υψηλού (κόκκινο ★), μέτριου (πορτοκαλί ★) και χαμηλού (μαύρο ★) επιπέδου φαίνεται μέσω των χρωμάτων των κελιών του πίνακα 3.7, όπως προκύπτουν από τα αριθμητικά αποτελέσματα των υπολογισμών. Ακολουθεί μια, πιο ποιοτική, εναλλακτική παράσταση του παραπάνω πίνακα (πίνακας 3.8) κι επεξήγηση του τι αντιπροσωπεύει το κάθε επίπεδο κινδύνου (πίνακας 3.9) (Stoneburner, Goguen και Feringa, 2001):

Επιπτώσεις					
Επικίνδυνη (5)	Μέτριας Σοβαρότητας	Υψηλής Σοβαρότητας	Υψηλής Σοβαρότητας	Υψηλής Σοβαρότητας	Υψηλής Σοβαρότητας
Σοβαρή (4)	Μέτριας Σοβαρότητας	Μέτριας Σοβαρότητας	Μέτριας Σοβαρότητας	Μέτριας Σοβαρότητας	Υψηλής Σοβαρότητας
Μέτρια (3)	Χαμηλής Σοβαρότητας	Μέτριας Σοβαρότητας	Μέτριας Σοβαρότητας	Μέτριας Σοβαρότητας	Υψηλής Σοβαρότητας
Μικρή (2)	Χαμηλής Σοβαρότητας	Χαμηλής Σοβαρότητας	Μέτριας Σοβαρότητας	Μέτριας Σοβαρότητας	Υψηλής Σοβαρότητας
Αμελητέα (1)	Χαμηλής Σοβαρότητας	Χαμηλής Σοβαρότητας	Χαμηλής Σοβαρότητας	Μέτριας Σοβαρότητας	Μέτριας Σοβαρότητας
	Απίθανο (1)	Σπάνιο (2)	Πιθανό (3)	Πολύ Πιθανό (4)	Σχεδόν Βέβαιο (5)
	Πιθανότητα				

Πίνακας 3.8: Πίνακας πιθανότητας - επιπτώσεων.

Επίπεδο κινδύνου	Περιγραφή κινδύνου και απαραίτητες ενέργειες
Υψηλό	Εάν μια κατάσταση αξιολογείται ως υψηλός κίνδυνος, τότε υπάρχει ισχυρή ανάγκη για διορθωτικά μέτρα. Ενδεχομένως τα μέτρα αυτά να μην επαρκούν και να αποφασιστεί η ματαίωση υλοποίησης του έργου. Αν, τελικά, το υπάρχον σύστημα μπορεί να συνεχίσει να λειτουργεί, ένα πρόγραμμα διορθωτικής δράσης πρέπει να τεθεί σε ισχύ το συντομότερο δυνατόν.
Μέτριο	Εάν μια κατάσταση εκτιμάται ως μέσος κίνδυνος, απαιτούνται διορθωτικές ενέργειες και πρέπει να αναπτυχθεί ένα σχέδιο για να ενσωματώσει αυτές τις ενέργειες εντός μιας λογικής χρονικής περιόδου.
Χαμηλό	Εάν μια κατάσταση περιγράφεται ως χαμηλός κίνδυνος, η διοίκηση του οργανισμού πρέπει να καθορίσει αν θα γίνουν διορθωτικές ενέργειες ή αποφασίζει να δεχτεί τον κίνδυνο.

Πίνακας 3.9: Περιγραφή επιπέδων κινδύνου.

Τα αποτελέσματα από αυτή την ποιοτική διαδικασία αξιολόγησης επιπέδου έκθεσης στους κινδύνους είναι τα εξής:

Συνολικό επίπεδο έκθεσης σε κινδύνους του έργου

Το επίπεδο κινδύνου μπορεί να παρουσιάσει τη συνολική έκθεση σε κίνδυνο του έργου σχετικά με άλλα πληροφοριακά έργα, συγκρίνοντας το αριθμητικό αποτέλεσμα του συνυπολογισμού πιθανότητας – επιπτώσεων. Μπορεί να χρησιμοποιηθεί για την ορθή κατανομή προσωπικού και πόρων σε τμήματα του έργου με διαφορετική διαβάθμιση κινδύνου ή και μεταξύ διαφορετικών έργων που έχει αναλάβει η ίδια εταιρεία για τη λήψη αποφάσεων σχετικών με ανάλυση οφέλους - κόστους για το έργο και για την υποστήριξη προτάσεων για εκκίνηση, συνέχιση ή ματαίωση της υλοποίησης του έργου λογισμικού.

Λίστα κινδύνων βάση προτεραιότητας

Οι κίνδυνοι μπορούν να καταταχθούν με τη χρήση ενός πλήθους κριτηρίων. Αυτά μπορεί να είναι το επίπεδο κινδύνου (υψηλό, μέτριο και χαμηλό) ή ο βαθμός στον οποίο μπορεί να προκληθεί απώλεια εργασίας. Οι κίνδυνοι μπορούν ακόμα να κατηγοριοποιηθούν σε αυτούς που απαιτούν άμεση επέμβαση και σε αυτούς των οποίων ο χειρισμός μπορεί να γίνει και στο μέλλον χωρίς επιπρόσθετες επιπτώσεις. Κίνδυνοι που αφορούν το κόστος, τις χρονοτριβές, τη λειτουργικότητα και την ποιότητα μπορούν να εξεταστούν ξεχωριστά, χρησιμοποιώντας διαφορετική αξιολόγηση του επιπέδου τους. Σοβαροί κίνδυνοι πρέπει να έχουν επιπλέον περιγραφή για τη βάση της εκτιμώμενης πιθανότητας και των επιπτώσεών τους.

Λίστα κινδύνων που απαιτούν επιπλέον ανάλυση και διαχείριση

Κίνδυνοι που έχουν χαρακτηριστεί ως υψηλοί ή μέτριοι είναι σοβαροί υποψήφιοι για περισσότερη ανάλυση, συμπεριλαμβανομένης ποσοτικής ανάλυσης κινδύνου και διενέργειας διαχείρισης κινδύνων.

Τάση αποτελεσμάτων ποιοτικής ανάλυσης κινδύνων

Καθώς η ανάλυση επαναλαμβάνεται, μπορεί να γίνει φανερή κάποια τάση των αποτελεσμάτων της που θα κάνει την αντίδραση έναντι του κινδύνου ή την επιπλέον ανάλυσή του περισσότερο ή λιγότερο επιτακτική και σημαντική.

Τεκμηρίωση παραγόντων κινδύνου – Σύνταξη αναφοράς

Το τελευταίο βήμα της διαδικασίας εκτίμησης κινδύνων είναι η σύνταξη της τελικής αναφοράς των αποτελεσμάτων της. Η συγγραφή αυτής της αναφοράς θα πρέπει να γίνει με ιδιαίτερη προσοχή, καθώς θα αποτελέσει βασικό εργαλείο για το επόμενο στάδιο, της αποτίμησης κινδύνου, που έχει να κάνει με το σχεδιασμό αντιμετώπισης των απειλών στις οποίες εκτίθεται το πληροφορικό έργο. Στην αναφορά αυτή θα περιλαμβάνονται, φυσικά, όλοι οι πιθανοί κίνδυνοι που απειλούν το έργο, η πιθανότητα εμφάνισης του καθενός, η έκταση των επιπτώσεων από την εκδήλωση καθενός από αυτούς τους κινδύνους καθώς και τα αποτελέσματα της εκτίμησης (είτε αυτή είναι ποιοτική είτε είναι ποσοτική) των εν λόγω κινδύνων.

Πέραν αυτών, όμως, η αναφορά για να είναι πλήρης θα πρέπει να εμπεριέχει:

- τις πηγές από τις οποίες αντλήθηκαν όλες οι πληροφορίες
- τις μεθόδους που χρησιμοποιήθηκαν για την έκδοση των αποτελεσμάτων
- τα πρόσωπα που συμμετείχαν σε κάθε στάδιο της διαδικασίας
- πλήρη τεκμηρίωση των συμπερασμάτων, των μεθόδων και των πηγών που χρησιμοποιήθηκαν (και αναγνώριση της αξιοπιστίας τους)
- σχόλια και παρατηρήσεις ειδικών που εκφράστηκαν σε οποιαδήποτε φάση της διαδικασίας

Ολοκληρώνοντας, θα πρέπει να τονιστεί ότι όλα τα παραπάνω βήματα της διαδικασίας εκτίμησης κινδύνου δεν πραγματοποιούνται εφάπαξ, αλλά επαναλαμβάνονται σε όλη τη διάρκεια υλοποίησης του έργου. Αυτό έχει ως στόχο όχι μόνο να συνυπολογίζονται οι αλλαγές των συνθηκών και να εκτιμώνται και πάλι οι ήδη αναγνωρισμένοι κίνδυνοι, αλλά και να προστίθενται και νέοι στη λίστα των κινδύνων αν αυτό κριθεί αναγκαίο.

Ποσοτικός προσδιορισμός του κινδύνου

Οι ποσοτικές τεχνικές, όπως ξεκαθαρίστηκε προηγουμένως, είναι πολύ δύσκολο να εφαρμοστούν στην πράξη, για αυτό και σπάνια χρησιμοποιούνται. Για τον υπολογισμό με αριθμητικό τρόπο των πιθανοτήτων εμφάνισης των παραγόντων κινδύνου και των επιπτώσεών τους, εφόσον εμφανιστούν, στους στόχους του έργου, καθώς και για την αριθμητική ανάλυση της συνολικής έκθεσης του έργου σε κίνδυνο είναι απαραίτητη η ύπαρξη ενός πολύ πλούσιου και καλά ενημερωμένου ιστορικού από την διαχείριση αντίστοιχων έργων για ένα εύγλωττο βάθος χρόνου.

Επιπλέον, για να είναι εφικτό οι αριθμητικές τιμές που θα προσδιοριστούν για τις πιθανότητες και τις επιπτώσεις των παραγόντων κινδύνου να μπορούν να χρησιμοποιηθούν για πράξεις μεταξύ τους, προκειμένου να υπολογιστεί αριθμητικά η σοβαρότητα κάθε παράγοντα και η συνολική έκθεση σε κίνδυνο, θα πρέπει να ισχύουν οι ακόλουθες προϋποθέσεις:

- Τα κόστη να είναι αθροιστικά, δηλαδή το συνολικό κόστος να μπορεί να υπολογιστεί ως το αριθμητικό άθροισμα των επιμέρους.
- Ο χρόνος να είναι, επίσης, άθροισμα των επιμέρους χρόνων (αυτό συμβαίνει στις διαδοχικές δραστηριότητες).
- Οι παράγοντες κινδύνου να μπορούν να συμβαίνουν ανεξάρτητα.

Η διαδικασία ποσοτικού προσδιορισμού του κινδύνου χρησιμοποιεί τεχνικές, όπως η προσομοίωση Monte Carlo και η ανάλυση αποφάσεων, για να:

- υπολογίσει την πιθανότητα επίτευξης ενός συγκεκριμένου στόχου του έργου
- ποσοτικοποιήσει την έκθεση του έργου σε κίνδυνο
- να υπολογίσει τον επιπλέον χρόνο και το επιπλέον κόστος που ενδεχομένως να απαιτούνται για την αντιμετώπιση των πιθανών κινδύνων
- αναγνωρίσει και κατατάξει τους κινδύνους που απαιτούν τη μεγαλύτερη προσοχή, ποσοτικοποιώντας τη συμβολή τους στη συνολική έκθεση του έργου σε κίνδυνο
- σχεδιάσει ρεαλιστικούς και πραγματοποιήσιμους στόχους για το κόστος, το χρόνο, τις δυνατότητες και την ποιότητα του έργου

Η ποσοτική αξιολόγηση κινδύνου συνήθως έπεται χρονικά της ποιοτικής. Απαιτεί πρώτα από όλα τον πλήρη καθορισμό του κινδύνου. Η ποιοτική και η ποσοτική αξιολόγηση κινδύνων μπορούν να χρησιμοποιούνται διακριτά ή και μαζί. Η συνεκτίμηση του χρόνου και των κονδυλίων που είναι διαθέσιμα και η ανάγκη για σύνταξη ποιοτικών ή ποσοτικών αναφορών για τον κίνδυνο και τις επιπτώσεις του θα

καθορίσουν ποια μέθοδος θα χρησιμοποιηθεί. Η τάση των αποτελεσμάτων της ποσοτικής διαδικασίας καθώς αυτή επαναλαμβάνεται θα υποδείξει την ανάγκη για περισσότερη ή λιγότερη διενέργεια διαχείρισης κινδύνου. Η ποσοτική ανάλυση ακολουθεί, γενικά, τις ίδιες διαδικασίες με την ποιοτική ανάλυση που περιγράφηκε προηγουμένως.

Στη συνέχεια παρατίθενται πληροφορίες και στοιχεία που χρειάζονται για την όσο το δυνατόν πιο πλήρη και ορθή ποσοτική αξιολόγηση των κινδύνων.

- *Σχεδιασμός εκτίμησης κινδύνων:* Περιγράφει με ποιο τρόπο σχεδιάζονται, εφαρμόζονται και ελέγχονται οι διαδικασίες αναγνώρισης κινδύνων καθώς και ποιοτικής και ποσοτικής τους ανάλυσης καθ' όλη τη διάρκεια υλοποίησης του έργου.
- *Κατάλογος αναγνωρισμένων κινδύνων*
- *Κατάλογος σημαντικότερων κινδύνων*
- *Κατάλογος κινδύνων που χρειάζονται επιπλέον ανάλυση*
- *Πληροφορίες πρότερης πείρας:* Πληροφορίες από παλαιότερα έργα, μελέτες για παρόμοια έργα από ειδικούς σε θέματα κινδύνων ή σε τεχνολογικά θέματα, βάσεις δεδομένων που μπορεί να είναι διαθέσιμες από άλλες βιομηχανικές ή ιδιωτικές πηγές κ.α.
- *Απόψεις ειδικών:* Αυτές μπορεί να προέρχονται από τα μέλη της ομάδας που έχει αναλάβει το σχεδιασμό του έργου, από άλλους ειδικούς στο αντικείμενο που ανήκουν στην εταιρεία αλλά και από πρόσωπα που δεν ανήκουν στο δυναμικό της. Πηγές αξιόλογων πληροφοριών μπορούν να αποτελέσουν μηχανικοί και στατιστικολόγοι.
- *Αποτελέσματα ποιοτικής αξιολόγησης κινδύνων (εάν αυτή έχει προηγηθεί)*
- *Αποτελέσματα άλλων εκθέσεων:* Εκθέσεις που θα μπορούσαν να φανούν ιδιαίτερα χρήσιμες είναι αυτές που αφορούν στον υπολογισμό της διάρκειας ολοκλήρωσης κάθε τμήματος του έργου με σκοπό την κατάρτιση του συνολικού χρονοδιαγράμματος υλοποίησης του έργου, το σχηματισμό καταλόγου με τα έξοδα του έργου και τον τρόπο υπολογισμού αυτών και τη δημιουργία μοντέλων των τεχνικών δυνατοτήτων του έργου.

Παρακάτω παρουσιάζονται τεχνικές και εργαλεία ποσοτικού προσδιορισμού του κινδύνου (Ding, 2002):

Συνεντεύξεις

Μια συνέντευξη των διοικούντων του οργανισμού και των ειδικών στους σχετικούς τομείς του έργου και στη διαχείριση κινδύνων μπορεί να αποτελέσει το πρώτο βήμα για

τον ποσοτικό υπολογισμό του κινδύνου. Οι πληροφορίες που θα συλλεχθούν εξαρτώνται από τον τρόπο με τον οποίο θέλουμε να περιγράψουμε τις διάφορες καταστάσεις. Για παράδειγμα, μπορούμε να αναζητήσουμε πληροφορίες για τη μέγιστη, την ελάχιστη και την ποιο πιθανή τιμή μιας κατάστασης, όπως το μέγιστο, το ελάχιστο και το πιο πιθανό κόστος κατασκευής ή τα ίδια για το χρόνο, το επίπεδο ποιότητας και την εκπλήρωση των σκοπών κατασκευής του έργου. Ακόμα, μπορούμε να αναζητήσουμε τις πληροφορίες μας ανάλογα με το αν μία κατάσταση προκαλεί μεγάλες ή μικρότερης έκτασης αποκλίσεις από το αρχικό πλάνο. Στον πίνακα 3.10 φαίνεται ένα τυχαίο παράδειγμα υπολογισμού του κόστους κάθε σταδίου υλοποίησης ενός έργου, συλλέγοντας πληροφορίες τριών σημείων.

Υπολογισμός κόστους και εύρους κόστους			
Στάδιο Υλοποίησης	Ελάχιστο	Πιθανότερη Τιμή	Μέγιστο
Σχεδιασμός	4	6	10
Κατασκευή	16	20	35
Έλεγχος Λειτουργίας	11	15	23
Σύνολο Έργου		41	

Πίνακας 3.10: Παράδειγμα υπολογισμού κόστους και εύρους κόστους ενός έργου.

Η αναπαράσταση τις πιθανότητας εμφάνισης καταστάσεων γραφικά, μπορεί να πραγματοποιηθεί σε διάφορες μορφές με πιο συνηθισμένες την ομοιόμορφη, την τριγωνική, τη normal, τη log-normal και τη beta.

Η αναγνώριση της λογικής της διακύμανσης κινδύνου είναι ένα σημαντικό εργαλείο που προκύπτει από τις συνεντεύξεις, καθώς βοηθά στο σχεδιασμό αποτελεσματικών στρατηγικών για την αντίδραση έναντι των πιθανών κινδύνων.

Υπολογισμοί αναμενόμενης αξίας (Expected value calculations)

Εάν η πιθανότητα να συμβεί ένα γεγονός είναι p_1, p_2, …, p_n και μία αντίστοιχη επίπτωση κόστους εκφράζεται ως c_1, c_2, …, c_n, τότε η συνολική αναμενόμενη αξία του κινδύνου είναι το άθροισμα των επιμέρους γινομένων. Δηλαδή, ο συνολικός αναμενόμενος κίνδυνος ισούται με $p_1 \cdot c_1 + p_2 \cdot c_2 + \cdots + p_n \cdot c_n$.

Δέντρα αποφάσεων-πιθανοτήτων (Decision-probability trees)

Τα δέντρα αποφάσεων-πιθανοτήτων είναι γραφικές αναπαραστάσεις (διαγράμματα) του συνόλου των πιθανών στρατηγικών και είναι περισσότερο χρήσιμα σε έργα που απαιτούν διαδοχικές αποφάσεις. Οι διαφορετικές στρατηγικές οδηγούν σε

διαφορετικά αποτελέσματα, ανάλογα με τις συνθήκες και τα γεγονότα που λαμβάνουν χώρα. Περιγράφουν, δηλαδή, τη διαδικασία λήψης μιας απόφασης λαμβάνοντας υπόψη τις εναλλακτικές επιλογές που είναι διαθέσιμες. Συνυπολογίζουν τις πιθανότητες εμφάνισης των κινδύνων και τα κόστη ή τα κέρδη από κάθε λογική διαδρομή γεγονότων ή μελλοντικών αποφάσεων. Η χρήση ενός δέντρου αποφάσεων-πιθανοτήτων μας παρέχει την απόφαση με το μεγαλύτερο αναμενόμενο κέρδος όταν όλοι οι αβέβαιοι παράγοντες (κόστος, κέρδος και εναλλακτικές αποφάσεις) έχουν ποσοτικοποιηθεί.

Συνδυασμός κατανομών (Combination of distributions)

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.

Ανάλυση ευαισθησίας

- Πρόκειται για τον υπολογισμό του τρόπου με τον οποίο διαφορετικά σενάρια, όσον αφορά τις τιμές των πιθανοτήτων, των επιπτώσεων ή των βαρών και της σοβαρότητας των παραγόντων κινδύνου, θα είχαν επιπτώσεις στις καθαρές παρούσες αξίες (NPVs), στις συνολικές δαπάνες ή σε άλλες παραμέτρους του έργου. Η ανάλυση ευαισθησίας, δηλαδή, βοηθά στο να καθοριστεί ποιοι κίνδυνοι έχουν τις ποιο σοβαρές αρνητικές επιπτώσεις στη λειτουργία του έργου και εξετάζει την έκταση των επιπτώσεων στη λειτουργία του πληροφοριακού συστήματος από την εμφάνιση μιας απειλής, όταν οι υπόλοιποι κίνδυνοι δεν εκδηλώνονται. Συγκεκριμένα, για κάθε αριθμητική τιμή επιλέγεται ο υπολογισμός όλων των παραμέτρων με βάση τη διακύμανση αυτής της τιμής, είτε προς τα πάνω είτε προς τα κάτω. Με αυτόν τον τρόπο δίνεται η δυνατότητα να εξακριβωθεί ποιες ακριβώς μεταβλητές επιβάλλεται να προσδιοριστούν με μεγάλη ακρίβεια και ποιες όχι. Ως αποτέλεσμα, προσδιορίζεται και η εμπιστοσύνη στους αρχικούς υπολογισμούς, δεδομένου ότι αν όλες οι μεταβλητές (η μικρή μεταβολή των οποίων επηρεάζει σημαντικά όλες τις παραμέτρους του έργου) έχουν προσδιορισθεί με μεγάλη ακρίβεια, τότε αντίστοιχα μεγάλη θα είναι και η εμπιστοσύνη που θα πρέπει να δίνεται στα αποτελέσματα των υπολογισμών, ανεξάρτητα από την ακρίβεια με την οποία έχουν προσδιορισθεί οι υπόλοιπες μεταβλητές. Αντίστροφα, αν κάποια από αυτές τις σημαντικές μεταβλητές έχει προσδιοριστεί με μικρή ακρίβεια, τότε δεν είναι δυνατόν να υπάρξει εμπιστοσύνη στους αρχικούς υπολογισμούς, παρά μόνο σχετική εφόσον συνεκτιμηθούν όλα τα εναλλακτικά σενάρια.

- Είναι χρήσιμη μέθοδος στην περίπτωση διαφορετικών αξιολογητών, προκειμένου να αποκτήσουν πλήρη εικόνα για το πώς οι διαφορετικές απόψεις τους για τις πιθανές δαπάνες και τα κέρδη θα έχουν επιπτώσεις στο αποτέλεσμα.

- Οι αναλύσεις ευαισθησίας απαιτούν καλή σχεδίαση και σαφή παρουσίαση. Τα εναλλακτικά σενάρια πρέπει να επιλέγονται προσεκτικά, έτσι ώστε να εστιάζουν ειδικά σε εκείνες τις αβεβαιότητες που είναι οι πιο σημαντικές και εκεί όπου οι αβεβαιότητες είναι πολύ μεγαλύτερες σε μια κατεύθυνση από μια άλλη. Όλοι οι σημαντικοί παράγοντες κινδύνου πρέπει να εξετάζονται και να δίνεται προσοχή σε οποιεσδήποτε σημαντικές σχέσεις υπάρχουν μεταξύ των διαφόρων αιτιών που προκαλούν τους παράγοντες.

- Οι αναλύσεις ευαισθησίας πρέπει να ενημερώνονται, όπου αυτό είναι δυνατόν, με την χρήση προηγούμενων στοιχείων (π.χ. αρχεία παρελθόντος για τις υπερβάσεις δαπανών και χρόνου στα έργα κατασκευής και αρχεία για την ακρίβεια προηγούμενων προβλέψεων) για να αξιολογείται καλύτερα η αξιοπιστία των εκτιμήσεων.

- Επίσης, ενδέχεται να φανεί χρήσιμο να συγκεντρωθούν οι μεταβλητές στην ανάλυση ευαισθησίας με τη σύσταση “απαισιόδοξων” και “αισιόδοξων” παραλλαγών, οι οποίες επιτρέπουν μια ευρεία αξιολόγηση της πιθανότητας αυτών των εκβάσεων για την απόφαση εάν ένα έργο πρέπει να προχωρήσει.

- Η ανάλυση ευαισθησίας, είναι ιδιαίτερα χρήσιμη όταν ένας μόνο παράγοντας (κρίσιμος παράγοντας) καθορίζει την απόφαση αποδοχής ενός έργου ή μιας επιλογής. Σε αυτή την περίπτωση, σκοπός της ανάλυσης ευαισθησίας είναι να φανερώσει τη μέγιστη μεταβολή της αξίας αυτού του παράγοντα, η οποία καθιστά μη αξιόλογη την ανάληψη του έργου. Η μεταβολή της αξίας αναφέρεται σε μείωση στην περίπτωση οφέλους και σε αύξηση στην περίπτωση κόστους.

Προσομοίωση

Η προσομοίωση ενός έργου χρησιμοποιεί ένα μοντέλο, το οποίο μεταφράζει τις αβεβαιότητες ενός συγκεκριμένου επιπέδου στις επιπτώσεις που αυτές έχουν στην ικανοποίηση των στόχων όλου του έργου. Οι προσομοιώσεις έργων συνήθως υλοποιούνται με την τεχνική Monte Carlo, η οποία χρησιμοποιεί τυχαίους αριθμούς και στατιστικές πιθανότητες για να δημιουργήσει τα σενάρια ενός προβλήματος, με σκοπό να εξάγει ένα αποτέλεσμα. Η μέση λύση των σεναρίων θα δώσει μια κατά προσέγγιση απάντηση στο πρόβλημα, η ακρίβεια της οποίας μπορεί να βελτιωθεί με την προσομοίωση περισσότερων σεναρίων.

Τα αποτελέσματα από την ποσοτική αξιολόγηση των κινδύνων είναι τα εξής:

- *Λίστα κινδύνων με προτεραιότητα, που πηγάζει από την ποσοτική ανάλυση:* Η λίστα αυτή περιλαμβάνει τους κινδύνους που αποτελούν τη μεγαλύτερη απειλή για το πληροφοριακό έργο, μαζί με το υπολογιζόμενο μέγεθος του αντίκτυπου αυτών των κινδύνων.

- *Πιθανοτική ανάλυση του έργου.* Η ανάλυση αυτή μας παρέχει προβλέψεις για την υπολογιζόμενη διάρκεια του έργου και το υπολογιζόμενο κόστος του, μαζί με το επίπεδο εγκυρότητας αυτών των τιμών.
- *Την πιθανότητα επίτευξης των στόχων για το κόστος και το χρόνο ολοκλήρωσης του έργου.*
- *Τάσεις των αποτελεσμάτων της ποσοτικής αξιολόγησης κινδύνων:* Καθώς επαναλαμβάνεται η διαδικασία, μπορεί να εμφανιστεί μία συγκεκριμένη τάση των αποτελεσμάτων.

Εκτίμηση Κινδύνου με τη Μέθοδο Βάρους – Σοβαρότητας

▪ **Ποιο είναι το βάρος κάθε παράγοντα κινδύνου;** ▪ **Πόσο σοβαρός είναι;**	
Επιλογή βάρους κάθε παράγοντα κινδύνου	• Επιλογή του βάρους κάθε παράγοντα κινδύνου (ποσοτικά).
Εκτίμηση της σοβαρότητας παράγοντα κινδύνου	• Εκτίμηση της σοβαρότητάς κάθε παράγοντα κινδύνου (ποσοτικά).
Εκτίμηση της έκθεσης σε κίνδυνο	• Εκτίμηση της συνολικής έκθεσης σε κίνδυνο (ποσοτικά). • Ταξινόμηση των έργων ανάλογα με το βαθμό έκθεσης σε κίνδυνο.
Τεκμηρίωση παραγόντων κινδύνου – Σύνταξη αναφοράς	• Καταγραφή πορίσματος σχετικά με τα βάρη των παραγόντων κινδύνου, τη σοβαρότητά τους και την έκθεση σε κίνδυνο.

Πίνακας 3.11: Φάσεις εκτίμησης κινδύνου με τη μέθοδο βάρους - σοβαρότητας (Στάδιο 2).

Ποσοτικός προσδιορισμός του κινδύνου

Επιλογή βάρους κάθε παράγοντα κινδύνου

Σύμφωνα με τη μέθοδο πιθανότητας-επίπτωσης που περιγράψαμε παραπάνω, τις περισσότερες φορές η πιθανότητα (probability) εμφάνισης ενός παράγοντα κινδύνου υπολογίζεται και εκφράζεται ποιοτικά σύμφωνα με την εμπειρία ή τη διαίσθηση. Όπως, επίσης, αναφέρθηκε προηγουμένως, και οι επιπτώσεις (impacts) συχνά προκύπτουν από υποκειμενική ποιοτική εκτίμηση βασισμένη στη γνώση τόσο της κατηγορίας κινδύνου όσο και των λεπτομερειών του ίδιου του έργου.

Οι παραπάνω λόγοι, σε συνδυασμό με το μεγάλο πλήθος παραγόντων κινδύνου που συναντάμε σε ένα έργο, και πολύ περισσότερο σε ένα ολόκληρο επιχειρησιακό πρόγραμμα, οδήγησαν στην ανάγκη χρήσης μιας πιο πρακτικής και εύχρηστης ποσοτικής μεθόδου για την εκτίμηση του κινδύνου. Έτσι, φτάσαμε στην εκτίμηση κινδύνου με τη μέθοδο βάρους-σοβαρότητας.

Υπάρχουν διάφορες μέθοδοι επιλογής βαρών για τους παράγοντες κινδύνου ενός έργου. Σκοπός είναι να επιλέγεται κάθε φορά, ανάλογα με τις συνθήκες και την εφικτότητα, η σχετικά απλούστερη μέθοδος, ώστε αυτή να γίνεται κατανοητή από τους εμπλεκόμενους στη διαδικασία της απόφασης. Από την άλλη, όμως, απαιτείται η ύπαρξη κατάλληλου μεθοδολογικού υπόβαθρου, το οποίο θα αξιοποιεί ψυχολογικούς κανόνες και παρατηρήσεις, ώστε να προσδιορίζει τις προτιμήσεις των αποφασιζόντων-κριτών. Οι κυριότερες μέθοδοι εκλογής βαρών είναι οι εξής:

Μέθοδος απευθείας εκλογή των βαρών

Οι αποφασίζοντες-κριτές επιλέγουν τα βάρη των κριτηρίων σε μια κλίμακα από το 1 (το λιγότερο σημαντικό) έως το 7 (το περισσότερο σημαντικό). Στη συνέχεια, βαθμολογούν τα ίδια κριτήρια ξεκινώντας από το 1 για το λιγότερο σημαντικό. Κάθε κριτήριο αξιολογείται σε σχέση με το λιγότερο σημαντικό και βαθμολογείται ανάλογα με το πόσες φορές οι αποφασίζοντες-κριτές το θεωρούν πιο σημαντικό.

Παρατηρήθηκε ότι στη συγκεκριμένη μέθοδο παρουσιάζονται μικρές διαφορές στις δυο βαθμολογήσεις. Για το λόγο αυτό στην επόμενη φάση γίνεται σύνθεση των διαφορετικών βαθμολογιών. Σε περίπτωση που η κατανομή των βαρών παρουσιάζει μεγάλη διασπορά, τότε η επιλογή της μέσης τιμής δεν είναι αντιπροσωπευτική κι επιλέγεται η τιμή του βάρους που έχουν επιλέξει οι περισσότεροι αποφασίζοντες-κριτές.

Μέθοδος του Mousseau

Εκτός από μαθηματικά στοιχεία, χρησιμοποιεί και ψυχολογικά στοιχεία για τον προσδιορισμό των βαρών των κριτηρίων. Γίνονται ανά ζεύγη συγκρίσεις ενός συνόλου φανταστικών επιλογών, οι οποίες διαφέρουν το μέγιστο κατά τρία κριτήρια και από αυτές παράγονται γραμμικές ανισότητες. Από τις ανισότητες αυτές ουσιαστικά προκύπτουν οι οριακές τιμές των βαρών. Ο προσδιορισμός των βαρών με τη μέθοδο αυτή θεωρείται πολύ ειδικός γιατί απαιτεί πολύπλοκο λογισμικό.

Μέθοδος των καρτών

Είναι γνωστή και ως τεχνική του Simos. Σύμφωνα με τη μέθοδο αυτή, σε κάθε κριτήριο αντιστοιχεί μια κάρτα και όλες οι κάρτες τοποθετούνται από κάθε αποφασίζοντα-κριτή σε αύξουσα σειρά σημαντικότητας. Κάθε αποφασίζων-κριτής έχει τη δυνατότητα να παρεμβάλει λευκές κάρτες, ώστε να αυξήσει τη διαφορά σημαντικότητας και να ομαδοποιήσει κριτήρια που θεωρεί το ίδιο σημαντικά. Με τον απλό αυτό τρόπο, η κατάταξη που προκύπτει προσδιορίζει τα βάρη τους.

Οι τρεις παραπάνω μέθοδοι, παρά την ευρεία χρήση τους, παρουσιάζουν κάποια μειονεκτήματα. Η απευθείας εκλογή και η μέθοδος των καρτών, οι οποίες ουσιαστικά καθορίζουν την αξιολογική σειρά των κριτηρίων, δεν προσεγγίζουν τον πραγματικό βαθμό σημαντικότητάς τους και δεν έχουν ιδιαίτερο μεθοδολογικό υπόβαθρο σε σχέση με τη μέθοδο του Mousseau, η οποία, όμως, περιορίζεται από τις φανταστικές επιλογές που χρησιμοποιεί. Ειδικά στην περίπτωση που οι δύο εναλλακτικές διαφέρουν μεταξύ τους κατά περισσότερο από τέσσερα κριτήρια, η μέθοδος γίνεται εξαιρετικά πολύπλοκη και η αξιοπιστία της ελαττώνεται.

Μέθοδος αναλυτικής ιεράρχησης (Analytic hierarchy process - AHP)

Πρόκειται για μια μέθοδο αναγωγής σε ένα κριτήριο που βασίζεται στις συγκρίσεις ανά ζεύγη (paired comparisons) και χρησιμοποιεί με έμμεσο τρόπο τη συνάρτηση χρησιμότητας, δίνοντάς τη δυνατότητα στους αποφασίζοντες-κριτές να επιλέγουν βάρη και ποσοστά.

Η ιδέα πίσω από τη μέθοδο των συγκρίσεων ανά ζεύγη είναι να υπολογίσει το μέγεθος n οντοτήτων, ζητώντας από έναν ή περισσότερους ειδικούς να βαθμολογήσουν τα σχετικά μεγέθη τους, παρά να μας εξασφαλίσει απόλυτες τιμές. Οι οντότητες μπορεί να είναι απαιτήσεις, χαρακτηριστικά, αντικείμενα ή όποιο άλλο μέγεθος θα μπορούσε αργότερα να χρησιμοποιηθεί για σκοπούς σχεδιασμού. Ζητώντας πολλαπλές και σαφείς αποφάσεις για τα σχετικά μεγέθη ανά δύο οντότητες και χρησιμοποιώντας εύκολα διαθέσιμα ιστορικά δεδομένα – αντί για απλές συγκρίσεις βασισμένες σε αόριστες αντιλήψεις για τα μεγέθη, επηρεασμένες από την κρίση του αποφασίζοντα –, η συγκεκριμένη μέθοδος βελτιώνει την ακρίβεια και την ορθότητα των υπολογισμών. Αυτές οι διαπιστώσεις είναι σύμφωνες και με μελέτες που δείχνουν ότι η χρήση ιστορικών δεδομένων και τεκμηριωμένων συγκρίσεων παράγει καλύτερους υπολογισμούς από αυτούς που βασίζονται στη διαίσθηση και τις εικασίες.

Τρεις βασικές αρχές τη χαρακτηρίζουν:

1. Η ***αρχή της ανάλυσης***, όπου το πρόβλημα της απόφασης αναλύεται με ιεραρχικό τρόπο, ώστε τα υψηλότερα ιεραρχικά στοιχεία να αποτελούν τους ευρύτερους στόχους και τα χαμηλότερα να αποτελούν τα κριτήρια. Σε αυτά, σε χαμηλότερο επίπεδο, συνδέονται οι εναλλακτικές λύσεις. Τα στοιχεία του ίδιου επιπέδου πρέπει να είναι συγκρίσιμα μεταξύ τους.
2. Η ***αρχή των συγκρίσεων***, όπου τα στοιχεία ενός επιπέδου συγκρίνονται ανά ζεύγη με βάση το στοιχείο του ανωτέρου επιπέδου, με τελικό αποτέλεσμα τοπικές προτεραιότητες.
3. Η ***αρχή των προτεραιοτήτων*****,** όπου οι τοπικές προτεραιότητες συντίθενται σε ολικές για κάθε εναλλακτική λύση που βρίσκεται στη βάση της ιεραρχίας.

Για την επιτυχή εφαρμογή της μεθόδου αναλυτικής ιεράρχησης απαιτούνται ειδήμονες αποφασίζοντες-κριτές και ένα εργαλείο ικανό για την αυτοματοποίηση των υπολογισμών. Όταν ο αριθμός των κριτηρίων που πρέπει να αξιολογηθούν είναι μεγάλος, μπορεί να μοιραστεί η εργασία ανάμεσα σε πολλαπλούς αποφασίζοντες-

κριτές. Μπορεί επίσης να ακολουθηθεί αυτή η προσέγγιση ώστε να μειωθεί η προκατάληψη που εισάγεται από έναν μόνο αποφασίζοντα-κριτή.

Ο αριθμός των αποφασιζόντων-κριτών που χρειάζονται για να αξιολογήσουν n κριτήρια δεν πρέπει να ξεπερνά τους n/3, αλλιώς το πλεονέκτημα της μεθόδου όσον αφορά την ακρίβεια και την ορθότητα των υπολογισμών θα χαθεί, γιατί κάθε αποφασίζοντας-κριτής δεν θα έχει την ευκαιρία να κάνει πολλαπλές συγκρίσεις για ένα δεδομένο κριτήριο. Ένας απλός τρόπος να διανεμηθούν οι συγκρίσεις στους κριτές-αποφασίζοντες είναι να αναθέτουμε κάθε επόμενη σύγκριση σε έναν διαφορετικό κριτή-αποφασίζοντα με συνεχή τρόπο.

Εκτίμηση της σοβαρότητας παράγοντα κινδύνου

Χρησιμοποιώντας μια λεκτική κλίμακα σύγκρισης, απλοποιείται και επιταχύνεται η διαδικασία υπολογισμού, χωρίς να διακινδυνεύεται η ακρίβεια των αποτελεσμάτων. Αν και δεν αποτελεί ουσιαστικό κομμάτι της μεθοδολογίας, έχοντας μια γενική αντίληψη του πόσο μικρό είναι το ‘μικρότερο’ και πόσο μεγάλο είναι το ‘μεγαλύτερο’ βοηθά τους συμμετέχοντες να φτάσουν ομόφωνα στη διαδικασία βαθμολόγησης. Μια προκαθορισμένη κλίμακα τιμών εμποδίζει να χάνεται χρόνος, συζητώντας τιμές μέχρι το δεύτερο δεκαδικό όταν το σφάλμα των κρίσεών μας είναι πολλές τάξεις μεγέθους μεγαλύτερο από αυτό.

Ο Saaty, λοιπόν, προτείνει τη χρησιμοποίηση μιας εννιαβάθμιας λεκτικής κλίμακας από το 1 έως το 9 και τα αντίστροφά τους για τη διαδικασία βαθμολόγησης. Ο πίνακας 3.12 καταγράφει την ισοδυναμία μεταξύ των λεκτικών εκφράσεων και των σχετικών μεγεθών:

Προσδιορισμός	**Σχετική τιμή**	**Αντίστροφες τιμές**
Ίσης σημασίας	1	1.00
Ασθενώς μεγαλύτερης / μικρότερης σημασίας	3	0.33
Μεγαλύτερης / μικρότερης σημασίας	5	0.20
Πολύ μεγαλύτερης / μικρότερης σημασίας	7	0.14
Απόλυτα μεγαλύτερης / μικρότερης σημασίας	9	0.11

Πίνακας 3.12: Λεκτική κλίμακα σύγκρισης Saaty.

Οι τιμές 2, 4, 6, 8 και 0.5, 0.25, 0.16, 0.12 αντίστοιχα θεωρούνται ενδιάμεσες και χρησιμοποιούνται όταν απαιτείται συμβιβασμός μεταξύ γειτονικών κλιμάκων.

Υποψιαζόμενοι πως οι τιμές που προτάθηκαν από τον Saaty θα μπορούσαν να είναι διαφορετικές για την υλοποίηση λογισμικού, διεξήχθη μια ανεπίσημη διεθνής έρευνα ανάμεσα σε τριάντα ανθρώπους από το χώρο της βιομηχανίας και ακαδημαϊκούς, οι οποίοι χορήγησαν δεδομένα εισαγωγής για την κλίμακα. Τα αποτελέσματα υποδηλώνουν πως η αντιστοιχία μεταξύ των μεγεθών και των λεκτικών περιγραφών για την υλοποίηση λογισμικού είναι πιο κοντά σε αυτή που παρουσιάζεται στον πίνακα 3.13, παρά σε αυτή του Saaty.

Προσδιορισμός	**Σχετική τιμή**	**Αντίστροφες τιμές**
Ίσης σημασίας	1.00	1.00
Ασθενώς μεγαλύτερης / μικρότερης σημασίας	1.25	0.80
Μεγαλύτερης / μικρότερης σημασίας	1.75	0.57
Πολύ μεγαλύτερης / μικρότερης σημασίας	4.00	0.25
Απόλυτα μεγαλύτερης / μικρότερης σημασίας	7.50	0.13

Πίνακας 3.13: Λεκτική κλίμακα σύγκρισης για την υλοποίηση λογισμικού.

Εκτίμηση της έκθεσης σε κίνδυνο

Η έκθεση σε κίνδυνο ορίζεται με βάση το συνδυασμό του βάρους κάθε παράγοντα κινδύνου και της σοβαρότητας που έχει για το έργο. Εάν τα βάρη και οι σοβαρότητες των παραγόντων κινδύνου έχουν ποσοτικοποιηθεί, η έκθεση σε κίνδυνο μπορεί να υπολογιστεί ως το άθροισμα των γινομένων των βαρών με τις αντίστοιχες σοβαρότητες των παραγόντων κινδύνου.

Τεκμηρίωση παραγόντων κινδύνου – Σύνταξη αναφοράς

Όπως και στην εκτίμηση κινδύνου με τη μέθοδο πιθανότητας-επίπτωσης, όμοια κι εδώ, στην αναφορά θα περιλαμβάνονται όλοι οι πιθανοί κίνδυνοι που απειλούν το έργο, το βάρος και η σοβαρότητα του καθενός καθώς και τα αποτελέσματα της έκθεσης σε κίνδυνο.

Ποιοτική έναντι Ποσοτικής Εκτίμησης Κινδύνου

Κατά τη διαδικασία εκτίμησης κινδύνων θα πρέπει να ληφθούν υπόψη τα πλεονεκτήματα και τα μειονεκτήματα της ποσοτικής έναντι της ποιοτικής ανάλυσης. Η ποσοτική ανάλυση προσπαθεί να προσδιορίσει αντικειμενικές αριθμητικές τιμές (πχ. χρηματικά ποσά) για κάθε συνιστώσα της ανάλυσης κινδύνων. Για παράδειγμα, προσπαθεί να υπολογίσει τη χρηματική αξία των απωλειών ή την πιθανότητα να συμβεί ένα περιστατικό. Στην περίπτωση που ποσοτικοποιηθούν όλες οι συνιστώσες (αξία περιουσιακών στοιχείων, συχνότητα απειλών, αποτελεσματικότητα αντιμέτρων, κόστος αντιμέτρων, αβεβαιότητα και πιθανότητα), τότε η ανάλυση ονομάζεται πλήρως ποσοτική.

Η ποσοτική ανάλυση κινδύνων παρουσιάζει τα εξής 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/οφέλους (cost/benefit) είναι πιο εύκολη και άμεση, παρέχοντας συγκεκριμένα υπολογίσιμα μεγέθη για την εκτίμηση του ύψους των επιπτώσεων.
- Η αξία των περιουσιακών στοιχείων του πληροφοριακού συστήματος (όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα) γίνεται καλύτερα κατανοητή όταν εκφράζεται σε χρηματικά ποσά. Αυτό βοηθάει στην μεγαλύτερη αποδοχή της ασφάλειας.

Αντίστοιχα, τα μειονεκτήματα της ποσοτικής ανάλυσης κινδύνου είναι τα ακόλουθα:

- Οι υπολογισμοί μπορεί να είναι πολύπλοκοι, τα αριθμητικά αποτελέσματα, δηλαδή, ενδεχομένως να μην οδηγούν σε ξεκάθαρα συμπεράσματα και για το λόγο αυτό να απαιτείται επιπλέον ποιοτική εξέταση των αποτελεσμάτων.
- Η ανάλυση χρειάζεται πολύ χρόνο για να ολοκληρωθεί.
- Χρειάζεται μεγάλη ποσότητα προκαταρτικής εργασίας.
- Η καθοδήγηση των συμμετεχόντων στην ανάλυση δε μπορεί να γίνει εύκολα, με αποτέλεσμα, συνήθως, να χρειάζεται η συμμετοχή έμπειρων στην ποσοτική ανάλυση ατόμων.
- Ιστορικά, η ποσοτική ανάλυση λειτουργεί καλά μόνο με τη χρήση κάποιου αυτοματοποιημένου εργαλείου συνδεδεμένου με μια γνωστική βάση (knowledge base).

Η ποιοτική ανάλυση, από την άλλη, δεν προσπαθεί να δώσει ακριβείς αριθμητικές τιμές στις συνιστώσες της ανάλυσης κινδύνου. Αντιθέτως, αρκείται να τις χαρακτηρίζει με εκφράσεις, όπως για παράδειγμα μεγάλο, μέτριο, μικρό ή να δίνει τιμές από μια προαποφασισμένη κλίμακα, παρακάμπτοντας έτσι πολύπλοκους υπολογισμούς. 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, οπότε πρόκειται, προφανώς, για μια υποκειμενική μέθοδο. Προσπαθεί να εκμεταλλευτεί τη 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 διαθέτουν την απαιτούμενη γνώση και εμπειρία για το πληροφοριακό σύστημα που εξετάζεται.

Η ποιοτική ανάλυση κινδύνων παρουσιάζει τα εξής πλεονεκτήματα:

- Αποφεύγονται πολύπλοκοι υπολογισμοί.
- Δεν είναι απαραίτητος ο αριθμητικός υπολογισμός της αξίας των περιουσιακών στοιχείων.
- Θέτει προτεραιότητες μεταξύ των κινδύνων και αναγνωρίζει τους τομείς του έργου που χρειάζονται άμεση βελτίωση, καταδεικνύοντας τις ευπαθείς περιοχές του.
- Είναι ευκολότερη η συμμετοχή ατόμων που δεν έχουν σχέση με την ασφάλεια και την πληροφορική.
- Χρειάζεται λιγότερο χρόνο και λιγότερους πόρους σε σχέση με την ποσοτική.
- Η διαδικασία της ανάλυσης είναι πιο ευέλικτη.

Αντίστοιχα, τα μειονεκτήματα της ποιοτικής ανάλυσης κινδύνου είναι τα ακόλουθα:

- 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.
- Η ποιότητα των αποτελεσμάτων βασίζεται εξολοκλήρου στη γνώση και την εμπειρία των ατόμων που συμμετέχουν στην ανάλυση.
- Δεν παρέχονται συγκεκριμένα υπολογίσιμα μεγέθη για την εκτίμηση του ύψους των επιπτώσεων, με αποτέλεσμα η ανάλυση κόστους-οφέλους (cost/benefit) για προτεινόμενες δράσεις να είναι πολύ δύσκολη, μιας και δε βασίζεται σε μαθηματική απόδειξη.

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 στη δημιουργία πιο ποιοτικών μεθόδων ανάλυσης οι οποίες τελικά έγιναν και οι πιο διαδεδομένες. Στην πραγματικότητα οι περισσότερες τεχνικές που χρησιμοποιούνται σήμερα είναι μια μίξη ποσοτικής και ποιοτικής ανάλυσης. Τον χαρακτηρισμό ποιοτική ή ποσοτική ανάλυση τον παίρνουν ανάλογα με το ποια ανάλυση προσεγγίζουν καλύτερα.

Συνοψίζοντας, μπορούμε να πούμε ότι η ποιοτική ανάλυση βασίζεται κυρίως στη λογική και την εμπειρία και τις δυνατότητες των προσώπων που την εκπονούν, ενώ η ποσοτική βασίζεται στα αριθμητικά αποτελέσματα και στην αξιοπιστία των μεθόδων και των μοντέλων προσομοίωσης που χρησιμοποιούνται. Όταν τίθεται θέμα κόστους χρησιμοποιείται μόνο η ποιοτική εκτίμηση για την εξαγωγή συμπερασμάτων, ενώ όταν το κόστος δεν αποτελεί ανασταλτικό παράγοντα συνήθως εκπονούνται και οι δύο εκτιμήσεις κινδύνου για την εξαγωγή ασφαλέστερων πορισμάτων.

Τέλος, αξίζει να σημειωθεί ότι για την πληρέστερη εκτίμηση των κινδύνων, είτε αυτή είναι ποιοτική είτε είναι ποσοτική, θα πρέπει να ληφθούν υπόψη και οι παράγοντες της επαναλαμβανόμενης εμφάνισης ενός κινδύνου σε μια συγκεκριμένη χρονική περίοδο (για παράδειγμα σε ένα χρόνο) σε συνδυασμό με το κόστος των επιπτώσεων που επιφέρει σε κάθε εμφάνισή του.

3.1.3 Αποτίμηση Κινδύνου

Η αποτίμηση κινδύνου είναι μία διαδικασία που έχει ως αντικείμενο την εκτίμηση του βαθμού της αποδοχής της έκθεσης του έργου σε κάθε παράγοντα κινδύνου, σε σχέση με τα κριτήρια κινδύνου που καθορίζονται για το έργο. Διερευνά, επίσης, σε πρώτο επίπεδο και τις αντιδράσεις/μέσα, με τις οποία μπορούν να μειωθούν τα απαράδεκτα επίπεδα έκθεσης σε κίνδυνο (πίνακας 3.14) (Ξανθόπουλος, 2004).

▪ **Είναι αποδεκτοί οι παράγοντες κινδύνου;** ▪ **Τι μπορεί να γίνει για να μειωθούν;**	
Αποδοχή	• Καθιέρωση κριτηρίων αποδοχής των παραγόντων κινδύνου. • Εκτίμηση του βαθμού αποδοχής της έκθεσης σε κάθε παράγοντα κινδύνου.
Προσδιορισμός εναλλακτικών	• *Μεταφορά*: Μεταφορά του παράγοντα κινδύνου σε τρίτους. • *Δράση*: Εξέταση των μέσων μείωσης της έκθεσης σε αποδεκτά επίπεδα. • *Αποφυγή*: Αν είναι εφικτό, επιλογή μιας εκ των εναλλακτικών λύσεων, η οποία εξασφαλίζει μηδενικά επίπεδα έκθεσης στον υπό εξέταση παράγοντα κινδύνου.
Τεκμηρίωση παραγόντων κινδύνου – Σύνταξη αναφοράς	• Καταγραφή για κάθε παράγοντα κινδύνου του βαθμού αποδοχής του και των προτεινόμενων εναλλακτικών αντιδράσεων για την αντιμετώπισή του.

Πίνακας 3.14: Φάσεις αποτίμησης κινδύνου (Στάδιο 3).

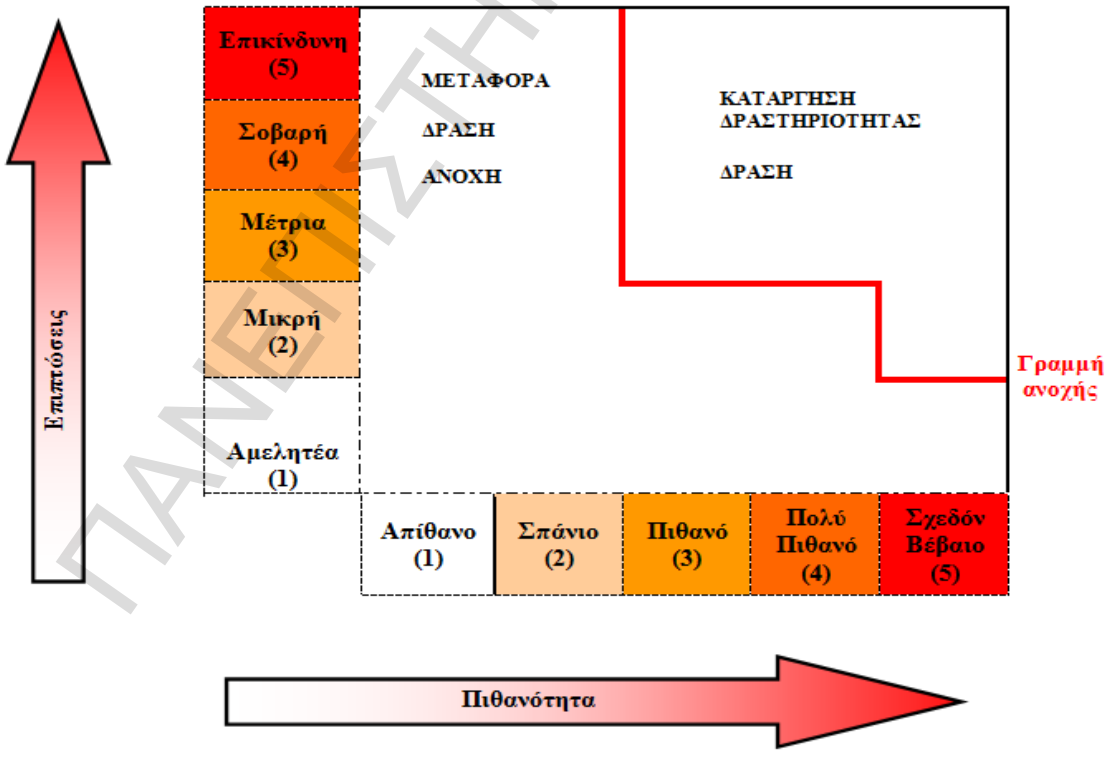
Αποδοχή

Η αποτίμηση κινδύνου είναι ένα ζωτικής σημασίας προαπαιτούμενο βήμα για τη ανάλυση κινδύνου. Χωρίς αυτή, δε μπορεί να πραγματοποιηθεί αποτελεσματική ανάλυση, δεδομένου ότι οι υπεύθυνοι δε θα έχουν γνώση και άποψη για τους σημαντικότερους παράγοντες κινδύνου που θα οδηγήσουν το έργο σε αστοχίες. Υπάρχει, επομένως, ο γενικότερος κίνδυνος αυτοί 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. Στην προκειμένη περίπτωση, η επιτυχής επίτευξη των στόχων του έργου γίνεται πολύ λιγότερο πιθανή.

Εάν η εκτίμηση κινδύνου έχει εκτελεσθεί σε ποσοτική βάση, μετά είναι σχετικά εύκολο να συγκριθούν τα αριθμητικά επίπεδα έκθεσης με τα αποδεκτά όρια που εκφράζονται στις ίδιες μονάδες. Για τις ποιοτικές αξιολογήσεις πρέπει να υιοθετηθούν περισσότερο προσεγγιστικές μέθοδοι, όπως είναι η γραμμή ανοχής η οποία φαίνεται στον πίνακα 3.15. 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 έργο, 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 έργου, 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 διακινδυνεύεται να προκύψουν από τις αντιδράσεις αυτές. Η ανοχή απέναντι σε έναν παράγοντα κινδύνου μπορεί να ποικίλει ανάλογα με τη σοβαρότητα του, το χρόνο αλλά και την περιοχή που ενδέχεται να προκύψει.

Ακολουθεί ένα παράδειγμα γραμμής ανοχής (κόκκινη γραμμή) στον πίνακα πιθανότητας-επιπτώσεων και οι πιθανές αντιδράσεις για την αντιμετώπιση παραγόντων κινδύνου που βρίσκονται σε αντίστοιχες περιοχές:



Πίνακας 3.15: Πίνακας πιθανότητας - επιπτώσεων (με τις πιθανές αντιδράσεις).

Προσδιορισμός εναλλακτικών

Τα εναλλακτικά σενάρια πρέπει να επιλέγονται προσεκτικά, έτσι ώστε να εστιάζουν ειδικά σε εκείνες τις αβεβαιότητες που είναι οι πιο σημαντικές και εκεί όπου οι αβεβαιότητες είναι πολύ μεγαλύτερες σε μια κατεύθυνση από μια άλλη. Πρέπει να περιλαμβάνουν τις ενέργειες αντιμετώπισης ενός σημαντικού παράγοντα κινδύνου, μετά την εκδήλωσή του. Οι ενέργειες αυτές είναι αναγκαίο να περιγράφονται όσο πιο αναλυτικά γίνεται, σε όρους κόστους, χρονοδιαγράμματος και πόρων.

Τεκμηρίωση παραγόντων κινδύνου – Σύνταξη αναφοράς

Όπως και στα προηγούμενα στάδια της ανάλυσης κινδύνου, όμοια και εδώ, στην αναφορά θα περιλαμβάνονται ο βαθμός αποδοχής για όλους τους παράγοντες κινδύνου που απειλούν το έργο καθώς και οι εναλλακτικές δράσεις για την αντιμετώπισή τους.

3.2 Μεθοδολογία Ανάλυσης Κινδύνων Υψηλού Επιπέδου (M.A.K.Y.E.)

Σε περιπτώσεις ελλιπούς ενημέρωσης για το έργο, σε τέτοιο βαθμό που δεν είναι δυνατή η περαιτέρω ανάλυση και αναγνώριση καθενός παράγοντα κινδύνου ξεχωριστά, υπάρχει η δυνατότητα χρησιμοποίησης της μεθόδου ανάλυσης κινδύνου υψηλού επιπέδου. Η μέθοδος αυτή έχει ακριβώς την ίδια προσέγγιση, όσον αφορά στα στάδια ανάλυσης, με την μέθοδο που περιγράφηκε προηγουμένως, με τη διαφορά, όμως, ότι δεν υπεισέρχεται σε λεπτομέρειες για κάθε παράγοντα κινδύνου και σε μεγάλο βάθος ανάλυσης, παρά αρκείται στην εφαρμογή αρκετά απλούστερων διαδικασιών.

Έτσι, αντί για τον προσδιορισμό κάθε παράγοντα κινδύνου ξεχωριστά, η μέθοδος αυτή προτείνει τον προσδιορισμό των κατηγοριών κινδύνου (classes). Κατά συνέπεια, προσδιορίζεται ο βαθμός έκθεσης του έργου σε κάθε κατηγορία κινδύνου, χωρίς να αναλώνεται χρόνος στη διαδικασία προσδιορισμού με σαφήνεια συγκεκριμένων παραγόντων κινδύνου και των επιπτώσεών τους.

Η έκθεση σε κάθε κατηγορία κινδύνου αποτιμάται σύμφωνα με τον παρακάτω πίνακα:

Επίπεδο έκθεσης σε κίνδυνο	Ορισμός
Κρίσιμο (Critical)	Μεγάλη πιθανότητα να οδηγήσει το έργο σε αποτυχία.
Πάνω από τον μέσο όρο (Above average)	Σημαντικές αποκλίσεις από τους στόχους του έργου.
Μέσος όρος (Average)	Όχι σοβαρές επιπτώσεις στην επιτυχία του έργου.
Κανένα (None)	Δεν τίθεται θέμα για το συγκεκριμένο έργο. Δεν υπάρχει πιθανός κίνδυνος από αυτή την κατηγορία.

Πίνακας 3.16: Επίπεδα έκθεσης σε κίνδυνο στη μέθοδο ανάλυσης κινδύνου υψηλού επιπέδου.

Με δεδομένη τη φύση της M.A.K.Y.E. είναι πιο δύσκολο να εξεταστούν μέτρα μείωσης συγκεκριμένων παραγόντων κινδύνου.

Στην περίπτωση εφαρμογής της M.A.K.Y.E. τα στάδια ανάλυσης κινδύνων είναι αντίστοιχα τα εξής:

I. Αναγνώριση Κινδύνου

i) Προετοιμασία
Συγκέντρωση των στόχων του έργου και δήλωση όλων των παραδοχών.

ii) Προσδιορισμός του είδους των παραγόντων κινδύνου
Δεν υπάρχει σαφής προσδιορισμός μεμονωμένων παραγόντων κινδύνου, παρά μόνο των ειδών των παραγόντων κινδύνου.

iii) Προσδιορισμός των επιπτώσεων
Δεν υπάρχει σαφής προσδιορισμός μεμονωμένων επιπτώσεων.

iv) Τεκμηρίωση
Το συγκεκριμένο στάδιο δεν εφαρμόζεται στην παρούσα φάση.

II. Εκτίμηση Κινδύνου

i) Πιθανότητα εμφάνισης ή βάρος του παράγοντα κινδύνου.
Δεν υπάρχει σαφής προσδιορισμός για μεμονωμένους παράγοντες κινδύνου.

ii) Μέγεθος σοβαρότητας ή επιπτώσεων.

Δεν υπάρχει σαφής προσδιορισμός για μεμονωμένους παράγοντες κινδύνου.

iii) Έκθεση σε κίνδυνο.

Προσδιορισμός της συνολικής έκθεσης σε κίνδυνο. Αυτό γίνεται με την εκτίμηση της έκθεσης σε κίνδυνο για κάθε κατηγορία κινδύνου.

iv) Τεκμηρίωση παράγοντα κινδύνου.

Μία σαφώς απλή διαδικασία για την καταγραφή των συμπερασμάτων των προηγούμενων σταδίων.

III. Αποτίμηση Κινδύνου

i) Αποδοχή

Αποτίμηση του βαθμού της αποδοχής της έκθεσης, με τη διαφορά ότι η αποτίμηση αυτή πραγματοποιείται πλέον στο επίπεδο της κατηγορίας του κινδύνου και όχι σε μεμονωμένους παράγοντες κινδύνου.

ii) Εναλλακτικά σενάρια

Το συγκεκριμένο στάδιο είναι πιο δύσκολο να εφαρμοστεί στην παρούσα μέθοδο. Παρ' όλ' αυτά, μπορούν να προταθούν εναλλακτικές δράσεις για κατηγορίες κινδύνου.

iii) Τεκμηρίωση παραγόντων κινδύνου

Μία σαφώς απλή διαδικασία για την καταγραφή των συμπερασμάτων των προηγούμενων σταδίων.

ΚΕΦΑΛΑΙΟ 4

Διαχείριση Κινδύνων σε Έργα Πληροφοριακών Συστημάτων

4.1 Γενική Μεθοδολογία Διαχείρισης Κινδύνων

Ο τρόπος αντιμετώπισης των κινδύνων στην ανάπτυξη των πληροφοριακών συστημάτων απασχολεί πολλούς ερευνητές τα τελευταία χρόνια. Ο εντοπισμός και η διαχείριση κινδύνων έχουν ύψιστη σπουδαιότητα για την επιτυχή διοίκηση έργων πληροφορικής. Μερικές χώρες διαθέτουν καλά δοκιμασμένες μεθοδολογίες και πρακτικές σε αυτόν τον τομέα, ενώ άλλες βρίσκονται σε πορεία αναζήτησης. Οι διάφορες στρατηγικές αντιμετώπισης των κινδύνων μπορούν να ταξινομηθούν σε ομάδες που έχουν σχέση με (Τσουτσαίος, 2005):

- *το ξεκίνημα του έργου:* Οι στρατηγικές που σχετίζονται με το ξεκίνημα του έργου είναι όλες όσες δίνουν ιδιαίτερη έμφαση στη διαδικασία, στον τρόπο επιλογής αναδόχου του έργου, στην αξιολόγηση των προσφορών, στη σύμβαση ανάθεσης του έργου κ.α..
- *την οργάνωση του τρόπου ανάπτυξης του πληροφοριακού συστήματος*: Οι στρατηγικές οργάνωσης του έργου της ανάπτυξης ενός πληροφοριακού συστήματος αντιμετωπίζουν θέματα σχετικά με τη δημιουργία των επιμέρους ομάδων εργασίας, τον καθορισμό του αριθμού των δραστηριοτήτων του έργου και των πόρων που απαιτεί κάθε δραστηριότητα, τη μεθοδολογία ανάπτυξης που ακολουθείται κ.λπ..
- *τη διοίκηση του έργου ανάπτυξης του πληροφοριακού συστήματος:* Οι στρατηγικές διοίκησης του έργου καλύπτουν τόσο το εκτελεστικό όσο και το διοικητικό επίπεδο διαχείρισης. Περιλαμβάνουν, επίσης, το πρόγραμμα ανασκοπήσεων, τα θέματα ποιοτικού ελέγχου, το χρόνο-προγραμματισμό εργασιών, την εκτίμηση κόστους σε σχέση με τη διάρκεια του έργου κ.λπ..
- *τον τρόπο αντιμετώπισης του χρήστη:* Έχει δημιουργηθεί μια τάση που υποστηρίζει ότι ο τρόπος συμμετοχής του χρήστη στην ανάπτυξη ενός πληροφοριακού συστήματος πρέπει να επανεξεταστεί (Barki, 1989). Μέσα στα πλαίσια της θέσης αυτής έχουν προταθεί διάφορες μεθοδολογίες που διαχειρίζονται τον τρόπο συνεργασίας ή και συμμετοχής του χρήστη στο έργο της ανάπτυξης. Η μέθοδος ETHICS και η μέθοδος prototyping είναι δύο χαρακτηριστικές μεθοδολογίες του είδους αυτού.
- *τη λειτουργία του πληροφοριακού συστήματος:* Ένα πληροφοριακό σύστημα μπορεί να αποτύχει στη φάση της λειτουργίας του, είτε όταν το σύστημα δεν καλύπτει πλέον τους αντικειμενικούς σκοπούς και στόχους που υπηρετούσε,

είτε όταν οι σκοποί και οι στόχοι αυτοί δεν ικανοποιούν πλέον τις ανάγκες του υπερσυστήματος, δηλαδή της επιχείρησης ή του οργανισμού. Κατά συνέπεια, η σχεδίαση των πληροφοριακών συστημάτων πρέπει να προβλέψει την ύπαρξη ενός ομοιοστατικού μηχανισμού μέσα στο πληροφοριακό σύστημα, που θα του επιτρέψει να λειτουργεί κάτω από υποβαθμισμένες συνθήκες (π.χ. χειρογραφικά).

Η απόφαση για το κατάλληλο πλάνο ασφάλειας σε ένα σύστημα και η επιλογή των κατάλληλων μηχανισμών είναι μέρος της δραστηριότητας της διαχείρισης κινδύνου (Turn, 1986). Γενικά, τις ενέργειες διαχείρισης κινδύνου μπορούμε να τις εκλάβουμε ως δύο κατηγοριών:

1. Μείωση του βαθμού επικινδυνότητας για την πλήρη αποβολή των όποιων επιβλαβών συνεπειών.
2. Εφόσον είναι αδύνατη η εξάλειψη του κινδύνου, περιορισμός ή ισοστάθμιση της έκτασής του μέσω ασφαλιστικών μέτρων.

Η υλοποίηση ενός πλάνου διαχείρισης και αντιμετώπισης κινδύνων είναι μια σημαντική διαδικασία για κάθε επιχείρηση. Σκοπός αυτού του πλάνου είναι η αποφυγή προβλέψιμων κινδύνων, η προστασία από λάθος επενδυτικές αποφάσεις και η ελαχιστοποίηση των απωλειών και ζημιών από απρόβλεπτα γεγονότα. Επειδή η πλήρης αποβολή των κινδύνων είναι συνήθως μη εφικτή, ευθύνη της ανώτερης διαχείρισης και των λειτουργικών και επιχειρησιακών στελεχών είναι να εφαρμόσουν τα μέτρα με το χαμηλότερο κόστος και τη μεγαλύτερη καταλληλότητα για να μειώσουν το βαθμό έκθεσης του έργου σε κίνδυνο σε αποδεκτό επίπεδο, με τις μικρότερες δυνατές παραχωρήσεις όσον αφορά την καθυστέρηση της ολοκλήρωσής του, την ποιότητά του και την επίτευξη των στόχων για τους οποίους υλοποιείται.

Η επιχειρησιακή διαχείριση κινδύνων είναι η διαδικασία σχεδιασμού, οργάνωσης, καθώς και ελέγχου των δραστηριοτήτων μίας επιχείρησης, προκειμένου να ελαχιστοποιηθούν οι επιπτώσεις του κινδύνου. Δεν περιλαμβάνει μόνο κινδύνους που σχετίζονται με τυχαίες ζημιές, αλλά και οικονομικά, στρατηγικά, λειτουργικά και άλλα συναφή είδη κινδύνων.

Η λειτουργική διαδικασία του πλάνου διαχείρισης και αντιμετώπισης κινδύνων παρέχει στην ουσία ένα χάρτη πορείας, εργαλεία και πόρους για την επίτευξη της ασφάλειας των συστημάτων της εταιρείας. Η τυποποίησή τους γίνεται απαραίτητη για την ασφαλή λειτουργία της γιατί παρέχει επιπλέον σταθερότητα στην επιχείρηση. Πιο συγκεκριμένα, το πλάνο διαχείρισης και αντιμετώπισης κινδύνων των πληροφοριακών συστημάτων της εταιρείας προϋποθέτει όλα τα παρακάτω (Μανούσης, 2003):

1. Την εκτίμηση και τον ακριβή καθορισμό των κρίσιμων περιουσιακών στοιχείων της εταιρείας.
2. Την αναγνώριση των απειλών κατά των πληροφοριακών συστημάτων της εταιρείας.

3. Την αναγνώριση των επιμέρους ευπαθειών.
4. Την αναγνώριση των πιθανών κατηγοριών απωλειών.
5. Την εκτίμηση της πιθανότητας να συμβεί μια απώλεια.
6. Τον προσδιορισμό των απαραίτητων προφυλάξεων/αντίμετρων για την αντιμετώπιση των κινδύνων.
7. Την διαμόρφωση και υλοποίηση του πλέον αποτελεσματικού και ενδεδειγμένου, από άποψη κόστους, συστήματος ασφαλείας.

Έχοντας καταγράψει, λοιπόν, την υφιστάμενη κατάσταση της εταιρείας και αναλύοντας στη συνέχεια τους κινδύνους ως προς τα αγαθά της, αναγνωρίστηκαν όλες οι απειλές και οι ευπάθειες αυτών, τόσο σε φυσικό όσο και σε λογικό επίπεδο, καθώς και η πιθανότητα εμφάνισης τους. Επιπλέον, έγινε καταγραφή όλων των πιθανών απωλειών που αυτά μπορεί να επιφέρουν, και ακολούθως προσδιορίστηκαν και οι απαραίτητες προφυλάξεις που πρέπει να ληφθούν από την εταιρεία. Το επόμενο βήμα είναι η διαμόρφωση ενός αποδοτικού συστήματος ασφαλείας που θα εξασφαλίζει και θα εγγυάται την ακεραιότητα, την εμπιστευτικότητα αλλά και τη διαθεσιμότητα των δεδομένων της εταιρείας, χωρίς να την επιβαρύνει ιδιαιτέρα.

Η διαχείριση κινδύνων, λοιπόν, είναι ο προγραμματισμός και η εφαρμογή ενεργειών για να μειωθεί η σοβαρότητα των παραγόντων κινδύνου που έχουν προσδιοριστεί κατά τη διάρκεια της ανάλυσης κινδύνων. Η διαδικασία διαχείρισης κινδύνων, ως αναπόσπαστο μέρος της διαχείρισης έργου, επιβάλλεται να έχει μια συνέχεια και να εφαρμόζεται σε όλη τη διάρκεια του έργου με συγκεκριμένες δραστηριότητες σε ορισμένη συχνότητα και απτά προϊόντα. Με τον τρόπο αυτό θα επιτευχθεί μια συνεχής μείωση της έκθεσης σε κινδύνους σε συνδυασμό με αυξανόμενα οφέλη. Αποτελείται, ουσιαστικά, από τέσσερεις κύριες δραστηριότητες (Ξανθόπουλος, 2004):

1. ***Προγραμματισμός Διαχείρισης Κινδύνου (Risk Management Planning):*** Ανάπτυξη των κατάλληλων ενεργειών για κάθε παράγοντα κινδύνου και προετοιμασία ενός σχεδίου-πλάνου διαχείρισής του.
2. ***Διαχείριση Πόρων (Resourcing):*** Κατανομή των πόρων και των ευθυνών για την υλοποίηση του σχεδίου-πλάνου.
3. ***Έλεγχος Διαδικασίας Διαχείρισης Κινδύνου (Controlling of Risk Management Process):*** Εξέταση του κατά πόσον οι σχεδιαζόμενες ενέργειες συμβαδίζουν με την κατανομή πόρων του σχεδίου-πλάνου και τις ισχύουσες διαδικασίες διαχείρισης του έργου.
4. ***Παρακολούθηση Διαδικασίας Διαχείρισης Κινδύνου (Monitoring of Risk Management Process):*** Έλεγχος της αποτελεσματικότητας της εφαρμογής του σχεδίου-πλάνου και εξέταση της ανάγκης για τυχόν αναθεώρησή του.

Στόχος της διαδικασίας διαχείρισης κινδύνων είναι η χρησιμοποίηση των συμπερασμάτων των προηγούμενων σταδίων της ανάλυσης κινδύνων για την παραγωγή ενός βασικού σχεδίου δράσης. Εκτός του βασικού σχεδίου, παράγωγα της διαδικασίας διαχείρισης κινδύνων αποτελούν και τα εναλλακτικά σχέδια έκτακτης ανάγκης. Τα σχέδια αυτά θα πρέπει να περιλαμβάνουν τις ενέργειες αντιμετώπισης ενός σημαντικού παράγοντα κινδύνου μετά την εκδήλωσή του. Οι εν λόγω ενέργειες, όπως ακριβώς και οι δράσεις του βασικού σχεδίου, είναι αναγκαίο να περιγράφονται όσο πιο αναλυτικά γίνεται, σε όρους κόστους, χρονοδιαγράμματος και πόρων. Η κύρια διαφοροποίηση των εναλλακτικών σχεδίων έκτακτης ανάγκης από το βασικό σχέδιο δράσης είναι ότι τα πρώτα περιέχουν όλες τις «κατασταλτικές» ενέργειες μετά την εκδήλωση του παράγοντα κινδύνου, ενώ το βασικό σχέδιο ενσωματώνει όλες τις προληπτικές ενέργειες διαχείρισης κινδύνων. Η ύπαρξη πλάνων έκτακτης ανάγκης είναι απαραίτητη για την καλή διαχείριση του έργου. Χωρίς αυτά δε μπορούν να γίνουν διορθωτικές κινήσεις όταν ανακύπτουν προβλήματα κατά την εκτέλεση της εργασίας. Δεν πρέπει να διαφεύγει της προσοχής ότι δεν είναι σωστό να «κρύβονται» τα έκτακτα μέτρα μέσα στους προϋπολογισμούς άλλων δραστηριοτήτων, αλλά να βασίζονται στο ποσοστό του κινδύνου που τους αναλογεί στο έργο.

Είναι, ωστόσο, αξιοσημείωτο ότι πολλές αποτυχίες οφείλονται στην ελλιπή συμμόρφωση προς πολύ καλές μεθοδολογικές κατευθύνσεις και επιτυχώς δοκιμασμένες πρακτικές. Επομένως, είναι αναγκαίο να εφαρμόζονται συστήματα διαχείρισης της γνώσης καθώς και συστήματα ελέγχου των αποτελεσμάτων, προσαρμοσμένα στις κατά περίπτωση ανάγκες. Παραδοτέα των διαδικασιών αυτών είναι τα σχέδια αντιμετώπισης κρίσεων, οι εφεδρείες, οι νομικές καλύψεις, οι διορθωτικές ενέργειες κ.α..

Τα πλάνα ενεργειών που σχεδιάζονται πρέπει να είναι ξεκάθαρα στους άμεσα εμπλεκόμενους, αλλά και στους τρίτους. Η δέσμευση στις προγραμματισμένες ενέργειες είναι πολύ κρίσιμο θέμα, από τα πρώτα κιόλας στάδια προγραμματισμού του έργου, για τις επερχόμενες σημαντικές αποφάσεις. Όσο πιο ξεκάθαρες είναι οι αποφάσεις της διοίκησης, τόσο πιθανότερη είναι η επιτυχία ολοκλήρωσης του έργου εντός των συμφωνημένων προδιαγραφών και στόχων. Και αυτό γιατί είναι πολύ ευκολότερο να αξιολογεί κανείς τα αποτελέσματα των προγραμματισμένων ενεργειών και να παρακολουθεί τους στόχους που έχουν τεθεί, όταν έχουν ξεκαθαριστεί από τα πρώιμα στάδια του έργου και έχει περιγραφεί με σαφήνεια το πλαίσιο δράσης. Οι επιμέρους στόχοι δε θα πρέπει να εμπλέκονται με τους τελικούς στόχους του έργου.

4.1.1 Προγραμματισμός Διαχείρισης Κινδύνου

Το επίπεδο του προγραμματισμού στη διαχείριση κινδύνων παρουσιάζει ομοιότητες με το επίπεδο της αποτίμησης στην ανάλυση κινδύνων. Στην πραγματικότητα, αυτά τα δύο επίπεδα μπορούν να πραγματοποιηθούν παράλληλα. Εντούτοις, ενώ στην ανάλυση κινδύνων το κύριο μέλημα είναι να προσδιοριστούν τα

μέσα και οι τρόποι για να μειωθεί ο κίνδυνος του έργου, στη διαχείριση κινδύνων δίνεται έμφαση στην ανάπτυξη αυτών των ενεργειών μέσα από μία πιο αναλυτική και λεπτομερή έρευνα της εφικτότητας των μεθόδων, με στόχο να επιτευχθεί το προσδοκώμενο αποτέλεσμα χωρίς να υπάρξουν ανεπιθύμητες επιπτώσεις. Στο τέλος αυτού του σταδίου ετοιμάζεται ένα σχέδιο διαχείρισης κινδύνου σε πρώιμη μορφή.

Η φάση του προγραμματισμού διαχείρισης κινδύνου αποτελείται από τα ακόλουθα στάδια:

- *Προσδιορισμός των μέτρων προστασίας:* Εκτιμούνται τα ήδη υπάρχοντα μέτρα προστασίας, αν φυσικά υπάρχουν. Στη συνέχεια, πραγματοποιείται μια μελέτη προτεραιοτήτων στα προτεινόμενα μέτρα προστασίας, ώστε να διαπιστωθούν εκείνα που είναι άμεσα υλοποιήσιμα και εκείνα που απαιτούν περαιτέρω μελέτη. Έπειτα, εφαρμόζεται ανάλυση κόστους/οφέλους για κάθε προτεινόμενο μέτρο προστασίας, ώστε να αποφευχθεί το ενδεχόμενο επιλογής αντιμέτρου που είναι αδύνατη η υλοποίηση του. Τέλος, γίνεται η οριστική επιλογή των νέων μέτρων προστασίας.
- *Πολιτική ασφάλειας του συστήματος:* Προκειμένου να επιτευχθεί το επιθυμητό επίπεδο ασφάλειας του συστήματος, είναι αναγκαίος ο προσδιορισμός και η καταγραφή των στόχων ασφάλειάς του. Αναπτύσσεται, λοιπόν, η πολιτική ασφάλειας για το υπάρχον σύστημα (ή προσαρμόζεται η ήδη υπάρχουσα). Περιγράφεται, δηλαδή, το σύνολο των κανόνων, των μέτρων και των διαδικασιών που καθορίζουν τα φυσικά, διαδικαστικά και προσωπικά μέτρα ασφάλειας που λαμβάνονται στη διοίκηση, διανομή και προστασία των αγαθών. Μέσα στα πλαίσια της πολιτικής αυτής διευθετούνται θέματα, όπως δέσμευση των απαραίτητων πόρων (χρηματικών και μη) για την υλοποίηση των αντιμέτρων, κατανομή ευθυνών και καθηκόντων, προσδιορισμός και οριοθέτηση του χώρου εφαρμογής της εκάστοτε πολιτικής (σε περίπτωση που εξαιρούνται ορισμένα στοιχεία του συστήματος).
- *Υλοποίηση των νέων μέτρων προστασίας:* Στο σημείο αυτό ξεκινά η διαδικασία υλοποίησης των μέτρων προστασίας που επιλέχθηκαν προηγουμένως.

Αποτελεί πλέον πεποίθηση ότι ο κίνδυνος είναι μια αναπόφευκτη πραγματικότητα της επιχειρηματικής δραστηριότητας. Οι δυνατότητες που παρέχονται στον προγραμματισμό διαχείρισης κινδύνου ταξινομούνται ουσιαστικά σε τέσσερις μεγάλες κατηγορίες-κατευθύνσεις:

i. Αποφυγή κινδύνου (risk avoidance)
ii. Μεταφορά κινδύνου (risk transfer)
iii. Έλεγχος/περιορισμός κινδύνου (risk controlling/reduction)
iv. Αποδοχή κινδύνου (rik acceptance)

Αποφυγή κινδύνου

Πρόκειται είτε για τη χρησιμοποίηση εναλλακτικών προσεγγίσεων, οι οποίες δεν περιέχουν καθόλου κίνδυνο, είτε για τη μη υλοποίηση του τμήματος του έργου που τίθεται σε κίνδυνο. Αυτή η δυνατότητα, αν και είναι η πιο αποτελεσματική από τις τεχνικές προγραμματισμού διαχείρισης κινδύνου, δεν είναι πάντα διαθέσιμη, καθώς σε πάρα πολλές περιπτώσεις είτε είναι πρακτικά αδύνατη η υιοθέτηση μιας στρατηγικής χωρίς καθόλου κίνδυνο, είτε υπάρχουν έργα που εκτίθενται εν γνώση των υπευθύνων σε κίνδυνο για τη μεγιστοποίηση του κέρδους, καθώς σχεδόν πάντοτε η πορεία προς την υλοποίηση σημαντικών στόχων δεν μπορεί να γίνει χωρίς κίνδυνο. Επιπρόσθετα, ορισμένα τμήματα του έργου είναι ζωτικής σημασίας για τη λειτουργία του και προσφέρουν τα μέγιστα στην εκπλήρωση των στόχων του συστήματος, με αποτέλεσμα να μη μπορούν να παραληφθούν. Φυσικά, μια ασφαλέστερη επιλογή σημαίνει και μικρότερη απόδοση της επένδυση του έργου. Μαζί με την αποφυγή του κινδύνου, δηλαδή, χάνονται και τα οφέλη που θα αποκομίζονταν από το αρχικό σχέδιο υλοποίησης και την έκθεση σε αυτόν. Παρ' όλ' αυτά, η αποφυγή κινδύνου αποτελεί την πιο αποτελεσματική μέθοδο αντιμετώπισης κινδύνων που μπορεί να εφαρμοστεί και ενδείκνυται σε περιπτώσεις κινδύνων, οι οποίοι είναι πέραν του ελέγχου της ομάδας έργου. Παράδειγμα αποτελεί η διάθεση λογισμικού, που επειδή δε μπορεί να προστατευθεί από την πειρατεία, παρέχεται δωρεάν.

Μεταφορά κινδύνου

Πρόκειται για τη μεταφορά του κινδύνου (στο σύνολό του ή μέρος του) σε κάποιο άλλο εμπλεκόμενο μέρος (στον ειδικό). Πρακτικά, η υλοποίηση αυτής της τακτικής γίνεται με την μεταφορά του κινδύνου μέσα σε μια σύμβαση και άρα με την ανάληψή του από το έτερο συμβαλλόμενο μέρος. Κοινό παράδειγμα αποτελεί η ασφάλιση των ευπαθών τομέων, όπου για ένα χρηματικό ποσό κάποιος τρίτος (ασφαλιστήρια εταιρεία) αναλαμβάνει τον κίνδυνο, όπως κλοπή, πυρκαγιά, σεισμό, κ.τ.λ., με αποτέλεσμα να μειώνει την έκθεση της επιχείρησης σε κινδύνους. Άλλα παραδείγματα είναι οι συμβάσεις όπου ο κίνδυνος μεταφέρεται ή διανέμεται και σε τρίτους, η ανάθεση υπεργολαβιών ή/και οι συμβάσεις προκαθορισμένου κόστους με πρόστιμα σε περίπτωση αθέτησης των όρων, κ.α..

Έλεγχος/περιορισμός κινδύνου

Πρόκειται για την πιο κοινή τακτική όλων των στρατηγικών χειρισμού κινδύνων, στην οποία υπάγονται οι περισσότεροι παράγοντες κινδύνου. Σε αυτή εντάσσονται

όλες οι δράσεις που, μέσω εναλλακτικών σχεδίων αντιμετώπισης κινδύνων, στοχεύουν στη μείωση, είτε της πιθανότητας εμφάνισης ενός παράγοντα κινδύνου, είτε των συνεπειών από την εμφάνισή του. Οι δράσεις περιορισμού του κινδύνου δεν είναι δυνατόν να εξειδικευτούν περαιτέρω σε αυτό το επίπεδο, καθώς εξαρτώνται από την φύση και το είδος του υπό εξέταση παράγοντα κάθε φορά. Σημαντικοί παράγοντες, ωστόσο, είναι η ικανότητα ανίχνευσης του επερχόμενου κινδύνου και η "απόσταση" μεταξύ παρακολούθησης του υπάρχοντος κινδύνου και ενεργοποίησης του σχεδίου επείγουσας επέμβασης. Η στρατηγική αυτή, όπως και η αποφυγή κινδύνου, ενδείκνυται σε περιπτώσεις κινδύνων όπου η ομάδα έργου αδυνατεί να τους ελέγξει. Αν και το πιο σύνηθες εναλλακτικό πλάνο είναι η φύλαξη ενός χρηματικού αποθέματος που θα επενδυθεί στο έργο μόνο στην περίπτωση εμφάνισης του κινδύνου για τον οποίο φυλάσσεται, παραδείγματα αποτελούν, επίσης, τα συστήματα άμεσης αντιμετώπισης, η εγκατάσταση συστημάτων ανίχνευσης και εργασίες μηχανικών.

Αποδοχή κινδύνου

Πρόκειται για την ανοχή του κινδύνου και επομένως των συνεπειών του, χωρίς να προγραμματιστεί καμία απολύτως ενέργεια διαχείρισης του. Με την επιλογή απραξίας για την αποφυγή του κινδύνου, δεν επιβαρύνεται το έργο με επιπλέον κόστος και πολυπλοκότητα. Πρόκειται, όμως, για μια επικίνδυνη επιλογή, καθώς η αγνόηση ενός κινδύνου μπορεί να έχει καταστροφικές συνέπειες για την πορεία του έργου. Η αποδοχή του κινδύνου, λοιπόν, είναι δυνατό να συμβεί σε αρκετές περιπτώσεις που αφορούν μη κρίσιμους για την επιτυχία του έργου 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. Στις περιπτώσεις αυτές, η επιχείρηση είναι έτοιμη να επωμιστεί τις συνέπειες του κινδύνου, εάν και όποτε συμβεί.

Κατά την υιοθέτηση οποιασδήποτε από τις παραπάνω επιλογές, θα πρέπει να λαμβάνονται υπόψη οι στόχοι και η αποστολή του οργανισμού, για λογαριασμό του οποίου εγκαθίσταται το πληροφοριακό έργο, καθώς και του ίδιου του έργου. Η μέθοδος που θα εφαρμοστεί για το μετριασμό του κινδύνου ποικίλει ανάλογα με τη φύση του αλλά και τις ιδιαιτερότητες του κάθε έργου λογισμικού. Σε κάθε επιλεγόμενη στρατηγική ενδείκνυται η μελέτη των πλεονεκτημάτων και μειονεκτημάτων αυτής, καθώς μια στρατηγική μπορεί να αντιμετωπίζει έναν κίνδυνο αλλά ταυτόχρονα να αναζωπυρώνει έναν άλλον. Στην περίπτωση ανάθεσης υπεργολαβίας, για παράδειγμα, ο αναθέτων οργανισμός μειώνει τον αρνητικό κίνδυνο μετατοπίζοντάς τον στον υπεργολάβο, αλλά ταυτόχρονα αυξάνει τον κίνδυνο της ελλιπούς επικοινωνίας μεταξύ των δύο μερών και πρέπει να αναπτύξει μια νέα στρατηγική για την αντιμετώπιση αυτού του νέου

αρνητικού κινδύνου. Ο αποτελεσματικότερος τρόπος επιλογής στρατηγικής διαχείρισης ενός κινδύνου είναι να χρησιμοποιηθούν οι κατάλληλες τεχνολογίες μεταξύ των διαφόρων προϊόντων ασφάλειας, παράλληλα με την κατάλληλη επιλογή μεθόδου μετριασμού κινδύνου καθώς και με τα μη τεχνικά, σχεδιαστικά και διοικητικά μέτρα.

Οι διαδικασίες προγραμματισμού διαχείρισης κινδύνου εφαρμόζονται σε όλες τις φάσεις του έργου. Όσο νωρίτερα, όμως, ενταχθούν στη διαδικασία διαχείρισης του έργου, τόσο μεγαλύτερα θα είναι τα οφέλη, καθώς είναι φανερό ότι άλλες δυνατότητες παρέχονται για αποτελεσματική διαχείριση κινδύνου όταν το έργο είναι στην φάση της σύλληψης και του σχεδιασμού του, και άλλες δυνατότητες παρέχονται όταν πια το έργο βρίσκεται στη διαδικασία εφαρμογής του. Χαρακτηριστικά αναφέρεται ότι η τακτική της αποφυγής κινδύνου είναι, ουσιαστικά, ανέφικτη σε προχωρημένα στάδια της εφαρμογής του έργου, στα οποία είναι εξαιρετικά δύσκολο να γίνουν αλλαγές στον σχεδιασμό ώστε να αποφευχθεί κάποιος παράγοντας κινδύνου.

4.1.2 Διαχείριση Πόρων

Το στάδιο της διαχείρισης πόρων εμπεριέχει τόσο τον καταμερισμό των διαθέσιμων πόρων στη διαχείριση κινδύνων, όσο και τον επιμερισμό των ανάλογων ευθυνών σε συγκεκριμένα πρόσωπα. Κατά τη διάρκεια κατανομής των πόρων, ιδιαίτερη έμφαση θα πρέπει να δίνεται στις ανάγκες για πόρους των δραστηριοτήτων διαχείρισης του έργου, έτσι ώστε να εξακριβώνεται ότι οι διατιθέμενοι πόροι στη διαχείριση κινδύνων μπορούν όντως να διατεθούν και δεν είναι δεσμευμένοι για κάποια άλλη δραστηριότητα.

4.1.3 Έλεγχος Διαδικασίας Διαχείρισης Κινδύνου

Το στάδιο του ελέγχου προτίθεται να βεβαιώσει ότι η επιτευχθείσα κατά το στάδιο του σχεδιασμού-προγραμματισμού πρόοδος είναι συμβατή με τους διαθέσιμους πόρους και ότι η εφαρμογή του σχεδίου διαχείρισης κινδύνου έχει συντονιστεί (είναι σε αρμονία) με τις δραστηριότητες διαχείρισης του έργου. Το καλύτερο, βέβαια, αποτέλεσμα επιτυγχάνεται όταν η διαδικασία διαχείρισης κινδύνου δε θεωρείται επιπρόσθετη, αλλά είναι πλήρως ενσωματωμένη στη διαδικασία διαχείρισης του έργου.

4.1.4 Παρακολούθηση Διαδικασίας Διαχείρισης Κινδύνου

Το στάδιο της παρακολούθησης είναι το κλειδί που επιβεβαιώνει την αποτελεσματικότητα της εφαρμογής του σχεδίου διαχείρισης κινδύνου συνολικά, αλλά και κάθε επιμέρους δράσης για τη μείωση του κινδύνου. Σε αυτό το στάδιο παρακολουθούνται και καταγράφονται οι παράγοντες κινδύνου που τελικά εμφανίστηκαν και πότε συνέβη αυτό, καθώς επίσης και οι ενέργειες διαχείρισής τους που λήφθηκαν τελικά, από ποιους και τι αποτελεσματικότητα είχαν. Τα καταγραφόμενα στοιχεία συγκρίνονται με αυτά του σχεδίου διαχείρισης κινδύνου και εξετάζονται τυχόν αποκλίσεις από αυτό, σε συνδυασμό με τους λόγους που οδήγησαν στις εν λόγω διαφοροποιήσεις.

Μελετώντας τα αποτελέσματα και τις παρατηρήσεις που προέκυψαν από τους προηγούμενους ελέγχους, προβαίνουμε στις απαραίτητες αλλαγές, όταν κριθεί απαραίτητο. Παρόλο που μερικοί κίνδυνοι μπορεί να βρίσκονται χαμηλά στην ιεράρχηση και μπορούν να θεωρηθούν χαμηλού ρίσκου ή ρουτίνας, θα πρέπει σε τακτά χρονικά διαστήματα να αξιολογούνται εκ νέου, με σκοπό την εξασφάλιση ότι δεν έχουν μετατραπεί σε σημαντικούς κινδύνους. Οποιεσδήποτε αλλαγές πρέπει να αξιολογούνται, προκειμένου να διαπιστωθεί εάν έχουν αρνητικές συνέπειες και εάν οι υπάρχοντες μηχανισμοί ελέγχου είναι επαρκείς. Σε ραγδαίως μεταβαλλόμενα περιβάλλοντα, η πρόσληψη, για παράδειγμα, νέου προσωπικού μπορεί να αυξήσει την πιθανότητα κινδύνου, εφόσον όλοι οι άλλοι παράγοντες παραμένουν σταθεροί. Στην επανεξέταση θα πρέπει να λαμβάνονται υπόψη τα εξής:

- η κρισιμότητα, δηλαδή ο βαθμός εμφάνισης των αρνητικών συνεπειών, ως αποτέλεσμα της έκθεσης στον κίνδυνο και της μη λήψης άμεσων διορθωτικών ενεργειών.
- ο βαθμός επηρεασμού του έργου, των ανθρώπων και του περιβάλλοντος.
- ο χρόνος επίδρασης των αρνητικών συνεπειών (στο εγγύς μέλλον ή πολύ αργότερα).
- η πιθανή διακοπή στην εξέλιξη των εργασιών.
- η δυνατότητα ανάκαμψης και γρήγορης ανάκτησης του χαμένου εδάφους.
- η επίπτωση στο κόστος του έργου σε περίπτωση προσφυγής του πελάτη στα δικαστήρια για διεκδίκηση αποζημιώσεων.
- η επίπτωση στη δημόσια εικόνα της επιχείρησης και στα οικονομικά της.

Γίνονται, δηλαδή, οι αναγκαίες αναθεωρήσεις του σχεδίου διαχείρισης κινδύνου, όπου και όταν χρειάζεται. Για παράδειγμα, αποσύρουμε ή αντικαθιστούμε κάποιο μέτρο προστασίας αν αντιληφθούμε ότι δεν είναι αποτελεσματικό ή είναι περιττό. Τέτοιου είδους τροποποιήσεις είναι επιβεβλημένες όταν είτε εμφανιστεί ένας παράγοντας κινδύνου που δεν έχει προβλεφθεί, είτε αποδειχτεί ότι η υπάρχουσα εκτίμηση του μεγέθους της σοβαρότητας των παραγόντων κινδύνου βρίσκεται συστηματικά εκτός των ανεκτών ορίων διακύμανσης, είτε διαπιστωθεί ότι η αποτελεσματικότητα των

σχεδιαζόμενων δράσεων είναι μειωμένη σε σχέση με τις προσδοκίες, είτε τέλος εξαιτίας κάποιας ριζικής αλλαγής στα πλαίσια του συστήματος (π.χ. μπορεί τα δεδομένα που διαχειρίζεται το σύστημα να μετατραπούν σε ευαίσθητα και κρίσιμα δεδομένα για αυτό, οπότε επιβάλλεται η επανεξέταση και αναθεώρηση των μέτρων προστασίας). Για το λόγο αυτό, ο υπεύθυνος διαχείρισης κινδύνων πρέπει περιοδικά να αναφέρεται στο διαχειριστή υλοποίησης του έργου, παρουσιάζοντας την αποτελεσματικότητα του σχεδίου, οποιεσδήποτε μη προβλεφθήσες επιδράσεις και την ενδεχόμενη ανάγκη λήψης έκτακτων μέτρων αντιμετώπισης.

Συνοπτικά, η παρακολούθηση της διαδικασίας διαχείρισης κινδύνου είναι μια συνολική διαδικασία, η οποία ξεκινάει από τον προσδιορισμό των κινδύνων, τα αποτελέσματα του οποίου εισάγονται στην εκτίμηση των κινδύνων, εκ νέου προσδιορισμό των κινδύνων αν χρειαστεί κ.ο.κ.. Στόχος της επαναληπτικής αυτής διαδικασίας σε όλες τις φάσεις είναι η ύπαρξη ενός ασφαλούς πληροφοριακού συστήματος. Ουσιαστικά, πρόκειται για μια συνεχή διαδικασία ελέγχου της αποτελεσματικότητας των μέτρων προστασίας, αλλά και παρακολούθησης της όλης λειτουργίας του συστήματος (αν είναι η αρμοστή).

Σκοπός, επομένως, του σταδίου της παρακολούθησης είναι να εξασφαλιστεί ότι:

- τα μέτρα, οι κατάλληλες πολιτικές και διαδικασίες ενάντια στους κινδύνους εφαρμόζονται βάση του αρχικού σχεδιασμού και η διαδικασία ανάπτυξης και υλοποίησης των μέτρων προστασίας εξελίσσεται ομαλά και κάτω από τις υπάρχουσες απαιτήσεις.
- οι σχεδιασθείσες ενέργειες για τη μείωση της πιθανότητας εμφάνισης του παράγοντα κινδύνου είναι όντως αποτελεσματικές.
- οι σχεδιασθείσες ενέργειες για την μείωση των επιπτώσεων που συνδέονται με τον παράγοντα κινδύνου είναι αποτελεσματικές.
- το σύνολο των δραστηριοτήτων παραμένει μέσα στο προκαθορισμένο όριο ανοχής κινδύνου (γραμμή ανοχής).
- όταν κάποιοι κίνδυνοι πάψουν να αποτελούν απειλή, τότε η διάθεση κονδυλίων για την αντιμετώπισή τους δεν είναι πλέον αναγκαία.
- όταν οι παράγοντες κινδύνου, για τους οποίους δεν υπάρχει καμία πιθανή δράση μετριασμού, φτάσουν σε ένα σημείο όπου η πιθανότητα να προκύψουν έχει μεγαλώσει, εφαρμόζεται εκείνο το σχέδιο που περιλαμβάνει το συγκεκριμένο ενδεχόμενο.

Οι πληροφορίες που απαιτούνται για την επόπτευση των κινδύνων κατά τη διάρκεια υλοποίησης του πληροφοριακού έργου είναι:

- σχέδιο διαχείρισης κινδύνων
- σχέδιο αντιμετώπισης κινδύνων

- αναφορές λειτουργίας του έργου (*λίστες δράσης-αντικειμένου, προειδοποιήσεις κινδύνων, αναφορές προόδου, αναφορές ποιότητας λειτουργίας*)
- επιπρόσθετη αναγνώριση και ανάλυση κινδύνων (*για κινδύνους που αναγνωρίστηκαν ή εκδηλώθηκαν στην πορεία υλοποίησης του έργου και για τους οποίους επαναλαμβάνονται οι διαδικασίες διαχείρισης κινδύνων*)
- αλλαγές στις απαιτήσεις του έργου (*προσθήκη νέων λειτουργιών στα συστήματα που ενδεχομένως να αντιμετωπίζουν απειλές που δεν εμφανίζονται στον αρχικό σχεδιασμό*)

Οι μέθοδοι που χρησιμοποιούνται για την παρακολούθηση της διαδικασίας διαχείρισης κινδύνου είναι οι ακόλουθες:

- *Έλεγχοι αντιμετώπισης κινδύνων:* Οι έλεγχοι αυτοί εξετάζουν και καταγράφουν την αποτελεσματικότητα της αντιμετώπισης των κινδύνων σε ότι αφορά την αποφυγή, τη μεταφορά ή το μετριασμό αυτών. Οι συγκεκριμένοι έλεγχοι πραγματοποιούνται καθ' όλη τη διάρκεια υλοποίησης του έργου.
- *Περιοδική ανασκόπηση των κινδύνων που απειλούν το έργο:* Τέτοιου είδους αναφορές θα πρέπει να ακολουθούν τακτικό προγραμματισμό. Κρίνεται απαραίτητο να τηρείται ένα ημερολόγιο κινδύνων, καθώς ο βαθμός κινδύνου και οι προτεραιότητες ενδεχομένως να μεταβάλλονται στην πορεία υλοποίησης του έργου και οι αλλαγές αυτές μπορεί να απαιτούν εκ νέου ποιοτική και ποσοτική ανάλυση. Παράλληλα, θα υποδεικνύουν και τις απειλές που δε μπορούν πια να βλάψουν το πληροφοριακό σύστημα και τις διαδικασίες υλοποίησής του και θα προτείνουν τους ελέγχους που είναι σε θέση πλέον να "απενεργοποιηθούν".
- *Ανάλυση κεκτημένης αξίας:* Η ανάλυση αυτή χρησιμοποιείται για την παρακολούθηση της πορείας του έργου βάση του αρχικού σχεδιασμού. Τα αποτελέσματά της μπορεί να προβλέψουν πιθανή απόκλιση από το αρχικώς προβλεφθέν κόστος και από τον προγραμματισμένο χρόνο υλοποίησης. Όταν ένα έργο αποκλίνει ξεκάθαρα και σε αξιοσημείωτο βαθμό από το αρχικό πλάνο, τότε απαιτείται εκτέλεση εκ νέου διαχείρισης κινδύνων, για να εντοπιστούν και να αντιμετωπιστούν τα αίτια και οι επιπτώσεις αυτής της απόκλισης.
- *Τεχνική αξιολόγηση επιδόσεων:* Με την αξιολόγηση αυτή συγκρίνονται οι δυνατότητες και οι επιδόσεις του συστήματος με αυτές οι οποίες είχαν τεθεί ως στόχος κατά το σχεδιασμό του έργου. Εάν το σύστημα δεν αποδίδει τα αναμενόμενα, σημαίνει ότι διορθωτικές κινήσεις θα πρέπει να εκτελεστούν. Η εν λόγω αξιολόγηση πρέπει να γίνεται σε κάθε τμήμα του έργου που ολοκληρώνεται, λαμβάνοντας υπόψη και τις απαιτήσεις των συστημάτων που πρόκειται να εγκατασταθούν, έτσι ώστε να μειωθεί η έκταση των επιπτώσεων και η πολυπλοκότητα των επιδιορθώσεων για την επίτευξη του αρχικού στόχου.
- *Επιπρόσθετος σχεδιασμός αντιμετώπισης κινδύνω:*. Ο σχεδιασμός αυτός είναι απαραίτητος όταν παρουσιαστεί ένας κίνδυνος που δεν είχε αρχικά προβλεφθεί, όταν διαπιστωθεί ότι οι επιπτώσεις ενός κινδύνου είναι μεγαλύτερες από τις αναμενόμενες ή όταν η σχεδιασμένη αντίδραση έναντι ενός κινδύνου αποδειχθεί ανεπαρκής.

Τα αποτελέσματα της διαδικασίας επόπτευσης κινδύνων κατά την υλοποίηση έργων πληροφοριακών συστημάτων είναι τα εξής:

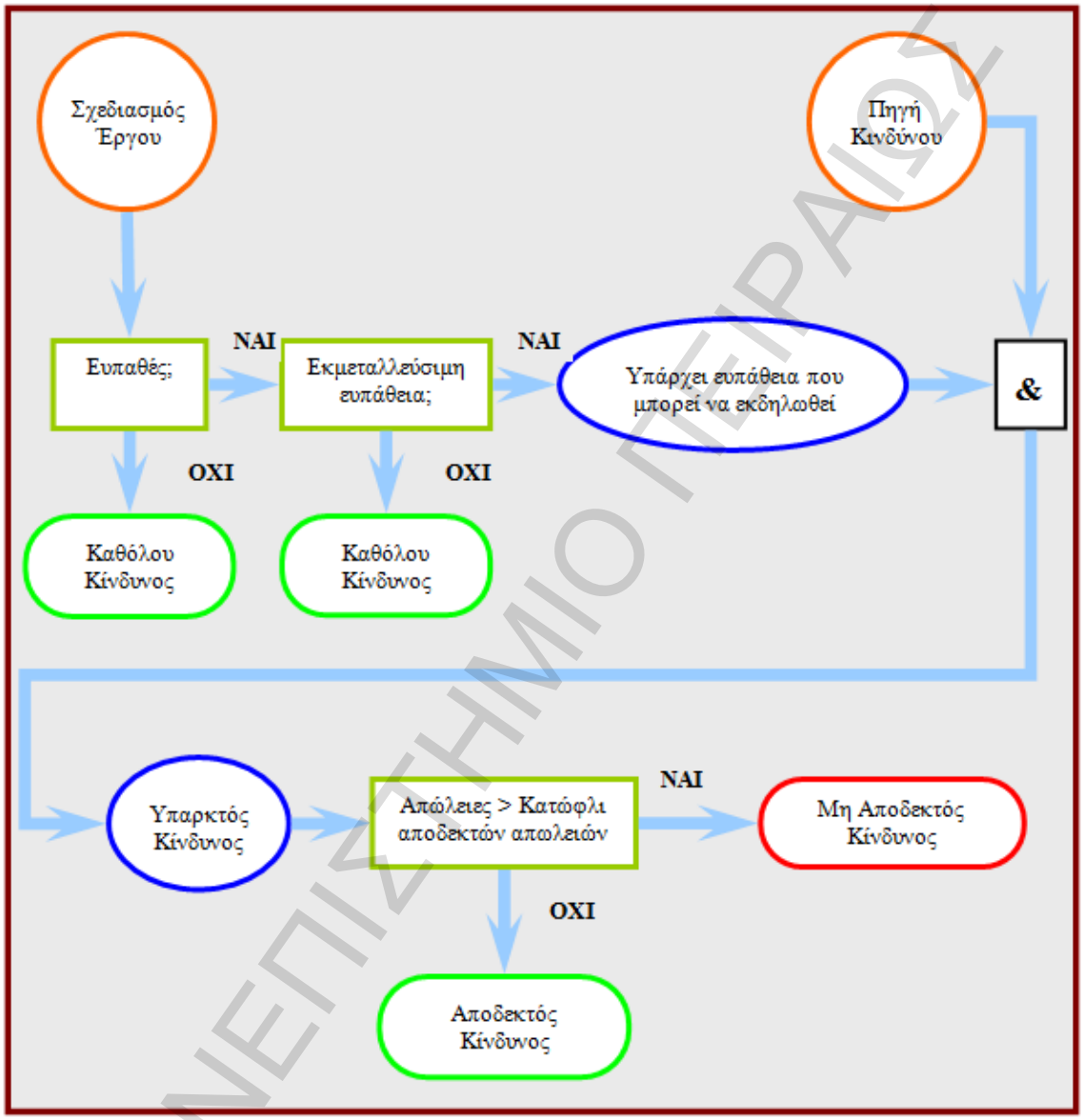
- *Δράση εκτός αρχικού σχεδιασμού:* Αναφερόμαστε σε ενέργειες που πραγματοποιούνται για κινδύνους που εκδηλώνονται και αιφνιδιάζουν με την εμφάνισή τους, καθώς δεν είχαν προβλεφθεί και απαιτούν την άμεση λήψη δράσης για την αντιμετώπισή τους.
- *Διορθωτικές ενέργειες:* Είναι ενέργειες που πραγματοποιούνται για να διορθώσουν παραλείψεις και προχειρότητες του αρχικού σχεδιασμού. Επίσης, χρησιμοποιούνται και για την αλλαγή ορισμένων διαδικασιών, καθώς στην πράξη αναδείχτηκαν κάποιες πιο αποτελεσματικές εφαρμογές.
- *Αλλαγές των απαιτήσεων του έργου:* Οι διορθωτικές ενέργειες στον αρχικό σχεδιασμό καθώς και οι εντελώς νέοι έλεγχοι που πιθανώς να απαιτηθούν μπορεί να μεταβάλλουν σημαντικά κάποιες πτυχές του έργου και να κριθεί αναγκαία η επανεκτίμηση όχι μόνο του σχεδίου αντιμετώπισης κινδύνων, αλλά και του σχεδίου υλοποίησης του έργου.
- *Ενημέρωση βάση των εξελίξεων του σχεδίου αντιμετώπισης κινδύνων:* Οι κίνδυνοι μπορεί να εκδηλωθούν ή όχι. Κατά τη διάρκεια ενός έργου, οι κίνδυνοι που εκδηλώνονται καταγράφονται και αξιολογούνται. Το σχέδιο αντιμετώπισης κινδύνων μπορεί να βελτιώνεται και να ενισχύεται βάση των νέων στοιχείων. Οι κίνδυνοι που, τελικά, δεν εκδηλώθηκαν πρέπει, επίσης, να καταγράφονται και να τίθενται εκτός σχεδιασμού (εξοικονόμηση κονδυλίων, μείωση πολυπλοκότητας, μείωση προσωπικού).
- *Τήρηση αρχείων με στοιχεία κινδύνων:* Τα αρχεία αυτά θα βοηθήσουν στην καλύτερη προστασία του σχεδίου υλοποίησης του έργου, στην καλύτερη λειτουργία του, αλλά και θα αποτελέσουν πολύτιμη βάση δεδομένων για έργα που θα υλοποιηθούν στο μέλλον.

4.2 Στρατηγική Μετριασμού Κινδύνων

Τα στελέχη που έχουν την ευθύνη για το σχεδιασμό και την υλοποίηση του έργου και που γνωρίζουν τους πιθανούς κινδύνους και τη σημαντικότητα αυτών, οφείλουν να απαντήσουν στα εξής ερωτήματα (Ritchie και Marshall, 1993):

- Πότε και υπό ποιες συνθήκες θα πρέπει να δραστηριοποιηθούν;
- Πότε θα εφαρμόσουν τις διαδικασίες μετριασμού των κινδύνων και προστασίας της πορείας υλοποίησης του έργου λογισμικού;

Το σχήμα 4.1, που περιγράφει τη διαδικασία μετριασμού κινδύνου, δίνει τις απαντήσεις στα παραπάνω ερωτήματα με περιγραφικό τρόπο (Stoneburner, Goguen και Feringa, 2001).



Σχήμα 4.1: Σημεία δράσης διαδικασίας μετριασμού κινδύνου.

Κάθε επιλογή του παραπάνω διαγράμματος αποτελεί και ένα σημείο που πρέπει να εξεταστεί:

- *Υπάρχει ευπάθεια (αδυναμία):* Εφαρμογή τεχνικών για τη μείωση της πιθανότητας εμφάνισης της ευπάθειας.
- *Η ευπάθεια μπορεί να εκδηλωθεί:* Εφαρμογή των σχεδίων προστασίας του έργου και διοικητικών ελέγχων για την ελαχιστοποίηση της πιθανότητας

εμφάνισης του κινδύνου ή την πλήρη αποτροπή της εμφάνισής του. Σχεδιασμός για την αντιμετώπιση των δυσμενών επιπτώσεων από την εκδήλωση του κινδύνου.

- *Οι απώλειες από την εκδήλωση του κινδύνου είναι πολύ μεγάλες:* Όταν η εφαρμογή του αρχικού σχεδιασμού προστασίας και των τεχνικών και μη τεχνικών μέτρων για τον περιορισμό της έκτασης των επιπτώσεων αποδειχτεί επιζήμια ή αδύναμη να αντιμετωπίσει τον επικείμενο κίνδυνο, θα πρέπει να επαναληφθεί η διαδικασία με σκοπό την υιοθέτηση νέων μέτρων, ενώ δεν αποκλείεται και το ενδεχόμενο να κριθεί μη κερδοφόρα η υλοποίηση του έργου και να εγκαταλειφθεί.

Εάν αναφερόμαστε σε κινδύνους που οφείλονται σε εκούσια ανθρώπινη δράση, πρέπει να προσθέσουμε και μια επιλογή με τη σύγκριση κόστους-οφέλους για το δράστη, πριν από την επιλογή της σύγκρισης των απωλειών με το κατώφλι των αποδεκτών απωλειών.

4.3 Εργαλεία Διαχείρισης Κινδύνων

Η διαχείριση κινδύνων δεν είναι απλή διαδικασία και συνήθως παράγει ένα πολύ μεγάλο αριθμό δεδομένων για επεξεργασία. Όσο μεγαλύτερο είναι το εύρος της ανάλυσης, τόσο πιο δύσκολη είναι η διαχείριση των πληροφοριών που συλλέγονται. Αναγνωρίζοντας την παραπάνω δυσκολία, πολλές εταιρείες έχουν αναπτύξει λογισμικό για την διευκόλυνση της διαχείρισης κινδύνων. Αυτή η ανάπτυξη λογισμικού δεν είναι καινούργια υπόθεση, αλλά ξεκίνησε από τη δεκαετία του ’80. Αρχικά, τα προγράμματα που σχεδιάστηκαν ήταν απλά και περιορίζονταν σε απλούς υπολογισμούς. Στη συνέχεια, όμως, λόγω της αύξησης της πολυπλοκότητας των πληροφοριακών συστημάτων καθώς και των προβλημάτων ασφαλείας, τα προγράμματα για ανάλυση κινδύνων έλαβαν πιο ενεργό ρόλο, αναλαμβάνοντας τη διευκόλυνση του συνόλου της διαχείρισης κινδύνων με πολλά διαφορετικά εργαλεία. Μάλιστα, κατά τη δεκαετία του ’90, που τέτοια προγράμματα βγήκαν στην ελεύθερη αγορά, ο ανταγωνισμός οδήγησε τις εταιρείες ανάπτυξής τους να προσθέσουν νέα χαρακτηριστικά, ώστε τελικά να καταλήξουν σε μεγάλα πακέτα εφαρμογών.

Μετά την ολοκλήρωση των σταδίων του προγραμματισμού, της διαχείρισης πόρων, του ελέγχου και της παρακολούθησης, λοιπόν, είναι απαραίτητο να καταγραφούν τα συμπεράσματα και οι προτεινόμενες λύσεις σε μια αντίστοιχη βάση με αυτή της αποτύπωσης των παραγόντων κινδύνου, που ονομάζεται μητρώο διαχείρισης κινδύνου (risk management register). Η αποτύπωση, με ενιαίο κωδικοποιημένο τρόπο,

των ενεργειών διαχείρισης κινδύνων εξασφαλίζει τη διάχυση των πληροφοριών που περιέχονται στο σχέδιο διαχείρισης κινδύνου και συμβάλλει στην ουσιαστική παρακολούθηση των δράσεών του με βάση τα χρονοδιαγράμματα που περιέχονται σε αυτό. Συγκεκριμένα, το μητρώο διαχείρισης κινδύνου:

- αναφέρεται σε ένα συγκεκριμένο πίνακα και εκεί καταγράφονται όλες οι απαραίτητες ενέργειες για τη διαχείριση των παραγόντων κινδύνου που έχουν προσδιοριστεί
- περιλαμβάνει μια καταγραφή στοιχείων, σχετικά με την κατανομή πόρων για τη διαχείριση των επιμέρους παραγόντων κινδύνου
- είναι ίσως, μαζί με το μητρώο παραγόντων κινδύνου, το βασικό εργαλείο της διαδικασίας διαχείρισης κινδύνου
- απαιτεί τον καθορισμό του πιθανού υπεύθυνου διαχείρισης για κάθε παράγοντα κινδύνου
- διευκολύνεται στη χρήση του με την ανάπτυξη μιας εφαρμογής υπολογιστών, για την ταχύτερη και πληρέστερη εισαγωγή των στοιχείων στα πεδία και την ενοποίηση με την αντίστοιχη εφαρμογή για το μητρώο παραγόντων κινδύνου

Δυστυχώς, ακόμα και ένας βέλτιστος σχεδιασμός μπορεί να οδηγήσει σε προβλήματα, τα οποία ενδέχεται να έχουν ως αποτέλεσμα απόκλιση από τους αρχικούς στόχους ή και ματαίωσή τους. Οτιδήποτε παρεμβαίνει σε αυτό το σχεδιασμό μειώνει τις πιθανότητες επιτυχίας του έργου. Για το λόγο αυτό, η διαχείριση κινδύνου αποτελεί βασική και αναπόσπαστη διαδικασία της διαχείρισης έργου.

4.4 Ενδεικτικές Μεθοδολογίες Διαχείρισης Κινδύνων

Προκειμένου οι διαχειριστές να πάρουν σωστές αποφάσεις για την αποφυγή, τη μεταφορά, τον έλεγχο/περιορισμό ή την αποδοχή 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 (Δημοσχάκης, 2010).

Με τον καιρό έχει δημιουργηθεί μια πληθώρα διαδικασιών (περισσότερες από 100) που ήρθαν να καλύψουν διαφορετικές ανάγκες της διαχείρισης κινδύνων. Οι περισσότερες από αυτές διατίθενται και σε αυτοματοποιημένη μορφή, δηλαδή

επιτρέπουν τη χρήση υπολογιστή. Αν και υπάρχουν πολλές διαφορετικές διαδικασίες, η βασική μέθοδος παραμένει η ίδια. Η επιλογή της καταλληλότερης μεθόδου για τις ανάγκες μιας επιχείρησης ή οργανισμού είναι πολύ σημαντική αλλά και καθόλου εύκολη. Οι παράγοντες που δυσκολεύουν μια τέτοια επιλογή είναι οι εξής:

- Δεν υπάρχει καταγεγραμμένος πλήρης κατάλογος όλων των διαθέσιμων μεθοδολογιών με τα ιδιαίτερα χαρακτηριστικά τους.
- Δεν υπάρχει κοινά αποδεκτό σύνολο κριτηρίων αξιολόγησης για τις μεθοδολογίες.
- Κάποιες μεθοδολογίες καλύπτουν μόνο τμήματα της όλης διαδικασίας διαχείρισης κινδύνων. Για παράδειγμα, μερικές μεθοδολογίες αναφέρονται μόνο στον υπολογισμό του βαθμού επικινδυνότητας και καθόλου στην επιλογή των κατάλληλων μέτρων προστασίας. Άλλες επικεντρώνονται μόνο σε κάποιο μικρό τμήμα της όλης διαδικασίας, όπως για παράδειγμα στο σχεδιασμό διαδικασιών ανάκαμψης μετά από καταστροφή. Κάποιες μέθοδοι, επίσης, ασχολούνται μόνο με τον έλεγχο των μέτρων προστασίας και όχι με τον υπολογισμό του βαθμού ευπάθειας κ.ο.κ..
- Οι μεθοδολογίες διαφέρουν πολύ στο επίπεδο ανάλυσης που χρησιμοποιούν. Κάποιες χρησιμοποιούν υψηλού επιπέδου περιγραφές του πληροφοριακού συστήματος που μελετούν, ενώ κάποιες άλλες απαιτούν λεπτομερειακές περιγραφές.
- Μερικές μέθοδοι δε διατίθενται στην ελεύθερη αγορά, γεγονός που κάνει την αξιολόγησή τους πολύ δύσκολη, αν όχι αδύνατη.

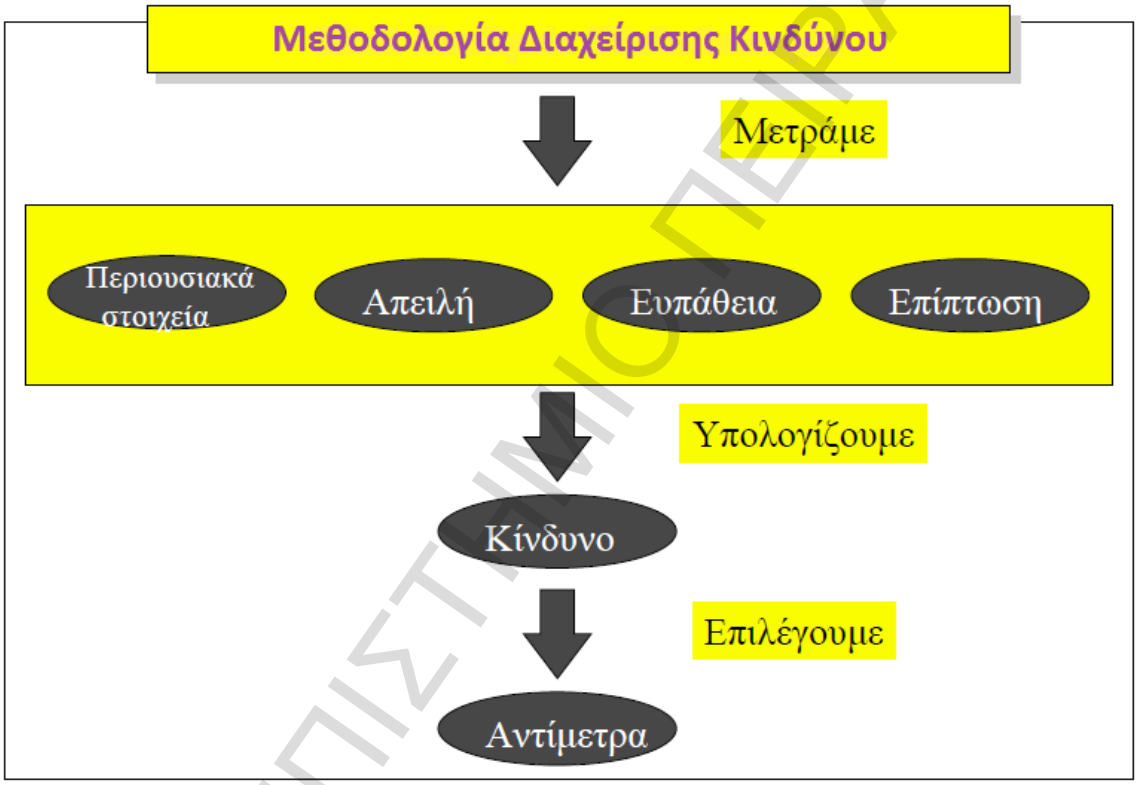
Μία μέθοδος διαχείρισης κινδύνων, λοιπόν, θα πρέπει να έχει τα παρακάτω χαρακτηριστικά:

- Να είναι δοκιμασμένη σε ανάλογου μεγέθους, πολυπλοκότητας και σημαντικότητας πληροφοριακά συστήματα.
- Να υπάρχει ικανή εμπειρία από την εφαρμογή της.
- Να ταιριάζει στα οργανωσιακά χαρακτηριστικά και στην κουλτούρα του οργανισμού.
- Να καλύπτει όλα τα στάδια της ανάλυσης κινδύνων.
- Να καλύπτει όλες τις συνιστώσες της ασφάλειας πληροφοριακού συστήματος (τεχνικές και κοινωνικές).
- Να συνοδεύεται από αυτοματοποιημένο εργαλείο με εξειδικευμένο λογισμικό.
- Να έχει σχετικά χαμηλό κόστος εφαρμογής.

Αξίζει, επίσης, να σημειωθεί ότι εκείνο που κάνουν οι μεθοδολογίες διαχείρισης κινδύνων είναι να (σχήμα 4.2):

- δημιουργούν αφηρημένο μοντέλο,
- καταγράφουν και αποτιμούν τα περιουσιακά στοιχεία,

- εκτιμούν τις επιπτώσεις από τη χρήση των τεχνολογιών πληροφορικής και επικοινωνιών (αυτές μπορεί να είναι διαρροή, τροποποίηση, καταστροφή ή μη διαθεσιμότητα),
- αναλύουν τις ευπάθειες,
- αναλύουν τις απειλές που αντιμετωπίζει το έργο,
- υπολογίζουν το βαθμό επικινδυνότητας,
- επιλέγουν και προτείνουν κατάλληλα αντίμετρα (αυτά μπορεί να είναι φυσικά, διαδικαστικά, τεχνικά ή προσωπικού) και
- παρακολουθούν την πορεία υλοποίησης των αντιμέτρων.



Σχήμα 4.2: Μεθοδολογία διαχείρισης κινδύνου.

Σύμφωνα με το παραπάνω σχήμα, η βασική μεθοδολογία διαχείρισης κινδύνων περιλαμβάνει ουσιαστικά τα εξής 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 αυτή.
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. Εδώ γίνεται προσπάθεια αναγνώρισής τους και προσδιορισμός της αξίας τους προς τον οργανισμό.

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 ευπαθές 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: $ευπάθεια = πιθανότητα\ να\ συμβεί\ μια\ απειλή \times πιθανότητα\ να\ είναι\ επιτυχής$.
5. ***Υπολογισμός του κινδύνου:*** Ο βαθμός του κινδύνου υπολογίζεται ξεχωριστά για κάθε απειλή ως προς κάθε περιουσιακό στοιχείο. Είναι συνάρτηση όλων των παραπάνω, δηλαδή:
   - των επιπτώσεων μιας απειλής (που έχουν σχέση με την αξία του περιουσιακού στοιχείου) και
   - της ευπάθειας του περιουσιακού στοιχείου ως προς την απειλή
6. ***Επιλογή τρόπων αντιμετώπισης των κινδύνων:*** Υπάρχουν 4 τρόποι αντιμετώπισης του κινδύνου, οι οποίοι αναφέρονται εκτενέστερα παραπάνω:
   i. αποφυγή του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη δραστηριότητα
   ii. μεταφορά του κινδύνου
   iii. έλεγχο/περιορισμό του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας): Με τα αντίμετρα μπορούν να επιτευχθούν τα εξής:
      - Μεταφορά κινδύνου, πχ. αγορά ασφάλειας
      - Μείωση ευπάθειας: α) μείωση πιθανότητας να συμβεί μια απειλή, π.χ. απαγορεύοντας το κάπνισμα σε μια ευαίσθητη περιοχή β) μείωση πιθανότητας μια απειλή να είναι επιτυχής, π.χ. χρήσιμοποιώντας κρυπτογράφηση, firewall κ.α.
      - Μείωση αντίκτυπου, πχ. σύστημα πυρόσβεσης
      - Μέτρα ανάνηψης/επαναφοράς, π.χ. backup

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

   iv. αποδοχή του κινδύνου
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 κ.τ.λ.. Τα αντίμετρα που έχουν επιλεχθεί ελέγχονται συνεχώς για την αποτελεσματικότητα τους. Πολλά από αυτά με τον καιρό σταματούν να συμφέρουν τον οργανισμό και πρέπει να καταργηθούν ή να αντικατασταθούν από νέα.

Μια μεθοδολογία, λοιπόν, δίνει το πλαίσιο εντός του οποίου αναπτύσσονται και εφαρμόζονται μία ή περισσότερες μέθοδοι. Με άλλα λόγια, μέθοδος είναι ένας συστηματικός και προγραμματισμένος τρόπος για να εκτελεστεί ένα έργο όσον αφορά την προσέγγιση, την εξέταση, την ανάλυση και την ερμηνεία προβλημάτων ή φαινομένων βάσει συγκεκριμένων κανόνων. Το αποτέλεσμα είναι μια αιτιολογημένη πρόταση εφαρμογής συγκεκριμένων αντιμέτρων, τα οποία μπορούν να αντιμετωπίσουν επαρκώς τις απειλές εναντίον του υπό μελέτη έργου πληροφοριακού συστήματος. Στη συνέχεια περιγράφονται αλφαβητικά οι περισσότερες, από τις υπάρχουσες, μέθοδοι και αναλύονται εκτενέστερα οι δημοφιλέστερες (Πετραντωνάκης, 2008).

4.4.1 Μεθοδολογία @RISK

Ποσοτική

Πρόκειται για ένα πρόγραμμα που χρησιμοποιεί την εξομοίωση Monte Carlo και ανήκει στην ίδια ομάδα με τα 123/Symphony/Excel, τα οποία είναι προορισμένα για ανάλυση του κινδύνου. Οι κατανομές της πιθανότητας προστίθενται στα κελιά, χρησιμοποιώντας 30 νέες κατανομές πιθανότητας οι οποίες είναι ενσωματωμένες στις συναρτήσεις. Κάνοντας χρήση μενού της γνωστής μορφής του Lotus ή του Excel, οι κατανομές αυτές επιτρέπουν στους χρήστες να επιλέξουν δειγματοληψία της μορφής Monte Carlo ή Latin Hypercube, να διαλέξουν τα εξαγόμενα διαστήματα τιμών καθώς και να εκτελέσουν προσομοίωση. Τα αποτελέσματα παρουσιάζονται γραφικά και στατιστικά και στη συνέχεια υπολογίζονται και εμφανίζονται σε μορφή αναφοράς.

4.4.2 Μεθοδολογία ALRAM (Automated Livermore Risk Analysis Methodology)

Ποσοτική

Αποτελώντας ένα σύστημα που αναπτύχθηκε αποκλειστικά για κυβερνητικές εφαρμογές, η μεθοδολογία αυτή είναι σχεδιασμένη να επιτρέπει το διαχωρισμό των συνδυασμών πόρων/απειλών, έτσι ώστε *να εξετάζονται μόνο οι υψηλής επιρροής γνωστοί κίνδυνοι*. Η μεθοδολογία αυτή επικεντρώνει την προσοχή της στην αποτελεσματικότητα των συνιστώμενων ελέγχων ασφάλειας, καθώς και των ήδη υπαρχόντων. Το ALRAM χωρίζεται σε τρεις βασικές φάσεις που περιλαμβάνουν το σχεδιασμό του έργου, την ανάλυση των κινδύνων του έργου και βέβαια τη λήψη των αποφάσεων για αυτούς τους διαπιστωμένους κινδύνους. Η αρχική φάση καθορίζει το σκοπό της ανάλυσης, τους απαραίτητους πόρους και το προσωπικό που απαιτείται, ενώ η δεύτερη φάση συλλέγει και αναλύει τα δεδομένα που συλλέχθηκαν στην πρώτη

φάση. Σε αυτή τη δεύτερη φάση, αναγνωρίζονται τα στοιχεία του κινδύνου μέσω της διαπίστωσης των ανάλογων απειλών και παρέχονται τα αποτελέσματα σαν είσοδος για την τελική φάση της λήψης των αποφάσεων. Η τελική αυτή φάση παρουσιάζει τις εκτιμήσεις του κόστους για κάθε προτεινόμενη λύση, μαζί με το πλάνο για την επιλογή και την ιεράρχηση των απειλών.

4.4.3 Μεθοδολογία ARES (Automated Risk Evaluation System Version 1.1)

Ποσοτική

Χρησιμοποιεί μια μηχανή αποτελεσμάτων, η οποία είναι βασισμένη σε κανόνες και καθοδηγούμενη από μενού και λίστα επιλογών για την περάτωση της ανάλυσης του κινδύνου. Δεν πρόκειται για ένα σύστημα βασισμένο σε αριθμούς, καθώς το ARES συλλέγει δεδομένα από το χρήστη (τοποθεσία, τηλεφωνικό αριθμό, διεύθυνση κ.τ.λ.) με οδηγίες συμπλήρωσης άδειων φορμών. Τα στοιχεία αυτά παρουσιάζουν το σύστημα ασφαλείας του υπολογιστή και του λειτουργικού τους συστήματος, μαζί με ένα μεγάλο εύρος άλλων πληροφοριών που συλλέγονται από τη λίστα των επιλογών. Τα στοιχεία που έχουν συλλεχθεί περιλαμβάνουν τα *υψηλότερα βαθμολογημένα δεδομένα* στο σύστημα, το επίπεδο πιστοποίησης του χρήστη, το επίπεδο εμπιστοσύνης του συστήματος και διάφορα άλλα πρακτικά θέματα, όπως τη διαχείριση των κωδικών κ.α.. Όταν παράγονται οι τελικές ή οι ενδιάμεσες αναφορές, το ARES συγκρίνει τις λίστες που έχουν συλλεχθεί με τους βασικούς κανόνες. Η συμπερασματική αναφορά αποτελείται από εξώφυλλο, επιστολές έγκρισης και απαρίθμηση των πιθανών κινδύνων στον υπεύθυνο ασφαλείας, δίνοντάς του τη δυνατότητα επιλογής ή διόρθωσης καθενός από τους πιθανούς κινδύνους ως μέρος της διαδικασίας επικύρωσης. Η αναφορά γράφεται σε ένα ASCII αρχείο, επιτρέποντας στον υπεύθυνο να ελέγξει επιμελώς την αποτελεσματικότητα του λογισμικού στο συγκεκριμένο εργασιακό περιβάλλον.

4.4.4 Μεθοδολογία BDSS (Bayesian Decision Support System)

Ποσοτική / Ποιοτική

Το σύστημα BDSS είναι προγραμματισμένο να συλλέγει στοιχεία αξιολόγησης και να συντάσσει ερωτήσεις οι οποίες βοηθούν στην επίλυση των πιθανών κινδύνων, χρησιμοποιώντας ποσοτικές βάσεις δεδομένων που παρέχονται από τον προμηθευτή. Πιο συγκεκριμένα, ο χρήστης μπορεί να συμπεριλάβει απειλές που είναι ειδικές ως προς τις ανάγκες του και να συλλέξει τις εμπειρίες του με τη βοήθεια ειδικών αλγορίθμων που θα επεξεργαστούν τα δεδομένα μαζί με την ποσοτική βάση γνώσης

τους. Με τον τρόπο αυτό, το μοντέλο διαλέγει ασφαλείς τρόπους για τη συλλογή των εν λόγω απειλών και των ευάλωτων σημείων. Επιπλέον, το σύστημα αξιολογεί και βαθμολογεί τις απειλές πριν και μετά την υλοποίηση της προτεινόμενης λύσης, έτσι ώστε να είναι δυνατή η παρουσίαση του προβλήματος και να γίνεται εφικτή η αποφυγή της επανάληψής αυτών των απειλών. Τα αποτελέσματα της ανάλυσης παρουσιάζονται τυπικά σε γραφικό περιβάλλον με καμπύλες κινδύνου βασισμένες στο κόστος της απώλειας και στην πιθανότητα της επανεμφάνισης. Οι κεντρικοί αλγόριθμοι του BDSS είναι βασισμένοι στο θεώρημα του Bayes και διευθύνουν την αβεβαιότητα και τις στατιστικές μεθόδους. Το λογισμικό του BDSS παράγει μια ποικιλία τυπωμένων αναφορών, καθώς και αρχεία ASCII που μπορούν να εξάγονται από το χρήστη στο διαθέσιμο χώρο του επεξεργαστή κειμένου. Υπάρχει ευελιξία όσον αφορά το πώς το BDSS θα χρησιμοποιείται. Για παράδειγμα, η ανάλυση της ευπάθειας που παρέχει η εφαρμογή του BDSS διαθέτει μια ποσοτική παρουσίαση των αδυναμιών του συστήματος προστασίας.

4.4.5 Μεθοδολογία BUDDY SYSTEM

Ποιοτική

Το BUDDY SYSTEM είναι μια αυτόματη μεθοδολογία διαχείρισης κινδύνων για περιβάλλοντα μικροϋπολογιστών και καλύπτει δύο στάδια:

1. την επισκόπηση στη λήψη αντιμέτρων
2. την ανάλυση της ασφάλειας και τη διαχείρισή της

Το συγκεκριμένο πακέτο λογισμικού μελετά το επίπεδο της ευπάθειας και είναι βασισμένο στο ήδη εγκατεστημένο σύστημα προστασίας. Ανάλογα με το επίπεδο των πληροφοριών που επεξεργάζονται στο σύστημα, διαπιστώνεται αν το επιθυμητό επίπεδο ευπάθειας είναι αποδεκτό. Συνιστώμενες ενέργειες για τη διόρθωση κάθε ευπάθειας που ξεφεύγει από το επιθυμητό εύρος παρέχονται μέσω της χρήσης των δυναμικών “what if” σεναρίων. Μια βάση δεδομένων που περιέχει πάνω από 100 συστήματα προστασίας περιέχεται στο πακέτο λογισμικού. Περαιτέρω, η διαχείριση κινδύνου από τα σύστημα επιτρέπει στον αναλυτή να παρακολουθεί τις προτεινόμενες διορθωτικές ενέργειες μέσω αναφορών.

4.4.6 Μεθοδολογία CCA (Cause-Consequence Analysis)

Ποσοτική / Ποιοτική

Η CCA είναι ένα μείγμα από FAULT TREE ANALYSIS και EVENT TREE ANALYSIS. Συνδυάζει ανάλυση αιτιών και ανάλυση αποτελεσμάτων με τη βοήθεια των δύο τεχνικών. Σκοπός της CCA είναι ο προσδιορισμός αλυσίδας γεγονότων που οδηγούν σε πτώση. Με τη βοήθεια πιθανοθεωρητικών μοντέλων καθορίζεται η επικινδυνότητα των γεγονότων και το ρίσκο του συστήματος.

4.4.7 Μεθοδολογία COBRA (Consultative, Objective & Bi-functional Risk Analysis)

Ποιοτική

Το εργαλείο COBRA είναι ένα από τα πιο παλιά που κυκλοφορούν στην αγορά. Σχεδιάστηκε από την εταιρεία C&A Security Systems Ltd και έχει φτάσει σήμερα στην έκδοση 3. Χρησιμοποιεί την δική του μέθοδο για διαχείριση κινδύνων, η οποία βοηθάει στην επίτευξη συμμόρφωσης με το διεθνές στάνταρ ISO17799/BS7799. Ένα από τα σημαντικότερα πλεονεκτήματά του είναι η αυτόματη προσαρμογή της διαχείρισης κινδύνων στις συγκεκριμένες ανάγκες του κάθε οργανισμού. Επίσης, για πιο απαιτητικές αναλύσεις επιτρέπεται η πλήρης 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 COBRA έχει τη δυνατότητα δημιουργίας αναφορών επαγγελματικού επιπέδου που δε 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 στη διοίκηση του οργανισμού.

Το COBRA “τρέχει” σε πλατφόρμα MS Windows με ελάχιστες απαιτήσεις, αλλά και με interface που παραπέμπει σε λίγο παλαιότερες εποχές.

4.4.8 Μεθοδολογία CONTROL-IT

Ποιοτική

Πρόκειται για έλεγχο με προσέγγιση φύλλου εργασίας. Το λογισμικό αυτό παρέχει μια προσέγγιση ελέγχου με χρήση φύλλων εργασίας για το σχεδιασμό των ελέγχων μέσα σε μικροεπεξεργαστικά περιβάλλοντα. Αναγνωρίζει ποιοι έλεγχοι είναι απαραίτητοι για τη διασφάλιση των επαρκών ασφαλειών της επιχείρησης ή των

επιστημονικών συστημάτων. Το πακέτο λογισμικού περιέχει τέσσερα ξεχωριστά συστήματα:

- Το 1ο πακέτο (σχεδιασμός ελέγχων σε υπολογιστικά συστήματα) είναι ένα εκπαιδευτικό εργαλείο που διδάσκει το χρήστη πώς να σχεδιάζει και να αναπτύσσει έναν πίνακα ελέγχου.
- Το 2ο πακέτο (αξιολόγηση των κινδύνων του πίνακα) διδάσκει τη χρήση των Delphi και τη σύγκριση κινδύνων για την αξιολόγηση των απειλών και των ελέγχων τους.
- Το 3ο πακέτο (αυτοματοποιημένος σχεδιασμός πίνακα ελέγχου από υπολογιστή) είναι ένα πακέτο υλοποίησης πινάκων ελέγχου που περιέχει μια βάση δεδομένων από ελέγχους καθώς και μια ξεχωριστή βάση από απειλές και εξαρτήματα υπολογιστή. Το πακέτο αυτό επιτρέπει σε κάποιον να σχεδιάσει έναν πρόχειρο πίνακα ελέγχου, να αναζητήσει τη βάση δεδομένων από ελέγχους και να τους μεταφέρει σε μια λίστα από πίνακες ελέγχου.
- Το 4ο πακέτο (προβολή κειμένου και παρουσίαση γραφικών) χρησιμοποιείται για το σχεδιασμό του τελικού πίνακα από τις ακολουθίες απειλών, εξαρτημάτων και ελέγχων.

4.4.9 Μεθοδολογία CORA (Cost Of Risk Analysis)

Ποσοτική

Η βοήθεια που προσφέρει το σύστημα CORA διατίθεται σε δύο διαδικασίες. Πρώτα, το CORA παρέχει ένα περιβάλλον για να οργανώσει, να συλλέξει, να αποθηκεύσει και να πιστοποιήσει δεδομένα που περιγράφουν τον κίνδυνο και τις εκθέσεις σε απώλειες μιας επιχείρησης. Επίσης, χρησιμοποιεί σκεπτόμενους αλγόριθμους για να κατασκευάσει ένα ποσοτικό μοντέλο κινδύνου. Πιο συγκεκριμένα, υπολογίζει το *κόστος απλού συμβάντος (SOL)* και προβάλλει τα αποτελέσματα γραφικά. Ακολούθως, οι χρήστες του μπορούν να πειραματιστούν με το ποσοτικό μοντέλο της επιχείρησης για να εκτελέσουν *εκτιμήσεις διαχείρισης κινδύνου* και να διαπιστωθεί το πακέτο των βέλτιστων λύσεων. Αυτό το πακέτο λογισμικού αντικαθιστά επάξια τα IST/RAMP και το CRITI-CALC. Το CORA έχει μοναδικά χαρακτηριστικά:

- Μπορεί να εισάγει βασικά στοιχεία από το βασικό πληροφοριακό σύστημα της επιχείρησης, οπότε είναι δε θέση να συλλέγει δεδομένα που είναι έγκυρα.
- Οι ειδικοί μπορούν να καθορίσουν παράγοντες κινδύνου και να τους αποθηκεύσουν ως αρχεία “risk rules”. Έτσι, έχουν τη δυνατότητα να προσαρμόσουν πλήρως τις ιδιότητες της διαχείρισης.
- Ο Financial Simulator ενισχύει τα οικονομικά αποτελέσματα.
- Έχει βάση δεδομένων που επιτρέπει τη βέλτιστη ανάκτηση δεδομένων των IT Systems.

4.4.10 Μεθοδολογία CRAMM (CCTA Risk Analysis and Management Methodology)

Ποιοτική

Η CRAMM είναι ένα τυπικό σύστημα διαχείρισης κινδύνου, το οποίο αναπτύχθηκε το 1985 από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (CCTA - Central Computer and Telecommunications Agency) της Βρετανικής Κυβέρνησης, ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο διαχείρισης κινδύνων πληροφοριακών συστημάτων. Το συγκεκριμένο εργαλείο, το οποίο έχει υποστεί σημαντικές αναθεωρήσεις και βρίσκεται σήμερα στην έκδοση 5, συνεχίζει να αναπτύσσεται πλέον από την εμπορική εταιρεία Insight Consulting που έχει έδρα στην Αγγλία. Η CRAMM έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε παραπάνω από 500 οργανισμούς σε 23 χώρες, συμπεριλαμβανομένου και του NATO. Ακολουθεί τη δική της μέθοδο, η οποία αποτιμά και βοηθάει τους οργανισμούς να επιτύχουν συμμόρφωση με το διεθνές στάνταρ ISO17799/BS7799. Αποτελείται από τρία στάδια, το καθένα από τα οποία υποστηρίζεται από ερωτηματολόγια και οδηγίες καθοδήγησης.

Το 1^{ο} στάδιο (προσδιορισμός και αξιολόγηση των αγαθών) εκτελεί μια αξιολόγηση των βοηθημάτων του συστήματος ή του δικτύου. Από τη διαδικασία αυτή καθορίζονται οι ποιοτικές τιμές για τα βοηθητικά δεδομένα σε κλίμακα από το 1 έως το 10, ταξινομημένα σύμφωνα με τις πιθανές παρενέργειες των αλλαγών, της έλλειψης διαθεσιμότητας και της καταστροφής. Τα φυσικά βοηθήματα κοστολογούνται και με κριτήριο την αντικατάσταση ή το κόστος της επιδιόρθωσης και μετατρέπονται σε κλίμακα από 1 έως 10. Οπουδήποτε η τιμή των βοηθημάτων είναι χαμηλή (<3) το σύστημα τίθεται υπό αξιολόγηση. Αυτό είναι το πρώτο στάδιο βασικής προστασίας και τα αποτελέσματά του προωθούνται στο επόμενο στάδιο.

Το 2ο στάδιο (ανάλυση επικινδυνότητας) εξακριβώνει τις απειλές και τα ελαττώματα κάθε ομάδας βοηθημάτων και βαθμολογεί το εκάστοτε ζευγάρι σε κλίμακα 1 έως 5, όπου το 5 αντανακλά το χειρότερο σενάριο.

Το 3ο στάδιο (διαχείριση επικινδυνότητας) αφορά την επιλογή των συστημάτων ασφαλείας και αναφέρεται σε μια βιβλιοθήκη με περισσότερες από 900 εφαρμογές. Ακολούθως, η διαχείριση στοχεύει στη λήψη απόφασης για το καταλληλότερο σύστημα ασφαλείας και η CRAMM παρέχει λειτουργίες που προορίζονται για τη διερεύνηση αυτών των επιλογών. Ένα εύρος από αναφορές διαχείρισης είναι διαθέσιμες.

Το λογισμικό CRAMM παρέχει, επίσης, ένα σύστημα κωδικού ασφαλείας για τη μείωση των κινδύνων από μη εξουσιοδοτημένη πρόσβαση στα δεδομένα που αναλύονται. Ενδείξεις που υποδηλώνουν την ευαισθησία των πληροφοριών παρέχονται σε όλες τις οθόνες καθώς και στο τυπωμένο αντίτυπο αυτών.

Για την επιτυχία της μεθόδου CRAMM απαιτείται, αρχικά, ικανοποιητική συνεργασία ανάμεσα στην ομάδα των τεχνικών εμπειρογνωμόνων ασφαλείας και στην επιτροπή παρακολούθησης του έργου, ως εκπροσώπων της διοίκησης του φορέα. Πέραν της συνήθους αναγκαιότητας για ικανοποιητική συνεργασία, η ανάδραση που παρέχει η επιτροπή παρακολούθησης του έργου σε όλη τη διάρκεια μελέτης του είναι

καθοριστική για τον επιτυχή προσδιορισμό και την αξιολόγηση των αγαθών του υπό εξέταση συστήματος, καθώς και για την επιβεβαίωση του βαθμού επικινδυνότητας.

Επιπλέον, απαιτείται προσεκτική επιλογή του δείγματος για τη διενέργεια συνεντεύξεων, με αρμόδια στελέχη σε διάφορα επίπεδα ιεραρχίας και ειδικότητας, ώστε να εξασφαλίζεται στους αναλυτές ασφαλείας πλήρης εικόνα, κυρίως κατά το στάδιο της αποτίμησης των αγαθών/περιουσιακών στοιχείων που πρέπει να προστατευτούν.

Σημαντική παράμετρο και βασική προϋπόθεση διασφάλισης ενός ελάχιστου πλαισίου επιτυχίας αποτελεί η συναποδοχή του χώρου – πλαισίου εργασίας και η ακριβής οριοθέτηση της μελέτης. Σε αντίθετη περίπτωση, υπάρχει διαρκής δυσκολία προσδιορισμού των ενεργειών, των διαδικασιών και των παραμέτρων που είναι εξωτερικές στο υπό μελέτη σύστημα και ως εξωτερικές και μόνο θα πρέπει να αντιμετωπιστούν.

Πλεονεκτήματα CRAMM

Το μεθοδολογία CRAMM παρουσιάζει τα εξής πλεονεκτήματα:

- Αποτελεί πρότυπη μεθοδολογία και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλης κλίμακας οργανισμούς και επιχειρήσεις κοινής ωφέλειας.
- Έχει δοκιμαστεί με επιτυχία και υπάρχει μεγάλη διεθνής εμπειρία από την εφαρμογή της.
- Καλύπτει όλες τις φάσεις της ανάλυσης και διαχείρισης κινδύνων, με δυνατότητα προσαρμογής στις ανάγκες κάθε οργανισμού (σε συνεννόηση με την εταιρεία).
- Καλύπτει όλες τις συνιστώσες της ασφάλειας (πχ. θέματα προσωπικού, διαδικασιών, τεχνικά θέματα, φυσική ασφάλεια κ.λπ.), καθώς περιέχει μια τεράστια βάση αντιμέτρων (3000 αντίμετρα) που ανανεώνεται συνεχώς.
- Συνοδεύεται από αυτοματοποιημένο εργαλείο που διευκολύνει την εφαρμογή της και επιλέγει τα αντίμετρα από βιβλιοθήκη αντιμέτρων.

Μειονεκτήματα CRAMM

Τα μειονεκτήματα της CRAMM είναι τα ακόλουθα:

- Εξαρτάται σε μεγάλο βαθμό από τη συνεργασία των αναλυτών με τους χρήστες και τη διοίκηση του οργανισμού, είναι, δηλαδή, άμεσα συνυφασμένο με τις δικές τους υποκειμενικέ απόψεις.

- Έχει υψηλό κόστος εφαρμογής (χρόνος και ανθρώπινη προσπάθεια), καθώς η χρήση του δεν είναι ιδιαίτερα απλή, με αποτέλεσμα να απαιτείται εκπαίδευση και εξοικείωση για να επιτευχθούν τα βέλτιστα αποτελέσματα..
- Απαιτεί μερικές φορές την επέμβαση του αναλυτή για την προσαρμογή των αποτελεσμάτων των αυτοματοποιημένων υπολογισμών στα ιδιαίτερα χαρακτηριστικά του υπό μελέτη πληροφοριακού συστήματος.
- Απαιτεί επεξεργασία του συνόλου των προτεινόμενων αντιμέτρων (ομαδοποίηση, εξειδίκευση, κ.λπ.) για την προσαρμογή τους στο υπό μελέτη πληροφοριακό σύστημα.

4.4.11 Μεθοδολογία CRITI-CALC

Ποσοτική / Ποιοτική

Αυτό το προϊόν χρησιμοποιεί τη μέθοδο της ετήσιας προσδοκώμενης απώλειας (ALE) για τον προσδιορισμό της ποσότητας και της κρισιμότητας του κινδύνου, κάτω από τις οποίες είναι εκτεθειμένες οι εφαρμογές. Το συγκεκριμένο λογισμικό συλλέγει πληροφορίες για κάθε πιθανού είδους αστοχία της εφαρμογής, για το κόστος της λήψης αντιγράφων ασφαλείας καθώς και για το κόστος της ανάκτησής τους. Στη συνέχεια, χρησιμοποιεί αυτές τις πληροφορίες για τον υπολογισμό της ετήσιας προσδοκώμενης απώλειας για κάθε εφαρμογή. Η κρισιμότητα κάθε εφαρμογής καθορίζεται από την πιθανότητα της απώλειας δεδομένων, η οποία μπορεί να προέρχεται είτε από διακοπή της επεξεργασίας είτε από μια συλλογή 14 πιθανών παραγόντων καθυστέρησης. Ο χρήστης αλληλεπιδρά με το σύστημα χρησιμοποιώντας οθόνες, οι οποίες προβάλλουν πληροφορίες για την τρέχουσα έκθεση που βρίσκεται σε κίνδυνο. Όταν ο χρήστης έχει λάβει γνώση για τα αρχικά δεδομένα, μια ανάλυση του τύπου “what if” εκτελείται, μεταβάλλοντας τα υπάρχοντα δεδομένα ως μια μέθοδο πιστοποίησης της αποτελεσματικότητας των συστημάτων ασφαλείας. Οι πληροφορίες που περιέχονται στις αναφορές που παράγονται μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση των σχεδίων αντιμετώπισης απρόοπτων συμβάντων. Η ALE, σα συνάρτηση με παράγοντα τη μέγιστη διάρκεια διακοπής λειτουργίας, είναι συγκρίσιμο μέγεθος με το κόστος της λήψης αντιγράφων ασφαλείας και με την αυτόματη βέλτιστη ανάκτηση των δεδομένων.

4.4.12 Μεθοδολογία DETAM (Dynamic Event Tree Analysis Method)

Ποσοτική / Ποιοτική

Η DETAM είναι μια μεθοδολογία η οποία χειρίζεται τη χρονική ανάπτυξη του υλικού του συστήματος και υπολογίζει μεταβλητές τιμές με τη βοήθεια ενός σεναρίου

κρίσεως. Γενικά, ένα δυναμικό δέντρο είναι ένα δέντρο γεγονότων στο οποίο επιτρέπεται η διακλάδωση σε διαφορετικά χρονικά σημεία. Αυτή η προσέγγιση περιέχει πέντε χαρακτηριστικά:

- σύνολο διακλαδώσεων
- σύνολο μεταβλητών που καθορίζουν το σύστημα
- κανόνες διακλαδώσεων
- συχνότητα επέκτασης κανόνα
- ποσοτικά εργαλεία

Το σύνολο των διακλαδώσεων αναφέρεται στις μεταβλητές που καθορίζουν το χώρο των πιθανών διακλαδώσεων για κάθε κόμβο του δέντρου. Οι κανόνες διακλάδωσης, από την άλλη μεριά, αναφέρονται σε κανόνες που καθορίζουν ποιο κλαδί πρέπει να λάβει μέρος. Η προσέγγιση αυτή μπορεί να χρησιμοποιηθεί για την αναπαράσταση ενός ευρύτερου πλήθους συμπεριφορών τελεστών, ενώ παράλληλα μοντελοποιεί τις συνέπειες της πράξης ενός τελεστή και λειτουργεί ως πλαίσιο λήψης αποφάσεων για το διαχειριστή του συστήματος. Τέλος, επιτρέπει τη δοκιμή διαδικασιών κινδύνου για την εξαγωγή χρήσιμων συμπερασμάτων.

4.4.13 Μεθοδολογία DIGRAPH MATRIX ANALYSIS ή FAULT GRAPH METHOD

Ποσοτική / Ποιοτική

Η μεθοδολογία DIGRAPH MATRIX ANALYSIS ή FAULT GRAPH METHOD χρησιμοποιεί μαθηματικά και γραφήματα στηριζόμενα στη θεωρία γραφημάτων, όπως ειδικότερα το “path set” (ένα σύνολο από μοντέλα που κινούνται σε ένα μονοπάτι) και το “reachability” (το ολικό σύνολο όλων των πιθανών μονοπατιών μεταξύ δύο κόμβων).

Η μέθοδος αυτή χρησιμοποιεί λογικές πύλες and και or. Ο πίνακας συνδεσιμότητας φανερώνει αν ένας ελαττωματικός κόμβος θα οδηγήσει στην κορυφή του γραφήματος, ενώ οι μετρήσεις δείχνουν αν απλοί κόμβοι ή ζευγάρια κόμβων οδηγούν σε πτώση του συστήματος. Η DIGRAPH MATRIX ANALYSIS ή FAULT GRAPH METHOD επιτρέπει βρόχους ανάδρασης (feedback loops), οι οποίοι ενισχύουν τη δυναμικότητα του συστήματος.

4.4.14 Μεθοδολογία EVENT TREE ANALYSIS

Ποσοτική / Ποιοτική

Η EVENT TREE ANALYSIS είναι μια μεθοδολογία η οποία παρουσιάζει τη συχνότητα των αποτελεσμάτων που εμφανίζονται μετά την υλοποίηση ενός επιλεγμένου αρχικού γεγονότος. Χρησιμοποιείται, κυρίως, για την ανάλυση επιπτώσεων προ-καταστροφικών φαινομένων και μετα-καταστροφικών καταστάσεων, ενώ χρησιμοποιείται, επίσης, στον προσδιορισμό κρίσεων σε πυρηνικά εργοστάσια.

4.4.15 Μεθοδολογία FAULT TREE ANALYSIS

Ποσοτική / Ποιοτική

Η μεθοδολογία FAULT TREE ANALYSIS είναι ένα λογικό διάγραμμα, το οποίο δείχνει τη σχέση μεταξύ πτώσης συστήματος και πτώσης των στοιχείων του συστήματος. Είναι μια τεχνική που στηρίζεται σε αφαιρετική λογική. Πρώτα ορίζεται ένα ανεπιθύμητο γεγονός και προσδιορίζονται οι σχέσεις μεταξύ των πτώσεων.

Η FAULT TREE ANALYSIS μπορεί να χρησιμοποιηθεί τόσο ποιοτικά όσο και ποσοτικά. Η διαφορά μεταξύ τους είναι ότι η ποιοτική ανάλυση είναι πιο χαλαρή και δεν απαιτεί αυστηρή λογική, όπως η ποσοτική

4.4.16 Μεθοδολογία FMEA (Failure Mode Effect Analysis)

Ποιοτική

Το FMEA είναι ένα εργαλείο βελτίωσης ποιότητας, το οποίο σε αντίθεση με άλλα αντίστοιχα εργαλεία, παράγει σημαντικά αποτελέσματα χωρίς να απαιτεί πολύπλοκες στατιστικές αναλύσεις. Πρόκειται για μια συστηματική μέθοδο αναγνώρισης και πρόληψης προβλημάτων σε προϊόντα και διαδικασίες πριν αυτά εμφανιστούν. Τα FMEA εστιάζουν στην πρόληψη σφαλμάτων, στη βελτίωση της ασφάλειας και στην αύξηση της ικανοποίησης των πελατών.

Σκοπός των εργαλείων FMEA είναι η πρόληψη προβλημάτων στις διαδικασίες και στα προϊόντα. Με τη χρήση τους στις διαδικασίες σχεδίασης και κατασκευής βοηθούν σημαντικά στη μείωση του κόστους, αναγνωρίζοντας δυνατές βελτιώσεις στα αρχικά στάδια των προαναφερθέντων διαδικασιών, όταν οι αλλαγές είναι ακόμα εύκολες και φθηνές. Το αποτέλεσμα είναι η μείωση ή ακόμα και η εξάλειψη της ανάγκης λήψης μέτρων εκ των υστέρων, που μπορούν να οδηγήσουν ακόμα και σε κρίσεις στα τελικά στάδια της διαδικασίας.

Στόχος μιας μελέτης FMEA είναι ο εντοπισμός όλων των τρόπων με τους οποίους ένα προϊόν ή μια διεργασία μπορούν να παρουσιάσουν πρόβλημα. Οι τρόποι αυτοί ονομάζονται καταστάσεις αποτυχίας και κάθε ένας έχει κάποια πιθανότητα να συμβεί, η οποία ονομάζεται σχετικό ρίσκο. Κάθε κατάσταση αποτυχίας έχει ορισμένες ενδεχόμενες συνέπειες, μερικές από τις οποίες είναι πιο πιθανές από κάποιες άλλες. Η αξιολόγηση των παραπάνω περιλαμβάνει τους εξής τρεις παράγοντες:

- Σοβαρότητα (Severity): Οι επιπτώσεις στην περίπτωση που παρουσιαστεί το πρόβλημα.
- Εμφάνιση (Occurrence): Η πιθανότητα ή η συχνότητα εμφάνισης του προβλήματος.
- Εντοπισμός (Detection): Η πιθανότητα να εντοπιστεί το πρόβλημα πριν γίνει αντιληπτός ο αντίκτυπός του.

Καθένας από τους παραπάνω παράγοντες αποτιμάται σε μια κλίμακα από το 1 έως το 10 και στη συνέχεια πολλαπλασιάζονται οι τρεις αριθμοί. Το αποτέλεσμα που προκύπτει ονομάζεται αριθμός προτεραιότητας ρίσκου (risk priority number, RPN) και παίρνει τιμές μεταξύ του 1 και του 1000. Ο RPN χρησιμοποιείται για να κατατάξουμε σε σειρά προτεραιότητας τις διορθωτικές κινήσεις που απαιτείται να γίνουν, ώστε να εξαλειφθούν ή να μειωθούν οι καταστάσεις αποτυχίας. Οι καταστάσεις αποτυχίας με το μεγαλύτερο RPN πρέπει να αντιμετωπιστούν πρώτα, αλλά πρέπει να δοθεί μεγάλη προσοχή και στις περιπτώσεις που η αποτίμηση της σοβαρότητας (severity) είναι υψηλή (9 ή 10) ανεξάρτητα από τον RPN.

Μετά τις διορθωτικές κινήσεις, η σοβαρότητα (severity), η εμφάνιση (occurrence) και ο εντοπισμός (detection) αποτιμώνται ξανά και έτσι προκύπτει ένας νέος RPN. Η διαδικασία αυτή επαναλαμβάνεται με συνεχείς βελτιώσεις και διορθωτικές κινήσεις μέχρι ο RPN να φτάσει σε αποδεκτές τιμές για όλες τις καταστάσεις αποτυχίας. Όλα τα FMEA προϊόντος και διαδικασίας ακολουθούν τα παρακάτω βήματα:

ΒΗΜΑ 1: Μελέτη προϊόντος/διαδικασίας.

ΒΗΜΑ 2: Brainstorming για πιθανά προβλήματα.

ΒΗΜΑ 3: Απαρίθμηση ενδεχόμενων συνεπειών για κάθε πρόβλημα.

ΒΗΜΑ 4: Αποτίμηση του παράγοντα σοβαρότητας (severity) για κάθε συνέπεια.

ΒΗΜΑ 5: Αποτίμηση του παράγοντα εμφάνισης (occurrence) για κάθε πρόβλημα.

ΒΗΜΑ 6: Αποτίμηση του παράγοντα εντοπισμού (detection) για κάθε πρόβλημα ή/και συνέπεια.

ΒΗΜΑ 7: Υπολογισμός του αριθμού προτεραιότητας ρίσκου για κάθε συνέπεια.

ΒΗΜΑ 8: Απόδοση προτεραιότητας αντιμετώπισης κάθε προβλήματος.

ΒΗΜΑ 9: Λήψη μέτρων για τα προβλήματα υψηλής προτεραιότητας.

ΒΗΜΑ 10: Υπολογισμός των νέων αριθμών προτεραιότητας ρίσκου.

Πλεονεκτήματα FMEA

Το σύστημα FMEA παρουσιάζει τα εξής πλεονεκτήματα:

- Είναι απλό στην προετοιμασία και στην υλοποίηση.
- Δεν απαιτεί πολύ χρόνο για την ολοκλήρωσή του.
- Δεν απαιτεί πολύπλοκες στατιστικές αναλύσεις.
- Οι ομάδες FMEA αποτελούνται από λίγα άτομα.
- Πληροί τις προϋποθέσεις του συστήματος QS-9000.

Μειονεκτήματα FMEA

Τα μειονεκτήματα του FMEA είναι τα ακόλουθα:

- Θα μπορούσε να χαρακτηριστεί «απλοϊκό».
- Βασίζεται αποκλειστικά στον ανθρώπινο παράγοντα, οπότε μπορεί να υπάρχουν λανθασμένες εκτιμήσεις.
- Δεν υποστηρίζεται από κάποιο σοβαρό λογισμικό.
- Ο δείκτης RPN δεν είναι αποδεκτός σε όλους τους χώρους δεδομένων και συστημάτων εφαρμογών.

4.4.17 Μεθοδολογία FRAP (Facilitated Risk Analysis Process)

Ποιοτική

Η μέθοδος FRAP σχεδιάστηκε ως μια αποδοτική και πειθαρχημένη διαδικασία για τη διασφάλιση ότι οι κίνδυνοι στην λειτουργία ενός οργανισμού που σχετίζονται με τα πληροφοριακά συστήματα αναγνωρίζονται και καταγράφονται. Η διαδικασία ορίζει την ανάλυση ενός συστήματος ή μιας εφαρμογής κάθε φορά. Συνέρχεται μια ομάδα ατόμων που περιλαμβάνει μέλη από τη διοίκηση που είναι εξοικειωμένα με τις πληροφοριακές ανάγκες του οργανισμού, καθώς και από το τεχνικό προσωπικό που έχουν λεπτομερή γνώση του συστήματος που εξετάζεται, των ευπαθειών του και των αντίμετρων που υπάρχουν για να τις αντιμετωπίσουν. Οι συσκέψεις της ομάδας, οι οποίες ακολουθούν συγκεκριμένο πρόγραμμα, υποβοηθούνται από ένα άτομο που είναι υπεύθυνο για το συντονισμό της διαδικασίας, τη διασφάλιση της σωστής επικοινωνίας μεταξύ των μελών της ομάδας και την τήρηση του προγράμματος. Το άτομο αυτό ονομάζεται «οργανωτής» του συστήματος FRAP.

Κατά τη διάρκεια της σύσκεψης, η ομάδα ανταλλάζει ιδέες για την αναγνώριση των ενδεχόμενων απειλών, των ευπαθειών και των επακόλουθων αντίκτυπων στην ακεραιότητα, στην εμπιστευτικότητα και στη διαθεσιμότητα των δεδομένων. Στη συνέχεια, η ομάδα αναλύει τις συνέπειες των αντίκτυπων αυτών στη λειτουργία του οργανισμού και κατατάσσει τους κινδύνους με βάση προτεραιότητας. Δεν προσπαθεί να ψάξει ή να καθορίσει συγκεκριμένους αριθμούς για την πιθανότητα των απειλών ή το ποσό των απωλειών, εκτός και αν αυτά τα δεδομένα υπάρχουν ήδη. Αντίθετα, βασίζεται στην γνώση και την εμπειρία των μελών της, καθώς και στη γενική γνώση που προκύπτει για τις απειλές και ευπάθειες από τη διεθνή βιβλιογραφία, τον τύπο, το internet κ.τ.λ..

Μετά την αναγνώριση και κατηγοριοποίηση των κινδύνων, η ομάδα επιλέγει τα αντίμετρα που θα μπορούσαν να υλοποιηθούν για την αντιμετώπιση τους, εστιάζοντας κυρίως, σε αυτά που έχουν τον καλύτερο λόγο κόστους/οφέλους. Ως σημείο εκκίνησης έχει μια λίστα από 26 γενικά αντίμετρα που έχουν σχεδιαστεί για να αντιμετωπίζουν διάφορους τύπους κινδύνων. Κατά τη διάρκεια της ανάλυσης μπορεί να συμφωνηθεί η προσθήκη νέων αντίμετρων στη λίστα. Η τελική απόφαση για το ποια αντίμετρα χρειάζονται ανήκει στη διοίκηση του οργανισμού, η οποία λαμβάνει υπόψη τη φύση των πληροφοριών, τη σημασία τους στη λειτουργία του οργανισμού και το κόστος των αντιμέτρων.

Τα συμπεράσματα της ομάδας για τους κινδύνους που υφίστανται, την προτεραιότητα τους και τα αντίμετρα που χρειάζονται καταγράφονται και στέλνονται στον υπεύθυνο του έργου (project leader) και στο διευθυντή του συγκεκριμένου τμήματος του οργανισμού για την επεξεργασία τους και την κατάρτιση του σχεδίου δράσης (action plan). Σε αυτό το σημείο, ένας ειδικός για θέματα ασφαλείας μπορεί να βοηθήσει το διευθυντή να προσδιορίσει ποια αντίμετρα προσφέρουν καλό λόγο κόστους/οφέλους και ικανοποιούν της ανάγκες του οργανισμού. Όταν κάθε κίνδυνος έχει αντιμετωπιστεί ή αποδεχτεί, υπογράφεται το ολοκληρωμένο κείμενο της ανάλυσης κινδύνων και η διαδικασία τελειώνει.

Η μεθοδολογία FRAP μπορεί να χωριστεί σε τέσσερα μέρη:

1. Την αρχική σύσκεψη, η οποία διαρκεί περίπου μια ώρα και περιλαμβάνει το διευθυντή, τον υπεύθυνο του έργου και τον οργανωτή της FRAP.
2. Την κυρίως σύσκεψη, που διαρκεί περίπου τέσσερις ώρες και στην οποία συμμετέχουν 7-15 άτομα (αν και έχουν γίνει με επιτυχία συσκέψεις από 4 έως και 50 άτομα).
3. Την ανάλυση FRAP και τη δημιουργία της αναφοράς (report), η οποία διαρκεί συνήθως 4-6 μέρες και ολοκληρώνεται από τον «οργανωτή» του FRAP και τον γραμματέα.
4. Την τελική σύσκεψη, που διαρκεί περίπου μια ώρα και συμμετέχουν τα ίδια άτομα με την αρχική σύσκεψη.

4.4.18 Μεθοδολογία GRA/SYS

Ποιοτική

Το GRA/SYS είναι ένα εργαλείο σχεδιασμένο για την προσφορά βοήθειας στους εσωτερικούς ελεγκτές και στο προσωπικό ασφαλείας, ώστε να αναπτύσσουν ένα σχέδιο καθορισμού προτεραιοτήτων για την εποπτεία των κινδύνων της επιχείρησης. Πιο συγκεκριμένα, το λογισμικό προετοιμάζει την εφαρμογή και τη δραστηριότητα των υπολογιστών, καθώς επίσης καθορίζει τον αριθμό των κινδύνων για διάφορες περιοχές ελέγχου ύψιστης σημασίας. Θέτει βαθμολογίες κινδύνου, οι οποίες αντικατοπτρίζουν το βαθμό επικινδυνότητας στην επιχείρηση όπου υπολογίζεται και δίνεται προτεραιότητα κατά φθίνουσα σειρά σε κλίμακα από 1 έως 9, με το 9 να αναπαριστά τη χειρότερη περίπτωση. Προετοιμάζεται, επιπλέον, μια αναφορά που αντικατοπτρίζει το πλήθος των φορών που κάθε κίνδυνος συμβαίνει ή πρόκειται να συμβεί. Χρησιμοποιώντας τις παραγόμενες αναφορές από αυτό το πακέτο λογισμικού, ο χρήστης είναι ικανός να αναγνωρίζει τους κινδύνους στους οποίους απαιτούνται πιο αποτελεσματικά συστήματα ασφαλείας.

4.4.19 Μεθοδολογία IST/RAMP (International Security Technology / Risk Analysis Management Program)

Ποσοτική

Το IST/RAMP είναι ένα λογισμικό που παραμένει στον κεντρικό υπολογιστή και αναλαμβάνει την ανάλυση κινδύνου με μια αυτοτελή μονάδα εισόδου, η οποία εγκαθίσταται στον υπολογιστή. Το λογισμικό υπολογίζει την ετήσια προσδοκώμενη απώλεια καθώς και την απώλεια ενός και μοναδικού συμβάντος. Το σύστημα μπορεί να παρέχει, επίσης, και ποιοτική ανάλυση. Το IST/RAMP παράγει φόρμες συλλογής δεδομένων για να βοηθήσει την ανάλυση κινδύνου, τη βέλτιστη οργάνωση και τον έλεγχο της συλλογής δεδομένων. Καθορίζονται πέντε κατηγορίες απωλειών:

- διακοπή υπηρεσιών
- φυσική απώλεια και ζημιά
- απάτη
- μη εξουσιοδοτημένη αποκάλυψη απορρήτων
- φυσική κλοπή

Μια βιβλιοθήκη από βάσεις δεομένων επιτρέπουν στον αναλυτή να συντηρεί τα ίχνη των αλλαγών στα δεδομένα εισόδου. Η δυνατότητα για χρήση του “what if” επιτρέπει στον αναλυτή να διαλέγει τα πιο συμφέροντα, από άποψη κόστους, αντίμετρα ασφαλείας.

Το RAMP↔LINK είναι ένα καθοδηγούμενο από μενού σύστημα εισαγωγής δεδομένων, το οποίο χρησιμοποιεί τις πληροφορίες κινδύνου, που εισάγονται από τον αναλυτή για τη δημιουργία ενός αρχείου που μπορεί να μεταφορτωθεί στο IST/RAMP για επεξεργασία.

4.4.20 Μεθοδολογία JANBER

Ποιοτική

Το JANBER ενεργοποιεί ένα ερωτηματολόγιο ναι/όχι και μια λίστα επιλογών για τη συλλογή πληροφοριών του ήδη υπάρχοντος συστήματος ασφαλείας. Το λογισμικό ζυγίζει τα τοποθετημένα συστήματα ασφαλείας και τα μετρά σε σχέση με την ταξινόμηση προτεραιότητας των δεδομένων που επεξεργάζονται στο σύστημα. Αυτά τα ταξινομημένα επίπεδα δεδομένων ξεκινούν από υψίστης ευαισθησίας αταξινόμητα, μέχρι ιδιαίτερα ταξινομημένα δεδομένα. Η ανάλυση παρέχει ένα χαρακτηριστικό του επιπέδου της ευπάθειας από 2-28, με το 28 να παριστάνει το χειρότερο σενάριο. Οι ευπάθειες, τα συστήματα ασφαλείας και τα βάρη τους μπορούν να προεγκατασταθούν από τον προμηθευτή σχεδιασμένα, έτσι ώστε να ικανοποιούν τις απαιτήσεις της επιχείρησης. Τα συστήματα ασφαλείας που απαιτούνται αλλά δεν υλοποιούνται σημαδεύονται στην αναφορά και στη συνέχεια παρέχονται προτεινόμενες οδηγίες και συμβουλές σύμφωνα με το καταστατικό της επιχείρησης. Έτσι, λοιπόν, οι χρήστες έχουν τη δυνατότητα να εκτελούν σενάρια “what if” για την εκτίμηση της αποτελεσματικότητας συγκεκριμένων συστημάτων ασφαλείας.

Επιπλέον, η εφαρμογή του JANBER επιτρέπει στους χρήστες να καθορίζουν πρότυπες τιμές για συγκεκριμένα πεδία δεδομένων. Τα αποτελέσματα από τη συλλογή των δεδομένων και από την ανάλυσή τους συντηρούνται σε ξεχωριστή βάση δεδομένων. Ο προμηθευτής συστήνει η ανάλυση και η συλλογή των δεδομένων να γίνεται από διαφορετικό προσωπικό με σκοπό να διασφαλιστεί ότι η ανάλυση που εκτελείται από τον υπεύθυνο ασφαλείας των υπολογιστών επιτυγχάνει τα βέλτιστα αποτελέσματα, καθώς το λογισμικό παρέχει τη δυνατότητα ανίχνευσης των ενεργειών που απορρέουν από την προηγούμενη εκτίμηση. Το JANBER, λοιπόν, δημιουργεί μια βάση δεδομένων από πληροφορίες σε όλα τα συστήματα που επιθεωρήθηκαν και, ταυτόχρονα, παρέχει μια βάση δεδομένων από ερωτήσεις για το σχεδιασμό των απρόοπτων συμβάντων και τις λειτουργίες ανάκτησής τους.

4.4.21 Μεθοδολογία LAVA (Los Alamos Vulnerability and Risk Assessment)

Ποσοτική / Ποιοτική

Το LAVA επιμελείται ερωτηματολόγια, τα οποία έχουν ως αποτέλεσμα την αναγνώριση των ελλιπών συστημάτων ασφαλείας, καλύπτοντας τομείς από τη διαχείριση των κωδικών ασφαλείας μέχρι την ασφάλεια του προσωπικού και τις πρακτικές του εσωτερικού ελέγχου. Το λογισμικό αξιολογεί τις πιθανές παρενέργειες και τις συνέπειες στην επιχείρηση και παράγει την τελική έκθεση απωλειών. Το LAVA λαμβάνει υπόψη του τρία είδη απειλών:

- τους φυσικούς και περιβαλλοντικούς κινδύνους
- τις τυχαίες και εσκεμμένες ανθρώπινες απειλές
- τις απομακρυσμένες ανθρώπινες απειλές

Το LAVA παρέχει λεπτομερείς αναφορές ποιοτικών και ποσοτικών αποτελεσμάτων των κινδύνων που αναγνωρίζονται.

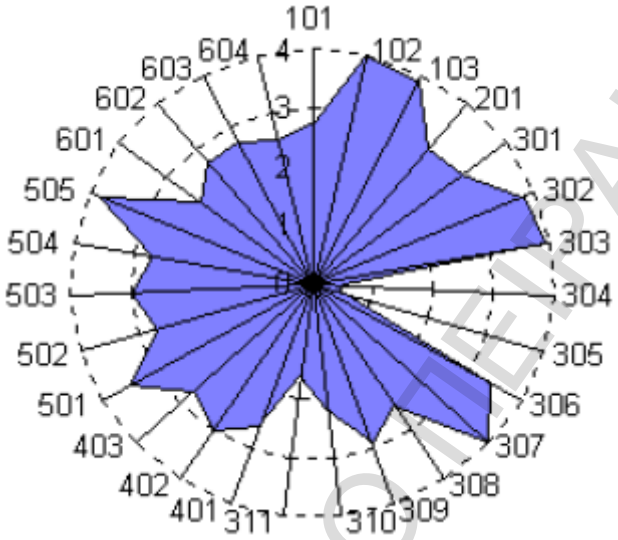
4.4.22 Μεθοδολογία MARION

Ποσοτική / Ποιοτική

Το σύστημα MARION εκτιμά τους κινδύνους της επιχείρησης που σχετίζονται με τα πληροφοριακά συστήματα, απορροφώντας γνώση από μια μεγάλη βάση δεδομένων πραγματικών περιστατικών. Το λογισμικό ενσωματώνει ένα ερωτηματολόγιο για την εκτίμηση του επιπέδου ασφαλείας που εφαρμόζεται ήδη μέσα στην επιχείρηση, δηλαδή εντοπίζονται και αξιολογούνται τα σημεία ευπάθειας (αδυναμίες) του συστήματος. Κάθε ερώτηση έχει προσδιοριστεί με ένα δείκτη βάρους, ο οποίος αντανακλά τη σχετική σημαντικότητα σύμφωνα με την ανάλυση της υποβοηθητικής βάσης δεδομένων με τα συμβάντα. Προσδιορίζεται ένας βαθμός για κάθε ερώτηση, με το αποτέλεσμα και το βαθμό να αποθηκεύονται. Τα αποτελέσματα της ανάλυσης απεικονίζονται σε μια “ροζέτα”, όπως αυτή του σχήματος 4.3. Η “ροζέτα” παρουσιάζει 27 δείκτες ευπάθειας σε έναν κύκλο και απεικονίζει το βαθμό ευπάθειας για κάθε ένα δείκτη. Το διάγραμμα αυτό βοηθά ώστε να έχουμε μια συνοπτική και περιεκτική εικόνα της κατάστασης του συστήματος, εντοπίζοντας άμεσα τους τομείς που απαιτούν μεγαλύτερη προστασία.

Όταν το προφίλ ασφαλείας καθοριστεί, το λογισμικό συγκρίνει κάθε κατηγορία με τι κανονικές τιμές, οι οποίες προέρχονται από τη βάση δεδομένων. Χρησιμοποιεί τις πληροφορίες για το κόστος, το οποίο, επίσης, κρατείται στη βάση δεδομένων για τον υπολογισμό της εκτιμώμενης δαπάνης σε σχέση με το γενικό προϋπολογισμό ασφαλείας. Τα υπολογισμένα έξοδα αναλύονται σύμφωνα με τις προδιαγραφές ασφαλείας της επιχείρησης και παρουσιάζονται γραφικά σε λεπτομερείς πίνακες. Η

δυνατότητα του MARION για σενάρια “what if” επιτρέπει σε κάποιον να χρησιμοποιήσει διαφορετικούς προϋπολογισμούς για να διαπιστώσει τις επιπτώσεις στο προφίλ ασφαλείας. Οι επιπτώσεις των προτεινόμενων μέτρων μπορούν, επίσης, να αναπαρασταθούν.



Σχήμα 4.3: Η “ροζέτα” της MARION.

Πλεονεκτήματα MARION

Το μεθοδολογία MARION παρουσιάζει τα εξής πλεονεκτήματα:

- Παρά το μεγάλο χρονικό διάστημα από την τελευταία ανανέωσή της, εξακολουθεί να είναι ιδιαίτερα αποτελεσματική.
- Είναι εύκολη στην εφαρμογή, καθώς το μεγαλύτερο μέρος της ανάλυσης βασίζεται σε ερωτηματολόγια που προσφέρονται μαζί με τη μέθοδο.
- Δίνει την ίδια βαρύτητα σε οργανωτικά και τεχνικά ζητήματα.
- Διαθέτει ιδιαίτερα πετυχημένες τεχνικές παρουσίασης των αποτελεσμάτων της ανάλυσης και διαχείρισης κινδύνων (όπως είναι η “ροζέτα”).

Μειονεκτήματα MARION

Τα μειονεκτήματα της MARION είναι τα ακόλουθα:

- Απουσιάζει μια βιβλιοθήκη μέτρων προστασίας.
- Δεν υπάρχει αυστηρή μέθοδος επιλογής μέτρων προστασίας.

4.4.23 Μεθοδολογία MEHARI (Méthode Harmonisée d' Analyse de Risques Informatiques)

Ποσοτική / Ποιοτική

Σχεδιάστηκε από ειδικούς ασφάλειας του CLUSIF (Club de la Sécurité Informatique Français) και αντικατέστησε τις προηγούμενες μεθόδους MARION και MELISA. Ανακοινώθηκε το 1996 και παρέχει ένα μοντέλο αποτίμησης επικινδυνότητας και αρθρωτά συστατικά και διαδικασίες. Περιέχει τύπους που διευκολύνουν την αναγνώριση και το χαρακτηρισμό των απειλών, καθώς και τη βέλτιστη επιλογή διορθωτικών μέτρων. Διαθέτει λίστα σημείων ευπαθειών που πρέπει να ελεγχθούν και είναι συμβατή με τα πρότυπα ISO/IEC 17799 και ISO/IEC 13335.

4.4.24 Μεθοδολογία MICROSECURE SELF ASSESSMENT

Ποιοτική

Πρόκειται για ένα αυτοματοποιημένο εργαλείο, το οποίο επιτρέπει στους χρήστες του υπολογιστή να πραγματοποιούν μια αυτοαξιολόγηση ασφαλείας. Το λογισμικό αναλύει το περιβάλλον του υπολογιστή, καθορίζει τις ευπάθειες και συστήνει ελέγχους ασφαλείας. Τα προτεινόμενα συστήματα ασφαλείας σχεδιάζονται για να αυξήσουν την ασφάλεια και να μειώσουν την έκθεση σε κίνδυνο σε έξι τομείς που περιλαμβάνουν:

- την ακεραιότητα του συστήματος
- την ασφάλεια των δεδομένων
- την αξιοπιστία και ακεραιότητα των δεδομένων
- τη λήψη αντιγράφων ασφαλείας
- την ανάκτηση λόγω καταστροφής
- την εμπιστευτικότητα και την ιδιωτικότητα

Το λογισμικό μπορεί να παραμετροποιηθεί για να πληροί τις ιδιαίτερες ανάγκες της επιχείρησης.

4.4.25 Μεθοδολογία MINIRISK

Ποιοτική

Το MINIRISK είναι ένα εργαλείο σχεδιασμένο για να βοηθά την αντιμετώπιση των ευπαθειών της ασφάλειας υπολογιστών σε ένα μικροεπεξεργαστικό περιβάλλον. Ένα ερωτηματολόγιο επιτρέπει στην επιχείρηση να εκτιμά την επάρκεια και την πληρότητα των ανεξάρτητων συστημάτων ασφαλείας και να επανεκτιμά τους τομείς εκείνους στους οποίους νέα συστήματα ασφαλείας έχουν υλοποιηθεί. Κατά τη διάρκεια της επεξεργασίας των απαντήσεων του ερωτηματολογίου, ο χρήστης αναγνωρίζει τα ελλιπή συστήματα ασφαλείας ανάμεσα σε 10 με 50 κατηγορίες ευπαθειών, που κυμαίνονται από τη διαχείριση των κωδικών ασφαλείας μέχρι το σχεδιασμό αντιμετώπισης απρόοπτων και τον εσωτερικό έλεγχο. Σε κάθε κατηγορία καθορίζονται για ανασκόπηση συστήματα ασφαλείας και έλεγχοι που θεωρούνται απαραίτητοι από την επιχείρηση. Η απουσία των ζωτικών συστημάτων ασφαλείας μεταβάλλει το επίπεδο της ευπάθειας σε μια κλίμακα από το 0 μέχρι το 9, με το 0 να αντιστοιχεί στην καλύτερη περίπτωση και το 9 στη χειρότερη. Το MINIRISK εφαρμόζει κατώτατο όριο με το οποίο αξιολογεί τις ευπάθειες που το υπερβαίνουν και, συνεπώς, ξεπερνούν τα αποδεκτά επίπεδα κινδύνου.

4.4.26 Μεθοδολογία MORT (Management Oversight Risk Tree)

Ποσοτική / Ποιοτική

Η MORT είναι μια διαγραμματική μεθοδολογία που ορίζει ασφαλή προγραμματιστικά στοιχεία σε σωστή και λογική σειρά. Η ανάλυσή της χρησιμοποιεί FAULT TREE ANALYSIS, όπου το ανώτερο γεγονός είναι συνήθως ένα από τα ακόλουθα: “βλάβη, καταστροφή, άλλα κόστη, απώλεια της παραγωγής ή μειωμένες δυνατότητες της επιχείρησης στα μάτια της κοινωνίας”.

Η MORT έχει πάνω από 1500 πιθανά βασικά γεγονότα, πάνω στα οποία στηρίζεται η ανάλυσή της και τα οποία αφορούν τομείς της πρόληψης ατυχημάτων, administration και management. Χρησιμοποιείται σαν μεθοδολογία για ανάλυση ατυχημάτων και εκτίμηση προγραμμάτων ασφαλείας.

4.4.27 Μεθοδολογία OCTAVE (Operationally Critical Threats, Asset and Vulnerability Evaluation)

Ποιοτική

Είναι μια αυτοκατευθυνόμενη (self-directed) μέθοδος, με την έννοια ότι το ίδιο το προσωπικό του οργανισμού αναλαμβάνει να διεκπεραιώσει την ανάλυση και να θέσει την στρατηγική ασφαλείας που θα ακολουθηθεί (όπως άλλωστε και στις περισσότερες σύγχρονες ποιοτικές μεθόδους). Η τεχνική αυτή βελτιώνει τη γνώση του προσωπικού για τα θέματα και τις πρακτικές ασφαλείας του οργανισμού και πετυχαίνει πιο εύκολη αποδοχή και αφομοίωση των μέτρων αντιμετώπισης που τελικά επιλέγονται.

Όπως δηλώνει και το πλήρες όνομά της, η μέθοδος επικεντρώνεται στα σημεία εκείνα που έχουν άμεση επίδραση στη λειτουργικότητα του οργανισμού και δεν αναλώνεται σε καθαρά τεχνικά θέματα ασφαλείας που δεν εξυπηρετούν τον οργανισμό. Έτσι, αναλύει τους πόρους, τις απειλές και τις ευπάθειες του οργανισμού που έχουν αναγνωριστεί ως τα πιο σημαντικά, ώστε ο οργανισμός να αποκτήσει μια σαφή εικόνα της ασφάλειας των συστημάτων του. Η OCTAVE είναι μια τεχνική που επιτρέπει στους οργανισμούς να εφαρμόζουν μια αυτοαξιολόγηση των συστημάτων και των αλλαγών που επέρχονται σε αυτά κατά την πάροδο του χρόνου.

Η μέθοδος OCTAVE ολοκληρώνεται σε 3 φάσεις, κατά τις οποίες εξετάζονται τα οργανωτικά και τα τεχνικά θέματα ασφαλείας, ώστε να δημιουργηθεί μια πλήρης εικόνα των αναγκών ασφαλείας του οργανισμού (Alberts και Dorofee, 2002). Αποτελείται από μια προοδευτική σειρά συσκέψεων (workshops), οι οποίες απαιτούν την ενεργή συμμετοχή όλων των συμμετεχόντων και απευθύνεται σε μεγάλους οργανισμούς με προσωπικό 200 ατόμων και πάνω. Για μικρότερους οργανισμούς είναι υπό ανάπτυξη η μέθοδος OCTAVE-S, αλλά ακόμα δεν έχει ολοκληρωθεί.

4.4.28 Μεθοδολογία PRA (Preliminary Risk Analysis ή Hazard Analysis)

Ποιοτική

Η PRA είναι μια ποιοτική τεχνική, η οποία περιλαμβάνει ανάλυση του γεγονότος που μπορεί να μετατραπεί σε ατύχημα. Με αυτή την τεχνική, εντοπίζονται οι πιθανές δυσμενείς καταστάσεις και στη συνέχεια αναλύονται. Για κάθε γεγονός προτείνονται βελτιώσεις και λύσεις. Το αποτέλεσμα της συγκεκριμένης μεθοδολογίας είναι μια βάση για τον προσδιορισμό των κατηγοριών στις οποίες κατατάσσονται οι κίνδυνοι και για τις μεθόδους αντιμετώπισής τους. Τα γεγονότα και οι κίνδυνοι κατηγοριοποιούνται έτσι ώστε να χρησιμοποιούνται τα κατάλληλα αντίμετρα ανάλογα με τη σημαντικότητά τους.

4.4.29 Μεθοδολογία PRISM Risk Analysis and Simulator for the PC

Ποσοτική

Το PRISM υποστηρίζει την ανάπτυξη της μοντελοποιημένης ανάλυσης κινδύνου, κάνοντας χρήση της εξομοίωσης, της ανάλυσης της ευαισθησίας καθώς και της γραφικής αναπαράστασης των αποτελεσμάτων. Περιέχει, επίσης, σύστημα λειτουργιών για την αποθήκευση, την ανάκτηση, την προβολή και τη μετατροπή των υπαρχόντων μοντέλων. Εκτός από τις απλές αλγεβρικές συναρτήσεις, το PRISM επιτρέπει τη χρήση γραμματικής παρόμοιας με την Basic για τη μοντελοποίηση πιο σύνθετων εφαρμογών.

4.4.30 Μεθοδολογία RA/SYS (Risk Analysis System)

Ποσοτική

Το RA/SYS είναι ένα αυτοματοποιημένο σύστημα ανάλυσης κινδύνου που λειτουργεί με μια σειρά από διασυνδεδεμένα αρχεία, τα οποία μπορούν να βοηθήσουν σε πάνω από 50 ευπάθειες και 65 απειλές. Οι υπολογισμοί πραγματοποιούνται σε ζευγάρια απειλών-ευπαθειών για να παράγουν βαθμολογίες και συχνότητες απειλών. Μια αναφορά συνοψίζει τις εκτιμήσεις απωλειών, την ανάλυση του οικονομικού κέρδους και της επιστροφής του κόστους στον επενδυτή.

4.4.31 Μεθοδολογία RANK-IT

Ποσοτική

Το RANK-IT είναι ένα πακέτο λογισμικού που προορίζεται για την εκτίμηση κινδύνου και χρησιμοποιεί τη μέθοδο Delphi. Η Delphi είναι ένα σύστημα εξειδικευμένης προσέγγισης για τη βαθμολόγηση των κινδύνων. Το λογισμικό αυτό αυτοματοποιεί τη *μέθοδο Delphi*, προσθέτοντας τη συγκριτική βαθμολόγηση κινδύνων για την εξασφάλιση μιας ενοποιημένης λίστας βαθμολογημένων κινδύνων ή για τον υπολογισμό του ποσοστού των τιμών κινδύνου. Κάθε βαθμολογημένο αντικείμενο έχει μια αριθμητική τιμή που μπορεί να χρησιμοποιηθεί σαν παράγοντας βάρους ή σαν απόλυτα αριθμητική τιμή.

Το RANK-IT χρησιμοποιείται για τη βαθμολόγηση των απειλών του συστήματος, των ελέγχων, των ευπαθειών, των εξαρτημάτων ή σε οποιοδήποτε άλλον τομέα. Επίσης, μπορεί να χρησιμοποιηθεί για τη βαθμολόγηση εναλλακτικών επιχειρηματικών αποφάσεων άλλων τύπων, είτε ποσοτικοποιημένων είτε όχι.

Ο προμηθευτής αναφέρει ότι ο χρόνος που απαιτείται για την παραγωγή μιας βαθμολόγησης κινδύνου, χρησιμοποιώντας αυτό τον συνδυασμό της Delphi και της

συγκριτικής βαθμολόγησης κινδύνου, κυμαίνεται μεταξύ 30 λεπτών και 3 ωρών. Ωστόσο, το πρόβλημα δεν είναι, βέβαια, ο χρόνος που απαιτείται, αλλά η ορθότητα της βαθμολόγησης του κινδύνου.

4.4.32 Μεθοδολογία RISKCALC

Ποσοτική

Σκοπός του RISKCALC είναι είτε να υπολογίζει την ετήσια προσδοκώμενη απώλεια ή παράλληλα με τη χρήση ερωτηματολόγιων, ανάλογα με το είδος των απαντήσεων, να χρησιμοποιεί άλλη μέθοδο μέτρησης. Ο χρήστης μπορεί προαιρετικά να αλλάξει τις τιμές των μεταβλητών του RISKCALC για να προσδιορίσει τα πιο εποικοδομητικά, από άποψη κόστους, συστήματα ασφαλείας και να προβάλλει τα αποτελέσματα στην οθόνη του χρήστη.

Πρωταρχικά, το RISKCALC επιτρέπει στο χρήστη να απαντάει σε ερωτήσεις και να τυπώνει αναφορές, οι τιμές των οποίων αποστώνται από το ερωτηματολόγιο και εισάγονται αυτόματα.

Δευτερευόντως, το Risk Minimizer αναγνωρίζει τους πιο σημαντικούς κινδύνους της επιχείρησης μέσα από την ολοκληρωμένη ανάλυση. Το Risk Minimizer μπορεί να χρησιμοποιηθεί με άλλα εργαλεία διαχείρισης κινδύνου, τα οποία χρησιμοποιούν το είδος αρχείων του RISKCALC.

Τρίτον, το System Manager βοηθά στο σχεδιασμό ή στην προσαρμογή των ήδη υπαρχόντων μοντέλων ανάλυσης κινδύνου, αλλά με ισχυρές παραδοχές (assumptions).

Τέταρτον, το Demonstration Models επιτρέπει στο χρήστη να αναπτύξει ένα προσαρμοσμένο ερωτηματολόγιο ή να επιλέξει ένα που μοντελοποιεί διάφορα σενάρια κινδύνου.

4.4.33 Μεθοδολογία RISKPAC

Ποσοτική / Ποιοτική

Το RISKPAC είναι ένα σύστημα που χρησιμοποιεί ερωτηματολόγιο για την αλληλεπίδραση με το χρήστη και τη μέτρηση του κινδύνου σε κυβερνητικές εφαρμογές και άλλους τομείς. Οι απαντήσεις του χρήστη στο ερωτηματολόγιο αποθηκεύονται σε ξεχωριστά αρχεία που καλούνται δημοσκοπήσεις. Συγκρίνονται διαφορετικές δημοσκοπήσεις για να διαπιστωθούν τα αποτελέσματα των διορθωτικών μέτρων ή για να εκτελεστούν αναλύσεις “what if”. Οι ερωτήσεις στο ερωτηματολόγιο ομαδοποιούνται

σε κατηγορίες, παρόμοιες με ένα βιβλίο διαιρεμένο σε κεφάλαια. Κάθε κατηγορία βαθμολογείται παρέχοντας μια λεπτομερή και λογική ανάλυση του υποκειμένου. Η αναφορά που παράγει το RISKPAC παρέχει το βαθμό του κινδύνου σε κάθε κατηγορία. Βασισμένο, λοιπόν, σε αυτό το βαθμό για την κάθε κατηγορία, το RISKPAC παρέχει συνιστώμενες ενέργειες για τη διόρθωση των ευπαθειών (καθώς μια βάση δεδομένων από διορθωτικές ενέργειες περιέχεται σε καθένα από τα ερωτηματολόγια).

Το RISKPAC, επίσης, περιέχει ένα module ανάλυσης, τον υπολογιστή A.L.E., για την ανάλυση της ετήσιας εκτιμώμενης απώλειας. Μπορούν να δημιουργηθούν πολλαπλά A.L.E. spreadsheets.

Μια λίστα από τις περιγραφές των απειλών αποθηκεύονται σε ξεχωριστά αρχεία, τα οποία μπορούν να φορτωθούν μέσα σε spreadsheets, μειώνοντας τα διαδικασία εισαγωγής δεδομένων και διευκολύνοντας την ανάλυση “what if”. Αναδιπλούμενες λίστες στο spreadsheet περιέχουν τα προτερήματα, τις απειλές, την επιρροή του δολαρίου και τη συχνότητα των συμβάντων. Οι τιμές του A.L.E. υπολογίζονται όσο ο χρήστης δουλεύει.

Το RISKPAC System Manager, το οποίο διατίθεται ξεχωριστά, χρησιμοποιείται για τη δημιουργία ή τη διαφοροποίηση των ερωτηματολογίων. Το RISKPAC System Manager επιτρέπει στο χρήστη να εισάγει ένα σετ ερωτήσεων, απαντήσεων και διορθωτικών ενεργειών και να τα μετατρέπει σε ένα εξαιρετικό σύστημα εκτίμησης κινδύνου. Προφανώς δε λειτουργεί για απροσδόκητες καταστάσεις, τις οποίες ο χρήστης δεν είχε καν υπόψη του.

4.4.34 Μεθοδολογία RISKWATCH

Ποσοτική / Ποιοτική

Το RISKWATCH είναι ένα εργαλείο διαχείρισης της ασφάλειας, ιδιαίτερα δημοφιλές στις ΗΠΑ και έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε πολλές κυβερνητικές υπηρεσίες και μεγάλους ιδιωτικούς οργανισμούς. Μερικοί από αυτούς είναι το Υπουργείο Αμύνης των ΗΠΑ, το Πεντάγωνο, το NSA (National Security Agency) και η Vodafone. Αποτελείται από εφτά υπομονάδες (modules):

1. Η 1η υπομονάδα είναι ένα εργαλείο ανάλυσης κινδύνου, το οποίο καλείται να εκτελέσει μια τυπική ανάλυση κινδύνου στα κέντρα αποφάσεων, στις εφαρμογές, στα δίκτυα ή σε απομακρυσμένες περιοχές.
2. Η 2η υπομονάδα υποστηρίζει τον τρέχοντα σχεδιασμό διαχείρισης κινδύνου.
3. Η 3η υπομονάδα αναπτύσσει ένα σχέδιο ασφαλείας.
4. Η 4η υπομονάδα αναπτύσσει σχέδια απρόοπτων περιστατικών.
5. Η 5η υπομονάδα διευθύνει ένα τεστ ασφαλείας και αξιολόγησης των επιλεγμένων συστημάτων ασφαλείας.

6. Η 6η υπομονάδα είναι ένα πρόγραμμα γραφικών.
7. Η 7η υπομονάδα είναι ένα εργαλείο εξειδικευμένης ανάπτυξης συστημάτων.

Το RISKWATCH περιέχει ένα εργαλείο ανάπτυξης ερωτηματολογίων, το οποίο επιτρέπει να εισάγονται οι ερωτήσεις και να ομαδοποιούνται. Οι υπομονάδες μπορούν να λειτουργούν και ανεξάρτητα. Παρέχει πλήρη παραμετροποίηση από το χρήστη, με δυνατότητες δημιουργίας καινούργιων κατηγοριών περιουσιακών στοιχείων, απειλών, ευπαθειών, αντιμέτρων, ερωτηματολογίων κ.τ.λ..

Επιπλέον, το RISKWATCH έχει μια ενσωματωμένη ευφυή βάση για την εξασφάλιση της εσωτερικής ασφάλειας. Έχει τη δυνατότητα να παράγει αναφορές, συμπεριλαμβανομένης και της αναζήτησης κειμένου, καθώς και γραφικό πρόγραμμα για την ερμηνεία των αποτελεσμάτων της ανάλυσης σε διαγράμματα ράβδων ή πίττας. Δεν απαιτείται κανένα άλλο λογισμικό.

Στη συνέχεια, το RISKWATCH είναι σχεδιασμένο να παρέχει όλα τα προαπαιτούμενα των ομοσπονδιακών πρακτορείων σε ό,τι αφορά τη διαχείριση κινδύνου και να διαπιστώνει αυτόματα την υλοποίηση των συστημάτων ασφαλείας, με δείκτη επιστροφής στην επένδυση για κάθε σύστημα.

Τέλος, το RISKWATCH μπορεί να δημιουργήσει ερωτηματολόγια σε βοηθητικές μνήμες για εύκολη διανομή ή να συλλέξει πληροφορίες μέσω δικτυακών ρυθμίσεων. Δημιουργείται αυτόματα μια αποτίμηση των ευπαθειών για κάθε απομακρυσμένη τοποθεσία. Ο έλεγχος του ιστορικού των ενεργειών συντηρείται σε όλα τα στάδια και τις διαδικασίες του προγράμματος και κάθε χρόνο είναι διαθέσιμες νέες εκδόσεις του.

4.4.35 Μεθοδολογία SBA (Security By Analysis)

Ποσοτική

Η SBA αναπτύχθηκε στη Σουηδία στις αρχές της δεκαετίας του 1980. Αν και είναι ελάχιστα γνωστή εκτός της Σκανδιναβικής χερσονήσου, αποτελεί την πιο δημοφιλή και ευρέως εφαρμοσμένη μέθοδο διαχείρισης κινδύνων στη Σουηδία. Θα πρέπει να αντιμετωπίζεται λιγότερο ως αυστηρή μέθοδος και περισσότερο ως μια ανθρωποκεντρική οπτική απέναντι στο ζήτημα της διαχείρισης κινδύνων, καθώς δίνει ιδιαίτερη βαρύτητα στη συμμετοχή των ανθρώπων που η εργασία τους σχετίζεται με το πληροφοριακό σύστημα και ενθαρρύνει τη δημιουργικότητα και τη φαντασία τους.

Η SBA βασίζεται στη διαπίστωση ότι οι άνθρωποι που συμμετέχουν στην καθημερινή λειτουργία του συστήματος, ανεξάρτητα από το ρόλο και τη θέση στην ιεραρχία, είναι αυτοί που έχουν τις περισσότερες πιθανότητες να εντοπίσουν τα προβλήματα ασφάλειας και να προτείνουν λύσεις. Τα είκοσι έτη επιτυχημένης εφαρμογής της μεθόδου ενισχύουν την παραπάνω θέση και καταδεικνύουν ότι η

ανθρωποκεντρική ανάλυση και διαχείριση κινδύνων αποτελεί μια ρεαλιστική και αποτελεσματική προσέγγιση.

Η SBA αποτελείται στην πραγματικότητα από ένα σύνολο μεθόδων που ακολουθούν την ίδια φιλοσοφία και λειτουργούν συμπληρωματικά. Οι κυριότερες από αυτές είναι η SBA Check και η SBA Scenario. Και οι δύο μέθοδοι υποστηρίζονται από ειδικό λογισμικό που διευκολύνει σημαντικά την εφαρμογή τους.

Πλεονεκτήματα SBA

Το μεθοδολογία SBA παρουσιάζει τα εξής πλεονεκτήματα:

- Υιοθετεί μια ολιστική προσέγγιση του ζητήματος της ασφάλειας, εξετάζοντας το πληροφοριακό σύστημα ως ενιαίο σύνολο και μελετώντας το από όλες τις πλευρές.
- Η ανάλυση γίνεται από τους ίδιους τους ανθρώπους που χρησιμοποιούν καθημερινά το σύστημα, γεγονός που ενισχύει την αποτελεσματικότητα της μεθόδου και, κυρίως, εξασφαλίζει σε μεγάλο βαθμό την αποδοχή και εφαρμογή του σχεδίου ασφαλείας που προκύπτει ως αποτέλεσμα της εφαρμογής της μεθόδου.
- Είναι αρκετά απλή και κατανοητή ακόμα και από μη-ειδικούς και μπορεί να υλοποιηθεί με σχετικά μικρό κόστος.
- Υποστηρίζεται από ειδικό λογισμικό, το οποίο είναι απλό και εύχρηστο.

Μειονεκτήματα SBA

Τα μειονεκτήματα της SBA είναι τα ακόλουθα:

- Στηρίζεται σε μεγάλο βαθμό στις ικανότητες, στη φαντασία κι στη διάθεση για συνεισφορά των εργαζομένων.
- Προϋποθέτει την ανάπτυξη ανθρωποκεντρικής και συμμετοχικής κουλτούρας. Αυτός είναι, ίσως, ο κυριότερος λόγος που η εφαρμογή της μεθόδου δεν έχει επεκταθεί ιδιαίτερα εκτός των Σκανδιναβικών χωρών.
- Δε συνοδεύεται από βιβλιοθήκες μέτρων προστασίας. Η επινόηση και ο σχεδιασμός των μέτρων προστασίας επαφίεται στις ομάδες εργασίας.

4.4.36 Μεθοδολογία SOS (Security On-Line System)

Ποσοτική / Ποιοτική

Το SOS είναι ένα εργαλείο το οποίο έχει σχεδιαστεί για τη διαχείριση της ασφάλειας και του κινδύνου ενός συστήματος. Ο χρήστης ξεκινά καθορίζοντας την ταυτότητα του συστήματός του στη γνωσιακή βάση δεδομένων. Χρησιμοποιώντας αυτή τη βάση δεδομένων, γίνεται μια βασική αποτίμηση των κινδύνων για να καθοριστεί η έκθεση απώλειας δολαρίων ή η μη εξουσιοδοτημένη αλλαγή των δεδομένων του συστήματος. Ο χρήστης μπορεί, στη συνέχεια, να χρησιμοποιήσει ένα προκαθορισμένο ή σχεδιασμένο ερωτηματολόγιο για την προσωπική του αποτίμηση, την επισκόπηση της ασφάλειας των δεδομένων ή τον έλεγχο του συστήματος. Με αυτές τις πληροφορίες, ο χρήστης είναι σε θέση να αναπτύξει μια βάση δεδομένων από απειλές, ευπάθειες και συστήματα ασφαλείας, η οποία μπορεί να χρησιμοποιηθεί ώστε να καταγραφεί ένα σχέδιο απρόοπτων συμβάντων.

Η συγκεκριμένη προσέγγιση του SOS επιτρέπει τη χαρτογράφηση των δεδομένων, ενώ η εφαρμογή διαμένει και εντοπίζεται το επίπεδο του κινδύνου για τον υπολογιστή, τις εφαρμογές, τα τοπικά δίκτυα, τις επικοινωνίες των δεδομένων, τα συστήματα βάσεων δεδομένων, τα κέντρα διαχείρισης δεδομένων, τα λειτουργικά συστήματα, τα προϊόντα ασφαλείας, τα συστήματα που βρίσκονται υπό κατασκευή και τα υλικά των υπολογιστών.

4.5 Αποτίμηση Πληροφοριακού Συστήματος

Η αποτίμηση ενός Πληροφοριακού Συστήματος (ΠΣ) είναι άρρηκτα συνδεδεμένη με όλες τις φάσεις της δημιουργίας του συστήματος, τόσο κατά τη διάρκεια της λειτουργίας του όσο και μετά τη λειτουργία του, στη φάση της συντήρησης. Υπάρχουν διάφορες προσεγγίσεις σχετικά με το πλαίσιο της αποτίμησης ενός πληροφοριακού συστήματος. Ο Symons (1991), υιοθετώντας τις ιδέες του A. M. Petigrew (ερευνητή της διοικητικής των μεταβολών σε μια επιχείρηση), πρότεινε να θεωρηθεί η αποτίμηση των πληροφοριακών συστημάτων ως μέρος των οργανωτικών αλλαγών που καθορίζονται από:

- τα περιεχόμενα (content),
- τις διεργασίες (process),
- το περιβάλλον (context) του οργανισμού.

Οι Hamilton και Chervany (1981) εισηγήθηκαν μια άλλη μεθοδολογία, η οποία συνδυάζει τους στόχους του οργανισμού και τον ίδιο τον οργανισμό ως σύστημα. Εδώ εξετάζεται τόσο η δυνατότητα όσο και η αποτελεσματικότητα. Οι Wolstenholme, Henderson και Gavine (1993) πρότειναν να χρησιμοποιηθεί η δυναμική συστημάτων (system dynamics) για την αποτίμηση ενός πληροφοριακού συστήματος. Η τεχνική αυτή έχει χρησιμοποιηθεί με επιτυχία και στη χώρα μας (Μπέλιας, 1999). Μια άλλη ευρύτατα γνωστή μέθοδος αποτίμησης είναι αυτή που στηρίζεται σε καθαρά οικονομικά κριτήρια. Οι αποτιμήσεις της κατηγορίας αυτής στηρίζονται:

- στην ποσοτικοποίηση και σύγκριση των οικονομικών παραμέτρων, όπως εκτίμηση απόδοσης επένδυσης, ανάλυση κόστους/οφέλους, ανάλυση απόδοσης διοίκησης, οικονομική των πληροφοριών κ.λπ..
- στην αποτίμηση με τη μέθοδο της έρευνας και του πειράματος, όπως μέθοδοι πολλαπλών στόχων/κριτηρίων, ανάλυση παραγόντων βασικής επιτυχίας, ανάλυση αξιών κ.λπ..
- στην εκτίμηση των μη απτών (άυλων) οφελών.

Πρόσφατες προσεγγίσεις (Garrity και Sanders, 1998) αναφέρονται στη μέτρηση της επιτυχίας ενός πληροφοριακού συστήματος σε διάφορα επίπεδα μέσα στον οργανισμό, χρησιμοποιώντας κριτήρια τα οποία μπορούν να ταξινομηθούν ως εξής:

Στο επίπεδο του οργανισμού ή της επιχείρησης

- Μερίδιο αγοράς, οφέλη και ποσοστό του δείκτη απόδοσης (rate of return index).
- Έσοδα από νέα προϊόντα ή υπηρεσίες, πρόσθετα κέρδη.
- Λειτουργική υπεροχή σε σχέση με του ανταγωνιστές.
- Κόστος λειτουργίας, διαθεσιμότητα συστήματος, χρόνος απόκρισης.
- Απόψεις του οργανισμού για την απόδοσή του.
- Βαθμός ευθυγράμμισης της στρατηγικής της τεχνολογίας της πληροφορικής με τη γενική στρατηγική του οργανισμού.

Στο επίπεδο των διεργασιών του οργανισμού

- Λειτουργική ικανότητα των διεργασιών.
- Μείωση του χρόνου κύκλου διεργασιών.
- Βαθμός συνοχής μεταξύ των διεργασιών.
- Βαθμός ενημερότητας πάνω στη σωστή χρησιμοποίηση των πόρων για την παραγωγή προϊόντων ή και υπηρεσιών.

Στο επίπεδο του ατόμου

- Ικανοποίηση του χρήστη.
- Αξιοποίηση του συστήματος.
- Ικανοποίηση του χρήστη στο επίπεδο του πληροφοριακού συστήματος.

Τέλος, να αναφέρουμε ότι έχουν γίνει πολλές ερευνητικές προσπάθειες για να εντοπιστούν τα αίτια μιας αστοχίας ενός πληροφοριακού συστήματος. Ιδιαίτερο ενδιαφέρον παρουσιάζει η προσπάθεια των Lyytinen και Hirschheim (1987), σύμφωνα με την οποία έχουμε τρία βασικά είδη αστοχίας:

- *Αστοχία συμφωνίας*, δηλαδή αποτυχία ικανοποίησης των αρχικών απαιτήσεων του συστήματος.
- *Αστοχία διεργασίας*, δηλαδή πλήρη αποτυχία δημιουργίας ενός τελικού συστήματος ή μερική αποτυχία δημιουργίας του, μέσα στους λογικούς οικονομικούς περιορισμούς που είχαν τεθεί.
- *Αστοχία αλληλεπίδρασης*, δηλαδή αστοχία στα επίπεδα χρήσης και στους βαθμούς ικανοποίησης του χρήστη.

Καθένα από τα τρία αυτά επίπεδα αστοχιών δε λαμβάνει υπόψη του τα άλλα δύο. Για το λόγο αυτό, οι Lyytinen και Hirschheim (1987) προτείνουν ένα τέταρτο είδος αστοχίας, που το ονομάζουν *αστοχία προσδοκιών* και το ορίζουν ως την ανικανότητα ενός πληροφοριακού συστήματος να ικανοποιήσει τις προσδοκίες μιας ομάδας ενδιαφερομένων που έχουν κάποιο συμφέρον (stakeholders). Η προσέγγιση της αστοχίας προσδοκιών δέχτηκε αρκετές κριτικές, κυρίως εξαιτίας των εξής λόγων:

- μερικές προσδοκίες είναι περισσότερο λογικές από κάποιες άλλες,
- η αστοχία στις προσδοκίες αγνοεί την πρόθεση του κάθε ενδιαφερόμενου και
- μερικοί ενδιαφερόμενοι διαθέτουν περισσότερες ικανότητες από κάποιους άλλους.

Τέλος, μια άλλη έρευνα των A. Holmes και A. Poulimenakou (1996), που έχει να κάνει με την αστοχία ενός πληροφοριακού συστήματος, ακολουθεί μια διαφορετική πορεία. Ξεκινάει από την κοινωνική φύση των πληροφοριακών συστημάτων, προχωράει στον καθορισμό ενός πλαισίου κατανόησης των διαφόρων μεμονωμένων περιστατικών, που υποδεικνύουν μια πλήρη ή μερική αστοχία του πληροφοριακού συστήματος προκειμένου να ληφθούν μέτρα αποφυγής, και καταλήγει στην οριοθέτηση ενός πλαισίου ενδεχομένων, τα οποία μπορεί να οδηγήσουν σε μια αποτυχία. Η συγκεκριμένη έρευνα διαχωρίζει αυτά τα ενδεχόμενα, τα ονομάζει «μεταβλητές» και τα κατηγοριοποιεί όπως παρακάτω:

- Μακρο-μεταβλητές:
  - κουλτούρα ενδιαφερόμενων
  - σχεδιασμός πληροφοριακού συστήματος
  - ερμηνείες συστήματος
  - ανορθολογιστική συμπεριφορά χρηστών
  - αποτίμηση πληροφοριακού συστήματος

- Μικρο-μεταβλητές
  - χρησιμοποιούμενες μέθοδοι και μεθοδολογίες
  - αντίσταση στις αλλαγές από τους χρήστες
  - ισχύς και πολιτική

Οι παραπάνω μεταβλητές επηρεάζουν τις διεργασίες του οργανισμού, άρα και το αποτέλεσμά τους. Η μελέτη τους μέσα στον οργανισμό μπορεί να οδηγήσει σε λήψη μέτρων αποφυγής των αστοχιών του πληροφοριακού συστήματος, είτε προβλέποντας μια αστοχία, είτε μετά από μεμονωμένα περιστατικά μέσα από την οργανωσιακή μάθηση. Έτσι, οδηγούμαστε στην αποτελεσματικότητα του ίδιου του συστήματος και του οργανισμού ως σύνολο. Η έρευνα καταλήγει στο συμπέρασμα ότι η συνεχής αποτίμηση του πληροφοριακού συστήματος και η σύνδεσή της με ενδεχόμενες αστοχίες του που βασίζονται στις παραπάνω μεταβλητές είναι ζωτικής σημασίας για τον οργανισμό.

ΚΕΦΑΛΑΙΟ 5

Ανάλυση και Διαχείριση Κινδύνων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) μιας Τσέχικης Εταιρείας

5.1 Γενικό Πλαίσιο Μελέτης

Παρουσιάζεται μια μελέτη που έχει πραγματοποιήσει η εταιρεία RAC (Risk Analysis Consultants) s.r.o., η οποία ασχολείται με την παροχή υπηρεσιών ασφάλειας πληροφοριών και λύσεων, και αφορά την ανάλυση και διαχείριση κινδύνων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) μιας τσέχικης εταιρείας (RAC s.r.o. CRAMM Case Study, 2010). Η RAC s.r.o., που έχει τη βάση της στην Τσεχία, από το 1995 έχει βοηθήσει κυβερνητικούς οργανισμούς και εμπορικούς τομείς για την προστασία των πληροφοριών τους. Είναι η μόνη εταιρεία που ειδικεύεται αποκλειστικά στον τομέα της ασφάλειας των πληροφοριών στην τσέχικη αγορά και μία από τα ελάχιστες στην Ευρώπη αλλά και στον κόσμο.

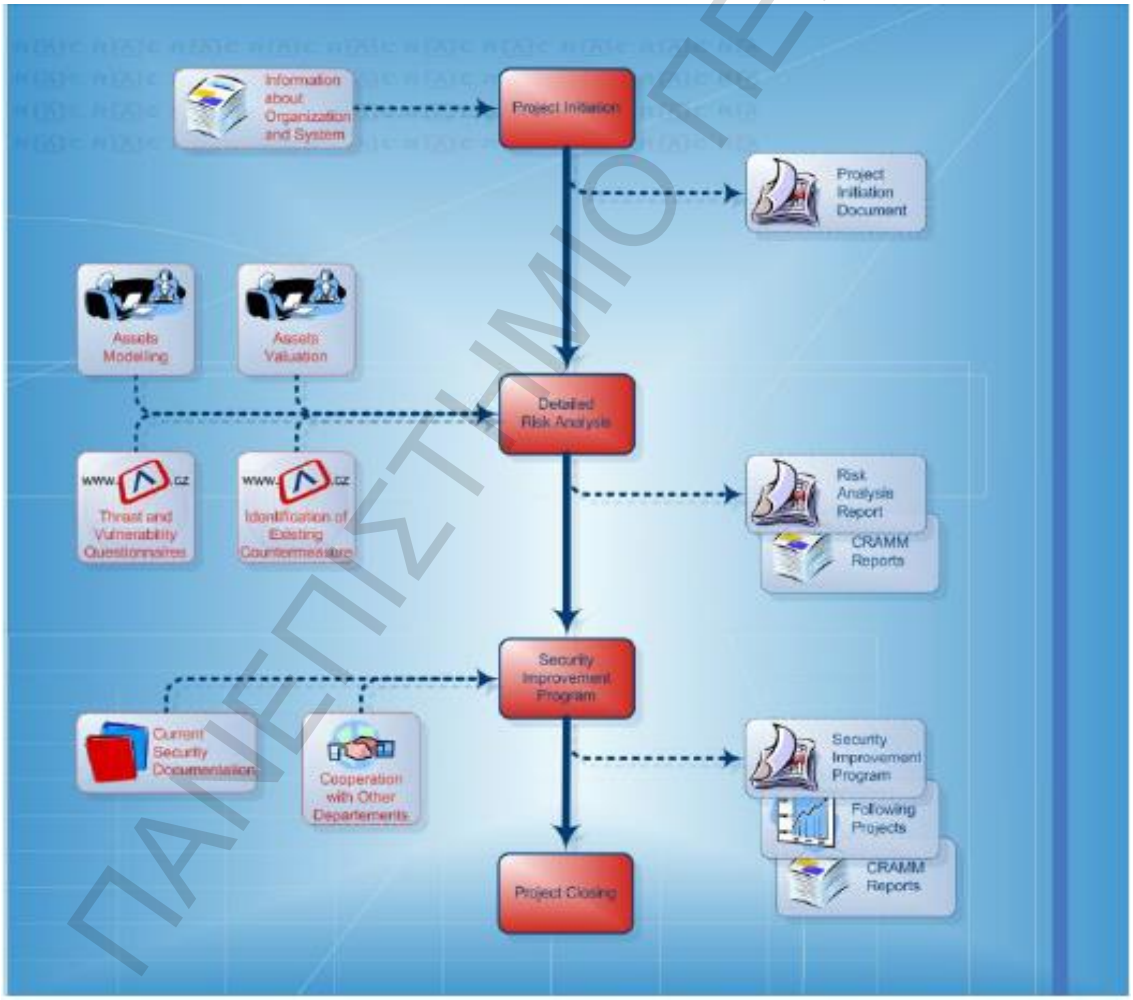
Η ανώτατη διοίκηση μιας μεγάλης τσέχικης εταιρείας, λοιπόν, αποφάσισε τη θέσπιση και λειτουργία ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ). Η ανάλυση και διαχείριση κινδύνων πραγματοποιήθηκε με τη μέθοδο CRAMM και ολοκληρώθηκε με την πιστοποίηση του συστήματος σύμφωνα με το πρότυπο ISO/IEC 27001 (BS 7799-2). Η μέθοδος CRAMM είναι η πιο ευρέως χρησιμοποιούμενη μεθοδολογία στην Ευρώπη για την ανάλυση και διαχείριση κινδύνων, καθώς η ποιότητά της έχει αποδειχθεί από πολλές επιτυχημένες πιστοποιήσεις και ικανοποιημένους πελάτες. Για τη θέσπιση και λειτουργία του ΣΔΑΠ ήταν πολύ χρήσιμα, κυρίως, η βιβλιοθήκη αντιμέτρων και τα πρότυπα σχεδίου ασφάλειας.

Ειδικοί του τμήματος ασφάλειας δε διέκριναν κάποια ανάγκη για αγορά της μεθοδολογίας και άλλων εργαλείων υποστήριξης και, επομένως, ζήτησαν βοήθεια από μια κορυφαία εταιρεία παροχής συμβουλευτικών υπηρεσιών στην Τσεχία. Επιλέχτηκε μια προσέγγιση στενής συνεργασίας, κατά την οποία εργάστηκαν μαζί όλοι οι ειδικοί της εταιρείας και οι εξωτερικοί σύμβουλοι. Αυτός ο τρόπος εργασίας χρησιμοποιήθηκε αποτελεσματικά από όλους τους πόρους και εξασφάλισε τη μετάδοση της τεχνογνωσίας στους ειδικούς που εμπλέκονται στη διαδικασία της απόφασης (εσωτερικοί ειδικοί).

5.2 Έναρξη της Ανάλυσης

Η ομάδα ανάλυσης αποτελείται από δύο εσωτερικούς ειδικούς και δύο συμβούλους, εκ των οποίων ο ένας καθοδήγησε την ανάλυση. Όπως ήδη αναφέρθηκε, χρησιμοποιήθηκε η μεθοδολογία CRAMM για τη διαχείρισή της και διεξήχθησαν αναλόγως όλες οι απαραίτητες δραστηριότητες για την ορθή έναρξή της. Στο πρώτο παραδοτέο (έγγραφο έναρξης της ανάλυσης) συνοψίστηκαν ο στόχος της ανάλυσης, η προσέγγιση, το σχέδιο διασφάλισης ποιότητας, το χρονοδιάγραμμα, η ομάδα και η περιγραφή των δραστηριοτήτων, συμπεριλαμβανομένων των πόρων.

Κατά το στάδιο της έναρξης πραγματοποιήθηκε συλλογή πληροφοριών σχετικά με τα συστήματα και την αναθεώρηση της ισχύουσας πολιτικής ασφάλειας.



Σχήμα 5.1: Ανάλυση του ΣΔΑΠ.

Στο έγγραφο έναρξης της ανάλυσης, λοιπόν, αναφέρονται:

- οι στόχοι της ανάλυσης
- μια προσέγγιση για την υλοποίηση της ανάλυσης, μεθοδολογίες που χρησιμοποιούνται
- η ομάδα της ανάλυσης και οι ρόλοι
- τα στάδια της ανάλυσης, οι πόροι, τα αποτελέσματα και οι ευθύνες
- το χρονοδιάγραμμα
- το σχέδιο διασφάλισης ποιότητας, οι κίνδυνοι της ανάλυσης

Αξίζει να αναφερθεί ότι οι πόροι ήταν περιορισμένοι, αλλά χάρη στην προσέγγιση στενής συνεργασίας η μεθοδολογία CRAMM χρησιμοποιήθηκε πολύ αποτελεσματικά.

5.3 Αναγνώριση και Μοντελοποίηση Περιουσιακών Στοιχείων

Τα περιουσιακά στοιχεία είναι σχεδόν τα πάντα σε έναν οργανισμό που σχετίζεται με την επεξεργασία πληροφοριών. Τα πιο σημαντικά περιουσιακά στοιχεία είναι τα δεδομένα, η αναγνώριση των οποίων δεν είναι πάντα εύκολη. Επεξεργάστηκαν τεράστιες ποσότητες πληροφοριών σχετικά με την παραγωγή, τους πελάτες, τους προμηθευτές, το προσωπικό, καθώς και τη στρατηγική διαχείρισης, όπως η λογιστική κ.λπ..

Καθορίστηκαν οι ομάδες δεδομένων και στο πλαίσιο της ανάλυσης ορίστηκαν οι υποομάδες, π.χ. ανάλογα με το περιεχόμενο, την κατηγορία, το τμήμα ή τα δεδομένα ευαισθησίας. Προέκυψαν, λοιπόν, στο σύνολο δέκα ομάδες και πενήντα τέσσερεις υποομάδες.

Κατά τη διάρκεια της αξιολόγησης συνοψίστηκαν οι συμπληρωματικές πληροφορίες για τη μοντελοποίηση των περιουσιακών στοιχείων. Κάθε διακομιστής (server), σταθμός εργασίας, συστατικό του δικτύου διανομής, εφαρμογή, σύνδεση κ.α. υποβλήθηκε σε μια απλή ανάλυση και δημιουργήθηκε το μοντέλο συσχέτισης των περιουσιακών στοιχείων, έτσι ώστε να μεταβιβάζονται σχέσεις μεταξύ των δεδομένων, του λογισμικού, των διαδικασιών, του υλικού και των τοποθεσιών.

5.4 Ανάλυση των Επιπτώσεων

Κατά τη διάρκεια της διαδικασίας αξιολόγησης των δεδομένων, πραγματοποιήθηκαν πολλές συνεντεύξεις με προεπιλεγμένους ερωτηθέντες. Οι ερωτηθέντες (συνήθως χρήστες των ομάδων ή των υποομάδες δεδομένων) περιέγραψαν πιθανές παραβάσεις που θα μπορούσαν να βλάψουν τη φήμη της εταιρείας, να επιφέρουν οικονομικές απώλειες ή να προκαλέσουν άλλες ζημιές. Ερευνήθηκαν όλες οι περιπτώσεις μη διαθεσιμότητας των δεδομένων, υποκλοπής και μετατροπής τους.

Κατά τη διαδικασία αξιολόγησης των δεδομένων ερευνήθηκαν οι οικονομικές απώλειες, η αποδιοργάνωση της παραγωγής, η απώλεια καλής θέλησης και οι τραυματισμοί ανθρώπων. Τα πραγματικά σενάρια των επιπτώσεων αυτών συγκρίθηκαν με τις κατευθυντήριες γραμμές αξιολόγησης που έχουν ενσωματωθεί στο εργαλείο της CRAMM. Υπήρξε, λοιπόν, μια αξιόπιστη υποστήριξη για τον προσδιορισμό της τελικής αξίας των δεδομένων.

Πρώτα, αξιολογήθηκαν οι υποομάδες δεδομένων σε μια κλίμακα από 1 έως 10 (πίνακας 5.1) και, στη συνέχεια, αποδόθηκαν οι υψηλότερες τιμές για κάθε ομάδα δεδομένων, αντιπροσωπεύοντας ένα περιουσιακό στοιχείο δεδομένων στο εργαλείο της CRAMM.

	Data 1	Data referent	Data model	Data 2	SAP	Data clearing
Loss of backup data	3	1	1	1	1	1
Total loss of all data	6	3	3	3	3	1
Disclosure to identified people	1	1	1	1	1	1
Disclosure to strangers	4	4	4	4	4	4
Minor errors	2	1	2	1	2	2
Major errors	3	2	3	2	3	3
Intentional modification	5	5	3	2	3	5
Undelivered	1	1	1	1	0	1
Routing error	3	1	3	1	0	0

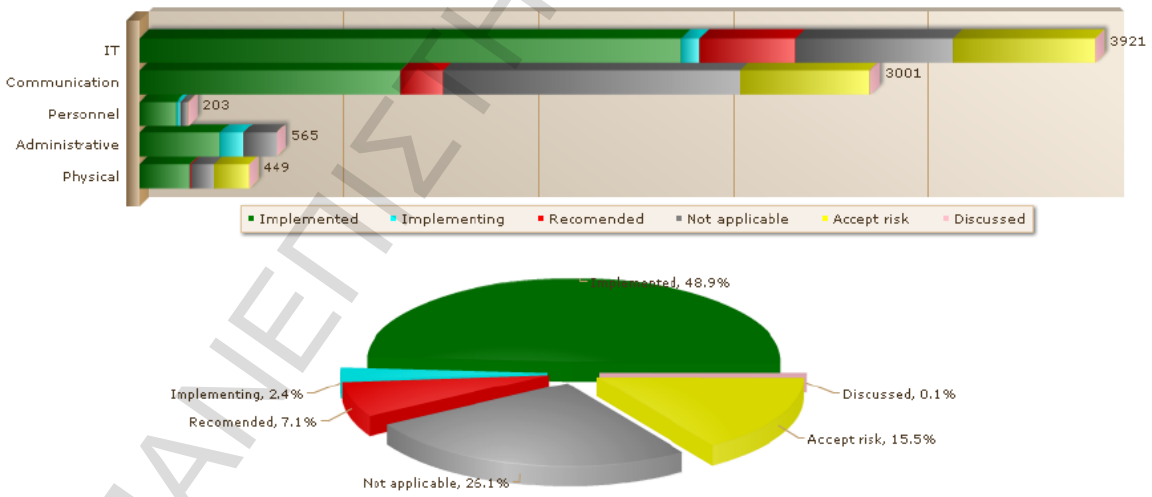
Πίνακας 5.1: Αξία δεδομένων - αξιολόγηση επιπτώσεων (max=10).

Η αξία των υλικών στοιχείων αποδόθηκε με βάση το κόστος αντικατάστασης και εγκατάστασης, σε περίπτωση ολικής καταστροφής.

5.5 Απειλές και Ευπάθειες

Στόχος ήταν ο υπολογισμός του βαθμού των κινδύνων που απειλούν το σύστημα. Συσχετίστηκαν συγκεκριμένες απειλές και ευπάθειες με τα περιουσιακά στοιχεία και στη συνέχεια αξιολογήθηκαν με τη μέθοδο των ερωτηματολογίων. Οι ερωτηθέντες, κυρίως διαχειριστές του συστήματος και ειδικοί από το τμήμα φυσικής ασφάλειας, απάντησαν στις ερωτήσεις μέσω της δικτυακής επιφάνειας αλληλεπίδρασης - διεπαφής (web interface) του εργαλείου της CRAMM, η οποία ήταν προσβάσιμη από το ενδοδίκτυο (intranet) της εταιρείας.

Ο βαθμός κινδύνου υπολογίστηκε αυτόματα μετά τη συμπλήρωση όλων των ερωτηματολογίων (σχήμα 5.2). Στη συνέχεια, παράχθηκαν από το εργαλείο της CRAMM τα αντίμετρα ασφάλειας για τη διαχείριση των κινδύνων.



Σχήμα 5.2: Αξιολόγηση κινδύνων του ΣΔΑΠ.

Το εργαλείο της CRAMM προσδιόρισε το σύνολο των συνιστώμενων αντιμέτρων για όλους τους χώρους ασφάλειας. Το επόμενο βήμα ήταν η καταγραφή των ήδη υφιστάμενων αντιμέτρων και η επιλογή εκείνων που θα εφαρμοστούν.

Στο σημείο αυτό παρενέβη και πάλι η δικτυακή εφαρμογή της μεθόδου CRAMM και οι ερωτηθέντες εκτίμησαν τα αντίμετρα ή αποφάσισαν σχετικά με την εφαρμοσιμότητά τους.

Για την αναφορά-έκθεση της ανάλυσης και διαχείρισης κινδύνων χρησιμοποιήθηκε η φόρμα (template) του εργαλείου της CRAMM. Εκτός από τη μοντελοποίηση και την αξιολόγηση των περιουσιακών στοιχείων, η έκθεση συνοψίζει και τα επίπεδα των απειλών και ευπαθειών καθώς και την τρέχουσα κατάσταση ασφάλειας.

Από τα στατιστικά εκτίμησης των αντιμέτρων προσδιορίστηκε το ποσοστό των προτεινόμενων αντιμέτρων που είχαν ήδη εγκατασταθεί και το μέρος αυτών που ακόμα χρειαζόταν να τεθεί σε εφαρμογή.

Όλα τα συμπεράσματα παρουσιάστηκαν σε μια αναφορά-έκθεση (σύνοψη) διαχειριστικού στυλ. Ωστόσο, για την υποστήριξη τους, δημιουργήθηκε από το εργαλείο της CRAMM ένα σύνολο των εκθέσεων αντιμέτρων, με σκοπό να παράσχει λεπτομερείς τιμές για κάθε περιουσιακό στοιχείο, το επίπεδο κινδύνου του, τη σχετική απειλή και τα ειδικά αντίμετρα. Παράχθηκαν περιληπτικές αναφορές σε πολλές παραλλαγές, αλλά μόνο σε ηλεκτρονική μορφή λόγω του σχετικά μεγάλου μήκους τους.

5.6 Πρόγραμμα Βελτίωσης της Ασφάλειας

Λεπτομερής ανάλυση των κινδύνων έδειξε αδυναμίες στην ασφάλεια του συστήματος. Για το λόγο αυτό, τα πεδία εφαρμογής των επόμενων έργων όρισαν τη διαδικασία υλοποίησης των αντιμέτρων.

Ο στόχος κάθε έργου ήταν η βελτίωση του επιπέδου ασφάλειας για συγκεκριμένα συστήματα ή περιοχές. Με βάση τις προτάσεις του εργαλείου της CRAMM και έργα όπως η ανάπτυξη σχεδίου ασφάλειας, ξεκίνησε η εγκατάσταση νέων τεχνολογιών και η αναβάθμιση φυσικής ασφάλειας κ.λπ..

Ο Στρατηγικός Σχεδιασμός Υλοποίησης (ΣΣΥ) των έργων που ακολούθησαν περιείχε όλες τις δραστηριότητες συμπεριλαμβανομένων των πόρων και των ευθυνών, τα σχέδια του έργου, τις εξόδους (outputs) κ.α.. Η έκθεση της διαχείρισης ασφάλειας ήταν, επίσης, ένα μέρος του ΣΣΥ, προκειμένου να υποστηρίξει την πραγματοποίησή του.

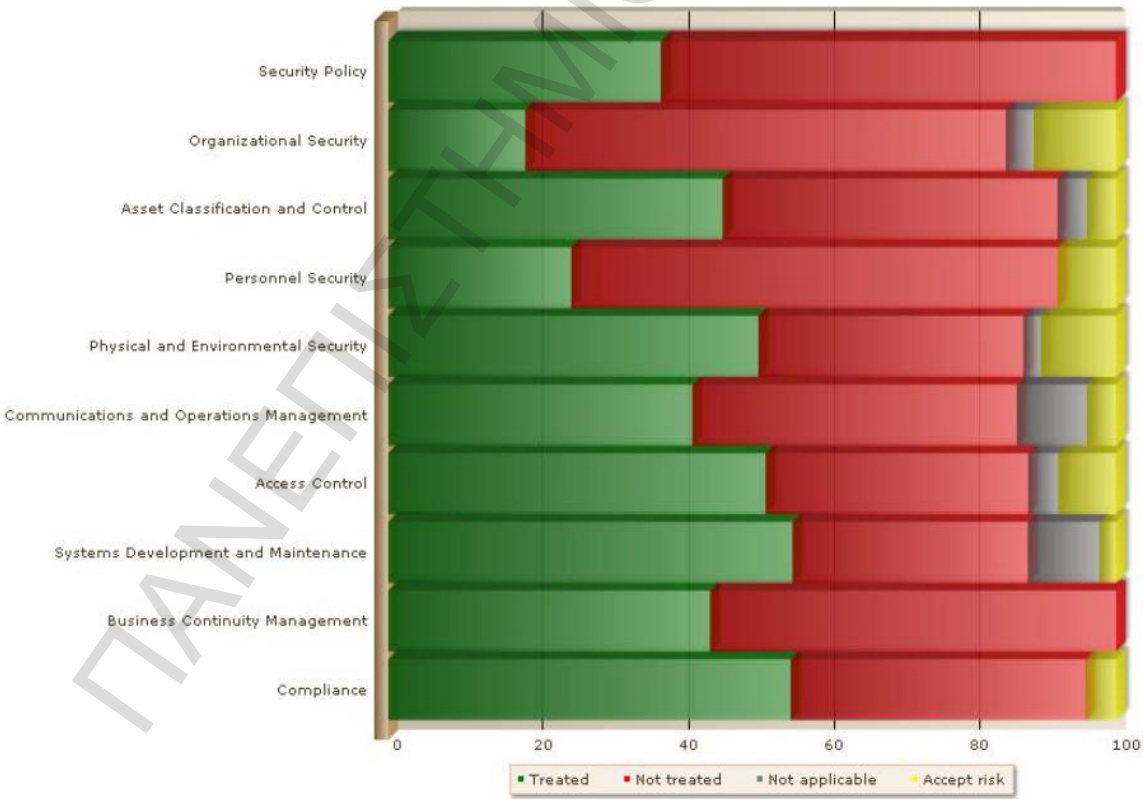
Το πεδίο δράσης των επόμενων έργων, λοιπόν, με σκοπό τη βελτίωση της ασφάλειας έχει να κάνει με:

- την ανάπτυξη τεκμηρίωσης (εγγράφων) ασφάλειας
- την οργανωτική δομή
- τη βελτίωση της φυσικής ασφάλειας
- το πρόγραμμα συνεχούς επίγνωσης της ασφάλειας
- την καθιέρωση διαχείρισης περιστατικών
- τη διαχείριση επιχειρηματικής συνέχειας
- την υποδομή ηλεκτρονικής ασφάλειας

Η ανάλυση και διαχείριση κινδύνων ήταν ένα βασικό βήμα προς την επιτυχή ανάπτυξη του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ).

Ο έλεγχος, που πραγματοποιήθηκε μερικές εβδομάδες αργότερα, επιβεβαίωσε ότι όλοι οι κίνδυνοι πληροφοριών είχαν πλέον διαχειριστεί σωστά.

Η νεοαποκτηθείσα πιστοποίηση του ΣΔΑΠ σύμφωνα με το πρότυπο ISO 27001 έγινε εμφανής για τους πελάτες και τους προμηθευτές, οι πληροφορίες για τους οποίους ήταν επαρκώς και αποτελεσματικά ασφαλείς.



Σχήμα 5.3: Επίπεδο συμμόρφωσης του ΣΔΑΠ κατά ISO 27001.

Αξίζει να σημειωθεί ότι το εργαλείο της CRAMM εξακολουθεί να χρησιμοποιείται από την τσέχικη εταιρεία για την ανάλυση και διαχείριση κινδύνων πληροφοριών και την υποστήριξη του ΣΔΑΠ. Συγχρόνως, εξετάζονται τα περιουσιακά στοιχεία για την εφαρμογή ενός συστήματος συνεχούς διαχείρισης, όπου η μέθοδος CRAMM σίγουρα παίρνει μέρος στο αναλυτικό κομμάτι της προετοιμασίας.

ΚΕΦΑΛΑΙΟ 6

Συμπεράσματα, Μελλοντικές Προοπτικές και Προκλήσεις

Σε όλα όσα προηγήθηκαν έγινε σαφής η αξία και η επιτακτικότητα της εφαρμογής των διαδικασιών ανάλυσης και διαχείρισης κινδύνων σε έργα πληροφοριακών συστημάτων. Όσο μεγαλύτερο είναι το κόστος αυτών των έργων, η πολυπλοκότητά τους και η αξία τους για τη λειτουργία ενός οργανισμού, τόσο σημαντικότερο εργαλείο για την εξασφάλιση της επιτυχημένης υλοποίησης τους αποτελεί η ανάλυση και διαχείριση κινδύνων. Μέσα από αυτή μπορούν να προβλεφτούν τα προβλήματα που ενδέχεται να εμφανιστούν κατά την πορεία υλοποίησης του έργου και να προκαλέσουν σημαντικές απώλειες, είτε από πλευράς κόστους, είτε από πλευράς χρόνου ολοκλήρωσης των εργασιών, είτε στην ποιότητα και την αξιοπιστία του. Η ευθύνη της ανάλυσης και διαχείρισης κινδύνων δεν τελειώνει εδώ, καθώς καλείται να παρουσιάσει και τον τρόπο με τον οποίο θα μειωθεί η έκθεση του έργου στον κάθε κίνδυνο, να παρακολουθεί την εφαρμογή των μέτρων που συνέστησε αλλά και τον κίνδυνο που απομένει και μετά την εφαρμογή των μέτρων αυτών (Γεωργίου, 2012).

Η ανάλυση και διαχείριση κινδύνων, λοιπόν, είναι μία καθολική έννοια, εφαρμόσιμη σε όλο σχεδόν το εύρος της ανθρώπινης δραστηριότητας. Οι οργανισμοί που διαθέτουν τους κατάλληλους πόρους για την καλύτερη κατανόηση των κινδύνων που αντιμετωπίζουν και την αποτελεσματικότερη διαχείρισή τους, μπορούν όχι μόνο να αποφύγουν ‘απρόβλεπτες’ δυσκολίες, αλλά ταυτόχρονα να απελευθερώσουν πόρους προς άλλες κατευθύνσεις και να επωφεληθούν ευκαιριών (για νέες επενδύσεις), οι οποίες διαφορετικά, ενδεχομένως, να απορρίπτονταν ως απλά πολύ ‘επικίνδυνες’. Γίνεται, έτσι, αντιληπτό ότι η οργανωμένη προσπάθεια ανάλυσης και διαχείρισης κινδύνου έχει να προσφέρει σημαντική βοήθεια, όχι μόνο προς την κατεύθυνση αποφυγής ή καλύτερα ελέγχου επικίνδυνων καταστάσεων που σε διαφορετική περίπτωση θα θεωρούνταν απρόβλεπτες, αλλά ταυτόχρονα και προς τη θεώρηση νέων πρακτικών ή προσπαθειών που προσφέρουν σημαντικές ευκαιρίες. Πρόκειται, δηλαδή, για μια αυστηρά δομημένη διαδικασία, της οποίας τα βήματα θα πρέπει να εκτελούνται με επιμέλεια και σύνεση, καθώς μόνο έτσι θα καταφέρει να επιτύχει τους στόχους της. Ουσιαστικά, στόχος της εν λόγω διαδικασίας είναι η άρτια υλοποίηση του αρχικού σχεδιασμού εγκατάστασης του πληροφοριακού έργου, χωρίς αυτή να επηρεαστεί από απρόοπτα γεγονότα.

Καθώς λοιπόν οι κίνδυνοι είναι ένα φαινόμενο το οποίο ο άνθρωπος καλούταν πάντα να αντιμετωπίσει και θα συνεχίσει να το αντιμετωπίζει και στο μέλλον, η χρήση ορθολογικών και επιστημονικών διαδικασιών, όπως η ανάλυση και διαχείριση κινδύνων, θα είναι πάντοτε ένα χρήσιμο εργαλείο. Πολύ περισσότερο, μάλιστα, στην υλοποίηση πληροφοριακών έργων, εξαιτίας της πολυπλοκότητάς τους αλλά και των νέων τεχνολογιών που αυτά εισάγουν. Θα μπορούσαμε να πούμε ότι η διαχείριση επικινδυνότητας είναι ιδιαίτερα κρίσιμη για μεγάλα έργα, για έργα που χαρακτηρίζονται

από υψηλή αβεβαιότητα ή για έργα των οποίων μια πιθανή δυσλειτουργία θα μπορούσε να προκαλέσει μη αναστρέψιμες καταστροφές.

Οι τεχνικές εντοπισμού και αξιολόγησης των επερχόμενων κινδύνων βρίσκονται ακόμα σε εμβρυϊκό στάδιο ανάπτυξης. Η πλειοψηφία των υπεύθυνων έργων αποδίδει αυτό το φαινόμενο στο υψηλό κόστος και στην πίεση που τους ασκείται από τους ιδιοκτήτες έργων για γρήγορη περάτωση του έργου. Στην επιχειρηματολογία αυτή, όμως, δε λαμβάνεται υπόψη το γεγονός ότι μπορεί η ανάλυση κινδύνων να είναι χρονοβόρα και κοστοβόρα κατά τη φάση σχεδιασμού του έργου, όμως εξασφαλίζει την αποδοτικότερη και ασφαλέστερη περάτωσή του, αποφεύγοντας την επανάληψη διαδικασιών λόγω μη προνοητικότητας. Το κόστος ανάλυσης και διαχείρισης κινδύνων είναι πιο εύκολα μετρήσιμο σε σχέση με το κόστος καθυστέρησης παράδοσης ή μερικής αστοχίας του έργου, παρόλο που αυτό είναι κατά κανόνα μεγαλύτερο. Με άλλα λόγια, οι ιδιοκτήτες και πολλές φορές οι εργολάβοι έργων θεωρούν κόστος τα κεφάλαια που «βγαίνουν από την τσέπη τους» και αγνοούν τις συνέπειες μιας πιο μακροπρόθεσμης ή/και επιπρόσθετης δέσμευσης κεφαλαίων, λόγω υποεκτίμησης κάποιων κινδύνων. Είναι βέβαιο ότι αν επιχειρηθεί η ποιοτική ή/και ποσοτική ανάλυση των κινδύνων ενός ενδεικτικού έργου τους, θα βρεθούν προ εκπλήξεως με τα αριθμητικά αποτελέσματα και θα αναθεωρήσουν την άποψή τους.

Αξίζει να αναφερθεί, επίσης, ότι σήμερα χρησιμοποιούνται όλο και περισσότερο οι στρατηγικές ανάθεσης υπεργολαβιών και ασφάλισης των έργων, ώστε οι ανάδοχοι εταιρείες να περιορίζουν το μερίδιο ευθύνης τους κατά την εμφάνιση ενός κινδύνου. Η στρατηγική ανάθεσης υπεργολαβιών γίνεται αφενός για τη διασπορά του κόστους επένδυσης, ακόμα και αν αυτό σημαίνει μικρότερα περιθώρια κέρδους, και αφετέρου για τη διασπορά των ευθυνών ανάληψης ενός ρίσκου, που σε δεύτερο επίπεδο ανάγεται και πάλι σε όρους κόστους και απόδοσης του έργου. Η στρατηγική αυτή ενισχύεται και από τη διεθνή οικονομική και πολιτική κρίση, που βάζει «φρένο» σε τολμηρότερες και πιο δραστικές στρατηγικές (π.χ. μελέτες μετριασμού των κινδύνων).

Αυτό, όμως, που πρέπει να γίνει κατανοητό είναι ότι ακόμα και αν έχουν αντιμετωπιστεί κατάλληλα οι κίνδυνοι στις προηγούμενες φάσεις, δεν υπάρχει ποτέ πιθανότητα να εκτελεστεί ένας τόσο εξαντλητικός έλεγχος, ο οποίος να μπορέσει να διασφαλίσει ότι όλα θα λειτουργήσουν κατά το προσδοκώμενο και ότι τίποτα δε θα μπορέσει να προκαλέσει μια αποτυχία του λογισμικού. Η πρόβλεψη κινδύνων, δηλαδή, σε οποιαδήποτε ενέργεια μας είναι αδύνατη, από την άποψη ότι οι πιθανοί συνδυασμοί ενεργειών που μπορούν να προκαλέσουν πρόβλημα είναι άπειροι. Ο δυσκολότερος παράγοντας είναι η ανθρώπινη φύση που κρύβει εκπλήξεις, άλλοτε ευχάριστες και άλλοτε δυσάρεστες. Αξίζει να αναφερθεί ότι η επιτυχημένη κατάρτιση ενός σχεδίου ανάλυσης και διαχείρισης κινδύνων οφείλεται σε μεγάλο βαθμό στην εμπειρία, στις ικανότητες, στην οξυδέρκεια, στη διορατικότητα και στην επιμέλεια των προσώπων που θα κληθούν να το συντάξουν.

Συγκεκριμένα, λοιπόν, η ανάλυση και διαχείριση κινδύνων του ΣΔΑΠ ανάδειξε σημαντικά προβλήματα και ελλείψεις ασφάλειας, τα οποία θα πρέπει να αντιμετωπιστούν. Το καλό είναι ότι τα περισσότερα από αυτά μπορούν να επιλυθούν με ιδία μέσα από την ίδια την εταιρεία, οπότε έχουν και μικρότερο κόστος υλοποίησης.

Η ανάλυση και διαχείριση κινδύνων, όμως, είναι μια συνεχής διαδικασία. Μετά την υλοποίηση των μέτρων προστασίας για την αντιμετώπιση των κινδύνων, πρέπει να υπάρχει συνεχής παρακολούθηση ώστε να διασφαλίζεται η σωστή και ικανοποιητική λειτουργία των πληροφοριακών συστημάτων του ΣΔΑΠ.

Σε γενικά πλαίσια, θα μπορούσαμε να πούμε ότι το πληροφοριακό σύστημα του ΣΔΑΠ είναι ένα ασφαλές πληροφοριακό σύστημα, προστατευόμενο από πολλών ειδών απειλές, είτε αυτές είναι ανθρώπινος παράγοντας, είτε φυσικό φαινόμενο. Οι αδυναμίες που παρουσιάζει δεν είναι σε θέση να το καταστήσουν εξαιρετικά ευάλωτο, ενώ το ποσοστό των απειλών που μπορεί να είναι επιβλαβείς παραμένει σε σχετικά χαμηλά επίπεδα. Υπάρχουν περιθώρια βελτίωσης, προκειμένου να αυξηθεί η ασφάλειά του και να μειωθεί ο βαθμός επικινδυνότητας των απειλών. Οι προτάσεις των αντιμέτρων είναι ικανές να μειώσουν αυτό τον βαθμό.

Όσον αφορά τη μελλοντική έρευνα, είναι γεγονός ότι η ανάλυση και διαχείριση κινδύνων αποτελεί έναν καινούργιο, αναγκαίο πλέον και κατ' επέκταση συνεχώς αναπτυσσόμενο κλάδο του management, ο οποίος χρησιμοποιείται σε ένα ολοένα και αυξανόμενο εύρος δραστηριοτήτων. Επίσης, οι μεθοδολογίες που αναφέρθηκαν για αρκετά μεγάλα επιχειρησιακά προγράμματα με μεγάλο πλήθος έργων απαιτούν τεράστιο αριθμό πράξεων, που δυσκολεύουν πολύ το έργο των αποφασιζόντων-κριτών και χρειάζονται ένα πολύπλοκο Ολοκληρωμένο Πληροφορικό Σύστημα (ΟΠΣ) για την υποστήριξή τους. Για τους λόγους αυτούς, η ανάλυση και διαχείριση κινδύνων, στη μορφή που είναι σήμερα και τη γνωρίσαμε όσο μπορούσαμε στα πλαίσια της παρούσας εργασίας, είναι ακόμα σε πρωταρχικό στάδιο.

Μια πολύ καλή πρόταση θα ήταν να δοθεί περισσότερη έκταση στη διαδικασία ανάλυσης της επικινδυνότητας των συστημάτων, αναλύοντας τα εργαλεία λογισμικού που υπάρχουν και να εκτιμηθεί η επικινδυνότητα μέσω ενός τέτοιου λογισμικού, όπως το CRAMM. Σε κάθε περίπτωση, το ανθρώπινο μυαλό δε μπορεί να προβλέψει τα πάντα. Με το κατάλληλο λογισμικό, όμως, η διαδικασία αυτή γίνεται ευκολότερη και δεν υπάρχει πιθανότητα παράλειψης.

Η συγκεκριμένη εργασία, επίσης, αποδεικνύοντας το γεγονός ότι πάντα υπάρχει ένα ποσοστό επικινδυνότητας που απομένει μετά την ολοκλήρωση του ελέγχου του λογισμικού, παρέχει μια καλή βάση πάνω στην οποία μπορεί να στηριχτεί περαιτέρω έρευνα του πεδίου που προκύπτει από τη συσχέτιση των εννοιών της διαχείρισης επικινδυνότητας λογισμικού και του ελέγχου που διεξάγεται σε αυτό.

Πιο συγκεκριμένα, λαμβάνοντας κανείς τους παράγοντες που επηρεάζουν το ποσοστό της εναπομείνασας επικινδυνότητας, θα μπορούσε να κάνει μια προσπάθεια ποσοτικοποίησής τους και ανεύρεσης κατάλληλων μετρικών, ώστε να δοθεί τελικά η δυνατότητα υπολογισμού αυτού του ποσοστού μέσω μαθηματικού τύπου. Επίσης, θα μπορούσε να πραγματοποιηθεί μοντελοποίηση της επικινδυνότητας του λογισμικού σε σχέση πάντα με τον έλεγχο.

Η έρευνα που πραγματοποιήθηκε στο πλαίσιο της παρούσας εργασίας θα μπορούσε, επίσης, να αποτελέσει το εφαλτήριο για μια ενδελεχή και ευρείας κλίμακας έρευνα, αποτελώντας αφορμή για σχολιασμό και προβληματισμό. Αυτό που είναι

σημαντικό να επιτευχθεί είναι ένας κατάλληλος ποιοτικός, αλλά κυρίως ποσοτικός, συνδυασμός της επικινδυνότητας του λογισμικού με τα διάφορα κριτήρια ποιότητας που το χαρακτηρίζουν, όπως είναι για παράδειγμα η αξιοπιστία ή η ασφάλεια, ώστε να παρέχεται στον ενδιαφερόμενο μια πληρέστερη και ακριβέστερη εικόνα του.

Υπάρχουν, επίσης, προοπτικές για περαιτέρω ανάπτυξη των σταδίων αναγνώρισης και αποτίμησης του κινδύνου καθώς και ανακάλυψης νέων μεθόδων εκτίμησης κινδύνου, ποιοτικής και κυρίως ποσοτικής, εύκολα χρησιμοποιήσιμες, αποδεδειγμένες και ελεγμένες μέσα από αρκετό χρόνο εφαρμογής. Επιπλέον, με τα χρόνια θα αναπτυχθούν και εργαλεία λογισμικού, προγράμματα και ολοκληρωμένα πληροφοριακά συστήματα για την ακριβή, εύκολη και έγκυρη εφαρμογή των μεθόδων και μεθοδολογιών ανάλυσης και διαχείρισης κινδύνων. Τέλος, άλλο ένα πεδίο με προοπτικές ανάπτυξης είναι η λήψη συλλογικών αποφάσεων και, κυρίως, η σύνθεση των επιμέρους αποφάσεων.

Η κατανομή των ρόλων είναι ένα ακόμα κομμάτι στο οποίο μπορεί να υπάρξει πλούσιο πεδίο για μελλοντική επέκταση. Οργανισμοί και επιχειρήσεις έχουν υποστεί καταστροφικά λάθη εξαιτίας λανθασμένων επιλογών στο κρίσιμο αυτό ζήτημα. Εκτός από τα παραπάνω, στο μέλλον θα μπορούσε κάποιος να εργαστεί πάνω στη βελτίωση της παρουσίασης των γραπτών αναφορών. Είναι σημαντικό, ο διαχειριστής να μελετάει μια αναφορά η οποία είναι οπτικά ελκυστική και τον βοηθάει στο να επικεντρωθεί στα καίρια σημεία της και, επίσης, έχει όσο το δυνατόν καλύτερες και κατατοπιστικές προτάσεις. Κάτι τέτοιο θα μπορούσε ως ένα βαθμό να επιτευχθεί, πιθανώς, με την προσθήκη στατιστικών γραφημάτων σε ορισμένα σημεία.

Τέλος, είναι γεγονός ότι στις διάφορες εταιρείες αυτό που έχει σημασία στο τέλος της ημέρας είναι το κόστος. Θα μπορούσαν, λοιπόν, να προστεθούν στο έργο ερωτήσεις, μέσα από τις οποίες στην τελική αναφορά θα προκύπτει κάποιο συμπέρασμα για το οικονομικό κόστος που θα υπάρξει από μια ενδεχόμενη παραβίαση ασφάλειας. Αυτό είναι ένα επιχείρημα που πείθει τους περισσότερους διοικητικούς στη λήψη των αναγκαίων μέτρων.

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Alberts C., Dorofee A., “Managing Information Security Risks: The OCTAVE(SM) Approach”, Addison Wesley, 2002.

2. Barki H., “Rethinking the Concept of User Involvement”, M.I.S. Quarterly, Volume 13 (1989), Pages 53-63.

3. Chapman C., Ward S., “Project risk management: processes, techniques and insights”, John Wiley & Sons, 1996.

4. Ding T., “Quantitative Risk Analysis Step-By-Step”, SANS Institute, 2002.

5. Eloff J., Labuschangne L. and Badenhorst K., “A comparative framework for risk analysis methods”, Computers & Security, Volume 12 (1993), No 6, Pages 597-603.

6. Gallati R., “Risk Management and Capital Adequacy”, McGraw Hill, 2003.

7. Garrity E., and Sanders G.L., “Introduction to Information Systems Success Measurement IDEA Group Publishing”, Hershey, U.S.A. 1998.

8. Gerber M. and Solms R., “Management of risk in the information age”, Computers & Security, Volume 24 (2005), Pages 6-30.

9. Hamilton S. and Chervany N.L., “Evaluating Information Systems Effectiveness Part I: Comparing Evaluation Approaches”, MIS Quarterly, Volume 5 (1981), No 3, Pages 55-69.

10. Hamilton S. and Chervany N.L., “Evaluating Information Systems Effectiveness Part II: Comparing Evaluator Viewpoints”, MIS Quarterly, Volume 5 (1981), No 4, Pages 79-86.

11. Holmes A. and Poulimenakou A., “Towards a conceptual framework for investigating Information Systems failure”, Europ. Jour. Of Infor. Systems, Volume 5 (1996), Pages 34-46.

12. Lyytinen K. and Hirschheim R., “Information Systems failures: a survey and classification of the empirical literature”, Oxford Surveys in Information Technology, Volume 4 (1987), Pages 257-309.

13. Murthi S., “Preventive Risk Management for Software Projects”, IEEE, 2002.

14. Nichols A., “A Perspective on Threats in the Risk Analysis Process”, SANS Institute, 2002.

15. RAC (Risk Analysis Consultants) s.r.o. CRAMM Case Study (http://www.rac.cz/rac/homepage.nsf/EN/CRAMM/$FILE/RAC%20CRAMM-Case%20study_Datasheet_EN_100908%20Print.pdf), Czech, 2010.

16. Ritchie B., Marshall D., “Business risk management”, Chapman & Hall, 1993.

17. Stoneburner G., Goguen A. and Feringa A., “Risk Management Guide for Information Technology Systems”, NIST (2001).

18. Symons V.J., “A review of Information Systems Evaluation: content, context and process”, Europ. Jour. Of Infor. Systems, Volume 1 (1991), No 3, Pages 205-212.

19. Turn R., “Security and Privacy requirements in computing”, Proceedings of 1986 ACM Fall joint computer conference (1986), Pages 1106-1114.

20. Visintine V., “An Introduction to Information Risk Assessment”, SANS Institute, 2003.

21. Wolstenholme E.F., Henderson S. and Gavine A., “The Evaluation of Management Information Systems: a Dynamic and Holistic Approach”, Published John Wiley, England 1993.

22. Γεωργίου Σ. “Ανάλυση και διαχείριση επικινδυνότητας στα Πληροφοριακά Συστήματα – Υλοποίηση μεθοδολογίας σε επιχειρησιακό περιβάλλον”, Μεταπτυχιακή Διατριβή, Μεταπτυχιακό Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιά, 2012.

23. Δημοσχάκης Λ. “Ανάλυση του εργαλείου CRAMM”, Διπλωματική Εργασία, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά, 2010.

24. Δρυμούσης Χ. “Διαχείριση έργων και κινδύνων έργων – Μελέτη περίπτωσης σε κατασκευαστικό έργο”, Διπλωματική Εργασία, Διαπανεπιστημιακό Πρόγραμμα Μεταπτυχιακών Σπουδών στη Διοίκηση Επιχειρήσεων, Athens MBA, 2007.

25. Θωμά - Τσοπουρίδου Μ. “Διαχείριση κινδύνου σε τεχνικά έργα: Θεωρία και πράξη”, Διπλωματική Εργασία, Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών στη Διοίκηση Επιχειρήσεων, 2011.

26. Κάτσικας Σ. “Ασφάλεια υπολογιστών”, Μελέτη, Σχολή Θετικών Επιστημών και Τεχνολογίας, Ελληνικό Ανοικτό Πανεπιστήμιο, 2001.

27. Κιουντούζης Ε., “Διαχείριση έργων πληροφορικής”, Εκδόσεις Αθ. Σταμούλης, Αθήνα 2004.

28. Λέρα Μ. “Μελέτη ασφάλειας πληροφοριών και Πληροφοριακών Συστημάτων”, Διπλωματική Εργασία, Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών, Πανεπιστήμιο Δυτικής Μακεδονίας, 2012.

29. Μανούσης Ν. “Ευφυές δυναμικό σύστημα διαχείρισης κινδύνου για τη μοντελοποίηση, βέλτιστη προσαρμογή και εγκατάσταση συστημάτων διαχείρισης επιχειρησιακών πόρων”, Διπλωματική Εργασία, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο, 2003.

30. Μπέλιας Ν. “Η δυναμική των συστημάτων στην αποτίμηση και βελτίωση της αποτελεσματικότητας των Πληροφοριακών Συστημάτων”, Διπλωματική Εργασία, Μεταπτυχιακό Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών, 1999.

31. Νικήτας Γ. “Ανάλυση κινδύνων Πληροφοριακών Συστημάτων”, Διπλωματική Εργασία, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Η/Υ, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2004.

32. Ξανθόπουλος Ν., “Σύγχρονες τεχνικές ανάλυσης και διαχείρισης κινδύνου (risk management) – Εφαρμογή σε επιχειρησιακό πρόγραμμα του Γ’ ΚΠΣ”, Διπλωματική Εργασία, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο, 2004.

33. Πετραντωνάκης Π. “Διοίκηση κινδύνου σε Πληροφοριακά Συστήματα – Εφαρμογές σε συστήματα Εθνικής Άμυνας”, Διδακτορική Διατριβή, Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιά, 2008.

34. Τσουτσαίος Α. “Τεχνικές διαχείρισης κινδύνων για την υλοποίηση πληροφοριακών έργων”, Διπλωματική Εργασία, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο, 2005.