Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

Αναγνώριση και Μοντελοποίηση Κινδύνου σε Μονάδες του Τομέα Υγείας

Διπλωματικη Εργασια

της

ΜΑΡΚΕΛΛΑΣ ΧΑΛΛΙΟΡΗ

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής ΕΜΠ

Αθήνα, Οκτώβριος 2020

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

Αναγνώριση και Μοντελοποίηση Κινδύνου σε Μονάδες του Τομέα Υγείας

Διπλωματικη Εργασια

της

ΜΑΡΚΕΛΛΑΣ ΧΑΛΛΙΟΡΗ

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 27/10/2020.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Αναπληρωτής Καθηγητής ΕΜΠ

Αθήνα, Οκτώβριος 2020

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Ηλεκτρικων Βιομηχανικων Διαταξεων και Συστηματων Αποφασεων

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

(Υπογραφή)

.....
Μαρκέλλα Χαλλιορή

27/10/2020

Περίληψη

Το ερευνητικό πεδίο της παρούσας διπλωματικής εργασίας αφορά στη διαχείριση του κινδύνου που εμφανίζεται στο περιβάλλον μονάδων του Τομέα Υγείας. Το σύστημα υγείας, ένας από τους βασικότερους θεσμούς του κοινωνικού κράτους, κρίνεται αποτελεσματικό όταν διασφαλίζει και βελτιώνει το επίπεδο υγείας των πολιτών με απώτερο σκοπό τη βελτίωση της ποιότητας ζωής τους. Η σημασία και η δυσκολία του εγχειρήματος αυτού είναι προφανής εάν σκεφτεί κανείς τις απειλές που ελλοχεύουν, που, εκτός από λειτουργίες του συστήματος ως οργανισμού, μπορεί να διακινδυνεύουν την απώλεια ανθρώπινων ζωών. Το περιβάλλον αυτό, εξαιτίας της κρισιμότητας του Τομέα Υγείας στην διατήρηση κοινωνικής ευημερίας, παρουσιάζει ιδιάζουσα πολυπλοκότητα που οφείλει να μοντελοποιείται επαρκώς σε κάθε πρόβλημα απόφασης. Η εισαγωγή της τεχνολογίας στον τομέα της υγείας και η ψηφιοποίηση των δεδομένων των ασθενών αλλά και των οργανωτικών και διαγνωστικών διαδικασιών, έχει συμβάλλει στην αυτοματοποίηση και την αύξηση των δεικτών απόδοσης. Ταυτόχρονα όμως, εισάγει στο περιβάλλον αυτό πολλές νέες απειλές. Καθώς περνούν τα χρόνια και οι κίνδυνοι στον κυβερνοχώρο γίνονται γνωστότεροι, γίνεται ολοένα και πιο συστηματική η προσπάθεια διαφύλαξης της ασφάλειας των πληροφοριών μέσω της δημιουργίας ισχυρότερων υπολογιστικών και πληροφοριακών συστημάτων.

Για τον σκοπό αυτό, παρουσιάζεται και μελετάται το μοντέλο GIRA, που ενσωματώνει μεθόδους Πολυκριτήριας Ανάλυσης Αποφάσεων στο ευρύτερο πλαίσιο των μεθοδολογιών Διαχείρισης Ρίσκου. Το μοντέλο που προτείνεται βασίζεται στη γενική θεωρία των διαγραμμάτων ροής, όμως χάρη στη δομή του, επιτυγχάνει μία υψηλού βαθμού δόμηση των προβλημάτων απόφασης που εμπεριέχουν τον παράγοντα του κινδύνου. Η αποδοτικότητα της χρήσης του μοντέλου ως εργαλείο υποστήριξης λήψης αποφάσεων καταδεικνύεται μέσω της χρήσης του σε 3 εφαρμοσμένα σενάρια κινδύνου.

Λέξεις Κλειδιά

Κίνδυνος, Διαχείριση κινδύνου, Εκτίμηση κινδύνου, GIRA model, Κυβερνοασφάλεια, Κρίσιμες Υποδομές, Σύστημα Υγείας

Abstract

The research field of this thesis concerns the management of the risk that appears in the environment of units of the Health Sector. The health system, one of the most basic institutions of the welfare state, is considered effective when it ensures and improves the level of health of citizens with the ultimate goal of improving their quality of life. The importance and difficulty of this endeavor is obvious if one considers the threats that lurk, which, in addition to the functions of the system as an organism, can endanger the loss of human lives. This environment, due to the criticality of the Health Sector in maintaining social well-being, presents a special complexity that must be adequately modeled on each decision problem. The introduction of technology in the field of health and the digitization of patient data as well as organizational and diagnostic procedures, has contributed to the automation and increase of performance indicators. At the same time, however, it introduces many new threats to this environment. As the years go by and the dangers in cyberspace become more known, the effort to safeguard information security through the creation of more powerful computer and information systems becomes more and more systematic.

For this purpose, the GIRA model is presented and studied.It incorporates Multi-Criteria Decision Analysis methods in the wider context of Risk Management methodologies. The proposed model is based on the general theory of flowcharts, but thanks to its structure, it achieves a high degree of structuring of decision problems involving the risk factor. The efficiency of using the model as a tool to support decision making is demonstrated through its use in 3 applied risk scenarios.

Keywords

Risk, Risk Management, Risk Assessment, GIRA model, Cybersecurity, Critical Infrastructure, Health System, Healthcare

στην οικογένειά μου

Ευχαριστίες

Θα ήθελα καταρχήν να ευχαριστήσω τον καθηγητή κ. Ασκούνη για την επίβλεψη αυτής της διπλωματικής εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω στο εργαστήριο Συστημάτων Αποφάσεων. Επίσης ευχαριστώ ιδιαίτερα τους Μιχαήλ Κοντούλη και Γιώργο Δούκα για την συνεργασία και την καθοδήγησή τους. Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου και τους φίλους μου, που με στήριζαν σε όλη αυτή την προσπάθεια.

27/10/2020

Μαρκέλλα Χαλλιορή

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Από την αρχαιότητα, η περιέργεια του ανθρώπου είναι αυτή που, μεταξύ των ενστικτωδών ορμών του, τον χαρακτηρίζει ως ον περισσότερο από κάθε άλλη. Η κατανόηση του κόσμου μέσω εμπειρικών διαδικασιών και η κατάκτηση της γνώσης του παρόντος, γρήγορα έδωσαν τη θέση τους στη δίψα για την πρόβλεψη του μέλλοντος. Αυτή η αγωνία για όσα πρόκειται να συμβούν, έγινε κινητήριος δύναμη και έσπρωξε τον άνθρωπο προς την έρευνα. Η ύπαρξη μοτίβων και περιοδικότητας σε πολλά φυσικά φαινόμενα, είχε επιτρέψει σε επιστήμονες και παρατηρητές να γνωρίζουν με ακρίβεια πότε θα γίνει έκλειψη ηλίου, ή την ταχύτητα με την οποία θα φτάσει στο έδαφος μία πέτρα συγκεκριμένου βάρους εάν αφεθεί από συγκεκριμένο ύψος. Η κατάρρευση του αυστηρού ντετερμινισμού ήρθε στα τέλη του 19ου αιώνα, με την εισαγωγή του όρου της αβεβαιότητας στις εξισώσεις της κβαντικής φυσικής. Η επιστημονική σκέψη κλονίστηκε διαπιστώνοντας τον αντικειμενικό χαρακτήρα της τυχαιότητας και κλήθηκε τότε πρώτη φορά να μοντελοποιήσει αντί-αιτιοκρατικές έννοιες. Δεν άργησε να γίνει καθολική η παραδοχή ότι, στο μικρόκοσμο, κάθε προσπάθεια πρόβλεψης είναι μάταιη.

Εξίσου μάταιη φαίνεται να είναι η προσπάθεια πρόβλεψης του μέλλοντος και στις σύγχρονες κοινωνίες, όπου η πληθώρα δεδομένων, τα ιδιάζοντα κοινωνικά σύνολα και η κυριαρχία της τεχνολογίας σε κάθε τομέα της καθημερινής ζωής, καθιστούν την μοντελοποίηση του περιβάλλοντος και την έγκαιρη προσαρμογή στις αλλαγές του, ιδιαίτερα απαιτητική διαδικασία. Παρ' όλα αυτά, στο σημερινό κόσμο, που λειτουργεί με όρους αποδοτικότητας και ταχύτητας, είναι πιο αναγκαία από ποτέ η ταυτοποίηση όλων των απειλών και η προετοιμασία, ώστε όταν αυτές πραγματοποιηθούν, το εκάστοτε σύστημα να είναι σε θέση να τις αποκρούσει χωρίς να υπάρξουν απώλειες. Αυτή η αναγκαιότητα είναι που οδήγησε στη δημιουργία των κλάδων της Εκτίμησης και της Διαχείρισης Ρίσκου (Risk Assessment, Risk Management) και την ενσωμάτωσή τους ως βασικές λειτουργίες κάθε οργανισμού. Στόχος είναι η παροχή ενός εργαλείου υποστήριξης λήψης αποφάσεων, το οποίο λαμβάνει υπόψη την πιθανότητα υλοποίησης των κινδύνων και την έλλειψη σιγουριάς του περιβάλλοντος, προς την κατεύθυνση της επίτευξης των επιδιώξεων ενός οργανισμού.

1.1 Περιγραφή και τόμος της εργασίας

Το σύστημα υγείας, ένας από τους βασικότερους θεσμούς του κοινωνικού κράτους, κρίνεται αποτελεσματικό όταν διασφαλίζει και βελτιώνει το επίπεδο υγείας των πολιτών με απώτερο

σκοπό τη βελτίωση της ποιότητας ζωής τους. Η σημασία και η δυσκολία του εγχειρήματος αυτού είναι προφανής εάν σκεφτεί κανείς τις απειλές που ελλοχεύουν, που, εκτός από λειτουργίες του συστήματος ως οργανισμού (για παράδειγμα οικονομικές) μπορεί να διακινδυνεύουν την απώλεια ανθρώπινων ζωών. Τις τελευταίες δεκαετίες με την επιβολή του κυβερνοχώρου ως κυρίαρχου μέσου σύνδεσης της παγκόσμιας κοινωνίας, οι όροι της επικοινωνίας, της συναλλαγής αλλά και της ασφάλειας έχουν αλλάξει. Ιδιαίτερα στον τομέα της υγείας, που στηρίζεται σε πληροφοριακά και επικοινωνιακά δίκτυα για την εκπόνηση των λειτουργιών και τη στήριξη του ιατρικού εξοπλισμού, η υψηλή εξάρτηση από αυτά τον καθιστά ευάλωτο σε κυβερνοεπιθέσεις. Εξαιτίας λοιπόν τη πληθώρας απειλών, κρίνεται αναγκαία για την ομαλή και ασφαλή διεκπαιραίωση των δραστηριοτήτων των ιατρικών μονάδων η ύπαρξη ενός πλάνου Διαχείρισης Κινδύνου. Η παρούσα διπλωματική εργασία έχει ως στόχο την μοντελοποίηση του ρίσκου που αντιμετωπίζουν οι μονάδες του τομέα υγείας (δημόσια νοσοκομεία, ιδιωτικές κλινικές, ιατρεία) και την ανάδειξη του τρόπου με τον οποίο ένα πλάνο Διαχείρισης Ρίσκου λειτουργεί υποστηρικτικά στη διαδικασία λήψης αποφάσεων. Στα 3 εφαρμοσμένα σενάρια που θα παρουσιαστούν, καταγράφονται οι ενδεχόμενες απειλές, εντοπίζονται τα ευάλωτα σημεία του συστήματος και προτείνονται εναλλακτικές που υπόσχονται να θωρακίσουν το σύστημα ενάντια στους κινδύνους λαμβάνοντας τα κατάλληλα μέτρα. Θα προταθεί και θα εφαρμοστεί μία μεθοδολογία ανάλυσης ρίσκου βασισμένη στο GIRA model, και στα πλαίσια αυτής θα παρουσιαστούν διαγραμματικά οι κίνδυνοι που αντιμετωπίζουν οι σύγχρονες μονάδες υγείας.

1.2 Οργάνωση του τόμου

Η εργασία αυτή είναι οργανωμένη σε 6 κεφάλαια.

Στο κεφάλαιο 1, γίνεται μία γενική εισαγωγή στο θέμα, δηλαδή στην πολυπλοκότητα του περιβάλλοντος μέσα στο οποίο καλούμαστε να λάβουμε αποφάσεις και στην σημασία και αναγκαιότητα περιορισμού του κινδύνου που υπεισέρχεται στην διαδικασία λήψης αποφάσεων από μονάδες του τομέα Υγείας.

Στο κεφάλαιο 2, τίθεται το θεωρητικό υπόβαθρο για την μελέτη του προβλήματος. Πιο συγκεκριμένα δίνεται ο ορισμός της (επιχειρηματικής) έννοιας του κινδύνου και των χαρακτηριστικών μεγεθών του και εξετάζεται ένα ιδιάζον είδος κινδύνου, αυτού στον κυβερνοχώρο. Για το σκοπό αυτό καθορίζονται οι βασικές παράμετροι των κυβερνοαπειλών και της κυβερνοασφάλειας. Προσεγγίζεται η λογική του κλάδου Λήψης Αποφάσεων, μέσω της παρουσίασης των αρχών των Συστημάτων Υποστήριξης Αποφάσεων και της Πολυκριτήριας Ανάλυσης Αποφάσεων. Στη συνέχεια παρατίθεται ο ορισμός της διαδικασίας Διαχείρισης Ρίσκου, Risk Management, και μέσω παραδειγμάτων διαφορετικών μεθόδων (Risk Matrix, Fault Tree Analysis, Event Tree Analysis, GIRA model) και κατάδειξης των μεταξύ τους διαφορών ως προς τη θεώρηση του κινδύνου, γίνεται κατανοητό το εύρος εφαρμογής αυτών.

Στο κεφάλαιο 3, παρουσιάζεται η θεωρία που σχετίζεται με τις Κρίσιμες Υποδομές. Συγκεκριμένα, αναφέρονται τα κριτήρια σύμφωνα με τα οποία οι υποδομές κατατάσσονται σε

κρίσιμες και μη, τα διαφορετικά είδη αλληλεξαρτήσεων που παρουσιάζουν μεταξύ τους και πότε αποτυγχάνουν. Τέλος περιγράφονται διεθνείς οργανισμοί και πρότυπα, με βάση τα οποία προστατεύονται οι Κρίσιμες Υποδομές.

Το κεφάλαιο 4 αφορά τις Υπηρεσίες Υγείας, μία από τις Κρίσιμες Υποδομές κάθε κράτους. Δίνεται ο ορισμός των μονάδων υγείας, υποδεικνύονται οι οικονομικοί και μη οικονομικοί τους στόχοι και τα γενικά χαρακτηριστικά του Συστήματος Υγείας. Τέλος εξετάζεται ο ψηφιακός μετασχηματισμός του Συστήματος Υγείας, μέσα από τις υπηρεσίες του ηλεκτρονικού φακέλου, της ηλεκτρονικής υγείας και της κινητής υγείας.

Στο κεφάλαιο 5 γίνεται μοντελοποίηση σεναρίων ρίσκου που αφορούν την τοπολογία ενός ιατρείου, για να σκοπό να γίνει κατανοητό το πώς η εφαρμογή μεθόδων Διαχείριση Κινδύνου είναι απαραίτητη για τη λήψη δομημένων αποφάσεων.

Στο κεφάλαιο 6 παρουσιάζονται τα συμπεράσματα της μελέτης.

Μέρος I

Θεωρητικό Μέρος

Κεφάλαιο 2

Θεωρητική προσέγγιση

Δεν υπάρχει αμφιβολία για το γεγονός ότι όσο ζούμε είμαστε εκτεθειμένοι σε χιλιάδες κινδύνους, άλλους λιγότερο και άλλους περισσότερο σοβαρούς. Παίρνοντας διαφορετική μορφή και βαρύτητα, η έννοια του κινδύνου εισάγεται σε όλες τις εκφάνσεις της καθημερινότητας, διατηρώντας την ιδιότητά της ως καθοριστικό κριτήριο στη διαδικασία λήψης αποφάσεων. Άλλοι τον αποφεύγουν κάνοντας συντηρητικές επιλογές, άλλοι προσπαθούν να τον μετριάσουν λαμβάνοντας μέτρα απόκρουσης, ενώ υπάρχουν και αυτοί που διακινδυνεύουν τα πάντα, ελπίζοντας στη μη πραγματοποίηση του κινδύνου και στην απρόσκοπτη επίτευξη των στόχων τους. Έτσι, θα μπορούσαμε να πούμε ότι, οι διαφορετικές στρατηγικές αντιμετώπισης είναι αυτές που καθορίζουν τελικά τη φιλοσοφία ζωής του ανθρώπου.

Παρόλα αυτά, εξαιτίας του εύρους σημασίας και εφαρμογών του όρου ¨κίνδυνος¨, αναδεικνύεται δύσκολη η ακριβής σκιαγράφηση της έννοιας και των προεκτάσεων της. Ποιά είναι λοιπόν τα χαρακτηριστικά που κατέστησαν το ρίσκο αντικείμενο επιστημονικής μελέτης και ενσωμάτωσαν την εκτίμηση και τη διαχείρισή του στις βασικές λειτουργίες ενός οργανισμού;

Ο θεμελιώδης λόγος ύπαρξης και η βασικότερη μετρική βιωσιμότητας ενός οργανισμού είναι η εκπλήρωση των στόχων του. Με την πάροδο των αιώνων, εξαιτίας της δαιδαλώδους ανάπτυξης του κοινωνικοπολιτικού γίγνεσθαι, των τεχνολογικών, οικονομικών και περιβαλλοντικών δεδομένων και τη συνεχή αλληλοσύνδεσή τους, η οικονομική ευημερία έχει πάψει να είναι αποκλειστική επιδίωξη. Πλέον οι στόχοι σχετίζονται με ολόκληρο το εύρος των δραστηριοτήτων, από στρατηγικές πρωτοβουλίες μέχρι βασικές λειτουργίες και μεταφράζονται, εκτός από τους οικονομικούς, σε όρους κοινωνικών, περιβαλλοντικών, τεχνολογικών και πολιτικών επιπτώσεων, που δεν πρέπει να ξεφεύγουν από τις νομικές υποχρεώσεις του φορέα και τη διατήρηση καλής φήμης. Η κύρια κατεύθυνση που ακολουθείται, λαμβάνοντας υπόψη τους στόχους, τις δυνάμεις και τις δυνατότητες, αποτελεί τη **στρατηγική** του οργανισμού. Ο προσδιορισμός της στρατηγικής περιλαμβάνει ένα σύνολο επιμέρους αλληλοεξαρτώμενων προβλημάτων, όπως η διάγνωση της ισχύουσας κατάστασης, ο καθορισμός των στόχων, καθώς και η επιλογή, η εφαρμογή και η αξιολόγηση της επιχειρηματικής στρατηγικής[1].

Η ανάγκη ανάπτυξης του κλάδου Διαχείρισης Ρίσκου κατέστη επιτακτική, ώστε να καθοδηγήσει τις οντότητες, επιχειρηματικές και μη, στην αναζήτηση βέλτιστων αποφάσεων, σε ένα περιβάλλον συνεχώς μεταβαλλόμενο (παγκοσμιοποίηση, χρηματαγορές, ανταγωνισμός, καινοτομίες κ.λπ.) το οποίο παρέχει νέες ευκαιρίες ανάπτυξης, αλλά ταυτόχρονα δημιουργεί και νέους κινδύνους. Χάρη στην εφαρμογή εξειδικευμένων μεθοδολογιών, οι οργανισμοί μπορούν να λειτουργήσουν στο πλαίσιο ενός κόσμου που ο κίνδυνος είναι πλέον καταγε-

γραμμένος και ει δυνατόν, σταθμισμένος, δίνοντας βάση σε χαρακτηριστικά της σύγχρονης εποχής όπως η σημαντικότητα της επιχειρηματικής γνώσης και ο αυξημένος ρόλος διαχείρισης ανθρώπινου δυναμικού.

2.1 Τί είναι κίνδυνος;

2.1.1 *Ορισμός Παραγόντων Κινδύνου*

Παρακάτω παρατίθενται οι βασικές έννοιες που απαιτούνται για την κατανόηση της διαδικασίας Διαχείρισης Ρίσκου.

Συντελεστές - Παράγοντες Κινδύνου

Συντελεστές του κινδύνου (*risk factors*) είναι τα ποιοτικά και ποσοτικά χαρακτηριστικά του, που αναλύονται ώστε αυτός να ταξινομηθεί και να αντιμετωπιστεί κατάλληλα.Οι μεθοδολογίες που εφαρμόζονται για την εκτίμηση του ρίσκου, λαμβάνουν ως είσοδο τους συντελεστές και την μεταξύ τους σχέση, με στόχο να καταφέρουν να σκιαγραφήσουν το περιβάλλον και να παρέχουν τις απαραίτητες πληροφορίες στα ενδιαφερόμενα μέρη (stakeholders) που καλούνται να λάβουν τις αποφάσεις. Η σημασία της ¨αποσύνθεσης¨ του κινδύνου στα επιμέρους χαρακτηριστικά του, έγκειται στο ότι, χάρη στην αποδόμηση αυτή, η διαδικασία αποκτά καθολικότητα και γίνεται πιο εύκολη, αφού όλοι οι κίνδυνοι συγκρίνονται σε κοινή βάση ανεξάρτητα από τη λειτουργία την οποία αφορούν.Οι πιο ευρέως χρησιμοποιούμενοι συντελεστές ρίσκου είναι: *η απειλή* (threat), *τα ευαίσθητα σημεία* (vulnerabilities), *η πιθανότητα υλοποίησης* (likelihood).

Απειλή (threat)

Ως απειλή ορίζεται η ενδεχόμενη ζημιά, ή αλλιώς οποιαδήποτε περίσταση/ γεγονός, που μπορεί να έχει αρνητική επίδραση στις λειτουργίες, τα περιουσιακά στοιχεία ενός οργανισμού, ή στα άτομα που εμπλέκονται.

Με βάση το κίνητρο της ¨πηγής" από την οποία προέρχεται, μία απειλή μπορεί να χαρακτηριστεί ως κακόβουλη/ ανταγωνιστική (adversarial) εάν πρόκειται για συνειδητή προσπάθεια καταστροφής, ή μη κακόβουλη/ μη ανταγωνιστική (non- adversarial), όταν πρόκειται για μία κατάσταση που κατά λάθος εκμεταλλεύεται αδύναμα σημεία του οργανισμού προκαλώντας βλάβες. Παράδειγμα ανταγωνιστικής απειλής είναι οι απόπειρες επιθέσεων στον κυβερνοχώρο, που καθίστανται πιθανές όταν εκμεταλλεύονται γνωστά αδύναμα σημεία, ενώ παραδείγματα μη ανταγωνιστικών απειλών είναι οι φυσικές καταστροφές όπως οι τυφώνες και οι σεισμοί. Όπως φαίνεται από τα παραπάνω παραδείγματα, οι απειλές μπορούν να κατηγοριοποιηθούν με βάση το πεδίο στο οποίο στοχεύουν να προκαλέσουν καταστροφή σε φυσικές και τεχνολογικές. Ως φυσικές ορίζονται οι απειλές για τη ζωή, την υγεία, την ιδιοκτησία ή το περιβάλλον, ενώ οι τεχνολογικές αφορούν τα πληροφοριακά συστήματα και τον εξοπλισμό.

Ευαίσθητα σημεία (vulnerabilities)

Ως ευαίσθητο σημείο ενός οργανισμού ορίζεται κάθε αδυναμία, ελάττωμα ή έλλειψη, την

οποία θα μπορούσε να εκμεταλλευτεί μια πηγή απειλής ώστε να προκαλέσει βλάβη.

Οι αδυναμίες ενός οργανισμού διαχωρίζονται σε τεχνικές και οργανωτικές. Μπορούν να βρεθούν στα πληροφοριακά του συστήματα και τον τεχνολογικό του εξοπλισμό, στις διοικητικές διαδικασίες αλλά και στις εξωτερικές σχέσεις, όπως για παράδειγμα η αλυσίδα προμηθειών. Αξίζει να σημειωθεί ότι, τα ευαίσθητα σημεία δεν είναι απαραίτητα αποτέλεσμα κακού σχεδιασμού ή απουσίας συνεννόησης, αλλά προκύπτουν και φυσικά με την πάροδο του χρόνου καθώς οι οργανωτικές λειτουργίες εξελίσσονται, τα περιβάλλοντα δραστηριοποίησης αλλάζουν και νέες τεχνολογίες εισάγονται μαζί με νέες απειλές.

Εκτίμηση Πιθανότητας (likelihood)

Η εκτίμηση πιθανότητας είναι ένα σταθμισμένο γνώρισμα του κινδύνου, που προκύπτει από την ανάλυση της προοπτικής που έχει μία συγκεκριμένη απειλή να εκμεταλλευτεί ένα από τα ευαίσθητα σημεία του οργανισμού. Με άλλα λόγια, προσδιορίζει πόσο πιθανό είναι μία απειλή να προκαλέσει ζημιά.

Αυτό το μέγεθος καθορίζεται στην ουσία από δύο άλλα: την εκτίμηση της πιθανότητας υλοποίησης ενός γεγονότος που απειλεί να προκαλέσει βλάβη στο σύστημα και την εκτίμηση της πιθανότητας επιπτώσεων (εάν η απειλή πυροδοτηθεί).

Για να εκτιμήσουμε την πιθανότητα υλοποίησης μίας ανταγωνιστικής απειλής adversarial threat) αρκεί να αξιολογήσουμε:

- την πρόθεση του ανταγωνιστή (adversary),
- την ικανότητά του,
- τον στόχο του.

Για τις μη ανταγωνιστικές απειλές, πρέπει να ανατρέξουμε σε ιστορικά ή εμπειρικά δεδομένα, όπως για παράδειγμα την πιθανότητα να ξεσπάσει τυφώνας κατά τη διάρκεια ενός συγκεκριμένου μήνα, σε μία συγκεκριμένη περιοχή.

Για να εκτιμήσουμε την πιθανότητα επιπτώσεων, αρκεί να εκτιμήσουμε πόσο πιθανό είναι να προκληθούν βλάβες, όσο σημαντικές ή ασήμαντες και αν είναι. Είναι προφανές ότι η πιθανότητα αυτή εξαρτάται άμεσα από τα χαρακτηριστικά του φορέα που απειλείται, δηλαδή την απόδοση της οργανωτικής δομής, την επαρκή συντήρηση και ενημέρωση του τεχνολογικού εξοπλισμού, την ύπαρξη συστηματικών ελέγχων που αποσκοπούν στην ασφάλεια κ.α.

Η τιμή της συνολικής πιθανότητας αποδίδεται αφότου έχει υπολογιστεί η πιθανότητα υλοποίησης της απειλής και η πιθανότητα ύπαρξης αρνητικών επιπτώσεων, ως συνδυασμός των παραπάνω δυο.

Επίπτωση (Impact- Consequence)

Ως επίπτωση ενός παράγοντα κινδύνου ορίζουμε τις συνέπειες αυτού. Στην ουσία πρόκειται για μία μετρική αξιολόγησης της σημαντικότητας και της βαρύτητας ενός κινδύνου.

Μία χρήσιμη κατηγοριοποίηση των επιπτώσεων είναι ως προς τον χρόνο ¨εμφάνισής" τους. Έτσι, διακρίνονται σε άμεσες και μακροπρόθεσμες και κάθε κατηγορία χρήζει διαφορετικής αντιμετώπισης. Μία ιδιάζουσα μορφή επιπτώσεων αποτελούν οι κλιμακωτές επιπτώσεις,

δηλαδή η αλυσιδωτή πρόκληση συνεπειών, εξαιτίας της υλοποίησης ενός μόνο κινδύνου. Ένα παράδειγμα αποτελεί, η απώλεια της αξιοπιστίας του οργανισμού και η οικονομική του παρακμή, εξαιτίας της απώλειας απόρρητων πληροφοριών όπως προσωπικά δεδομένα ασθενών.

Σε κάθε μία από τις παραπάνω περιπτώσεις, είναι κρίσιμης σημασίας ο συνεχής έλεγχος του συστήματος για πιθανές συνέπειες που δεν έχουν γίνει ακόμα αντιληπτές, είτε επειδή είναι μακροπρόθεσμες είτε επειδή πλήττουν δευτερεύοντα/ μη κρίσιμα τμήματα του οργανισμού, ούτως ώστε να είναι δυνατή η αποκατάσταση. Επίσης είναι πιθανό, ένας κίνδυνος που υλοποιείται να προκαλεί πολλαπλές αρνητικές συνέπειες, αλλά και διαφορετικοί κίνδυνοι να έχουν την ίδια επίπτωση στο σύστημα. Στην τελευταία περίπτωση, μπορεί η τελική βλάβη στο σύστημα να προκύπτει ως άθροισμα των επιμέρους (aggregation).

Κίνδυνος (Risk)

Εξαιτίας του εύρους χρήσης του όρου, οι ορισμοί για την έννοια του κινδύνου είναι πολυάριθμοι και διαφέρουν μεταξύ τους. Χωρίς αμφιβολία ο κίνδυνος αναπαριστά το αρνητικό ενδεχόμενο, οτιδήποτε μπορεί να προκαλέσει καταστροφή, να επιφέρει απώλειες και φθορές ή μπορεί να φέρει σε επιβλαβή θέση κάποιον/ κάτι. Ο κίνδυνος χαρακτηρίζεται ως βασική προϋπόθεση της επιτυχίας.

Πιο συγκεκριμένα, όσον αφορά στις επιχειρηματικές και οργανωτικές διαδικασίες, ως κίνδυνος ορίζεται μία συνάρτηση της πιθανότητας μία απειλή να πραγματοποιηθεί, και των αρνητικών επιπτώσεων/ συνεπειών στον οργανισμό, εάν αυτό συμβεί. Σε αυτά τα πλαίσια, κίνδυνος θεωρείται κάθε συνθήκη που εμποδίζει τον οργανισμό να εκπληρώσει την αποστολή του, δηλαδή να προστατεύσει τα άτομα, τα περιουσιακά στοιχεία και τις εγκαταστάσεις του, να διατηρήσει την καθημερινή του λειτουργία και να παραμένει συνεπής στις νομικές του υποχρεώσεις. Στις σύγχρονες οικονομίες, η άμεση παρουσία του κινδύνου σε κάθε σχέση του φορέα με τους συμμετέχοντες σε αυτόν (πελάτες, προμηθευτές, εργαζομένους κ.λπ.), τους έχει εύλογα αποδώσει τον όρο *"οικονομίες αβεβαιότητας"*. Το **επίπεδο του κινδύνου** καθορίζεται ως εξής:

$$Risk = Likelihood \times Impact$$

2.1.2 *Ταξινόμηση του Κινδύνου*

Αποσκοπώντας στην καταγραφή της εξελικτικής τάσης κρίσιμων παραγόντων κατά τη διάρκεια μακροχρόνιων περιόδων, οι οργανισμοί και οι επιχειρήσεις οφείλουν να συστηματοποιήσουν την παρακολούθηση οικονομικών, κοινωνικών, τεχνικών και πολιτικών μεγεθών. Με αυτόν τον τρόπο, καθίσταται δυνατή η ορθή διάγνωση των μελλοντικών εξελίξεων, και μέσω αυτού, η ορθή λήψη θεμελιωδών αποφάσεων για τη διοίκηση.

Η ταξινόμηση του κινδύνου με βάση τα χαρακτηριστικά του διευκολύνει την προσπάθεια που γίνεται για την αναγνώριση και την εκτίμησή του. Κάθε οργανισμός βέβαια πρέπει να επιλέξει μεταξύ των πιθανών κατηγοριοποιήσεων, αυτή που καλύτερα προσεγγίζει τη μορφή του και τις επιδιώξεις του. Η ταξινόμηση του κινδύνου μπορεί να γίνει:

i) ανάλογα με την προέλευσή του,

ii) ανάλογα με τον χρονικό ορίζοντα υλοποίησης,

iii) ανάλογα με το κίνητρό του.

i) Ταξινόμηση ανάλογα με την προέλευση

Ο κίνδυνος με βάση την προέλευσή του κατατάσσεται σε: [1]

- *Εσωτερικό Κίνδυνο*: Είναι άμεσα συνυφασμένος με την ίδια την φύση της επιχείρησης. Περιλαμβάνει τεχνικούς κινδύνους όπως παλιές εγκαταστάσεις ή επικίνδυνο εξοπλισμό που πρέπει να αντικατασταθεί. Η επικινδυνότητα αυξάνεται ιδιαίτερα στην περίπτωση που ο ευπαθής οργανισμός απειλείται από φυσικές καταστροφές (σεισμούς, κατακλυσμούς, τυφώνες κ.α.). Σε αυτή την κατηγορία επίσης αντιστοιχίζονται ανωμαλίες που αφορούν τα χαρακτηριστικά και τη διοίκηση των ανθρωπίνων πόρων. Περιλαμβάνονται οι σκληρές συνθήκες εργασίας, η στέρηση βασικών εργασιακών δικαιωμάτων, η λειτουργία του οργανισμού υπό ¨κοινωνική ένταση¨ και όσοι ακόμα παράγοντες μπορούν είτε να βλάψουν είτε να προκαλέσουν την αγανάκτηση των εργαζομένων, καθώς και την έκφρασή της με ακραίες στάσεις όπως απεργία ή lock-out.

- *Κίνδυνο της αγοράς*: Καθορίζεται από τη ζήτηση του προϊόντος ή της υπηρεσίας που προσφέρει ο φορέας. Οι μεταβολές τόσο στην αγορά που βρίσκεται σε ψηλότερη θέση από τον οργανισμό στην παραγωγική αλυσίδα (αγορά προμηθειών) όσο και στην αγορά που βρίσκεται κάτω από αυτόν (πώληση προϊόντων/υπηρεσιών), αποτελούν απειλή για τον ίδιο τον οργανισμό και τη λειτουργική σταθερότητα που επιδιώκει.

- *Κίνδυνο της εθνικής οικονομίας*: Παρά τις διαφορετικές επιπτώσεις που μπορεί να προκαλέσει ο κίνδυνος της εθνικής οικονομίας στους διαφορετικούς οργανισμούς/ επιχειρήσεις, αντιμετωπίζεται καθολικά. Η εθνική οικονομική συγκυρία και η εξέλιξή της, που συχνά επηρεάζονται από κοινωνικές και πολιτικές αναταραχές, είναι ένας παράγοντας σοβαρού κινδύνου, καθώς μεταβάλλει τις σχέσεις δυνάμεων ανάμεσα στους κλάδους.

- *Διεθνή κίνδυνο*: Λαμβάνοντας υπόψη την επίδραση της εθνικής οικονομίας ως παράγοντα κινδύνου, επαγωγικά προκύπτει ότι ο οργανισμός επηρεάζεται από τον κίνδυνο κάθε εθνικής οικονομίας με την οποία έχει σχέσεις. Η διεθνοποίηση των ανταλλαγών και της παραγωγής έχει διαμορφώσει τις ισορροπίες μεταξύ των χωρών, καθιστώντας τη συγκεκριμένη κατηγορία κινδύνου ιδιαίτερα σημαντική.

ii) Ταξινόμηση ανάλογα με τον χρονικό ορίζοντα υλοποίησης

Ο κίνδυνος με βάση την προθεσμία του κατατάσσεται σε:

- *Άμεσο/ Βραχυπρόθεσμο κίνδυνο*: Όλες οι μεταβλητές του εσωτερικού και εξωτερικού περιβάλλοντος του οργανισμού εμπεριέχουν την έννοια του κινδύνου, όπως έγινε κατανοητό από την προηγούμενη κατάταξη του κινδύνου με βάση την προέλευσή του. Τόσο οι κίνδυνοι που αφορούν τα συστατικά στοιχεία του οργανισμού όσο και η σχέση των στοιχείων αυτών με τον ίδιο τον οργανισμό, καθορίζουν τη σοβαρότητα των ενδεχόμενων

επιπτώσεων. Αυτό το είδος του κινδύνου είναι σχετικά εύκολο να προβλεφθεί και να εκτιμηθεί, οπότε θεωρείται λιγότερο δυνατός.

- *Έμμεσο/ Μακροπρόθεσμο κίνδυνο*: Πρόκειται για ένα είδος κινδύνου που είναι δύσκολο να προβλεφθεί, καθώς αποτελεί συνάρτηση πολλών διαφορετικών παραγόντων. Ένα αρχικό γεγονός προκαλεί μία αλληλουχία/αλυσίδα συνεπειών (cascading effects) με αποτέλεσμα οι τελικές επιπτώσεις να εκδηλώνονται σε βάθος χρόνου. Παράδειγμα μακροπρόθεσμου κινδύνου μπορεί να θεωρηθεί και η τεχνολογική πρόοδος, που αν και δεν οφείλεται σε ένα συγκεκριμένο αρχικό γεγονός, εξελίσσεται απρόβλεπτα, καθορίζοντας αντίστοιχα και το μέλλον των οργανισμών (εισαγωγή νέων τεχνολογιών, ανάγκη για ψηφιοποίηση δεδομένων, αντικατάσταση εξοπλισμού κ.α.).

iii) Ταξινόμηση ανάλογα με το κίνητρο

- *Κακόβουλο*: Το συγκεκριμένο είδος κινδύνου χαρακτηρίζεται έτσι, ανάλογα με το κίνητρο του δράστη που προκαλεί την απειλή. Εάν ο δράστης εκμεταλλεύεται συνειδητά τα ευαίσθητα σημεία του οργανισμού με στόχο να υπονομεύσει τη λειτουργία του, το κίνητρό του θεωρείται κακόβουλο.

- *Μη κακόβουλο*: Το συγκεκριμένο είδος κινδύνου οφείλεται σε ασθενείς πολιτικές ασφαλείας και σε ελλιπείς ελέγχους που επιτρέπουν στα αρνητικά ενδεχόμενα να πραγματοποιηθούν εκμεταλλευόμενα τα αδύναμα σημεία του φορέα που βάλλεται. Ένα παράδειγμα αυτού του κινδύνου είναι η καταστροφή εξοπλισμού ως απόρροια σφάλματος εργαζομένου.[2]

2.2 Ο κίνδυνος στον Κυβερνοχώρο

2.2.1 *Εισαγωγή στην έννοια του Κυβερνοχώρου*

Έχοντας κατατάξει τον κίνδυνο στις προαναφερθείσες κατηγορίες, γίνεται εύκολα αντιληπτό το πώς τα διαφορετικά χαρακτηριστικά του καθορίζουν τόσο τις συνέπειες που προκύπτουν σε περίπτωση πραγματοποίησης, όσο και τα μέτρα ασφαλείας και ελέγχου που υιοθετούνται από τον οργανισμό. Τις τελευταίες δύο δεκαετίες, η δυναμική της έννοιας της ασφάλειας έχει αλλάξει ριζικά με την επικράτηση του κυβερνοχώρου ως ραχοκοκαλιά της σύγχρονης κοινωνίας και οικονομίας.

Δεν είναι λίγοι οι διαφορετικοί ορισμοί που έχουν δοθεί για να προσδιορίσουν τον κυβερνοχώρο, και η ρίζα αυτής της ποικιλίας έγκειται κυρίως στη ρευστή μορφή της ίδιας της έννοιας. Σύμφωνα με τον Daniel Kuehl, *ο* ***κυβερνοχώρος*** *ορίζεται ως ένας παγκόσμιος τομέας μέσα στο πληροφοριακό περιβάλλον του οποίου ο ιδιαίτερος και μοναδικός χαρακτήρας πλαισιώνεται από την χρήση ηλεκτρονικών και του ηλεκτρομαγνητικού φάσματος για να δημιουργήσει, αποθηκεύσει, μετατρέψει, ανταλλάξει και εκμεταλλευτεί πληροφορίες μέσω ανεξάρτητων και αλληλένδετων δικτύων κάνοντας χρήση πληροφοριακών-επικοινωνιακών τεχνολογιών* [3]. Ο παγκόσμιος αυτός ιστός λοιπόν, αποτελεί εργαλείο για την κάλυψη

αναγκών διαφορετικού βεληνεκούς, από την δικτύωση χρηστών σε πλαίσια καθημερινής επικοινωνίας, έως την αποθήκευση κρίσιμων για τα κράτη πληροφοριών που σχετίζονται με τομείς όπως η υγεία, η οικονομία και η ασφάλεια [4].

Παραδείγματα της ενσωμάτωσης του ψηφιακού κόσμου στις σύγχρονες κοινωνίες είναι το υπολογιστικό νέφος (cloud computing), οι ηλεκτρονικές συναλλαγές και η ανάπτυξη της τεχνητής νοημοσύνης [5]. Τους επιτρέπει, το δίχως άλλο, να απολαμβάνουν πληθώρα ευκολιών, όπως η απρόσκοπτη διασύνδεση, η επιτάχυνση λειτουργιών, η συστηματοποίηση των διαδικασιών, η πρόσβαση στη γνώση και η ψυχαγωγία, και όλα αυτά μέσω ευέλικτων και φιλικών προς τον χρήστη συστημάτων. Ταυτόχρονα όμως, αυτός ο κόσμος εγκυμονεί απειλές και κινδύνους, με αυξανόμενη ισχύ και συχνότητα. Η απώλεια ρυθμιστικής αρχής και η ανωνυμία, καθιστούν τον κυβερνοχώρο περιβάλλον άνομο, και την κυβερνοασφάλεια διεθνές διακύβευμα.

2.2.2 *Κυβερνοασφάλεια*

Σύμφωνα με το σχέδιο πράξης της ΕΕ για την ασφάλεια στον κυβερνοχώρο, ως **κυβερνοασφάλεια** ορίζονται *όλες οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών τους και των προσώπων που υφίστανται τις συνέπειες κυβερνοαπειλών* (Ευρωπαϊκό Κοινοβούλιο, 2019). Σαν κλάδος καλύπτει την **πρόληψη** και την **ανίχνευση** κυβερνοπεριστατικών, την **αντίδραση** σε αυτά και την ανάκαμψη από αυτά. Τα περιστατικά μπορεί να είναι κακόβουλα ή μη και κυμαίνονται, ενδεικτικά, από την τυχαία κοινοποίηση πληροφοριών έως επιθέσεις κατά επιχειρήσεων και υποδομών ζωτικής σημασίας και την κλοπή δεδομένων προσωπικού χαρακτήρα, ή ακόμη και έως την παρέμβαση σε δημοκρατικές διαδικασίες. Όλα αυτά τα συμβάντα μπορούν να έχουν πολυποίκιλες επιζήμιες επιδράσεις σε πρόσωπα, οργανισμούς και κοινότητες [6]. Αξίζει να σημειωθεί ότι η κυβερνοασφάλεια δεν καλύπτει μόνο την ασφάλεια δικτύων και πληροφοριών, αλλά και κάθε παράνομη δραστηριότητα με τη χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο. Ως εκ τούτου, μπορεί να περιλαμβάνει κυβερνοεγκλήματα όπως την εξαπόλυση επιθέσεων με ιούς υπολογιστών ή την απάτη με μέσα πληρωμής πλην των μετρητών και να αφορά τόσο συστήματα όσο και περιεχόμενο, καθώς και τη δημοσιοποίηση ευαίσθητου υλικού στο διαδίκτυο. Η κυβερνοασφάλεια γίνεται λοιπόν αντιληπτή ως η προσπάθεια προστασίας των διαδικτυακών δεδομένων, της ανωνυμίας και της ιδιωτικότητας των πολιτών.

Σκοπός της κυβερνοασφάλειας είναι να διατηρήσει:

- **Το απόρρητο των δεδομένων**: Ιδιωτικά ή εμπιστευτικά δεδομένα δεν είναι διαθέσιμα σε κάποιον που δεν έχει την κατάλληλη έγκριση για πρόσβαση σε αυτά.
- **Την ακεραιότητα των δεδομένων**: Τα δεδομένα θα πρέπει να παραμένουν αμετάβλητα μετά την παύση της επεξεργασίας τους και να μην υπάρχει αλλοίωσή τους από κάποιον τρίτο.
- **Την διαθεσιμότητα των δεδομένων**: Τα δεδομένα που αποθηκεύονται θα πρέπει να είναι διαθέσιμα ανά πάσα στιγμή, δηλαδή να μπορούμε να έχουμε πρόσβαση σε αυτά.

Στο Σχήμα 2.1 φαίνεται πώς διαφορετικά είδη κυβερνοπεριστατικών επηρεάζουν τις αρχές τις κυβερνοασφάλειας.

Σχήμα 2.1: *Τα είδη απειλών και οι αρχές ασφάλειας που θέτουν σε κίνδυνο, Πηγή:ΕΕΣ*

2.2.3 *Παραδείγματα Κυβερνοεπιθέσεων*

Η αυξητική τάση τόσο του αριθμού όσο και της ισχύος των κυβερνοεπιθέσεων είναι η μεγαλύτερη πρόκληση που αντιμετωπίζει ο τομέας της κυβερνοασφάλειας τα τελευταία χρόνια. Οι χρήστες του κυβερνοχώρου (πολίτες, επιχειρήσεις, κρατικοί οργανισμοί κ.α.), αναγνωρίζοντας τα προτερήματα που τους παρέχει, έχουν εντείνει την παρουσία τους στον εικονικό κόσμο διατηρώντας προσωπικές και επαγγελματικές σχέσεις. Ταυτόχρονα, οι κυβερνοεγκληματίες εκμεταλλευόμενοι τόσο το παραπάνω όσο και τα ίδια τα χαρακτηριστικά του κυβερνοχώρου, και παρακινούμενοι από οικονομικά κίνητρα ως επί το πλείστον, έχουν δημιουργήσει ισχυρά ¨εργαλεία επίθεσης¨, με συχνότερους στόχους τις ηλεκτρονικές πληρωμές, το ηλεκτρονικό εμπόριο και το σύστημα υγείας (ENISA, 2020). Η ανωνυμία που επικρατεί στον ψηφιακό κόσμο, η μη-υπολογίσιμη έκταση αυτού, και η απαλλαγή από τον περιορισμό των γεωγραφικών ορίων, είναι μερικά από τα στοιχεία του κυβερνοχώρου που παρουσιάζουν διττό χαρακτήρα, δηλαδή διευκολύνουν και επιταχύνουν μεν τις ηλεκτρονικές συναλλαγές, επιτρέπουν δε τη συχνή και επιζήμια πραγματοποίηση επιθέσεων. Πιο συγκεκριμένα, σύμφωνα με την τεχνική αναφορά του Ponemon Institute, το 2018 το μέσο κόστος εξαιτίας των παραβιάσεων δεδομένων (data breaches) παγκοσμίως, έφτασε τα 3.86 εκατομμύρια δολάρια, σημειώνοντας αύξηση 6.4% σε σχέση με την τιμή του μεγέθους για το 2017 [7].

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), ιδρυθείς το 2004, στοχεύει στη διασφάλιση της ασφάλειας δικτύων και πληροφοριών, έναντι των απειλών και των επιθέσεων που δέχονται εντός της Ένωσης. Στην ετήσια αναφορά που εξέδωσε για το έτος 2018 [8], παρουσιάζει και αναλύει τις κυριότερες τάσεις και είδη κυβερνοεπιθέσεων, οι οποίες φαίνονται στο Σχήμα 2.2.

Παρακάτω παρουσιάζονται οι προαναφερθείσες κυβερνοεπιθέσεις και τα βασικά τους

Σχήμα 2.2: *Κυριότερα Είδη Κυβερνοεπιθέσεων για το 2018, Πηγή :ENISA*

χαρακτηριστικά :

- **Κακόβουλο Λογισμικό/Malware**: Πρόκειται για κακόβουλο κώδικα που αν εγκατασταθεί σε μία συσκευή, βλάπτει τα κύρια στοιχεία της, δηλαδή το υλισμικό (hardware), το λογισμικό (software) και τα δεδομένα της. Χρησιμοποιείται για να καταστρέψει είτε να υποκλέψει προσωπικά στοιχεία των χρηστών, απειλώντας έτσι την διαθεσιμότητα, την ακεραιότητα και το απόρρητο αυτών. Η ευρεία αυτή κατηγορία των malware, αποτελεί την συχνότερη απειλή που αντιμετωπίζεται στον κυβερνοχώρο, και είναι υπεύθυνη για το 30% των παραβιάσεων δεδομένων παγκοσμίως. Μερικοί από τους γνωστότερους τύπους κακόβουλου λογισμικού είναι :

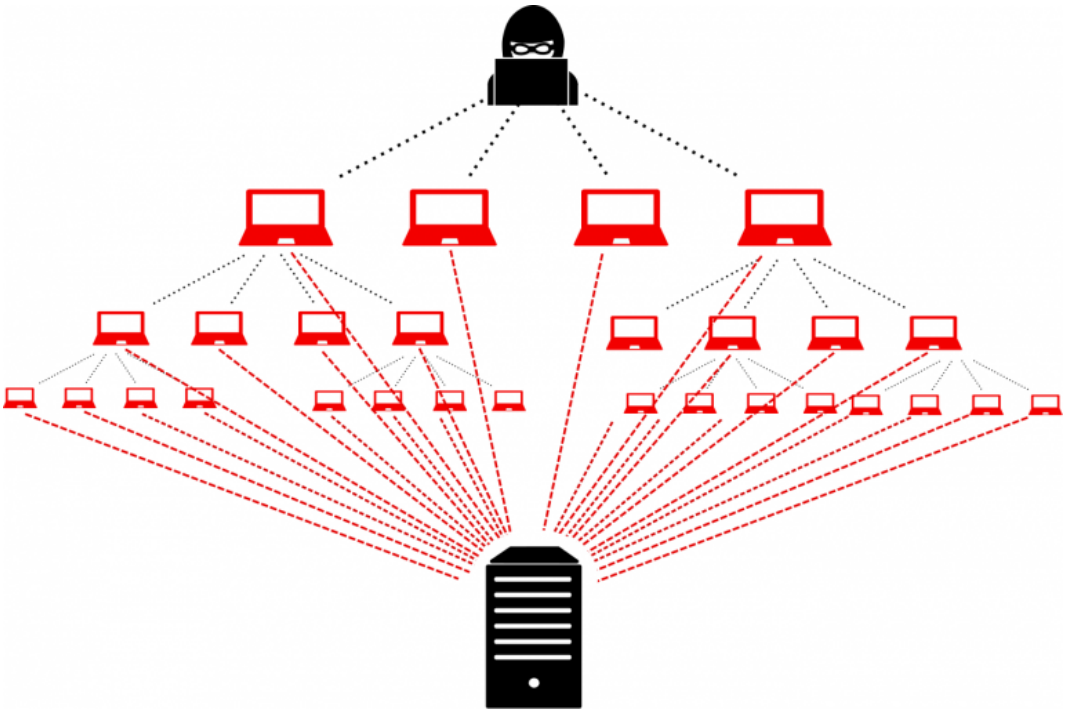
  1. **Ιοί/Viruses**: Σε πλήρη αντιστοιχία με τους ιούς του φυσικού κόσμου, ένας ιός υπολογιστή μολύνει υγιή αρχεία, αναπαράγεται και μεταδίδεται περαιτέρω με στόχο να βλάψει το σύστημα (και άλλα συστήματα, μεταδιδόμενος μέσω μολυσμένων αρχείων). Η τεχνικά εξελιγμένη και συνεχώς εξελισσόμενη φύση των ιών, καθιστά ιδιαίτερα δύσκολη την προσπάθεια εντοπισμού τους και απομάκρυνσής τους από το σύστημα. Παρόλα αυτά, οι χρήστες μπορούν να προστατευθούν εγκαθιστώντας στους υπολογιστές τους anti-malware λογισμικά και ενημερώνοντάς τα τακτικά.
  2. **Σκουλήκια/Worms**: Πρόκειται για προγράμματα που προσβάλλουν υπολογιστές που είναι συνδεδεμένοι σε δίκτυο. Αν και συναντώνται σπανιότερα από τους ιούς, τα worms είναι πολύ πιο επικίνδυνα γιατί αναπαράγονται και επιβιώνουν μόνα τους, χωρίς δηλαδή να χρειάζονται αρχεία για να διαδοθούν. Αντίθετα, εάν ένας υπολογιστής φέρει worm και συνδεθεί σε ένα δίκτυο, τότε μολύνεται το δίκτυο και μαζί με αυτό όλες οι συνδεδεμένες σε αυτό συσκευές.

3. **Κατασκοπευτικό πρόγραμμα/Spyware**: Το πρόγραμμα αυτό καταγράφει τις δραστηριότητες και τις ηλεκτρονικές κινήσεις του χρήστη, ακόμη και τι πληκτρολογεί. Παραμένει κρυμμένο από το λειτουργικό σύστημα και για αυτό χρησιμοποιείται για την απόκτηση - υποκλοπή απόρρητων πληροφοριών.
4. **Δούρειοι Ίπποι/Trojan Horses**: Έχει παρόμοια λειτουργία με το κατασκοπευτικό πρόγραμμα, μόνο που αντί να παραμένει κρυμμένο, χρησιμοποιεί τεχνικές παραλλαγής για να αποκρύψει τον σκοπό του. Ακόμη, σε αντίθεση με το κατασκοπευτικό πρόγραμμα, τα Trojans επιτρέπουν στο δράστη το (μερικό) έλεγχο του συστήματος του χρήστη. Η μεγαλύτερη διαφορά των Trojans σε σχέση με τους ιούς είναι ότι δεν μπορούν να αυτοπολλαπλασιαστούν και να μολύνουν αρχεία από μόνα τους.
5. **Λυτρισμικό/Ransomware**: Πρόκειται για επίθεση κατά την οποία κρυπτογραφούνται τα δεδομένα ενός υπολογιστή, εμποδίζοντας την πρόσβαση των χρηστών στα αρχεία τους έως ότου καταβληθούν λύτρα. Χρησιμοποιούν σύγχρονες τεχνικές κρυπτογράφησης, καθιστώντας αδύνατη την αποκρυπτογράφηση των δεδομένων χωρίς το αντίστοιχο κλειδί και έτσι οι χρήστες αναγκάζονται να ενδώσουν στις επιθυμίες των δραστών. Αυτού του είδους οι επιθέσεις γνώρισαν πρωτοφανή αύξηση σε αριθμό τα τελευταία χρόνια.

- **Botnets**: Πρόκειται για ακόμη ένα είδος malware. Τα botnets είναι δίκτυα ¨μολυσμένων¨ υπολογιστών που χρησιμοποιούνται για κακόβουλες δραστηριότητες. Οι υπολογιστές που απαρτίζουν ένα botnet προέρχονται από ολόκληρο τον κόσμο κάνοντας ιδιαίτερα δύσκολο τον εντοπισμό όλων, και συνήθως οι χρήστες τους δεν έχουν γνώση ότι η συσκευή τους έχει προσβληθεί. Τα bots, που λέγονται αλλιώς και ¨συστήματα ζόμπι¨, χρησιμοποιούνται συχνά για την πραγματοποίηση DDoS επιθέσεων, δρώντας συγχρονισμένα και συντονισμένα εναντίον ενός συστήματος-στόχου και συνθλίβοντας τις δυνατότητες επεξεργασίας του.

- **Επίθεση άρνησης υπηρεσιών/DDoS**: Στόχος της συγκεκριμένης επίθεσης είναι η διακοπή της υπηρεσίας, η αδυναμία λειτουργίας του δικτύου, μέσω της υπερφότωσής του με μεγάλο όγκο δεδομένων. Η υπερφόρτωση επιτυγχάνεται μέσω ταυτόχρονης αποστολής δεδομένων από σύνολο υπολογιστών (botnet) που ελέγχονται από έναν κεντρικό υπολογιστή/ τοποθεσία υπολογιστών. Μία επίθεση άρνησης υπηρεσιών πλήττει την διαθεσιμότητα των δεδομένων. Αυτή η δομή απεικονίζεται στο Σχήμα 2.3. Αποτελεί μία από τις σημαντικότερες απειλές που αντιμετωπίζουν οι επιχειρήσεις και οργανισμοί με διαδικτυακή παρουσία, που αυξάνεται όσο περισσότερο αυτοί εξαρτώνται από δίκτυα επικοινωνίας όπως το Διαδίκτυο των πραγμάτων (IoT). Είναι πλέον ξεκάθαρο ότι η εφαρμογή αμυντικών μηχανισμών και τεχνικών μέτρων ασφαλείας μειώνει κατά πολύ την πιθανότητα το δίκτυο να προσβληθεί από DDoS επίθεση, χωρίς να την εξαλείφει πλήρως, καθώς νέες επιθέσεις με νέα χαρακτηριστικά είναι αδύνατο να προβλεφθούν.

- **Phishing**: Το phishing, ή αλλιώς ηλεκτρονικό ψάρεμα, αποτελεί μία μορφή επίθεσης κατά την οποία ο δράστης προσπαθεί να κλέψει ευαίσθητες πληροφορίες του θύμα-



Σχήμα 2.3: *Η βασική δομή μίας DDoS επίθεσης*

τος, όπως κωδικούς και προσωπικά τραπεζικά δεδομένα. Αυτό επιτυγχάνεται όταν ο δράστης είτε μιμείται κάποια αξιόπιστη οντότητα (όπως την ίδια την τράπεζα), είτε προσπαθεί να δελεάσει το θύμα να ανοίξει κακόβουλα συνημμένα αρχεία και να επισκεφθεί επικίνδυνες ιστοσελίδες. Η συγκεκριμένη επίθεση βασίζεται στις αρχές της κοινωνικής μηχανικής (social engineering), και παρά το γεγονός ότι το "παραδοσιακό" ηλεκτρονικό ψάρεμα που συνδέεται με το spam υπάρχει ακόμα, τα τελευταία χρόνια παρατηρείται η επιτυχία μελετημένων και στοχευμένων επιθέσεων που εκμεταλλεύονται ειδικά χαρακτηριστικά.

- **Επιθέσεις μέσω Διαδικτύου/Web-based attacks**: Πρόκειται για το είδος επίθεσης που χρησιμοποιεί τα συστήματα και τις υπηρεσίες του Διαδικτύου ως πεδίο επίθεσης. Περιλαμβάνουν την "μόλυνση" και την εκμετάλλευση προγραμμάτων περιήγησης, των προεκτάσεών τους και ιστοσελίδων. Εξαιτίας του μεγάλου εύρους εφαρμογής τους και την συνεχή εξέλιξη των εργαλείων που χρησιμοποιούνται για την πραγματοποίησή τους, οι επιθέσεις μέσω Διαδικτύου θεωρούνται από τις σημαντικότερες απειλές που αντιμετωπίζονται στον ψηφιακό κόσμο.

2.3 Λήψη Αποφάσεων Υπό Αβεβαιότητα

2.3.1 Συστήματα Υποστήριξης Αποφάσεων

Ο μύθος της **βέλτιστης απόφασης** ταλανίζει την ανθρωπότητα σε κάθε πτυχή στην οποία καλείται να αποφασίσει: να δράσω, και αν ναι, με ποιόν τρόπο ; Η δυσκολία που αντιμετωπίζει κανείς σε ένα **πρόβλημα απόφασης** μπορεί να συνοψιστεί σε δύο μόνο παράγοντες: στο βαθμό βεβαιότητας που χαρακτηρίζει τα διαθέσιμα δεδομένα, και στην πολυπλοκότητα

των πιθανών επιπτώσεων των δράσεων. Ακόμα και αν έννοιες όπως το προαίσθημα και η διαίσθηση είναι παράγοντες που καθορίζουν, σε καθημερινή βάση, τις αποφάσεις που λαμβάνονται, δεν υπάρχει αμφιβολία για το ότι σε επίπεδο επιχειρήσεων και οργανισμών, όχι μόνο δεν αρκούν αλλά πρέπει πιθανώς να απαλλάσσεται κανείς από αυτές πριν λάβει οποιαδήποτε απόφαση. Η **διαδικασία λήψης της απόφασης** μπορεί να χωριστεί σε τέσσερα στάδια:

1. Την αναγνώριση του προβλήματος, της απειλής ή της ευκαιρίας που είναι η ρίζα του προβλήματος απόφασης,

2. Τον σχεδιασμό των εναλλακτικών στρατηγικών και την ανάλυση των πιθανών συνεπειών τους,

3. Την αξιολόγηση των εναλλακτικών με βάση κριτήρια επιλεγμένα από τον οργανισμό ώστε να συμφωνούν με τις επιδιώξεις του,

4. Την επιλογή εκείνης που φέρνει τα καλύτερα αποτελέσματα.

Παρόλο που η παραπάνω κατάτμηση είναι σαφής και νομίζει κανείς πως είναι απλό να ακολουθηθεί, στην πράξη η ποικιλότητα των κριτηρίων, και η ανεξαρτησία των συνεπειών των διαφορετικών δράσεων, προϋποθέτει την ανάλυση και τη σύνθεση μεγάλου όγκου πληροφορίας, εισάγοντας έτσι την ανάγκη η απόφαση να προκύπτει ως αποτέλεσμα σύγκλισης μίας οργανωμένης διαδικασίας [9]. Η συλλογή και επεξεργασία της απαραίτητης πληροφορίας ξεπερνά τα όρια της ανθρώπινης ικανότητας και απαιτεί την εισαγωγή μαθηματικών και πληροφοριακών μοντέλων με σκοπό την υποστήριξη της λήψης της απόφασης [10].

Από την πρώτη τους εμφάνιση στον κλάδο της επιχειρησιακής έρευνας, τις αρχές της δεκαετίας του 1970, τόσο ο ορισμός όσο και η φιλοσοφία των **Συστημάτων Υποστήριξης Αποφάσεων** ή αλλιώς ΣΥΑ (Decision Support Systems, DSS) αν και ασαφείς, περιστρέφονταν γύρω από την έννοια της ¨επιστημονικοποίησης¨ των αποφάσεων. Σε γενικές γραμμές αναπαριστούσαν μια γενική μεθοδολογία που στόχο είχε την ενίσχυση του ρόλου του αποφασίζοντος και την προαγωγή της αποτελεσματικότητας της λήψης αποφάσεων, κάνοντας χρήση μαθηματικών μοντέλων και εργαλείων πληροφορικής. Σήμερα, που ο ρόλος τους στη διοικητική διαδικασία έχει γίνει πλέον ξεκάθαρος, ορίζουμε *ένα Σύστημα Υποστήριξης Αποφάσεων ως μία σύζευξη ανθρώπου - υπολογιστή στο πλαίσιο της οποίας, ο αποφασίζων χρησιμοποιεί ένα σύνολο μοντέλων περισσότερο ή λιγότερο μορφοποιημένων για να διερευνήσει το περιβάλλον ενός προβλήματος χαμηλού βαθμού δόμησης και να καταλήξει στη λήψη μίας απόφασης, μέσα από μία διαδικασία ενίσχυσης της συλλογιστικής του* [9].

Βαθμός Δόμησης της Απόφασης

Ο βαθμός δόμησης του περιβάλλοντος που αναφέρεται στον ορισμό, στην ουσία καθορίζει και το είδος της απόφασης. Σύμφωνα με τους Keen, Scott - Morton οι αποφάσεις χωρίζονται σε τρείς κατηγορίες:

- Δομημένες Αποφάσεις : Αποφάσεις για τις οποίες υπάρχει μία καλά δομημένη διαδικασία. Συχνά λαμβάνονται αυτόματα χωρίς να απαιτούν τη συμμετοχή του αποφασίζο-

ντος. Κάθε στάδιο της απόφασης (αρχικά δεδομένα, εσωτερικές διαδικασίες, τελικά αποτελέσματα) μπορεί να προσδιοριστεί με υψηλό βαθμό ακρίβειας.

- Ημιδομημένες Αποφάσεις : Αποφάσεις κατά τις οποίες δεν είναι όλα τα στάδια δομημένα. Ο αποφασίζων, κατέχοντας πρωτεύοντα ρόλο, χρησιμοποιεί τον υπολογιστή τον οποίο έχει υπό τον πλήρη έλεγχό του.

- Αδόμητες Αποφάσεις : Αποφάσεις, τα στάδια των οποίων είτε είναι αδύνατο να προσδιοριστούν και να δομηθούν, είτε δεν έχει διερευνηθεί σε βάθος η δυνατότητα δόμησής τους. Σε αυτή την κατηγορία απόφασης ο υπολογιστής παίζει βοηθητικό ρόλο, εάν και η απόφαση θα ληφθεί από τον αποφασίζοντα.

Σχεδιασμός και Αρχιτεκτονική ΣΥΑ

Έχοντας ως στόχο την υποστήριξη λήψης ημιδομημένων ή αδόμητων αποφάσεων μέσω της διεύρυνσης του γνωστικού πεδίου του αποφασίζοντα, οι αναλυτές ΣΥΑ εμπλέκονται σε μία ιδιαίτερα περίπλοκη διαδικασία. Στο Σχήμα 2.4 παρουσιάζεται η γενική αρχιτεκτονική ενός ΣΥΑ.

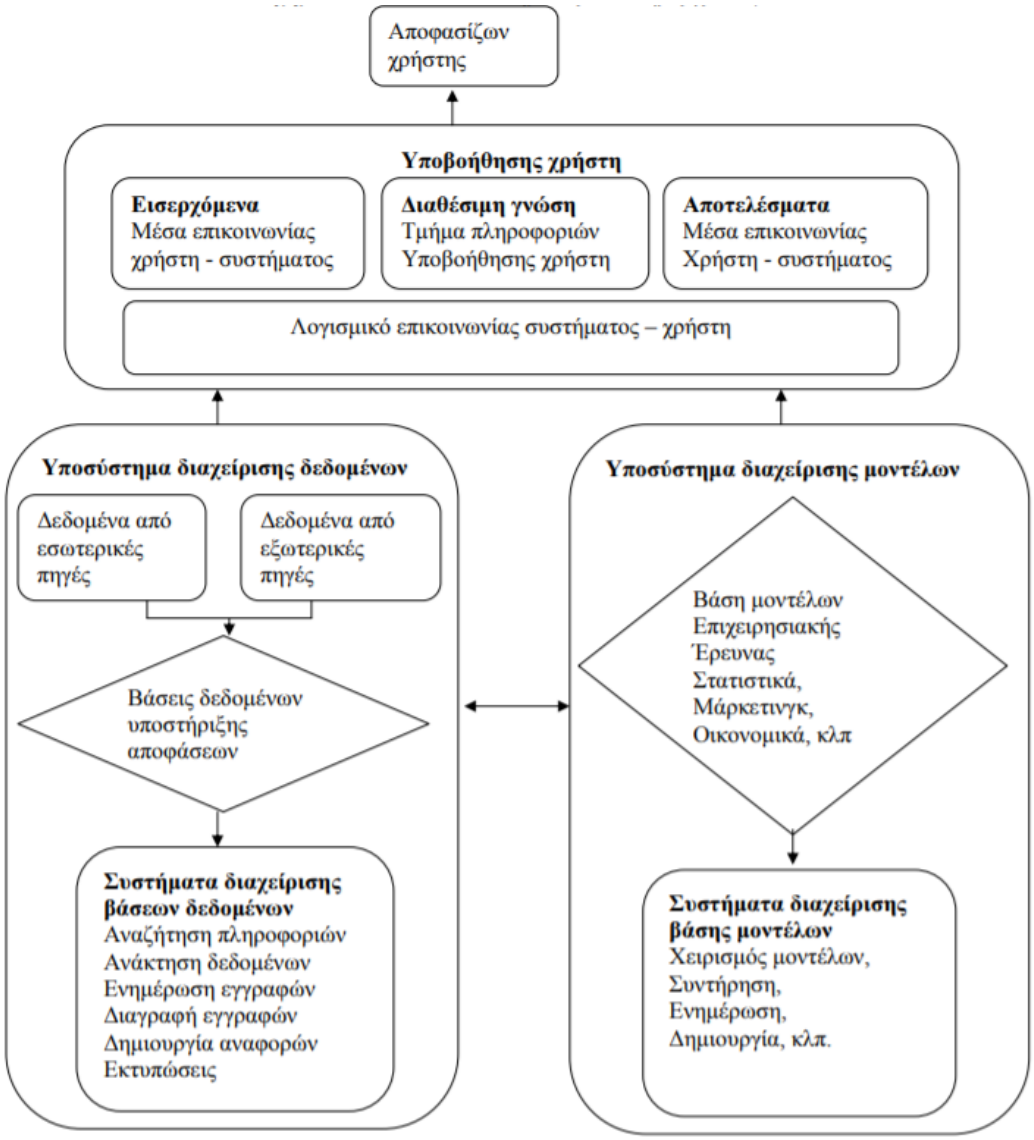
Τα βασικά βήματα που πρέπει να γίνουν για το σχεδιασμό του ΣΥΑ είναι [9]:

- **Σχεδιασμός βάσεων δεδομένων** : Κάνοντας χρήση εξωτερικών και εσωτερικών πηγών, γίνεται συλλογή των δεδομένων (συνήθως πρόκειται για δεδομένα του ίδιου του οργανισμού) που απαιτείται να εξεταστούν πριν ληφθεί η απόφαση και οργανώνονται κατάλληλα σε βάσεις δεδομένων. Οι βάσεις δεδομένων αποτελούν υποσυστήματα του Συστήματος Διαχείρισης Βάσεων Δεδομένων(DataBase Management System, DBMS) του οποίου στόχος είναι η αποθήκευση, η αναζήτηση και η επεξεργασία δεδομένων.

- **Σχεδιασμός και σύνθεση λογισμικού διαχείρισης των δεδομένων**, με τρόπο που να εξασφαλίζει αμεσότητα στην προσπέλαση και ευελιξία στην αναδιοργάνωση.

- **Επιλογή υπαρχόντων/ σχεδιασμός νέων μοντέλων**: Πρόκειται για ένα πακέτο λογισμικού που περιέχει οικονομικά, στατιστικά προγράμματα και διάφορα μοντέλα που προσφέρουν στο σύστημα αναλυτικές ικανότητες. Ως **μοντέλο** ορίζεται η αφαιρετική - απλουστευμένη αναπαράσταση της πραγματικότητας, στην οποία όλα τα στοιχεία που δεν σχετίζονται με το πρόβλημα απόφασης και η συναφής τους πολυπλοκότητα, παραλείπονται. Το λογισμικό αυτό περιέχει επίσης γλώσσες προγραμματισμού μοντέλων δίνοντας έτσι στους αναλυτές τη δυνατότητα δημιουργίας νέων μοντέλων προσαρμοσμένων στα χαρακτηριστικά του προβλήματος απόφασης.

- **Σχεδιασμός και σύνθεση λογισμικού διαχείρισης των μοντέλων**,με τη χρήση του Συστήματος Διαχείρισης Βάσεων Μοντέλων (Model Management System, MMS). Σε πλήρη αντιστοιχία με το Σύστημα Διαχείρισης Βάσεων Δεδομένων, το MMS αναλαμβάνει την επεξεργασία και την αποθήκευση των μοντέλων. Επίσης εγγυάται την αποτελεσματική χρησιμοποίησή τους.



Σχήμα 2.4: *Αρχιτεκτονική ενός Συστήματος Υποστήριξης Αποφάσεων. Πηγή: (Matsatsinis - Siskos, 2003)*

- **Σχεδιασμός και σύνθεση λογισμικού διαχείρισης διαλόγου** : Πρόκειται για το σημαντικότερο ίσως στάδιο στον σχεδιασμό.Το λογισμικό διαχείρισης διαλόγου αποτελεί την διεπαφή ανθρώπου - μηχανής, με άλλα λόγια το σημείο επικοινωνίας χρήστη και συστήματος. Από την αποτελεσματικότητα του σχεδιασμού του συγκεκριμένου σταδίου, εξαρτάται η αποδοτικότητα ολόκληρου του συστήματος.

2.3.2 Πολυκριτήρια Ανάλυση Αποφάσεων

Η Πολυκριτήρια Ανάλυση Αποφάσεων είναι ο κλάδος επίλυσης προβλημάτων απόφασης, στα οποία υπεισέρχονται περισσότερα του ενός, κριτήρια απόφασης. Αποτελεί μία από της σημαντικότερες κατηγορίες του κλάδου της Επιχειρησιακής Έρευνας καθώς ο πολυδιάστατος χαρακτήρας της, της επιτρέπει την θεώρηση όλων των αλληλοαντικρουόμενων σχέσεων που ενυπάρχουν στο περιβάλλον της απόφασης. Η πολυπλοκότητα του σύγχρονου περιβάλλο-

ντος μοντελοποιείται πιο ρεαλιστικά, όταν λαμβάνονται υπόψη τα πολλαπλά κριτήρια (συχνά αντικρουόμενα μεταξύ τους) που το απαρτίζουν. Οι αποφασίζοντες αποκτούν μία πλήρη κατανόηση του προβλήματος, και οι εναλλακτικές στρατηγικές που προτείνονται χαρακτηρίζονται από μεγαλύτερη ευελιξία και είναι τελικά πιο αποδοτικές. Η πολυκριτήρια ανάλυση αποφάσεων παρέχει τη δυνατότητα σύνθεσης των ανεξάρτητων κριτηρίων, στην κατεύθυνση της λήψης ορθολογικών αποφάσεων.

Θεωρία Πολυκριτήριας Χρησιμότητας (Multi-Attribute Utility Theory – MAUT)

Πολύ συχνά στο σύγχρονο οικονομικό περιβάλλον, η περίπτωση των πολυκριτηριακών συστημάτων απόφασης, συνοδεύεται από την έννοια της αβεβαιότητας. Αυτό σημαίνει ότι όλες ή ένα μέρος από τις πληροφορίες που αφορούν τα κριτήρια αξιολόγησης των στρατηγικών δεν είναι γνωστές με βεβαιότητα [9].

Μία από τις γνωστότερες μεθόδους Πολυκριτηριακής Ανάλυσης Αποφάσεων είναι η **Θεωρία πολυκριτήριας χρησιμότητας** (Multi-Attribute Utility Theory) γνωστή και ως MAUT. Η μέθοδος αυτή βασίζεται στην ιδέα της μοντελοποίησης των προτιμήσεων του αποφασίζοντα με χρήση μίας συνάρτησης χρησιμότητας (utility function), η οποία για κάθε δυνατή τιμή κέρδους g, προσδιορίζει την ψυχολογική αξία U(g) που αποδίδει ο αποφασίζων στο χρηματικό όφελος g. Συμβατικά έχει αποφασιστεί η U(g) να παίρνει τιμές μεταξύ του διαστήματος [0,1]. Η βασική ιδέα της μεθόδου είναι **η μοντελοποίηση και αναπαράσταση του συστήματος αξιών που συνειδητά ή ασυνείδητα ακολουθεί ο αποφασίζων, μέσω μιας συνάρτησης αξιών/χρησιμότητας U(g) καθώς και ο μετασχηματισμός των κριτηρίων απόφασης σε μία κοινή κλίμακα**. Η μεθοδολογία παρατίθεται στον Πίνακα 2.1:

Πίνακας 2.1: *Η μέθοδος MAUT*

Βήματα	**Περιγραφή**
Βήμα 1ο	Καταγράφονται οι εναλλακτικές και τα κριτήρια αξιολόγησής τους.
Βήμα 2ο	Με βάση κάθε κριτήριο αποδίδεται μία τιμή σε κάθε εναλλακτική, που αντιστοιχεί στην αξιολόγηση της εναλλακτικής σύμφωνα με την προτίμηση των αποφασιζόντων.
Βήμα 3ο	Αποδίδονται σχετικά βάρη στα κριτήρια, που υποδεικνύουν τη σημαντικότητά τους. Το σύνολο των βαρών πρέπει να αθροίζεται στο 1.
Βήμα 4ο	Υπολογίζεται η πολυκριτήρια χρησιμότητα κάθε εναλλακτικής, η οποία προκύπτει λαμβάνοντας υπόψη την ¨βαθμολογία¨ της εναλλακτικής σε όλα τα κριτήρια (συνήθως οι επιμέρους χρησιμότητες προστίθενται). Επιλέγεται η εναλλακτική που μεγιστοποιεί τη χρησιμότητα.

2.4 Διαχείριση Κινδύνου (Risk Management)

2.4.1 Εισαγωγή στην έννοια του Risk Management

Θεωρείται ότι η πρώτη οργανωμένη προσπάθεια του ανθρώπου να μοντελοποιήσει την αβεβαιότητα του περιβάλλοντός του, έγινε εξαιτίας της δίψας για νίκη στα τυχερά παιχνίδια, περίπου το 1600. Τότε, σταματώντας να αντιμετωπίζουν την αβεβαιότητα απλώς σαν τύχη ή

ατυχία, οι σπουδαιότεροι μαθηματικοί της εποχής, Πασκάλ και Φερμά, αναλύοντας μεθοδικά τις διαθέσιμες πληροφορίες και αναπτύσσοντας στρατηγικές που εγγυώνται τη νίκη στα διάφορα παιχνίδια, έθεσαν τα θεμέλια της θεωρίας πιθανοτήτων και της στατιστικής. Σήμερα, αν και το δυσνόητο και ποικιλόμορφο περιβάλλον τείνει να καταστήσει την σύγκριση άτοπη, μπορούμε να πούμε ότι ο κλάδος του Risk Management που εμφανίζεται βασίζεται, σε γενικές γραμμές, στην παραπάνω φιλοσοφία των τυχερών παιχνιδιών, δηλαδή στην προσπάθεια για μεγιστοποίηση του κέρδους, με το ελάχιστο δυνατό ρίσκο.

Ως Risk Management ορίζεται η διαδικασία με την οποία οι επιχειρήσεις προσεγγίζουν μεθοδικά τους κινδύνους που σχετίζονται με τις δραστηριότητες και τους στόχους τους, με σκοπό να εξασφαλίσουν τη διαχρονική και απρόσκοπτη ανάπτυξή τους. Η ιδέα πίσω από την αναγκαιότητα δημιουργίας και λειτουργίας του κλάδου της Διαχείρισης Ρίσκου, είναι ότι η προσπάθεια επίτευξης στόχων ενός οργανισμού πλέον είναι συνυφασμένη με την προσπάθεια ¨απόκρουσης¨ των ποικίλων κινδύνων που απειλούν να εμποδίσουν αυτό το εγχείρημα. Η έλλειψη σιγουριάς όχι μόνο δεν εξαλείφεται, αλλά αυξάνεται συνεχώς, εξαιτίας της πολυπλοκότητας του σημερινού κόσμου. Η Διαχείριση Ρίσκου επιτρέπει στους οργανισμούς να προετοιμάζονται για αυτή την αβεβαιότητα, ελαχιστοποιώντας την επικινδυνότητα που θα αντιμετωπίσουν, πριν την αντιμετωπίσουν. Η δυνατότητα της αποτύπωσης και του ελέγχου των κινδύνων έχει ως αποτέλεσμα, ο οργανισμοί να λαμβάνουν τις αποφάσεις τους με μεγαλύτερη αυτοπεποίθηση και σιγουριά. Κατά τον νομπελίστα Herbert Simon, *η λήψη αποφάσεων είναι κατάσταση συνώνυμη του management* (Simon, 1977). Συχνά υποστηρίζεται ότι η διαδικασία του Risk Management, αποτελεί υποκατηγορία των ΣΥΑ, άλλοτε ότι η διεκπεραίωση του Risk Management απαιτεί την βοήθεια εφαρμογής ΣΥΑ για να ολοκληρωθεί. Η προσπάθεια υπαγωγής του ενός κλάδου στον άλλο είναι αδόκιμη εφόσον και οι δύο αφορούν τη συστηματική εφαρμογή ποσοτικών μεθόδων, τεχνικών και εργαλείων στην ανάλυση των προβλημάτων. Αντιθέτως, η αναγνώριση της αναλογίας τους έχει σταθεί χρήσιμη σε επίπεδο έρευνας.

2.4.2 *Οφέλη Εφαρμογής της Διαχείρισης Ρίσκου*

Η Διαχείριση Ρίσκου προσφέρει στους αποφασίζοντες εργαλεία ανάλυσης και μοντελοποίησης των διαθέσιμων πληροφοριών ώστε να λαμβάνουν δομημένες αποφάσεις σχετικά με το πώς να αντιμετωπίσουν τον κίνδυνο και να επιλέξουν μεταξύ στρατηγικών [11] . Ορισμένα από τα οφέλη εφαρμογής της μεθόδου είναι:

- Η κατανόηση του ρίσκου ως παραμέτρου του περιβάλλοντος αλλά και ως προς τον αντίκτυπο που έχει στην πραγματοποίηση των επιδιώξεων
- Η δημιουργία και η διατήρηση ενός ασφαλούς περιβάλλοντος για όλα τα άτομα που εμπλέκονται στον οργανισμό
- Η παροχή πληροφοριών που διευκολύνουν τη λήψη αποφάσεων
- Η αναγνώριση των αδύνατων σημείων του οργανισμού και η προσπάθεια απαλοιφής των παραγόντων που συνεισφέρουν στην πραγματοποίηση του ρίσκου
- Ο καθορισμός σαφών προτεραιοτήτων και η απρόσκοπτη υπεράσπισή τους

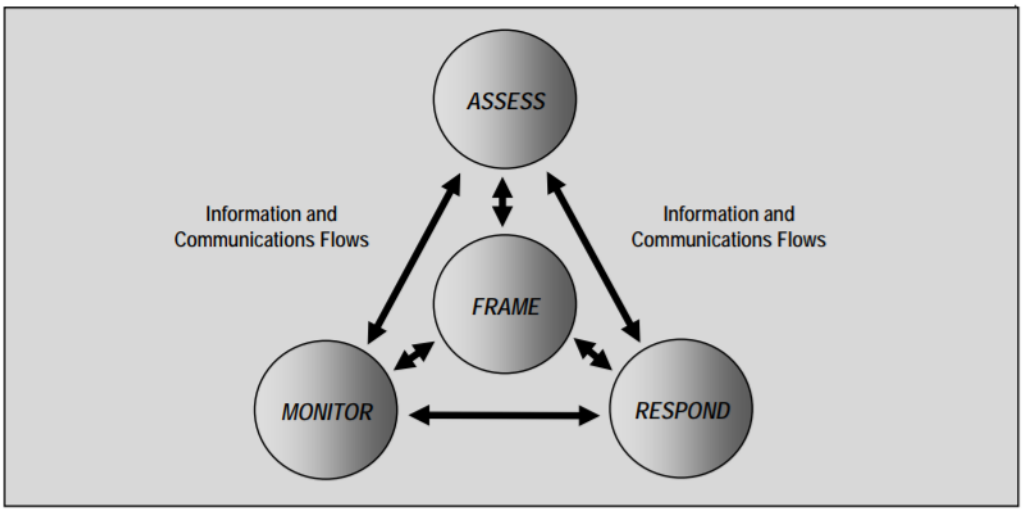
- Η διασφάλιση σταθερότητας και βιωσιμότητας για τον οργανισμό

2.4.3 *Ορισμός και σκιαγράφηση της μεθόδου*

Διαχείριση Ρίσκου είναι η διαδικασία κατα την οποία τα μέλη του επικείμενου οργανισμού:

1. επικοινωνούν και πραγματοποιούν συμβουλευτικές συναντήσεις (communication and consultation)
2. καταγράφουν το περιβάλλον/ πλαίσιο (establishing the context)
3. αναλύουν και εκτιμούν τον κίνδυνο μέσα σε αυτό (risk assessment)
4. ανταποκρίνονται σε αυτόν λαμβάνοντας τα κατάλληλα μέτρα για την εξάλειψή του (risk treatment)
5. παρακολουθούν το σύστημα για να ανιχνεύσουν περαιτέρω κινδύνους (monitoring and review)

Στο Σχήμα 2.5 παρουσιάζεται η βασική μορφή της διαδικασίας Διαχείρισης Ρίσκου, όπως αυτή εισήχθη από το NIST, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ. Κατά το NIST τα βασικά στάδια της μεθόδου που αναπαρίστανται είναι τέσσερα. Παραλείπει να αναπαραστήσει το στάδιο της επικοινωνίας ως ξεχωριστή οντότητα, αλλά το εισάγει ως ενδιάμεσο των υπολοίπων οντοτήτων.



Σχήμα 2.5: *Η μέθοδος του Risk Management, Πηγή:NIST*

Ακολουθεί αναλυτική περιγραφή του κάθε ενός από τους παράγοντες που αναφέρονται στον ορισμό, οι οποίοι ονομάζονται συνιστώσες πυρήνα (core functions).

1.Επικοινωνία και συμβουλευτικές συναντήσεις

Η επιτυχημένη αξιολόγηση των κινδύνων εξαρτάται πλήρως από την αποτελεσματική επικοινωνία των ενδιαφερόμενων μερών (stakeholders), δηλαδή των ατόμων που είναι σε θέση είτε να επηρεάσουν τον οργανισμό, είτε να επηρεαστούν από αυτόν. Λέγοντας επικοινωνία, εννοούμε την πραγμάτωση δραστηριοτήτων που στόχο έχουν την αλληλεπίδραση των ατόμων στο πλαίσιο του οργανισμού, παρέχοντας ή αποκτώντας χρήσιμες πληροφορίες και συμβουλές σχετικά με τις απειλές προς αντιμετώπιση: Αφορούν τόσο εσωτερικά ζητήματα, όπως η διοίκηση και οι επιχειρηματικές στρατηγικές, όσο και εξωτερικά, όπως η κατάσταση της αγοράς, η νομοθεσία και οι πηγές κινδύνου.

Προκειμένου να αποβεί επικερδής η ανταλλαγή πληροφοριών για τα επόμενα στάδια της μεθόδου, θα ήταν δόκιμο να πληρούνται ορισμένα κριτήρια:

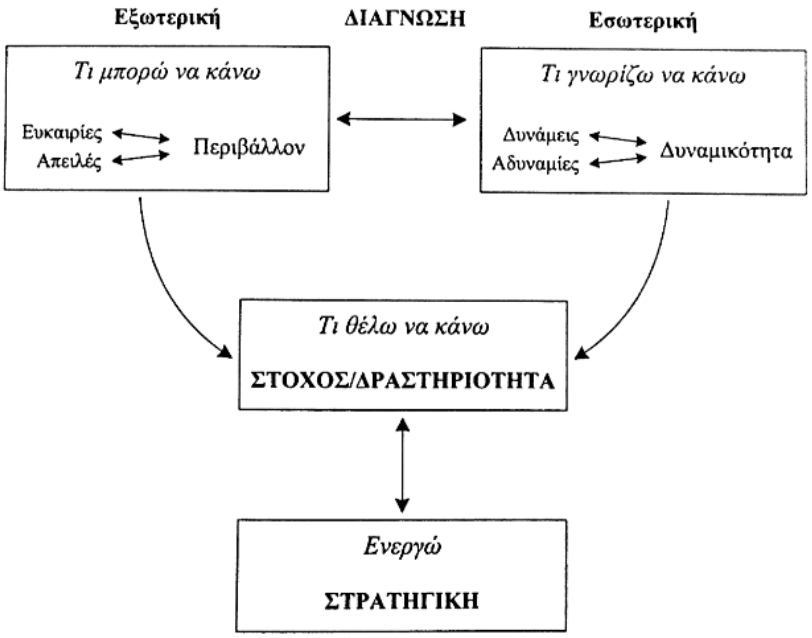
- Η ανάπτυξη ενός *πλάνου επικοινωνίας*, που ορίζει τακτικές συναντήσεις με προκαθορισμένη δομή,
- Ο σαφής και λεπτομερής *προσδιορισμός του οργανωτικού περιβάλλοντος* ώστε να είναι ευκολότερο να αναγνωριστούν οι απειλές και τα αδύναμα σημεία,
- Η εξασφάλιση ότι έχουν ληφθεί υπόψη οι *προτεραιότητες των ενδιαφερόμενων μερών* και ότι προστατεύονται τα συμφέροντά τους,
- Η ενσωμάτωση στη διαδικασία ατόμων με *διαφορετικές εξειδικεύσεις*, ίσως εκπροσώπους από διάφορα τμήματα του οργανισμού, για να χτιστεί ένα πλάνο που προστατεύει τον οργανισμό σαν σύνολο και να αποφευχθούν οι μεροληπτικές αποφάσεις υπέρ συγκεκριμένων επιδιώξεων,
- Η επαρκής *αναγνώριση των απειλών και των κινδύνων* και ο ορισμός και η έγκριση *πλάνων αντιμετώπισης* των κινδύνων στην περίπτωση που αυτοί πραγματωθούν.

Συμπερασματικά, η διαδικασία αυτή αναδεικνύεται ως ο κορμός της λήψης αποφάσεων, καθώς χάρη σε αυτή καθορίζονται οι προτεραιότητες και στόχοι και εξετάζονται οι εναλλακτικές.

2. Καταγραφή/ Διάγνωση περιβάλλοντος

Στο πλαίσιο των επιχειρήσεων και των οργανισμών, **περιβάλλον θεωρείται το σύνολο των φαινομένων που καθορίζουν το μέλλον της επιχείρησης** [1]. Σε γενικές γραμμές με τον όρο καταγραφή περιβάλλοντος εννοούμε την κατανόηση και την αποτύπωση των συνθηκών στις οποίες θα εφαρμοστεί η διαδικασία Διαχείρισης Ρίσκου. Μετά τον διαμοιρασμό πληροφοριών στο προηγούμενο στάδιο, οι υπεύθυνοι είναι πλέον σε θέση να θέσουν τους στόχους τους, να ορίσουν τα κριτήρια με βάση τα οποία θα αξιολογούν τους κινδύνους και να αναπτύξουν την *ακριβή δομή της μεθόδου ανάλυσης* που θα εφαρμοστεί.

Για να είναι αυτό δυνατό, πρέπει να προσδιοριστούν οι βασικές παράμετροι του οργανισμού, (εσωτερικές και εξωτερικές) και το πλαίσιο στο οποίο θα γίνει η ανίχνευση και η διαχείριση ρίσκου. Στο Σχήμα 2.6 φαίνεται η διαδικασία διάγνωσης του περιβάλλοντος και η επιρροή της στον καθορισμό της στρατηγικής που θα ακολουθηθεί.



Σχήμα 2.6: *Η λογική της διάγνωσης, Πηγή: Η Στρατηγική των Επιχειρήσεων*

- *Προσδιορισμός εξωτερικών παραμέτρων*: Προκύπτει αναλύοντας τις σχέσεις που διατηρεί ο οργανισμός με άλλους οργανισμούς, άτομα, ή το κράτος. Περιλαμβάνει πολιτικούς, πολιτιστικούς, κοινωνικούς, νομικούς και χρηματοοικονομικούς παράγοντες, οι οποίοι καταγράφονται με σκοπό να αναδείξουν τεχνικές ανάλυσης και διαχείρισης ρίσκου, που δεν ταιριάζουν μόνο στον ίδιο τον οργανισμό αλλά και στο ευρύτερο πλαίσιο μέσα στο οποίο λειτουργεί και αναπτύσσεται.

- *Προσδιορισμός εσωτερικών παραμέτρων* : Μπορούμε να προσδιορίσουμε το εσωτερικό πλαίσιο καταγράφοντας και θέτοντας :

  - Τους στόχους του οργανισμού και τις στρατηγικές που χαράζει για να τους πετύχει,
  - Τα ενδιαφερόμενα μέρη και τη συμπεριφορά τους απέναντι στις επιδιώξεις και τους κινδύνους,
  - Τη δομή των μεθόδων λήψης αποφάσεων,
  - Την κουλτούρα και τις αξίες του οργανισμού, δηλαδή το σύστημα αξιών και ιδεών σύμφωνα με το οποίο λειτουργεί,
  - Τις πολιτικές και τα πρότυπα που ακολουθεί και
  - Την διοικητική δομή (πώς έχουν αποδοθεί οι ρόλοι και οι υποχρεώσεις).

- *Προσδιορισμός πλαισίου εφαρμογής της διαδικασίας Διαχείρισης Ρίσκου* : Κατά τη διάρκεια αυτού του βήματος, λαμβάνοντας υπόψη τα δεδομένα που συλλέχθηκαν στα προηγούμενα στάδια, γίνεται ο καθορισμός της μεθόδου και των συντελεστών της, τα οποία παρέχονται σαν είσοδος στα επόμενα στάδια της ανάλυσης:

- Τίθενται οι ρόλοι και οι ευθύνες,
- Συμφωνείται η έκταση στην οποία θα γίνει η Διαχείριση Ρίσκου σε χρονικούς και τοπικούς όρους,
- Καθορίζεται ο τρόπος με τον οποίο θα γίνεται η σύνδεση, και ποιές θα είναι οι σχέσεις μεταξύ διαφορετικών δραστηριοτήτων του οργανισμού,
- Επιλέγεται η μεθοδολογία αποτίμησης και αξιολόγησης ρίσκου και ορίζονται τα κριτήρια ρίσκου,
- Ορίζεται η μέθοδος και οι μετρικές αξιολόγησης σύμφωνα με τις οποίες θα διαπιστωθεί εάν η διαδικασία Διαχείρισης Ρίσκου απέδωσε και τέλος
- Διευκρινίζονται οι αποφάσεις και οι δράσεις που πρέπει να ληφθούν.

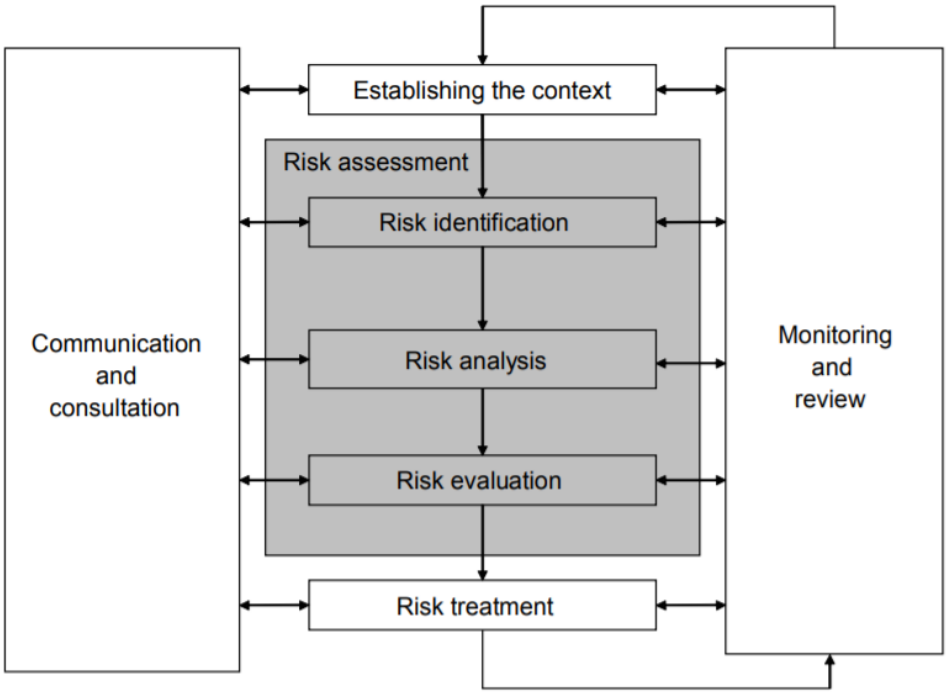
- *Προσδιορισμός κριτηρίων για την αξιολόγηση ρίσκου* : Προκειμένου να αποφασιστούν τα κριτήρια που θα εφαρμοστούν στην αξιολόγηση των κινδύνων, πρέπει προηγουμένως να έχουν διευκρινιστεί:
  - Τα είδη των συνεπειών που θα συμπεριληφθούν ώστε να αποφευχθούν και ο τρόπος με τον οποίο θα γίνει η ταξινόμησή τους σε κλίμακες σοβαρότητας,
  - Ο τρόπος με τον οποίο θα εκφράζονται οι πιθανότητες (ποσοτικός ή ποιοτικός),
  - Ο τρόπος με τον οποίο θα αποδίδονται τα επίπεδα σοβαρότητας στους κινδύνους (ως προς τις επιπτώσεις τους),
  - Τα κριτήρια με βάση τα οποία θα αποφασίζεται εάν ένας κίνδυνος πρέπει να αντιμετωπιστεί ή να αγνοηθεί και,
  - Πώς θα λαμβάνονται υπόψη (προσδιορισμός τακτικής) πολλαπλοί κίνδυνοι που απειλούν ταυτόχρονα τον οργανισμό.

Το στάδιο κατά το οποίο προσδιορίζονται τα κριτήρια και τα επίπεδα επιπτώσεων των κινδύνων είναι ιδιαίτερα σημαντικό παρά την φαινομενική απλότητά του. Για να προσδιοριστεί η κλίμακα μέτρησης της επικινδυνότητας, χρειάζεται πρώτα να έχει προσδιοριστεί η κλίμακα μέτρησης των επιπτώσεων και των αντίστοιχων πιθανοτήτων. Σκεπτόμενοι απλοϊκά, θα μπορούσαμε να χρησιμοποιήσουμε την ίδια κλίμακα μέτρησης επιπτώσεων, έστω σε όρους χρηματικών δαπανών, για όλα τα στοιχεία που προστατεύουμε. Αυτό γεννά πολλά προβλήματα καθώς δεν είναι πάντα δυνατό (ή δόκιμο) να υπολογίσουμε την οικονομική αποτίμηση μίας συνέπειας, όπως για παράδειγμα στην περίπτωση που αυτή η συνέπεια αφορά πρόκληση σωματικής βλάβης. Ως απόρροια αυτού, προτείνεται να επιλέγουμε την κλίμακα μέτρησης της συνέπειας, με βάση το στοιχείο που αφορά. Για παράδειγμα, αν προκύψει μη διαθεσιμότητα κάποιας λειτουργίας, τότε η συνέπεια μπορεί να δοθεί σε όρους χρόνου εκτός λειτουργίας. Συμπεραίνουμε λοιπόν ότι για κάθε στοιχείο που απειλείται, πρέπει πρώτα να θεωρήσουμε τη φύση και το είδος των πιθανών συνεπειών και το πώς αυτές θα εκτιμηθούν. Όσον αφορά την εκτίμηση των πιθανοτήτων, το μόνο που πρέπει να οριστεί είναι το είδος αναπαράστασης. Αυτό θα μπορούσε να είναι **ποσοτικό**, ή **ποιοτικό**, και επιλέγεται ανάλογα με τα **διαθέσιμα δεδομένα** και το ποσοστό ακρίβειας τους. Αποτέλεσμα της διαδικασίας αυτής είναι ο καθορισμός ενός συστήματος κριτηρίων που ονομάζεται ¨συνεπής οικογένεια κριτηρίων¨ και πρέπει να διέπεται από τις αρχές:

- της συνέπειας/μονοτονίας,
- της επάρκειας,
- του μη πλεονασμού.

3. Εκτίμηση Ρίσκου (Risk Assessment)

Σύμφωνα με τον νομπελίστα Daniel Kahneman, ¨*έχουμε μία δυσκολία στην εκτίμηση των ρίσκων: Είτε τα αγνοούμε εντελώς/ παραβλέπουμε είτε τους δίνουμε πολύ μεγάλη βαρύτητα*¨. Αυτό καθιστά πλήρως κατανοητούς τους λόγους για τους οποίους η Εκτίμηση Ρίσκου αποτελεί τον ακρογωνιαίο λίθο του εγχειρήματος περιορισμού των κινδύνων. Η διαδικασία περιλαμβάνει τρία διακριτά στάδια: την ***αναγνώριση***, την ***ανάλυση*** και την ***αξιολόγηση*** των κινδύνων που υφίστανται στο πλαίσιο του οργανισμού. Στο Σχήμα 2.7 παρουσιάζεται διαγραμματικά η συμβολή της Εκτίμησης Ρίσκου στη διαδικασία Διαχείρισης Κινδύνου. Αποτέλεσμα της διαδικασίας είναι η κατανόηση και αποδόμηση των κινδύνων, της πιθανότητας να εμφανιστούν και των ενδεχόμενων συνεπειών τους. Όντες εφοδιασμένοι με αυτά τα δεδομένα, οι υπεύθυνοι του οργανισμού είναι σε θέση να *λάβουν αποφάσεις*, όπως το πώς θα τεθεί υπό έλεγχο η επικείμενη επικινδυνότητα, πώς θα ενισχύσουν τα αδύναμα σημεία που εντοπίστηκαν και πώς να μεγιστοποιήσουν και να εκμεταλλευτούν τις ευκαιρίες του περιβάλλοντος. Παρακάτω περιγράφονται συνοπτικά τα βήματα αναγνώρισης, ανάλυσης και αξιολόγησης κινδύνου, για να είναι σαφές το πώς ενσωματώνονται στην διαδικασία, ενώ λεπτομερής παράθεση μεθόδων Ανάλυσης Ρίσκου και των διαφορών τους θα γίνει στην παράγραφο 2.5.



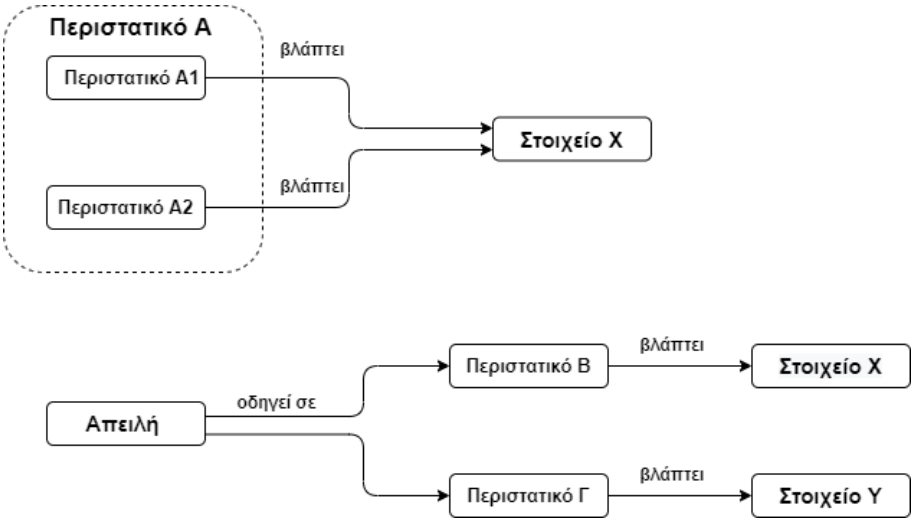
Σχήμα 2.7: *Η Συμβολή του Risk Assessment στη διαδικασία του Risk Management, Πηγή: ISO: 31010*

- *Αναγνώριση Ρίσκου (Risk Identification)* : Σε αυτό το βήμα πρέπει να καταγραφούν όλες οι καταστάσεις που δυνητικά θα μπορούσαν να προκαλέσουν στον οργανισμό υλικές ή άυλες καταστροφές. Πρέπει λοιπόν να διαγνωστούν όλα τα αδύναμα σημεία του οργανισμού, καθώς και οι απειλές που μπορούν να τα εκμεταλλευτούν. Για την ανίχνευση όλων των φυσικών κινδύνων και των πηγών τους, μπορούν να χρησιμοποιηθούν ιστορικά δεδομένα, αποτελέσματα ερωτηματολογίων, να γίνουν συνεντεύξεις ή να εφαρμοστούν συγκεκριμένες τεχνικές (πχ HAZOP). Δεν πρέπει να παραλείπεται η διαδικασία ανταλλαγής ιδεών καθώς χάρη στην διορατικότητα των συμμετεχόντων μπορεί να εντοπιστούν πιθανοί κίνδυνοι, μη καταγεγραμμένοι στην ήδη υπάρχουσα βιβλιογραφία. Αντίστοιχα, για την επισήμανση κυβερνοαπειλών, μπορούν να επιστρατευθούν εργαλεία αυτόματης ανίχνευσης ευαισθησιών, τεστ προσομοίωσης επιθέσεων ή αξιολόγηση κώδικα. Ο συστηματικός έλεγχος του συστήματος κρίνεται αναγκαίος για την αποφυγή επιθέσεων ¨**0-day**¨, κατά τις οποίες, τα αδύναμα σημεία του συστήματος γίνονται αντιληπτά πρώτα από τους αντιπάλους, που τα εκμεταλλεύονται πραγματοποιώντας τις σχετικές με αυτά επιθέσεις.

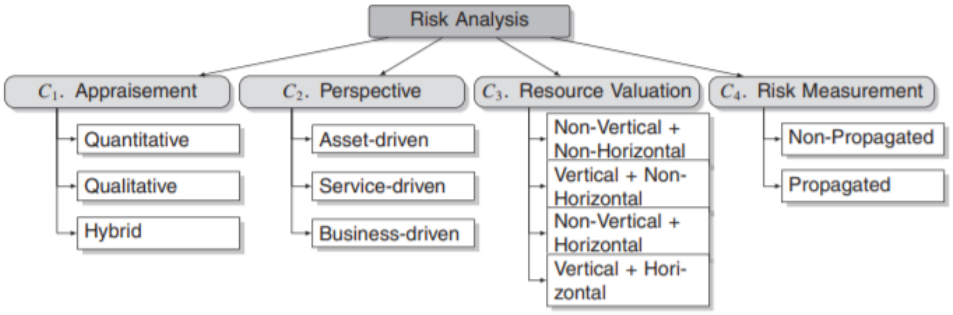
- *Ανάλυση Ρίσκου (Risk Analysis)* : Με τον όρο ανάλυση ρίσκου εννοούμε τη συστηματική προσπάθεια για εκτίμηση της σοβαρότητας του κινδύνου και της κατανόησης αυτού. Το *επίπεδο του κινδύνου* (level of risk) υπολογίζεται ως συνάρτηση/συνδυασμός της πιθανότητας πραγμάτωσης και των επιπτώσεων. Σε αυτή τη διαδικασία δεν πρέπει να παραβλεφθεί το ενδεχόμενο ένας κίνδυνος να έχει πολλαπλές συνέπειες στο σύστημα, επηρεάζοντας παραπάνω από ένα στοιχεία, και ίσως ορισμένες από αυτές με μακροπρόθεσμη επικινδυνότητα. Επίσης, όπως αναφέρθηκε και στον ορισμό του, το μοντέλο των επιπτώσεων στο σύστημα είναι αθροιστικό, επομένως για να εκτιμήσουμε τον κίνδυνο που αντιμετωπίζουν συγκεκριμένα στοιχεία του οργανισμού, πρέπει να ληφθούν υπόψη όλοι οι κίνδυνοι που το αφορούν, και να αθροιστούν τα επίπεδα των συνεπειών τους. Τα παραπάνω δύο ενδεχόμενα μοντελοποιούνται στο Σχήμα 2.8 Πριν εκτιμηθεί το επίπεδο σοβαρότητας, είναι αναγκαίο να ληφθούν υπόψη τα ήδη εφαρμοζόμενα μέτρα αντιμετώπισης, προληπτικά ή μη, και η επίδρασή τους στον περιορισμό των κινδύνων.

  Διακρίνονται τέσσερις γενικές κατηγορίες τεχνικών ανάλυσης ρίσκου [12] με βάση : την **αποτίμηση εκτιμηθείσας τιμής** (appraisement), **την προοπτική** (perspective), **την αξιολόγηση πόρων** (resource valuation) και **την αποτίμηση του κινδύνου** (risk measurement).Κάθε οργανισμός είναι σε θέση να επιλέξει την τεχνική που καλύπτει καλύτερα τις ανάγκες του, βάσει της μορφής των διαθέσιμων δεδομένων αλλά και του επιθυμητού επιπέδου λεπτομέρειας της ανάλυσης. Να σημειωθεί σε αυτό το σημείο, ότι το αποτέλεσμα αυτού του βήματος πρέπει να είναι συμβατό με τα ήδη ορισμένα κριτήρια, ώστε να είναι δυνατή η ¨ταξινόμηση¨ του κινδύνου με βάση αυτά και ο περιορισμός του. Η δομή της ανάλυσης ρίσκου παρουσιάζεται στο Σχήμα 2.9. Παρακάτω προσεγγίζονται εκτενέστερα οι τέσσερις προαναφερθείσες κατηγορίες. ′

  - **Αποτίμηση εκτιμηθείσας τιμής (Appraisement)**: Πρόκειται για την πιο συνηθισμένη ταξινόμηση των τεχνικών υπολογισμού επιπέδου του ρίσκου. Τις κατα-



Σχήμα 2.8: *Άθροιση κινδύνου όταν α) δύο περιστατικά αποτελούν στιγμιότυπα ενός κοινού, πιο γενικού ρίσκου και βάλλουν το ίδιο στοιχείο, β) μία απειλή έχει πολλαπλές συνέπειες στο σύστημα*



Σχήμα 2.9: *Ταξινόμηση τεχνικών Ανάλυσης Ρίσκου, Πηγή: Taxonomy of information security risk assessment (ISRA)*

τάσσει σε **ποιοτικές** (qualitative), **ημι-ποσοτικές** (semi-quantitative) και **ποσοτικές** (quantitative).

* Ποσοτικές τεχνικές: Ως είσοδο λαμβάνουν αριθμητικά δεδομένα και πιθανότητες τα οποία επεξεργάζονται μέσω μακροσκελών υπολογισμών και χρήσης στατιστικής θεωρίας. Για να εφαρμοστεί μια ποσοτική τεχνική πρέπει οι στόχοι του οργανισμού να εκφράζονται αριθμητικά (πχ χρηματική αξία, ποσοστά). Η μεγαλύτερη δυσκολία της χρήσης τέτοιων μεθοδολογιών έγκειται στο γεγονός ότι, στην πράξη, είναι πολύ σπάνιο όλοι οι στόχοι να εκφράζονται ποσοτικά.
* Ποιοτικές τεχνικές: Χάρη στην απλότητά της, αυτό το είδος τεχνικής είναι το πιο συχνά χρησιμοποιούμενο. Ανάλογα με το εύρος της επίπτωσής τους και την πιθανότητα να υλοποιηθούν, οι απειλές κατατάσσονται σε κλάσεις αφού τους ανατίθενται σχετικές τιμές, είτε γλωσσικές είτε εύρους, για παράδειγμα με χρήση μοντέλων ασαφούς λογικής/ fuzzy logic. Η ευελιξία χρήσης τους έγκειται στην αποτελεσματικότητά τους ανεξαρτήτως ύπαρξης διαθέσι-

μων ιστορικών δεδομένων για υπολογισμούς. Παρόλα αυτά, πολλές φορές ελλείπονται λεπτομέρειας, με αποτέλεσμα ανεπαρκή σχεδιασμό.

* Ημιποσοτικές/ Υβριδικές τεχνικές: Λαμβάνουν ως είσοδο τόσο ποσοτικά, όσο ποιοτικά δεδομένα και τα επεξεργάζονται κατάλληλα. Έτσι συνδυάζουν τα πλεονεκτήματα των παραπάνω κατηγοριών.

– **Προοπτική (Perspective)**: Οι τεχνικές υπολογισμού του ρίσκου κατατάσσονται **με βάση τα στοιχεία του οργανισμού** (asset-driven), **με βάση τις υπηρεσίες** (service-driven) και **με βάση την επιχειρηματική δραστηριότητα** (business-driven). Σε αυτή την κατηγορία οι αποφασίζοντες εστιάζουν σε ένα επίπεδο του οργανισμού (στοιχεία, υπηρεσίες ή επιχειρηματική δραστηριότητα) ώστε να διαγνώσουν όλες τις απειλές και τους κινδύνους που συνδέονται με αυτό.

* Με βάση τα στοιχεία του οργανισμού: Τα στοιχεία που ενδιαφέρουν τον οργανισμό, αναγνωρίζονται και αξιολογούνται με βάση τη σημασία τους. Για κάθε ένα από αυτά, ανιχνεύονται όλες οι πιθανές απειλές και υπολογίζονται τα σενάρια ρίσκου. Εάν λάβει κανείς υπόψη το πλήθος των στοιχείων σε συνδυασμό με το πλήθος των σεναρίων ρίσκου για καθένα από αυτά, αντιλαμβάνεται και το μεγάλο πλήθος σεναρίων ρίσκου που πρέπει να υπολογιστούν και να ενημερώνονται τακτικά. Η εκτενής λίστα των σεναρίων κάνει το είδος της μεθόδου αυτής επιρρεπές σε λάθος υπολογισμούς. Παρόλα αυτά, πρόκειται για το πιο συνηθισμένο αυτής της κατηγορίας γιατί χάρη στα διαθέσιμα εργαλεία είναι εύκολα υλοποιήσιμο και κατανοητό.
* Με βάση τις υπηρεσίες : Οι κίνδυνοι ταξινομούνται και εκτιμώνται με βάση την επίδραση που έχουν στις υπηρεσίες. Καθώς ο αριθμός των υπηρεσιών είναι σίγουρα μικρότερος από των αριθμό των ανεξάρτητων στοιχείων του οργανισμού, αυτό το είδος τεχνικής για ανάλυση του ρίσκου είναι ευκολότερα διαχειρίσιμο από το αντίστοιχο που αφορά τα στοιχεία.
* Με βάση την επιχειρηματική δραστηριότητα : Οι συγκεκριμένες μέθοδοι ανάλυσης ρίσκου συνδέονται απευθείας με τους επιχειρηματικούς στόχους και τους μηχανισμούς που τους στηρίζουν. Ο κύριος στόχος είναι να αναγνωριστούν τα αδύναμα σημεία και οι πιθανές απειλές που μπορεί να επηρεάσουν την υλοποίηση των επιχειρηματικών στρατηγικών.

– **Αξιολόγηση πόρων (Resource valuation)**: Οι πόροι του οργανισμού που αναφέρθηκαν στην προηγούμενη κατηγορία (στοιχεία, υπηρεσίες, επιχειρηματική δραστηριότητα), παρουσιάζουν μεταξύ τους σχέσεις και πολλές φορές εξαρτήσεις. Αυτή η κατηγορία τεχνικής υπολογισμού του ρίσκου διαφέρει από τις υπόλοιπες γιατί λαμβάνει υπόψη αυτές τις σχέσεις. Σύμφωνα με αυτήν, υπάρχουν δύο ιεραρχήσεις, η **κάθετη** (vertical view) και η **οριζόντια** (horizontal view).

* Κάθετη ιεράρχηση: Πρόκειται για ιεράρχηση από κάτω-προς-τα-πάνω, που δίνει βάση στη συνεισφορά των κατώτερων επιπέδων στα ανώτερα. Στη βάση της οργανωτικής πυραμίδας βρίσκονται τα στοιχεία του οργανισμού (υλικός εξοπλισμός, κτήρια, προϊόντα κ.α.), στη συνέχεια οι υπηρεσίες και τέλος η επιχειρηματική δραστηριότητα/ στόχος. Το αποτέλεσμα αυτής της ανάλυσης

διαφέρει ανάλογα με την ιεράρχηση που επιλέγουμε να αναπαραστήσουμε, και αυτό γίνεται εύκολα κατανοητό μέσα από ένα παράδειγμα. Η αξία δύο router που εξυπηρετούν διαφορετικά τμήματα του οργανισμού (έστω σε ένα νοσοκομείο, το ένα χρησιμοποιείται για πρόσβαση των επισκεπτών στο Internet και το άλλο για αποθήκευση και επεξεργασία ιατρικών δεδομένων), υπολογίζεται ίδια, εάν χρησιμοποίησουμε κάποια μέθοδο αποτίμησης με βάση τα στοιχεία του οργανισμού που παρουσιάστηκε προηγουμένως. Αντιθέτως, εάν χρησιμοποιηθεί μέθοδος κάθετης ιεράρχησης αποδίδεται μεγαλύτερη αξία στο router που θεωρείται πιο κριτικής σημασίας για την διεκπεραίωση των στόχων του οργανισμού. Πολλές φορές βέβαια, είναι ιδιαίτερα δύσκολο να αναγνωριστούν όλες οι πιθανές εξαρτήσεις.

  * Οριζόντια ιεράρχηση: Εκμεταλλεύεται εξαρτήσεις μεταξύ οντοτήτων του ίδιου οργανωτικού επιπέδου. Για παράδειγμα, μπορεί μία υπηρεσία του οργανισμού για να λειτουργήσει να βασίζεται απόλυτα στη λειτουργία μίας ή πολλών άλλων, δημιουργώντας έτσι αλυσίδες εξάρτησης.

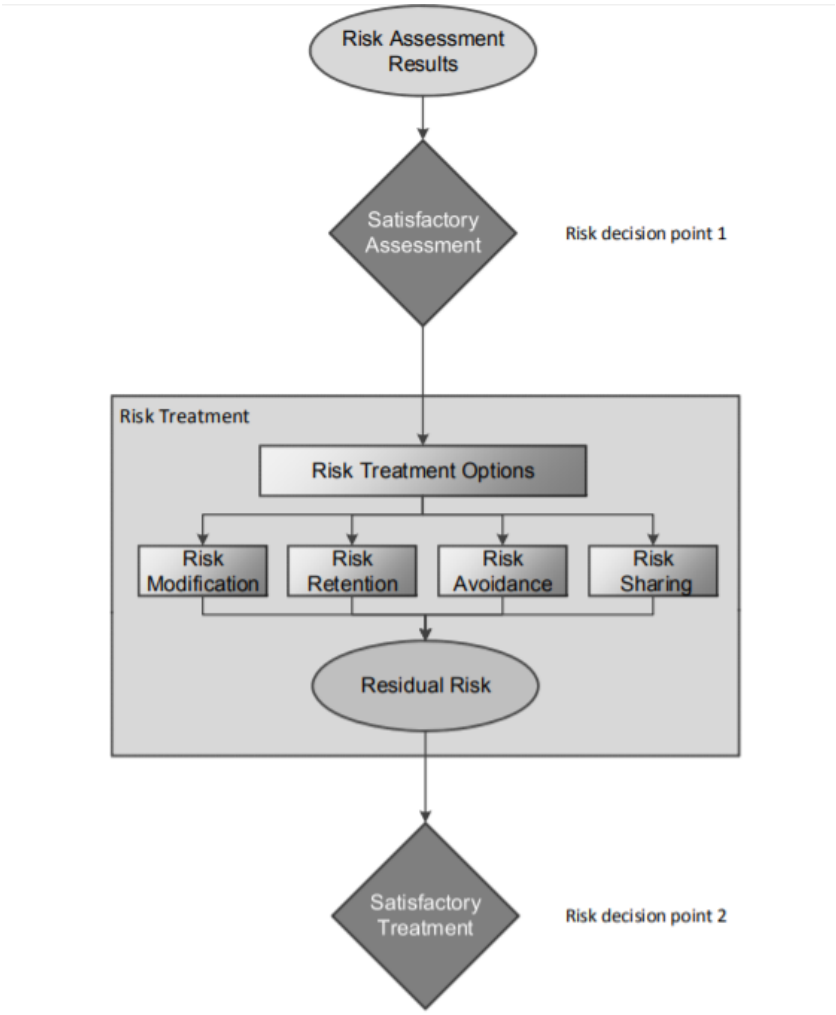
- **Μέτρηση του κινδύνου (Risk measurement)**: Σε αυτή την κατηγορία διακρίνουμε δύο είδη: μέτρηση χωρίς διάδοση του κινδύνου (non propagated) , μέτρηση λαμβάνοντας υπόψη τη διάδοση του κινδύνου (propagated) .

  * Μέτρηση χωρίς διάδοση του κινδύνου: Για να υπολογιστεί το επίπεδο του κινδύνου, αγνοείται η πιθανή επίδρασή του σε άλλους πόρους. Αρκεί να ληφθούν υπόψη μόνο τρείς παράγοντες, η αξία του πόρου ως προς τον οποίο εκτιμάται ο κίνδυνος, τα αδύναμα σημεία του, και το μέγεθος της απειλής.
  * Μέτρηση λαμβάνοντας υπόψη τη διάδοση του κινδύνου: Όταν ένας πόρος βάλλεται από κίνδυνο, αυτός ο κίνδυνος διαδίδεται και στους συσχετισμένους με αυτόν πόρους, σύμφωνα με το γράφο εξαρτήσεων των πόρων του οργανισμού. Το πλεονέκτημα αυτής της προσέγγισης είναι ότι μπορεί να προβλέψει συνέπειες που έχει η πραγματοποίηση του κινδύνου, ώστε να έχει λάβει εγκαίρως τα κατάλληλα μέτρα για την ελαχιστοποίησή τους. Αυτό βέβαια προϋποθέτει την ακριβή καταγραφή τόσο των χαρακτηριστικών του κινδύνου, όσο και των συνδέσεων μεταξύ των πόρων.

- *Αξιολόγηση Ρίσκου (Risk Evaluation)* : Με βάση την τιμή που υπολογίστηκε στο προηγούμενο βήμα, πρέπει να αποφασιστεί η συμπεριφορά απέναντι στον κάθε κίνδυνο. Για να είναι αυτό εφικτό, ορίζονται τα **κριτήρια αποδοχής κινδύνου** (risk acceptance criteria). Τα επίπεδα του κινδύνου συγκρίνονται με αυτά τα κριτήρια, ώστε να αποφασιστεί ποιοί κίνδυνοι χρειάζονται αντιμετώπιση, για ποιούς από αυτούς η δράση κρίνεται επείγουσα και ποιοί θα αγνοηθούν. Σε αυτό το στάδιο, για να τεθεί η προτεραιότητα ως προς τη σειρά αντιμετώπισης οι υπεύθυνοι πρέπει να αναλογιστούν ξανά ηθικούς νομικούς και οικονομικούς παράγοντες.

4. Αντιμετώπιση Ρίσκου (Risk Treatment)

Η διαδικασία αντιμετώπισης ρίσκου περιλαμβάνει το σαφή καθορισμό των στρατηγικών που θα ακολουθηθούν για τον χειρισμό του κινδύνου. Έχοντας ολοκληρώσει την εκτίμηση της επικινδυνότητας, οι υπεύθυνοι είναι σε θέση να προτείνουν εναλλακτικές με στόχο την μείωση της πιθανότητας πραγμάτωσης των κινδύνων, ή τον μετριασμό των επιπτώσεών τους. Όποια και αν είναι τα χαρακτηριστικά των προτεινόμενων εναλλακτικών, μπορούμε να τις κατατάξουμε σε τέσσερις ευρείες κατηγορίες, όπως φαίνεται και στο Σχήμα 2.10:



Σχήμα 2.10: *Η διαδικασία αντιμετώπισης ρίσκου, Πηγή: ISO-27005*

- Περιορισμός Ρίσκου (Risk Reduction) : Ο οργανισμός προτιμά να μειώσει την επικινδυνότητα που αντιμετωπίζει λαμβάνοντας τα κατάλληλα μέτρα.

- Διατήρηση Ρίσκου (Risk Retention) : Ο οργανισμός κρίνει ότι η επικινδυνότητα είναι σε ανεκτά επίπεδα, και ότι η ανάληψη ανασταλτικών δράσεων θα ήταν επιζήμια χωρίς να επιφέρει αποτελέσματα.

- Αποφυγή Ρίσκου (Risk Avoidance): Ο οργανισμός προσπαθεί πάση θυσία να αποφύγει κάθε πιθανότητα πραγμάτωσης κινδύνου. Η συγκεκριμένη τακτική είναι σπάνια εφαρμόσιμη.

– Διαμοιρασμός Ρίσκου (Risk Sharing): Ο οργανισμός μεταφέρει τον κίνδυνο, ή ποσοστό του, σε άλλο οργανισμό (πχ ασφαλιστικές παροχές).

Στην πράξη, ο συνδυασμός των παραπάνω στρατηγικών είναι η πιο ρεαλιστική και αποδοτική επιλογή. Τα κριτήρια αποδοχής του κινδύνου που διαμορφώθηκαν στο προηγούμενο βήμα, καθορίζουν το ποιές από τις απειλές θα αντιμετωπιστούν και με ποιόν τρόπο. Η επιλογή του βέλτιστου πλάνου για αντιμετώπιση ρίσκου, βασίζεται επίσης σε παράγοντες κόστους και ικανοποίησης των συμφερόντων των υπεύθυνων του οργανισμού. Το πλάνο θέτει το χρονικό πλαίσιο, την προτεραιότητα των μέτρων αντιμετώπισης, τον τρόπο υλοποίησης αυτών καθώς και τρόπους για να μετράται η αποδοτικότητα της εφαρμογής [13]. Ο υπολειμματικός κίνδυνος, μετά την εφαρμογή των μέτρων, πρέπει να αντιμετωπιστεί επίσης, οπότε η διαδικασία επαναλαμβάνεται μέχρι να επιτευχθεί το καλύτερο δυνατό αποτέλεσμα.

5. Παρακολούθηση και Επαναξιολόγηση (Monitoring and Review)

Μετά την διατύπωση και την εφαρμογή των στρατηγικών αντιμετώπισης κινδύνου, είναι απαραίτητη και η παρακολούθηση του σχεδίου, με στόχο να κριθεί το επίπεδο αποτελεσματικότητάς του. Καθώς το περιβάλλον του οργανισμού αλλά και των απειλών που αντιμετωπίζει δεν είναι στατικό, είναι πιθανό να χρειαστεί το πλάνο αυτό να αναθεωρηθεί.

Η παρακολούθηση λοιπόν, πρέπει να γίνεται σε δύο επίπεδα:

– Παρακολούθηση και επαναξιολόγηση σε επίπεδο κινδύνων : Εξετάζονται τυχόν αλλαγές που έχουν προκύψει, τόσο ως προς τους κινδύνους και τα χαρακτηριστικά τους, όσο και προς τον ίδιο τον οργανισμό και τα αδύναμά του σημεία.

– Παρακολούθηση και επαναξιολόγηση σε επίπεδο πλάνου Διαχείρισης Ρίσκου: Εξετάζεται κατά πόσο η εφαρμογή του πλάνου γίνεται με συνέπεια. Ελέγχεται η σχετικότητα και η επάρκεια του πλάνου για τις ανάγκες του οργανισμού. Πρέπει να λαμβάνονται υπόψη ενδεχόμενες αλλαγές στο εξωτερικό περιβάλλον του, όπως για παράδειγμα αλλαγή της νομοθεσίας, ώστε να αναπροσαρμόζεται έγκαιρα σε αυτές.

Στην επόμενη παράγραφο παρουσιάζεται με μεγαλύτερη λεπτομέρεια η διαδικασία Εκτίμησης Ρίσκου, μέσα από την ανάλυση συγκεκριμένων μεθοδολογιών.

2.5 Μεθοδολογίες Εκτίμησης Ρίσκου (Risk Assessment Methods)

Στην παράγραφο 2.2 παρουσιάστηκε η διαδικασία Διαχείρισης Ρίσκου και αναλύθηκαν οι περιεχόμενες διαδικασίες, με σκοπό να γίνει κατανοητό το πώς αυτές ενσωματώνονται και ενυπάρχουν στο σύνολο. Σε αυτή την παράγραφο παρουσιάζεται με μεγαλύτερη λεπτομέρεια η διαδικασία Εκτίμησης Ρίσκου, μέσα από την παράθεση και την ανάλυση συγκεκριμένων μεθοδολογιών.

Η Εκτίμηση Ρίσκου είναι ο πυλώνας της όλης μεθόδου. Οι διαφορές τόσο μεταξύ των οργανισμών που εφαρμόζουν τις τακτικές όσο και των κινδύνων που τους απειλούν έχουν οδηγήσει στην ανάπτυξη πληθώρας νέων μεθοδολογιών. Αυτές οι μεθοδολογίες, που δημιουργήθηκαν για να καλύπτουν διαφορετικές ανάγκες, παρουσιάζουν μεταξύ τους μεγάλη ανομοιότητα, της οποίας η μελέτη έχει ιδιαίτερο ενδιαφέρον. Συντελεστές όπως η πολυπλοκότητα του προβλήματος, η φύση και η ακρίβεια των διαθέσιμων πληροφοριών, το κόστος υλοποίησης ή οι ανάγκες κάθε μεθόδου σε όρους χρόνου και εξειδίκευσης, καθορίζουν την προτιμητέα εναλλακτική.

Έχουν ήδη αναφερθεί τέσσερις διαφορετικές ταξινομήσεις των μεθοδολογιών ανάλυσης ρίσκου με βάση : την **αποτίμηση εκτιμηθείσας τιμής** (appraisement), **την προοπτική** (perspective), **την αξιολόγηση πόρων** (resource valuation) και **την αποτίμηση του κινδύνου** (risk measurement). Ο διαχωρισμός αυτός διευκολύνει την επιλογή όταν τα δεδομένα που έχουμε για το ρίσκο βρίσκονται σε συγκεκριμένη μορφή, πχ είναι αριθμητικά. Παρόλα αυτά υπάρχουν περιπτώσεις κατά τις οποίες η ανωτέρω διάκριση δεν κρίνεται λειτουργική, ιδιαίτερα όταν θέλουμε να εστιάσουμε στην **χρονική παράμετρο** που υπεισέρχεται στην έννοια του υλοποιημένου κινδύνου, δηλαδή τί προηγείται και τί έπεται αυτού [14]. Σε αυτή την περίπτωση η ταξινόμηση των μεθόδων μπορεί να γίνει ως εξής:

- **Προς τα πάνω** (Upstream Methods) : Θεωρώντας ως αφετηρία τη στιγμή βλάβης του συστήματος εξαιτίας πραγμάτωσης κινδύνου, ανιχνεύονται τα γεγονότα εκείνα που είτε προκάλεσαν τον κίνδυνο, είτε επέτρεψαν στον κίνδυνο να υλοποιηθεί επηρεάζοντας τον οργανισμό. Στα αδύναμα σημεία που εντοπίζονται λαμβάνονται τα κατάλληλα μέτρα πρόληψης, με στόχο την απόκρουση της επικείμενης απειλής σε περίπτωση που ξαναεμφανιστεί.

- **Προς τα κάτω** (Downstream Methods) : Θεωρώντας ως αφετηρία τη στιγμή βλάβης του συστήματος εξαιτίας πραγμάτωσης κινδύνου, καταγράφονται όλες οι πιθανές συνέπειες, άμεσες ή έμμεσες και γίνεται προσπάθεια να μετριαστούν οι επιπτώσεις.

- **Υβριδικές** (Hybrid/Combined Methods) :Θεωρώντας ως αφετηρία τη στιγμή βλάβης του συστήματος εξαιτίας πραγμάτωσης κινδύνου, καταγράφονται οι πηγές και οι συνέπειες του κινδύνου, δηλαδή τι προηγείται και τι έπεται αυτού. Με την εφαρμογή της μεθόδου εντοπίζονται τόσο τα προληπτικά, όσο και τα μέτρα αντιμετώπισης ρίσκου.

Θα παρουσιαστούν παραδείγματα μεθοδολογιών, για να διαπιστωθούν οι διαφορές τους ως προς τη χρήση και την απόδοση.

2.5.1 *Μήτρα Κινδύνου (Risk Matrix)*

Ανήκει στην κατηγορία ποιοτικών μεθόδων εκτίμησης ρίσκου, αν και πολλές φορές χρησιμοποιείται και με ημι-ποσοτικά δεδομένα.

Η μέθοδος αυτή αποτελεί μέσο για να συνδυαστούν οι τιμές που αφορούν τις επιπτώσεις και την πιθανότητα υλοποίησης επικείμενων κινδύνων, προσδιορίζοντας έτσι το επίπεδό τους. Χάρη στην απλότητα της, η μήτρα κινδύνου χρησιμοποιείται συχνά όταν έχουν αναγνωριστεί πολλοί κίνδυνοι, υποδεικνύοντας ποιοί από αυτούς είναι σοβαροί και πρέπει να αναλυθούν

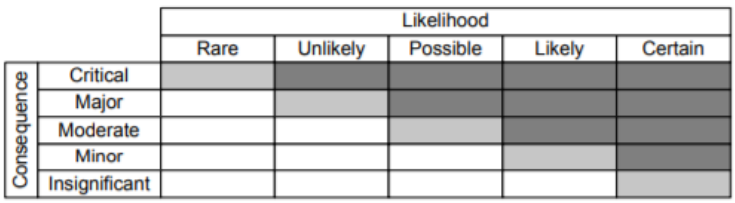
Πίνακας 2.2: *Ταξινόμηση επιπτώσεων κινδύνων*

Σοβαρότητα επίπτωσης	**Ορισμός**
Αμελητέα (Insignificant)	Σε περίπτωση υλοποίησης του κινδύνου δεν θα προκαλέσει επιπτώσεις στον οργανισμό
Μικρή (Minor)	Σε περίπτωση υλοποίησης του κινδύνου θα προκαλέσει επιπτώσεις αλλά δεν θα εμποδίσει την επίτευξη των στόχων του οργανισμού
Μέτρια (Moderate)	Σε περίπτωση υλοποίησης του κινδύνου θα προκαλέσει επιπτώσεις αλλά σημαντικοί στόχοι θα επιτευχθούν
Σοβαρή (Major)	Σε περίπτωση υλοποίησης του κινδύνου θα προκαλέσει πολύ σοβαρές επιπτώσεις στον οργανισμό και τους στόχους του
Επικίνδυνη (Critical)	Σε περίπτωση υλοποίησης του κινδύνου θα προκαλέσει αποτυχία εκπλήρωσης των στόχων του οργανισμού

Πίνακας 2.3: *Ταξινόμηση πιθανότητας υλοποίησης κινδύνων*

Πιθανότητα υλοποίησης	**Ορισμός**
Σπάνια (Rare)	Συμβαίνει μόνο σε εξαιρετικές περιπτώσεις
Απίθανη (Unlikely)	Συμβαίνει σε λίγες περιπτώσεις
Πιθανή (Possible)	Πιθανώς να συμβεί κάποια στιγμή
Πολύ πιθανή (Likely)	Ενδεχομένως συμβεί στις περισσότερες περιπτώσεις
Σχεδόν βέβαιο (Certain)	Αναμένεται να συμβεί στις περισσότερες περιπτώσεις

παραπάνω και ποιοί μπορούν να αγνοηθούν. Η επιλογή των κινδύνων που τίθενται σε προτεραιότητα, εξαρτάται από τη θέση στην οποία βρίσκονται στη μήτρα κινδύνου. Στο σχήμα 2.11 δίνεται ένα παράδειγμα μήτρας κινδύνου, στο οποίο οι ζώνες με το σκούρο χρώμα χρήζουν άμεσης ανάλυσης και αντιμετώπισης. Οι ορολογίες για τα διαφορετικά επίπεδα επιπτώσεων και πιθανοτήτων υλοποίησης δίνονται στους πίνακες 2.2 και 2.3 αντίστοιχα.



Σχήμα 2.11: *Η μήτρα κινδύνου, Πηγή: Cyber Risk Management, Springer*

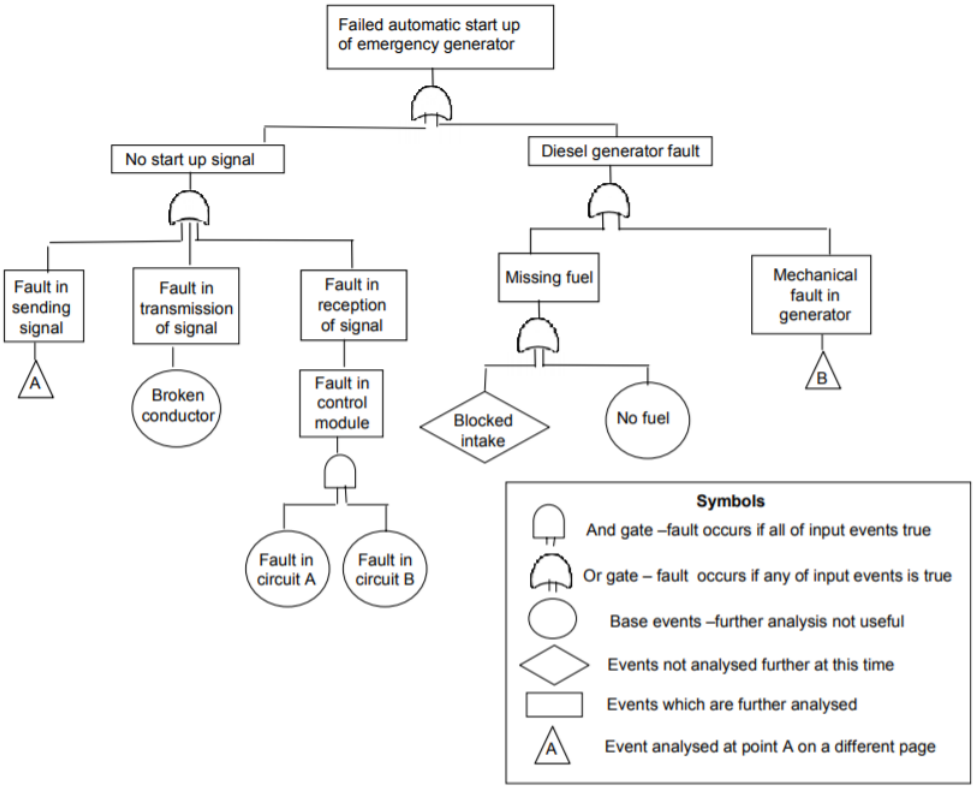
2.5.2 *Fault Tree Analysis (FTA)*

Ανήκει στην κατηγορία μεθόδων προς τα πάνω/ upstream.

Η μέθοδος αυτή αναπαριστά όλα τα γεγονότα που πιθανώς ευθύνονται για την πραγματοποίηση ενός αρνητικού ενδεχομένου, το οποίο ονομάζεται αρχικό/ κορυφαίο γεγονός (top event). Μέσω της αναγνώρισης όλων των πιθανών αιτιών της αποτυχίας, στην ουσία οι υπεύθυνοι είναι σε θέση να εξετάσουν διαφορετικές εναλλακτικές σχεδιασμού, με την ελπίδα

να αποφύγουν το ρίσκο. Μπορεί να λάβει ως είσοδο ποσοτικά και ποιοτικά δεδομένα. Για ποιοτική ανάλυση του κινδύνου, είναι απαραίτητη η πλήρης κατανόηση του συστήματος, των αιτιών αποτυχίας, καθώς και οι αλληλοεξαρτήσεις των αδύναμων σημείων. Για ποσοτική ανάλυση, πρέπει να είναι διαθέσιμα αριθμητικά δεδομένα όπως ποσοστά αποτυχίας τεχνικών μηχανισμών ή πιθανότητες υλοποίησης συγκεκριμένων απειλών. Με την εφαρμογή της μεθόδου, οι αναλυτές έχουν μία απλοποιημένη διαγραμματική αναπαράσταση των τρόπων με τους οποίους μπορεί να προκύψει το αρνητικό ενδεχόμενο. Εάν υπάρχουν ως δεδομένες οι πιθανότητες υλοποίησης των γεγονότων που κατέληξαν στα φύλλα του δέντρου, και οι μεταξύ τους σχέσεις, η πιθανότητα να πραγματωθεί ο κίνδυνος που φέρεται ως κορυφαίο γεγονός, μπορεί να υπολογισθεί.

Στο Σχήμα 2.12 παρουσιάζεται διαγραμματικό παράδειγμα και στη συνέχεια στον Πίνακα 2.4 δίδεται η περιγραφή της μεθόδου.



Σχήμα 2.12: *Παράδειγμα FTA, Πηγή: ISO:31010*

Με το πέρας της διαδικασίας, με μία απλή διάσχιση του δέντρου από κάτω προς τα πάνω, δηλαδή μέσω των μονοπατιών από κάθε φύλλο προς τη ρίζα, έχουν καταγραφεί όλοι οι εναλλακτικοί τρόποι που θα μπορούσαν να οδηγήσουν στην πραγματοποίηση του αρνητικού ενδεχομένου.

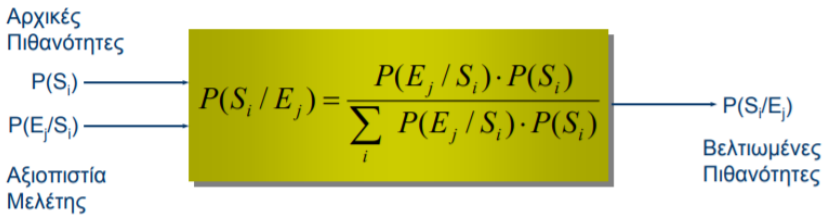
2.5.3 *Δέντρο αποφάσεων (Event Tree Analysis/ETA)*

Ανήκει στην κατηγορία μεθόδων προς τα κάτω/downstream.

Πίνακας 2.4: *Η μέθοδος FTA*

Βήματα	**Περιγραφή**
Βήμα 1ο	Ορίζεται το κορυφαίο γεγονός, το οποίο αποτελεί τη ρίζα του δέντρου που θα δημιουργηθεί
Βήμα 2ο	Καταγράφονται όλες οι αιτίες που ως άμεση συνέπεια έχουν το κορυφαίο γεγονός, και τοποθετούνται στο επόμενο επίπεδο του δέντρου
Βήμα 3ο	Κάθε μία από τις πιθανές αιτίες αναλύονται αναδρομικά, ώστε να βρεθεί τι τις προκάλεσε
Βήμα 4ο	Η διαδικασία συνεχίζεται μέχρι να μην μπορεί να γίνει - ή να μην είναι αποδοτικό να γίνει- περαιτέρω ανάλυση

Στα δένδρα απόφασης υιοθετείται η υπόθεση ότι η αβεβαιότητα μπορεί να μοντελοποιηθεί με πιθανότητες [15]. Σε κάθε τυχαίο γεγονός αντιστοιχεί μία πιθανότητα υλοποίησης, των οποίων το άθροισμα είναι η μονάδα. Οι πιθανότητες αυτές ονομάζονται **αρχικές ή a priori** πιθανότητες. Παρόλα αυτά, ο αποφασίζων διατηρεί το δικαίωμα να προσφύγει σε αγορά νέας πληροφορίας (έρευνες αγοράς, δημοσκοπήσεις κ.α.), προκειμένου να εμβαθύνει στην ποιότητα της πληροφορίας αυτής [9]. Οι πιθανότητες των καταστάσεων που θα προκύψουν από την αγορά πληροφορίας ονομάζονται **βελτιωμένες ή a posteriori** πιθανότητες. Ο υπολογισμός των βελτιωμένων πιθανοτήτων γίνεται με τη χρήση του τύπου δεσμευμένων πιθανοτήτων του Bayes, όπως φαίνεται στο σχήμα 2.13:



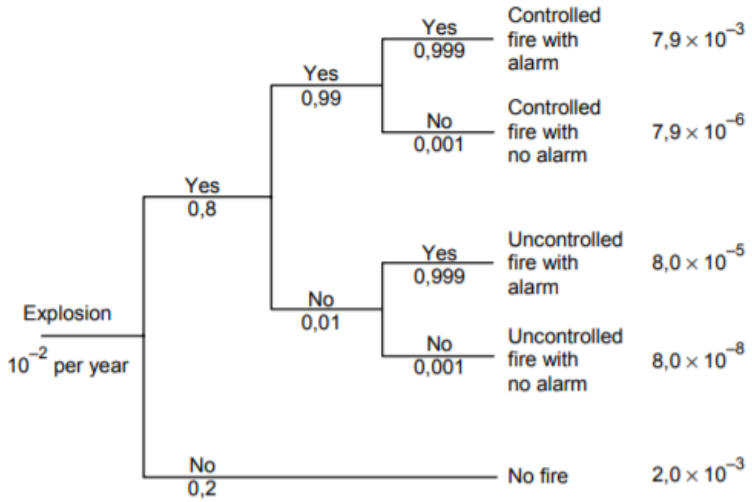
Σχήμα 2.13: *Υπολογισμός πιθανοτήτων με βάση τον τύπο Bayes, Πηγή: Εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης, ΕΜΠ*

Στην ουσία, η μέθοδος αυτή αναπαριστά όλα τα γεγονότα που πιθανώς προκαλούνται από την πραγματοποίηση ενός αρνητικού ενδεχομένου, λαμβάνοντας υπόψη τις περιπτώσεις εφαρμογής αλλά και μη εφαρμογής μέτρων ειδικά σχεδιασμένων για τον περιορισμό των συνεπειών. Επιτρέπει την επανεξέταση των ασφαλιστικών μέτρων που έχουν ληφθεί και την αξιολόγηση της επιτυχίας τους. Έτσι με το πέρας της ανάλυσης, οι υπεύθυνοι μπορούν να επιλέξουν την εναλλακτική που εγγυάται καλύτερη αντιμετώπιση του ρίσκου.

Μετά την ανάλυση, με διάσχιση του δέντρου από τη ρίζα (αρχικό γεγονός) προς τα φύλλα, προκύπτει μια ακολουθία γεγονότων που εκκινούν από το αρχικό, και χαρακτηρίζονται από την πραγματοποίηση ή τη μη πραγματοποίηση μέτρων αντιμετώπισης του κινδύνου. Στην ουσία πρόκειται για μια λίστα εναλλακτικών που στόχο έχουν να μειώσουν την επικινδυνότητα. Παράδειγμα της μεθόδου δίδεται στο Σχήμα 2.14. Στο παράδειγμα οι βελτιωμένες πιθανότητες δεν προκύπτουν από αγορά πληροφορίας, αλλά από εφαρμογή μεθόδων αντιμετώπισης.

Πίνακας 2.5: *Η μέθοδος ETA*

Βήματα	**Περιγραφή**
Βήμα 1ο	Ορίζεται το αρχικό γεγονός και τοποθετείται στη ρίζα του δέντρου που θα δημιουργηθεί
Βήμα 2ο	Καταγράφονται σειριακά όλα τα μέτρα αντιμετώπισης που έχουν καθοριστεί για να μετριάσουν τις αρνητικές επιπτώσεις στο σύστημα
Βήμα 3ο	Σε καθένα από τα παραπάνω μέτρα, αντιστοιχίζονται δύο γραμμές στο δέντρο, η μία αντιπροσωπεύει την εφαρμογή/ επιτυχία του μέτρου, και η άλλη την μη εφαρμογή/ αποτυχία
Βήμα 4ο	Υπολογίζονται οι δεσμευμένες πιθανότητες μέσω του τύπου Bayes και αναγράφονται στις αντίστοιχες γραμμές
Βήμα 5ο	Η διαδικασία συνεχίζεται όσο υπάρχουν μέτρα αντιμετώπισης που δεν έχουν εξεταστεί



Σχήμα 2.14: *Παράδειγμα ETA, Πηγή: ISO:31010*

Σημείωση: Όπως και η Fault Tree Analysis, έτσι και η μεθοδολογία των δέντρων αποφάσεων έχει ποιοτική και ποσοτική εφαρμογή. Σε αυτή την περίπτωση όμως, οι πιθανότητες που αναγράφονται στο διάγραμμα είναι δεσμευμένες πιθανότητες, που υπολογίζονται μέσω του τύπου Bayes. Με άλλα λόγια, η πιθανότητα που αντιστοιχεί στην επιτυχημένη εφαρμογή ενός μέτρου αντιμετώπισης δεν αφορά κανονικές συνθήκες, αλλά έχει υπολογιστεί δεδομένης της πραγμάτωσης του αρχικού γεγονότος.

2.5.4 *GIRA Model (General Model for Incident Risk Analysis)*

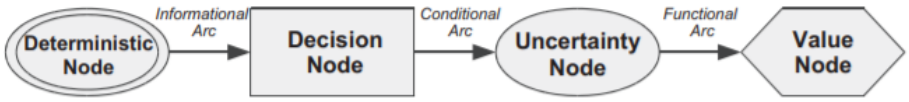
Ανήκει στην κατηγορία υβριδικών μεθόδων (combined methods).

Η μέθοδος αυτή, αφού μοντελοποιήσει όλες τις πιθανές συνέπειες που προκαλούνται από την έκθεση σε έναν κίνδυνο, και την επίδραση που θα είχε στο σύστημα η εφαρμογή

αντιδράσεων με στόχο τον περιορισμό των επιπτώσεων, βοηθά τους υπεύθυνους να αξιολογήσουν τις εναλλακτικές τους, λαμβάνοντας υπόψη τις επιδιώξεις του οργανισμού. Χωρίζεται δηλαδή σε δύο στάδια: στο πρώτο, ξεκινώντας από μία απειλή καταγράφονται όλες οι πιθανές συνέπειες, και παρουσιάζονται και εξετάζονται όλες οι εναλλακτικές δράσεις για την αντιμετώπιση του ρίσκου, και στο δεύτερο, αφού αξιολογηθούν οι εναλλακτικές και τα αποτελέσματά τους με βάση τους στόχους που έχουν τεθεί, επιλέγεται η εναλλακτική που ελαχιστοποιεί την επικινδυνότητα.

Το GIRA model ακολουθεί τη γενική δομή ενός **διαγράμματος ροής**, η οποία παρουσιάζεται στο Σχήμα 2.15 :

- Απόφασης (Decision Nodes),
- Ντετερμινιστικούς (Deterministic Nodes),
- Μη ντετερμινιστικούς/ Αβεβαιότητας (Uncertainty Nodes),
- Αριθμητικών Τιμών (Value Nodes).



Σχήμα 2.15: *Η γενική μορφή ενός διαγράμματος ροής, Πηγή: GIRA: a general model for incident risk analysis*

Πιο συγκεκριμένα το μοντέλο αναλύεται στα παρακάτω στοιχεία :

1. Κόμβο έκθεσης σε απειλή (Threat exposure node):
   Περιέχει την πιθανότητα το σύστημα υπό διαχείριση να είναι εκτεθειμένο σε μία συγκεκριμένη απειλή. Οι καταστάσεις του κόμβου αναπαριστούν υποψήφιες απειλές, ενώ οι αναγραφόμενες πιθανότητες εκφράζουν το πόσο πιθανό είναι κάποια από αυτές να υλοποιηθεί. Υπάρχει πάντα η πιθανότητα να μην υλοποιηθεί καμία απειλή.

2. Κόμβος μέτρων αντιμετώπισης απειλών (Incident Response Node):
   Περιέχει τις εναλλακτικές που θα μπορούσαν να εφαρμοστούν ώστε να αποφευχθούν ή να μετριαστούν οι συνέπειες της επικείμενης απειλής. Οι καταστάσεις του κόμβου αντιστοιχούν σε δράσεις μεταξύ τους ανεξάρτητες, γι' αυτό οι εναλλακτικές δράσεις υποδεικνύονται από την εφαρμογή όλων των πιθανών συνδυασμών δράσεων, συμπεριλαμβανομένης και της δυνατότητας να μην γίνει καμία δράση.

3. Κόμβος πραγματοποίησης κινδύνου (Incident Materialisation Node):
   Περιέχει την πιθανότητα πραγματοποίησης της απειλής, δεδομένου ότι έχουν εφαρμοστεί τα μέτρα αντιμετώπισης που καθορίστηκαν στο προηγούμενο βήμα. Οι πολλαπλές καταστάσεις του κόμβου αυτού αντιστοιχούν σε όλες τις πιθανές συνέπειες από

την πραγμάτωση του κινδύνου/ απειλής, και μπορεί να είναι **άμεσες**, **έμμεσες** ή να προέρχονται από **κλιμακωτές συνέπειες** (cascading consequences).

4. Κόμβος Συνεπειών στο Διαχειριζόμενο Σύστημα (Consequences in the Managed System Node):
   Περιέχει την πιθανότητα, να προκληθούν περαιτέρω αρνητικές συνέπειες στο σύστημα εξαιτίας της πραγματοποίησης του κινδύνου. Για διαφορετικές συνέπειες δημιουργούνται διακριτοί κόμβοι.

5. Κόμβος Στοιχείων υπό προστασία (Asset Node):
   Περιέχει την επίδραση που έχει η πραγματοποίηση του κινδύνου στα ενδιαφέροντα των υπευθύνων του οργανισμού, και στα στοιχεία των οποίων η προστασία έχει τεθεί ως προτεραιότητα. Μπορεί να υπάρχουν πολλοί κόμβοι, ένας για κάθε στοιχείο υπό προστασία. Με βάση την επίδραση διαφορετικών συνθηκών στα στοιχεία και των ποικίλων καταστάσεών τους, η σοβαρότητα και το είδος των επιπτώσεων σε αυτά μπορεί να αλλάζει. Αυτού του είδους οι κόμβοι είναι ντετερμινιστικοί μόνο αν ξέρουμε με σιγουριά το πώς αλλάζουν οι καταστάσεις των στοιχείων, αλλιώς μοντελοποιούνται σαν κόμβοι αβεβαιότητας. Επίσης, τα περιεχόμενα των κόμβων αυτών παραμένουν σταθερά για διαφορετικά σενάρια ρίσκου, καθώς δεν αφορούν τους επικείμενους κινδύνους αλλά τις προτεραιότητες που τέθηκαν από τον οργανισμό στα αρχικά στάδια της διαδικασίας.

6. Κόμβος Επίπτωσης στα Στοιχεία υπό προστασία (Asset status Node):
   Περιέχει την πιθανότητα, μία συνέπεια της πραγματοποίησης της απειλής να οδηγήσει σε περαιτέρω επιπτώσεις στα στοιχεία υπό προστασία ή στα δευτερεύοντα συστήματα, που συνδέονται με το σύστημα υπό διαχείριση. Η ανάλυση της αλυσίδας των πιθανών επιπτώσεων μπορεί να απαιτεί και την ανάλυση των δευτερευόντων συστημάτων.

7. Κόμβος Στόχων (Objective Node):
   Περιέχει του στόχους που έχουν τεθεί στο πρώτο στάδιο της μεθόδου Διαχείρισης Ρίσκου. Υπολογίζει τη σοβαρότητα των επιπτώσεων που μπορεί να έχει η πραγμάτωση της απειλής στην υλοποίηση των επιδιώξεων του οργανισμού.

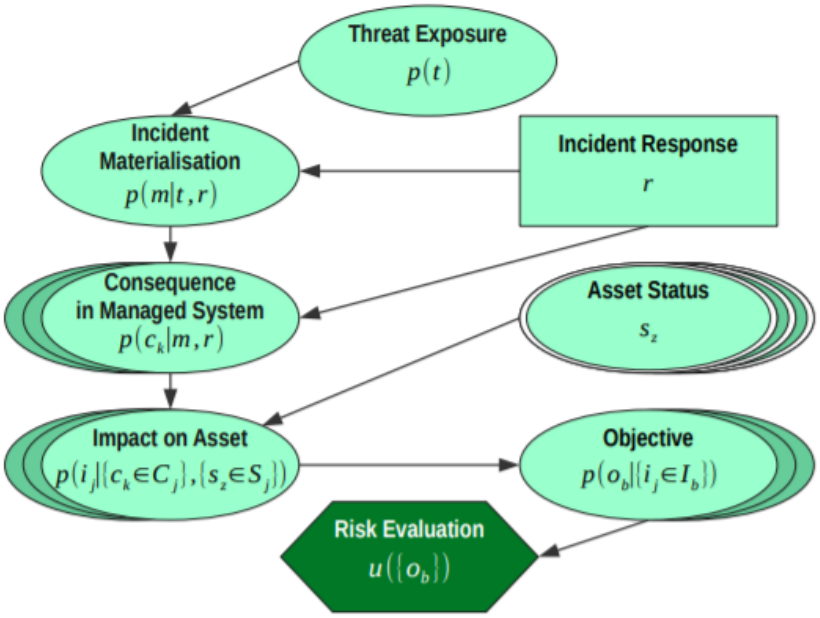
8. Σύνολο κόμβων Περιγραφής Κινδύνου (Risk Description Group of Nodes):
   Το σύνολο των κόμβων 1-7, ολοκληρώνει το περιγραφικό κομμάτι της Ανάλυσης Ρίσκου, και μένει μόνο η αξιολόγηση του κινδύνου κι ο καθορισμός της στρατηγικής που θα ακολουθηθεί. Χάρη στη δομή του GIRA και των διαγραμμάτων ροής, μοντελοποιούνται ταυτόχρονα διαφορετικά χαρακτηριστικά που αφορούν στους κινδύνους, όπως απειλές, μέτρα αντιμετώπισης και στόχοι, επιτρέποντας στους υπεύθυνους να λαμβάνουν συνεπείς αποφάσεις, εξυπηρετώντας όλες τις ανάγκες του οργανισμού. Για παράδειγμα, η αλυσιδωτή μορφή επιτρέπει τη γνώση της πιθανότητας η απειλή που εξετάζεται, να προκαλέσει βλάβη σε εγκαταστάσεις αλλά και την πιθανότητα να εμποδίσει την κατάκτηση των βασικών στόχων του οργανισμού, κάτι που άλλες μέθοδοι θα χρειαζόντουσαν πολλά στάδια ανάλυσης για να υπολογίσουν.

9. Κόμβος Αξιολόγησης Κινδύνου (Risk Evaluation Node):
   Είναι το τελικό στάδιο της ανάλυσης. Αναπαριστά την αξιολόγηση των σεναρίων από τους υπεύθυνους με στόχο την επιλογή, μεταξύ των εναλλακτικών στρατηγικών που

παρουσιάστηκαν στον Κόμβο Μέτρων Αντιμετώπισης, της τακτικής εκείνης που ελαχιστοποιεί τον κίνδυνο και ικανοποιεί τις επιδιώξεις του οργανισμού. Αυτό γίνεται μέσω ταξινόμησης όλων των πιθανών σεναρίων, από το περισσότερο έως το λιγότερο επιθυμητό.

Σημείωση: Η διαδικασία της αξιολόγησης γίνεται από ένα μοντέλο Αξιολόγησης Ρίσκου, και η επιλογή αυτού αφήνεται στα χέρια των αναλυτών. Για παράδειγμα θα μπορούσε να υλοποιηθεί **MAUT**, μέθοδος που περιγράφηκε στην παράγραφο 2.3.2.

Συνολικά, η μοντελοποίηση κατά GIRA ενός προβλήματος απόφασης βασισμένου στην εκτίμηση κινδύνου, μαζί με τα μεγέθη που το θεμελιώνουν μαθηματικά [16], παρουσιάζεται στο Σχήμα 2.16. Οι ποσότητες που παρουσιάζονται στο Σχήμα, ορίζονται και αναλύονται στον Πίνακα 2.6.



Σχήμα 2.16: *Συνολική μοντελοποίηση του προβλήματος με χρήση GIRA model, Πηγή: Decision Models for Cybersecurity Risk Analysis,Aitor Couce Vieira*

Ο υπολογισμός των μαθηματικών τιμών που παρουσιάζονται στον Πίνακα 2.6 γίνεται με χρήση της εξίσωσης :

$$p(\{o_b\},\{i_j\},\{s_z\},\{c_k\},m,r,t) = \left[\prod_{b=1}^{B} p\left(o_b \mid (i_j :\ni i_j \rightarrow o_b)\right)\right] \times \left[\prod_{j=1}^{J} p\left(i_j \mid (c_k :\ni c_k \rightarrow i_j),(s_z :\ni s_z \rightarrow i_j)\right)\right] \times \left[\prod_{k=1}^{K} p\left(c_k \mid m,r\right)\right] \times p(m \mid t,r)\, p(t) \tag{2.1}$$

Πίνακας 2.6: *Ορισμός μεγεθών GIRA*

Μέγεθος	**Κόμβος**	**Περιγραφή**
$p(t)$	Έκθεσης σε κίνδυνο	Η πιθανότητα μία απειλή να παρουσιάζεται στο σύστημα υπό διαχείριση.
r	Μέτρων Αντιμετώπισης Απειλής	Εναλλακτικές δράσεις που εφαρμόζονται με στόχο να αποφευχθεί το αρνητικό ενδεχόμενο ή να μετριαστούν οι συνέπειές του.
$p(m \mid t, r)$	Πραγματοποίησης Κινδύνου	Η πιθανότητα να πραγματοποιηθεί ο κίνδυνος, *δεδομένου ότι* έχουν εφαρμοστεί τα μέτρα αποφυγής που ορίστηκαν στο προηγούμενο βήμα. Πρόκειται για δεσμευμένη πιθανότητα, ο υπολογισμός της οποίας γίνεται με χρήση του τύπου του Bayes.
$p(c_k \mid m, r)$	Συνεπειών στο Διαχειριζόμενο Σύστημα	Η πιθανότητα η πραγματοποίηση του κινδύνου να προκαλέσει περαιτέρω αρνητικά γεγονότα, έστω πλήθους k, τα οποία μοντελοποιούνται σε ανεξάρτητους κόμβους και αντιστοιχούν σε διαφορετικές πιθανότητες για $c_k = c_1,\ldots,c_K$.
s_z	Στοιχείων υπό προστασία	Τα στοιχεία του συστήματος, $s_z = s_1,\ldots,s_Z$, των οποίων η προστασία ενδιαφέρει τους αποφασίζοντες.
$p\left(i_j \mid (c_k \in C_j), (s_z \in S_j)\right)$	Επίπτωσης στα Στοιχεία υπό προστασία	Η πιθανότητα το αρνητικό ενδεχόμενο να επηρεάσει τα στοιχεία υπό προστασία του κύριου, ή δευτερευόντων συστημάτων. Αυτή η πιθανότητα αναπαρίσταται ως : $p\left(i_j \mid (c_k :\ni c_k \rightarrow i_j), (s_z :\ni s_z \rightarrow i_j)\right)$ όπου $(c_k :\ni c_k \rightarrow i_j)$ το σύνολο των συνεπειών που προκαλούν την j-ιοστή επίπτωση στα στοιχεία και όπου $(s_z :\ni s_z \rightarrow i_j)$ το σύνολο των στοιχείων που επηρεάζονται από την επίπτωση.
$p\left(o_b \mid (i_j \in I_b)\right)$	Στόχων	Η πιθανότητα, το αρνητικό ενδεχόμενο να επηρεάσει την πραγματοποίηση των στόχων. Οι επιπτώσεις συντίθενται και ¨προβάλλονται¨ σε ένα μειωμένο αριθμό στόχων των αποφασιζόντων, απλοποιώντας τη διαδικασία κατανόησης. Οι συνέπειες στο σύστημα μεταφράζονται σε συνέπειες στην πραγματοποίηση των στόχων και η αναπαράσταση γίνεται : $p\left(o_b \mid (i_j :\ni i_j \rightarrow o_b)\right)$, όπου $o_b = o_1, \ldots, o_B$, οι στόχοι των αποφασιζόντων.

Κεφάλαιο 3

Η αναγκαιότητα Διαχείρησης Ρίσκου στις Κρίσιμες υποδομές

Οι Κρίσιμες Υποδομές αποτελούν τον ακρογωνιαίο λίθο των σύγχρονων κοινωνιών και της εξελικτικής τους τάσης, καθώς εξασφαλίζουν στο σύνολό του, το βιοτικό επίπεδο ενός κράτους. Η καθοριστική συμβολή τους στην διατήρηση μιας κοινωνικής ισορροπίας και ευημερίας, κάνουν την πιθανότητα αδυναμίας λειτουργίας τους καταστροφικό σενάριο, είτε αυτή η αποτυχία οφείλεται σε στοχευμένες κακόβουλες επιθέσεις, είτε σε αστοχίες της διοίκησης και φυσικές καταστροφές. Στο παρόν κεφάλαιο δίνεται ο ορισμός των Κρίσιμων Υποδομών και των χαρακτηριστικών τους, και προσεγγίζεται το θέμα της αναγκαιότητας προστασίας τους, καθώς και οργανισμοί και πρότυπα που το επιδιώκουν.

3.1 Βασικά Χαρακτηριστικά Κρίσιμων Υποδομών

3.1.1 Ορισμός Κρίσιμων Υποδομών

Κρίσιμη Υποδομή (ΚΥ) (Critical Infrastructure – CI) ή **Υποδομή Ζωτικής Σημασίας** (ΥΖΣ) ορίζεται ένα αγαθό, σύστημα ή υποσύστημα που είναι απαραίτητο για τη διατήρηση των ζωτικών λειτουργιών της κοινωνίας, την υγεία, τη φυσική προστασία (safety), την ασφάλεια (security), την οικονομική και την κοινωνική ευημερία των ανθρώπων. Στις Κρίσιμες Υποδομές συμπεριλαμβάνονται τόσο φυσικές όσο και ψηφιακές οντότητες, των οποίων η διακοπή λειτουργίας ή η καταστροφή, θα είχε σημαντικό αρνητικό αντίκτυπο για μία χώρα, ως αποτέλεσμα αδυναμίας συνέχισης ζωτικών λειτουργιών [17].

Οι **Κρίσιμες Πληροφοριακές Υποδομές** (CII) αποτελούν υποκατηγορίες των ΚΥ, οι οποίες κάνουν χρήση των πληροφοριακών και επικοινωνιακών τεχνολογιών και εξαρτώνται σημαντικά από αυτές. Να διευκρινίσουμε ότι οι Υποδομές αυτές είναι Κρίσιμες τόσο για τις ίδιες, όσο και για τη λειτουργία άλλων Κρίσιμων υποδομών που βασίζονται σε αυτές για αποθήκευση, επεξεργασία και διακίνηση πληροφοριών.

Για να έχει ο ορισμός τους νόημα, πρέπει οι Κρίσιμες Υποδομές να καθορίζονται προφανώς σε εθνικό επίπεδο. Εξαιτίας όμως των διαφορετικών ενδογενών χαρακτηρισικών κάθε έθνους, τόσο οι ορισμοί που υιοθετούνται όσο και ο τρόπος που αντιμετωπίζονται και προστατεύονται οι εν λόγω υποδομές αλλάζει. Στον Πίνακα 3.1 παρατίθενται παραδείγματα διαφορετικών ορισμών των ΚΥ. Στην κατεύθυνση της δημιουργίας ενός κοινού πλαισίου προ-

στασίας των ΚΥ, ωστόσο, ενθαρρύνεται η θέσπιση ενός κοινού καταλόγου Κρίσιμων Υποδομών και τομέων/υποτομέων. Σε αρμονία με την ευρέως χρησιμοποιούμενη μεθοδολογία προσδιορισμού ΚΥ ανά τομέα, στην (ENISA, 2014) (Σχήμα 3.1) προτείνεται μια παραλλαγή των μέχρι τότε σχετικών αναφορών η οποία ενσωματώνει την έννοια της υπηρεσίας ανά υποτομέα. Η έννοια της υπηρεσίας συχνά χρησιμοποιείται συνεκδοχικά, αντί του όρου υποδομή, καθώς ενσωματώνει σε ένα επίπεδο –αρκούντως αφαιρετικό και αρκούντως περιγραφικό– την έννοια ενός συνόλου αγαθών/προϊόντων και διεργασιών που (εν τέλει) χρήζουν προστασίας [18].

Τομέας	Υποτομέας	Υπηρεσία
1. Ενέργεια	Ηλεκτρική ενέργεια	Παραγωγή (όλοι οι τρόποι) Μεταφορά/Διανομή Αγορά ηλεκτρικής ενέργειας
	Πετρέλαιο	Εξόρυξη Διύλιση Μεταφορά Αποθήκευση
	Φυσικό αέριο	Εξόρυξη Μεταφορά/Διανομή Αποθήκευση
2. Τεχνολογίες Πληροφορικής & Επικοινωνιών (ΤΠΕ)	Τεχνολογίες Πληροφορικής	Υπηρεσίες Web Υπολογιστικά κέντρα/Υπηρεσίες Cloud Λογισμικό ως Υπηρεσία (SaaS)
	Επικοινωνίες	Επικοινωνίες Φωνής/Δεδομένων Διαδίκτυο
3. Ύδατα	Πόσιμο νερό	Αποθήκευση νερού Διανομή νερού/Διασφάλιση ποιότητας νερού
	Λύματα	Συλλογή και επεξεργασία λυμάτων
4. Τρόφιμα		Γεωργία /παραγωγή τροφίμων Εφοδιασμός τροφίμων Διανομή τροφίμων Ποιότητα/ασφάλεια τροφίμων
5. Υγεία		Επείγουσα περίθαλψη Νοσοκομειακή περίθαλψη Εφοδιασμός φαρμάκων, εμβολίων, αίματος, ιατρικών προμηθειών Έλεγχος λοιμώξεων και επιδημιών
6. Οικονομία		Τραπεζική Συναλλαγές πληρωμών Χρηματιστηριακές συναλλαγές
7. Δημόσια Τάξη & Ασφάλεια		Διατήρηση δημόσιας τάξης Σωφρονιστικό σύστημα
8. Μεταφορές	Αεροπορία	Υπηρεσίες αεροναυτιλίας Λειτουργία αεροδρομίων
	Οδικές μεταφορές	Υπηρεσίες Λεωφορείων/Τραμ Συντήρηση οδικού δικτύου
	Σιδηροδρομικές μεταφορές	Διαχείριση σιδηροδρομικού δικτύου Υπηρεσίες σιδηροδρομικών μεταφορών
	Θαλάσσιες μεταφορές	Έλεγχος ναυσιπλοΐας Λειτουργίες Παγοθραυστικών
	Ταχυδρομικές μεταφορές	Μεταφορές εγγράφων & δεμάτων Συναλλαγές πληρωμών
9. Βιομηχανία	Κρίσιμες βιομηχανίες	Εφοδιασμός προμηθειών
	Χημική / Πυρηνική βιομηχανία	Αποθήκευση και απόρριψη επικίνδυνων υλικών Ασφάλεια βιομηχανικών μονάδων υψηλής επικινδυνότητας
10. Δημόσια Διοίκηση		Κυβερνητικές λειτουργίες
11. Διάστημα		Προστασία διαστημικών συστημάτων
12. Πολιτική Προστασία		Υπηρεσίες πυρόσβεσης και διάσωσης
13. Περιβάλλον		Παρακολούθηση και έλεγχος ατμοσφαιρικής ρύπανσης Μετεωρολογική πρόγνωση και προειδοποίηση Παρακολούθηση και έλεγχος επίγειων υδάτων Παρακολούθηση και έλεγχος θαλάσσιας ρύπανσης
14. Άμυνα		Εθνική άμυνα

Σχήμα 3.1: *Ενδεικτικοί Κρίσιμοι Τομείς και Υπηρεσίες ανά Τομέα, Πηγή: ENISA, 2014*

Πίνακας 3.1: *Ορισμοί Κρίσιμων Υποδομών - CI*

Χώρες	**Ορισμός**
Γερμανία	¨Ως ΚΥ ορίζονται οι οργανισμοί μέγιστης σημασίας για την κοινωνία, των οποίων η αποτυχία ή βλάβη μπορεί να προκαλέσει παρατεταμένη έλλειψη προμηθειών, σημαντική αναστάτωση στην δημόσια οργάνωση και άλλες δραματικές συνέπειες¨
Γαλλία	¨Ένας τομέας δραστηριοτήτων ζωτικής σημασίας ορίζεται ως το σύνολο των δραστηριοτήτων που υποστηρίζουν υπηρεσίες και δημόσια αγαθά, όπως τα κυριαρχικά δικαιώματα, η λειτουργία της εθνικής οικονομίας, η τήρηση των εθνικών αμυντικών δυνατοτήτων και η ασφάλεια των συνόρων και των πολιτών ¨
Ηνωμένο Βασίλειο	¨ Η Εθνική Κρίσιμη Υποδομή περιλαμβάνει τα υλικά αγαθά, τις υπηρεσίες και τα συστήματα που υποστηρίζουν την οικονομική, πολιτική και κοινωνική ζωή του Ηνωμένου Βασιλείου, των οποίων η σημασία είναι τέτοια ώστε η απώλειά τους θα μπορούσε 1) να προκαλέσει μεγάλης κλίμακας απώλεια ζωής, 2) να έχει σοβαρή επίπτωση στην εθνική οικονομία, 3) να προκαλέσει δυσμενείς συνέπειες στην κοινωνία, 4) να απαιτήσει την άμεση κρατική μέριμνα¨
ΗΠΑ	¨Ο γενικός ορισμός των Κρίσιμων Υποδομών στο συνολικό πλάνο ΚΥ των ΗΠΑ είναι: συστήματα και αγαθά, φυσικά και εικονικά, ζωτικής σημασίας για τις ΗΠΑ ώστε η ανικανότητα ή η καταστροφή αυτών των συστημάτων και αγαθών να έχει ως αποτέλεσμα την εξασθένηση της ασφάλειας, της εθνικής οικονομίας, της εθνικής δημόσιας υγείας ή συνδυασμό αυτών. ¨

3.1.2 Τα κριτήρια Κρισιμότητας

Ως **κρισιμότητα** ορίζεται το *επίπεδο της συμβολής* μιας Υποδομής στην κοινωνία, ώστε να διατηρηθεί το ελάχιστο επίπεδο του εθνικού και διεθνούς νόμου και της τάξης, της δημόσιας ασφάλειας, της οικονομίας, της δημόσιας υγείας και του περιβάλλοντος, ή το επίπεδο του αντικτύπου που θα έχει στους πολίτες ή στην κυβέρνηση η έλλειψη ή η καταστροφή της Υποδομής. Σύμφωνα με την ευρωπαϊκή πρακτική αναγνωρίζονται δύο οικογένειες κριτηρίων με βάση τις οποίες, οι υποδομές κατατάσσονται σε κρίσιμες και μη, και έπειτα ιεραρχούνται ως προς την προτεραιότητά τους. Πρόκειται για τα τομεακά κριτήρια (sectoral criteria) και τα οριζόντια κριτήρια (cross-cutting criteria) τα οποία αναλύονται παρακάτω.

- **Τομεακά κριτήρια** (sectoral criteria) : Πρόκειται για τεχνικά ή λειτουργικά κριτήρια. Τα τομεακά κριτήρια μπορεί να σχετίζονται με (συνήθως ποσοτικά προσδιορίσιμες) συγκεκριμένες ιδιότητες ή χαρακτηριστικά μιας υποδομής που υποστηρίζει την εν λόγω υπηρεσία του τομέα. Τα χαρακτηριστικά αυτά μπορεί να είναι είτε τεχνικά (π.χ. ελάχιστη διάμετρος αγωγού πετρελαίου ή φυσικού αερίου, ελάχιστη χωρητικότητα κ.λπ.) είτε όχι (π.χ. χρόνος ή κόστος αποκατάστασης), και ποικίλλουν ανάλογα με τον τομέα. Για παράδειγμα, στην περίπτωση μιας Πληροφοριακής ΚΥ τα τομεακά κριτήρια θα μπορούσαν να είναι: η ταχύτητα διαμεταγωγής δεδομένων, ο χρόνος αποκατάστασης πληροφοριακού συστήματος, το πλήθος εγγραφών προσωπικών δεδομένων που τηρεί ή επεξεργάζεται το σύστημα κ.λπ.

- **Οριζόντια κριτήρια** (cross-cutting criteria) : Αξιολογούν τη βαρύτητα των επιπτώσεων που θα είχε η παρεμπόδιση ή η διακοπή λειτουργίας ή η καταστροφή μιας ενδεχόμενης ΚΥ . Ο χαρακτηρισμός αντανακλά τον αντίκτυπο σε εθνικό επίπεδο, που θα είχε ένα αναπάντεχο περιστατικό το οποίο πλήττει την εν λόγω υποδομή, στην κρίσιμη υπηρεσία η οποία παρέχεται μέσω της πληττόμενης υποδομής. Μια ενδεχόμενη ΚΥ νοείται ως ΚΥ όταν οι επιπτώσεις ενός συμβάντος που πλήττει την υποδομή πληρούν τουλάχιστον ένα ή περισσότερα ποσοτικά ή/και ποιοτικά κριτήρια. Τέτοια κριτήρια είναι (European Commission, 2005):

  - Το γεωγραφικό εύρος (scope): Μια υποδομή αξιολογείται ως προς το ελάχιστο εύρος της γεωγραφικής περιοχής που (δυνητικά) θα επηρεαστεί από ένα συμβάν το οποίο θα πλήξει την υποδομή.
  - Ανθρώπινες απώλειες (casualties) : Το κριτήριο αφορά τον ελάχιστο αριθμό θυμάτων ή/και τραυματιών που μπορεί να επιφέρει ένα συμβάν το οποίο θα πλήξει την υποδομή.
  - Οικονομικές επιπτώσεις (economic effects) : Το κριτήριο αφορά τις επιπτώσεις σε μακρο-οικονομικό επίπεδο [π.χ. απώλεια Ακαθάριστου Εθνικού Προϊόντος, απώλειες λόγω εξαρτήσεων,απώλεια γης, κόστος λόγω μετακινήσεων πληθυσμού, κόστος λόγω ρύπανσης] ή/και σε μακρο-κοινωνικό επίπεδο, συμπεριλαμβανομένων των δυνητικών περιβαλλοντικών επιπτώσεων.
  - Επιπτώσεις για το κοινό (public effects) : Το κριτήριο αξιολογεί πώς ένα (δυνητικό) συμβάν το οποίο πλήττει την υποδομή μπορεί να επηρεάσει μια μεγάλη μερίδα

ανθρώπων που απολαμβάνουν την κρίσιμη υπηρεσία η οποία εξαρτάται από την εν λόγω υποδομή.

3.1.3 Εξαρτήσεις των Κρίσιμων Υποδομών

Όπως έχει ήδη αναφερθεί, οι κρίσιμες υποδομές αποτελούν τον πυρήνα της κοινωνίας. Η αναλογία αυτή επικυρώνεται περισσότερο αν αναλογιστεί κανείς τις εξαρτήσεις μεταξύ των υποδομών που καθιστούν το σύνολό τους ¨συμπαγές¨. Στη διεθνή βιβλιογραφία, ενώ γίνεται συχνά αναφορά στη σημασία της κατανόησης και της καταγραφής των εξαρτήσεων μεταξύ διαφορετικών επιπέδων της ίδιας Υποδομής (intradependencies) και αυτών μεταξύ διαφορετικών Υποδομών(interdependencies), σπάνια παρέχονται διευκρινίσεις για τη μορφή, το είδος τους ή τον τρόπο με τον οποίο οι αναλυτές πρέπει να τις χειριστούν στην προσπάθειά τους να εκτιμήσουν και να αντιμετωπίσουν τον κίνδυνο. Σαν αποτέλεσμα, η έλλειψη πληροφορίας οδηγεί σε ασυνεπείς θεωρήσεις του κινδύνου.

Μπορούν να διακριθούν τέσσερις κατηγορίες εξαρτήσεων [19] :

- **Η φυσική** (physical) : Μία Υποδομή είναι φυσικά εξαρτώμενη από μία άλλη όταν η κατάσταση των λειτουργιών της είναι εξαρτημένη από την υλική έξοδο μίας άλλης Υποδομής.

- **Η κυβερνοχωρική** (cyber) : Μία Υποδομή είναι κυβερνοχωρικά εξαρτώμενη από μία άλλη όταν η κατάσταση των λειτουργιών της είναι εξαρτημένη από δεδομένα και πληροφορίες που μεταφέρονται ηλεκτρονικά σε αυτήν, από μία άλλη Υποδομή. Οι έξοδοι της πληροφοριακής Υποδομής λαμβάνονται ως είσοδοι από την άλλη, για την διεκπεραίωση των λειτουργιών της.

- **Η γεωγραφική** (geographical) : Μία Υποδομή είναι γεωγραφικά εξαρτώμενη από μία άλλη όταν τα στοιχεία τους βρίσκονται σε στενή χωρική εγγύτητα. Αν συμβεί κάποιο τοπικό περιβαλλοντικό περιστατικό, θα προκληθούν αλλαγές σε αυτές τις Υποδομές.

- **Η λογική** (logical) : Μία Υποδομή είναι λογικά εξαρτώμενη από μία άλλη όταν εξαρτάται απο αυτήν, μέσω ενός μηχανισμού που δεν είναι φυσική, κυβερνοχωρική ή γεωγραφική σύνδεση. Η λογική εξάρτηση συνήθως συνδέεται με αποφάσεις και δράσεις ατόμων, που δεν είναι αποτέλεσμα συστηματοποιημένων διαδικασιών.

3.1.4 Αποτυχία των Κρίσιμων Υποδομών

Όπως έγινε κατανοητό, ο βαθμός αλληλοσύνδεσης των Κριτικών Υποδομών, και αυτών με τον κυβερνοχώρο, κάνει την διάδοση αρνητικών περιστατικών ταχύτατη, και την προσπάθεια ελέγχου και αναστολής της ιδιαίτερα δύσκολη. Η αποτυχία των κρίσιμων υποδομών, δεν οφείλεται μόνο σε φυσικά ή οργανωτικά ατυχήματα, αλλά αποτελεί όλο και συχνότερα, στόχευση για δράστες που εξαπολύουν τρομοκρατικές και οικονομικές επιθέσεις, εκμεταλλευόμενοι κυρίως τον κυβερνοχώρο για να τις πραγματοποιήσουν. Εάν ο κίνδυνος πραγματοποιηθεί, η αποδιοργάνωση της Υποδομής που βάλλεται, μεταδίδεται και σε όλες τις υποδομές με τις οποίες παρουσιάζει εξαρτήσεις. Οι κλιμακωτές αυτές συνέπειες υποδεικνύουν την αναγκαιότητα ορισμού ενός πλάνου Διαχείρισης Κινδύνου. Για να ορισθεί και να εφαρμοσθεί το

πλάνο αποδοτικά, πρέπει πρώτα να έχουν κατανοηθεί και διαγνωσθεί οι αλληλοεξαρτήσεις, και όπου αυτό είναι δυνατό, να υιοθετηθούν εναλλακτικές λύσεις με στόχο να σταματήσει η εξάπλωση αποτυχιών και βλαβών.

3.2 Προστασία των Κρίσιμων Υποδομών μέσω Διαχείρισης Ρίσκου

Λαμβάνοντας υπόψη όλα τα ανωτέρω, είναι εμφανές πως οι Κρίσιμες Υποδομές μαζί με τις υπηρεσίες και τα συστήματά τους, πρέπει να προστατεύονται επαρκώς ενάντια σε όλα τα είδη αστοχιών ή ατυχημάτων, είτε πηγάζουν από ανθρώπινες πράξεις είτε από φυσικά φαινόμενα. Οι κρίσιμες υποδομές παρέχουν υπηρεσίες αναγκαίες για ένα έθνος προκειμένου να λειτουργήσει ορθά και να μπορεί να υποστηρίζει τις ανάγκες των πολιτών του, διαμέσου υπηρεσιών όπως το σύστημα Υγείας, οι μεταφορές κτλ. Ακόμα περισσότερο αφού τέτοιου είδους αστοχίες μπορούν να προξενηθούν από κακόβουλους επιτιθέμενους άλλων χωρών με σκοπο να πλήξουν το ίδιο το έθνος και τα εισοδήματά του [20]. Η Διαχείριση Ρίσκου είναι ένα από τα βασικότερα βήματα για την *προστασία των Κρίσιμων Υποδομών* (Critical Infrastructure Protection- CIP). Παρόλο που η βιβλιογραφία αριθμεί πολλές μεθοδολογίες και πρότυπα που στόχο έχουν την αντιμετώπιση του κινδύνου μέσω της θωράκισης των στοιχείων και των συστημάτων, ιδιαίτερα όσον αφορά τις Κρίσιμες Υποδομές πρέπει να λαμβάνονται υπόψη οι αλληλοεξαρτήσεις που υπάρχουν μεταξύ τους [21]. Με άλλα λόγια, η προοπτική με την οποία εφαρμόζεται η διαδικασία Διαχείρησης Ρίσκου στις Κρίσιμες Υποδομές είναι διττή: πρώτον στοχεύει στη θωράκιση της υποδομής ως αυτοτελούς οντότητας δίνοντας ιδιαίτερη έμφαση στον τομέα της κυβερνοασφάλειας, και δεύτερον την αντιμετωπίζει ως μέρος μίας αλυσίδας αλληλοεξαρτώμενων υποδομών, στο πλαίσιο της οποίας η διάδοση της αλληλουχίας αρνητικών ενδεχομένων πρέπει να περιοριστεί.

3.2.1 ISO/IEC 31010:2009 – Risk management/ Risk assessment techniques

Το ISO/IEC 31010 δημοσιεύθηκε το 2009 από τον Διεθνή Οργανισμό Τυποποίησης (ISO) σε συνεργασία με την Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC) και αποτελεί διεθνώς αναγνωρισμένο πρότυπο για την εφαρμογή των αρχών διαχείρισης κινδύνου. Ακολούθησε τη δημοσίευση του ISO 31000: Enterprise Risk Management που στόχο είχε την παροχή μιας δομημένης προσέγγισης στην εφαρμογή της διαχείρισης κινδύνων για τις επιχειρήσεις. Το ISO 31010 συμπληρώνει το ISO 31000, δίνοντας επιπλέον πληροφορίες που αφορούν την επιλογή και εφαρμογή μεθοδολογιών Εκτίμησης Ρίσκου. Τόσο η γενική μέθοδος όσο και οι επιμέρους μεθοδολογίες Εκτίμησης Ρίσκου που παρουσιάστηκαν στο Κεφάλαιο 2, ακολουθούν τη δομή που προτάθηκε στο πρότυπο ISO 31010.

3.2.2 ISO/IEC 27032:2012 – Information technology/ Security techniques/ Guidelines for cybersecurity

Το συγκεκριμένο πρότυπο αφορά την κυβερνοασφάλεια. Παρέχει καθοδήγηση που στόχο έχει την διατήρηση της κυβερνοασφάλειας, λαμβάνοντας υπόψη τα ιδιάζοντα χαρακτηριστικά των κυβερνο-δράσεων και τις εξαρτήσεις τους με άλλους τομείς όπως:

- η ασφάλεια πληροφοριών,
- η ασφάλεια δικτύων,
- η ασφάλεια του διαδικτύου,
- η προστασία πληροφοριακών Κρίσιμων Υποδομών (Critical Information Infrastructure Protection-CIIP).

Το πρότυπο αυτό παρέχει :

- Μία σύνοψη της έννοιας της Κυβερνοασφάλειας,
- Μία επισκόπηση των σχέσεων μεταξύ Κυβερνοασφάλειας και άλλων ειδών ασφάλειας,
- Μία εισαγωγή στην έννοια των ενδιαφερόμενων μερών δίνοντας περιγραφή του ορισμού και των ρόλων τους,
- Καθοδήγηση για την αντιμετώπιση κοινών ζητημάτων Κυβερνοασφάλειας,
- Ένα πλαίσιο εργασίας (framework) που επιτρέπει στα ενδιαφερόμενα μέρη να επιλύουν τα ζητήματα Κυβερνοασφάλειας.

Ο πρώτος τομέας στον οποίο επικεντρώνεται το Διεθνές Πρότυπο, είναι η αντιμετώπιση ζητημάτων ασφάλειας στον Κυβερνοχώρο, καθώς και η γεφύρωση του χάσματος μεταξύ διαφορετικών ειδών ασφάλειας στον Κυβερνοχώρο. Συγκεκριμένα, το πρότυπο σκιαγραφεί τεχνικά και παρέχει καθοδήγηση για την αντιμετώπιση (προστασία πληροφοριακών συστημάτων, ανίχνευση απειλών, διαχείριση των επιθέσεων) των εξής κινδύνων, που παρουσιάστηκαν αναλυτικά στην παράγραφο 2.2.3:

- επιθέσεις βασισμένες σε κοινωνική μηχανική (social engineering),
- πολλαπλασιαμός κακόβουλου λογισμικού (malware),
- εγκατάσταση κατασκοπευτικών προγραμμάτων (spyware) κ.α.

Ο δεύτερος τομέας στον οποίο επικεντρώνεται το Διεθνές Πρότυπο, είναι η συνεργασία στον Κυβερνοχώρο, με όρους αποδοτικής **ανταλλαγής πληροφοριών**, **συντονισμού** και **διαχείρισης περιστατικών**. Η συνεργασία αυτή πρέπει να γίνεται διατηρώντας την ασφάλεια και την αξιοπιστία της διαδικασίας ανταλλαγής πληροφοριών, καθώς και την ιδιωτικότητα των ατόμων, τα οποία μπορεί να βρίσκονται σε διαφορετικές τοποθεσίες ή χρονικές ζώνες.

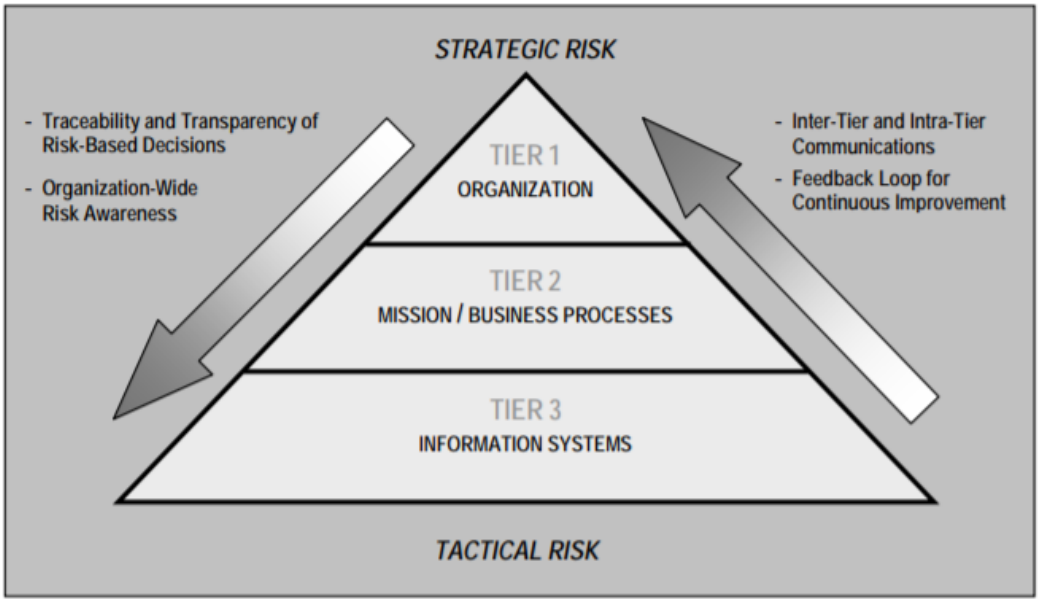
3.2.3 NIST Cybersecurity Framework

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) υπάγεται στο Υπουργείο Εμπορίου των ΗΠΑ και σαν οργανισμός στοχεύει στην προώθηση της καινοτομίας και της ανταγωνιστικότητας. Στην κατεύθυνση αυτή παράγει πρότυπα και πλαίσια εργασίας που αφορούν θέματα της Τεχνολογίας πληροφοριών και επικοινωνίας (Information and Communications

Technology, ICT). Στην πρόσφατη αναφορά ¨Framework for Improving Critical Infrastructure Cybersecurity¨ που εξέδωσαν το 2018, οι ερευνητές δήλωσαν: ¨Το πλαίσιο είναι μία βασισμένη στον κίνδυνο προσέγγιση διαχείρισης της κυβερνοασφάλειας και αποτελείται από τρία μέρη: τον πυρήνα του πλαισίου, τις διαφορετικές βαθμίδες εφαρμογής και τα προφίλ του πλαισίου. Κάθε ένα από τα παραπάνω συστατικά ενισχύει τη σύνδεση μεταξύ επιχειρηματικών/οργανωτικών δραστηριοτήτων και κυβερνονασφάλειας ¨. Η εφαρμογή του πλαισίου πραγματοποιείται σε επίπεδο :

- πληροφορικών συστημάτων (Information Systems Tier),
- επιχειρηματικών διαδικασιών (Business Processes Tier),
- συνολικής οργάνωσης του φορέα (Organization Tier),

όπως φαίνεται στο Σχήμα 3.2.



Σχήμα 3.2: *Τα επίπεδα εφαρμογής πλαισίου Διαχείρισης Ρίσκου, Πηγή: NIST: Special Publication 800-30*

Το πλαίσιο, μέσω των προτεινόμενων προτύπων και πρακτικών, κατευθύνει τους οργανισμούς στην αντιμετώπιση των κυβερνοαπειλών, παρέχοντας ταυτόχρονα ένα ισχυρό εργαλείο για να κατανοήσουν τα ενδιαφερόμενα μέρη την φύση των κινδύνων του Κυβερνοχώρου. Οι πρακτικές αυτές, που δεν διευκρινίζονται από το NIST με μεγάλη ακρίβεια, δίνουν ευελιξία επιλογής στους αποφασίζοντες, οι οποίοι πρέπει να λάβουν υπόψη εγγενή χαρακτηριστικά του οργανισμού πριν προσπαθήσουν να ελαχιστοποιήσουν το ρίσκο που αυτός αντιμετωπίζει.

Κεφάλαιο 4

Διαχείριση και Εκτίμηση Ρίσκου σε μονάδες Υγείας

Οι Υπηρεσίες Υγείας αποτελούν εξ ορισμού μία από τις Κρίσιμες Υποδομές κάθε κράτους, της οποίας η προστασία είναι αντικείμενο κρατικής μέριμνας. Η διασφάλιση του επιπέδου των παροχών του Συστήματος Υγείας συνεπάγεται την ποιότητα του βιοτικού επιπέδου των πολιτών. Γι' αυτό και η θωράκιση του Συστήματος Υγείας απέναντι στις απειλές που εγκυμονεί το περιβάλλον αποτελεί αντικείμενο επιστημονικής μελέτης και συστηματικής προσπάθειας. Σε αυτό το κεφάλαιο θα παρουσιαστούν τα χαρακτηριστικά των μονάδων Υγείας όπως αυτά έχουν διαμορφωθεί σήμερα, δίνοντας ιδιαίτερη έμφαση στα προτερήματα αλλά και τους κινδύνους που συνοδεύουν την εισαγωγή της τεχνολογίας στο Σύστημα Υγείας.

4.1 Αποστολή των Μονάδων Παροχής Υπηρεσιών Υγείας

Δεν είναι λίγοι οι ορισμοί που έχουν κατά καιρούς δοθεί για να σκιαγραφήσουν την φύση και το ρόλο της Δημόσιας Υγείας. Όλοι κινούνται πέρα από το πλαίσιο της παρεχόμενης ιατρικής φροντίδας, αναδεικνύοντας την ανάγκη για μία ολιστική - επιστημονική προσέγγιση που αφορά τη βελτίωση της ποιότητας ζωής και του κοινωνικοπολιτικού γίγνεσθαι.

Σύμφωνα με τον Winslow, ¨Δημόσια υγεία είναι η επιστήμη και η τέχνη να προλαμβάνεται η νόσος, να προάγεται η υγεία και να επιμηκύνεται η ζωή μέσα από οργανωμένη προσπάθεια της κοινωνίας¨ (C.E.A. Winslow 1923).

Στην ίδια κατεύθυνση έγινε και η τοποθέτηση των Beaglehole και Bonita οι οποίοι υποστήριξαν ότι ¨Δημόσια υγεία είναι η συλλογική δράση για αειφόρο ανάπτυξη της υγείας του πληθυσμού¨ (R. Beaglehole - R. Bonita 2004).

Σύμφωνα με τα άρθρα 1 και 2 του Ν.4675/2020, ¨Η δημόσια υγεία είναι επένδυση για τη **διατήρηση και βελτίωση του ανθρώπινου κεφαλαίου της χώρας**. Ως δημόσια υγεία ορίζεται το σύνολο των οργανωμένων δραστηριοτήτων της πολιτείας και της κοινωνίας, που είναι **επιστημονικά τεκμηριωμένες** και αποβλέπουν στην πρόληψη νοσημάτων, στην προστασία και την προαγωγή της υγείας του πληθυσμού, στην αύξηση του προσδόκιμου επιβίωσης και στη βελτίωση της ποιότητας ζωής. Η δημόσια υγεία έχει χαρακτήρα πολυτομεακό, απευθύνεται κυρίως σε πληθυσμούς και κοινότητες και, ως έννοια, είναι ευρύτερη της υγιεινής και της πρόληψης ή της κοινωνικής ιατρικής ή της ιατρικής στη δημόσια υγεία. Η δημόσια υγεία περιλαμβάνει διατομεακές δραστηριότητες και ασκείται με διεπιστημονική

μεθοδολογία και προσέγγιση. Η δημόσια υγεία είναι, πρωτίστως, **άσκηση δημόσιας πολιτικής** και γίνεται με την ευθύνη του κράτους¨. ¨Στενά συνδεδεμένες με την έννοια της δημόσιας υγείας είναι οι έννοιες της ανάπτυξης και προαγωγής της υγείας, της **εκτίμησης των επιπτώσεων** στην υγεία διαφόρων πολιτικών και προγραμμάτων, της **διαχείρισης του κινδύνου** για την υγεία, της **βελτίωσης της ποιότητας** των υπηρεσιών και των συνθηκών διαβίωσης, καθώς και των προτεραιοτήτων για την υγεία. Στην ευρύτερη έννοια της δημόσιας υγείας περιλαμβάνονται, επίσης, ο σχεδιασμός και η αποτίμηση των υπηρεσιών υγείας, καθώς και η κοινωνικοοικονομική αξιολόγηση των υγειονομικών προγραμμάτων και παρεμβάσεων. Δράσεις που σχετίζονται με την κοινωνική φροντίδα και τις ειδικές ανάγκες ευάλωτων ομάδων του πληθυσμού, που ζουν σε μειονεκτικές, κοινωνικά, συνθήκες, όπως η φτώχεια, η ανεργία, το γήρας, ο κοινωνικός αποκλεισμός, η απουσία εισοδήματος, και η προσπάθεια άμβλυνσης των κοινωνικοοικονομικών ανισοτήτων στην υγεία, περιέχονται στην ευρύτερη έννοια της δημόσιας υγείας.¨

Όπως γίνεται κατανοητό, στην ιεράρχηση των στόχων του τομέα της Δημόσιας Υγείας, συναντώνται υψηλότερα οι **μη οικονομικοί στόχοι** και στη συνέχεια οι **οικονομικοί** [1].

Στους **μη οικονομικούς στόχους** συγκαταλέγονται:

1. *Η εκπλήρωση της κοινωνικής αποστολής*, δηλαδή η παροχή ιατρικών υπηρεσιών υψηλής ποιότητας, που αφορούν τόσο τη σωματική όσο και την ψυχική υγεία. Η εξασφάλιση στους πολίτες, του ¨ύψιστου αγαθού¨, της υγείας.

2. *Η διατήρηση της ασφάλειας*. Αυτό επιτυγχάνεται λαμβάνοντας υπόψη πολλαπλά επίπεδα, όπως για παράδειγμα η φυσική ασφάλεια των ασθενών και του προσωπικού στο πλαίσιο της μονάδας, ή η επαγγελματική ασφάλεια των εργαζομένων.

3. *Οι επιδιώξεις της ανώτατης ιεραρχίας*. Πρόκειται για μία από τις πιο καθοριστικές παραμέτρους στη διαδικασία λήψης αποφάσεων και συχνά συνδέεται άμεσα με την διατήρηση της αξιοπιστίας της μονάδας. Η διατήρηση της καλής φήμης ως προς την παροχή υπηρεσιών υγείας είναι κριτικής σημασίας για την επιβίωση του οργανισμού.

Στους **οικονομικούς στόχους** περιλαμβάνονται:

1. *Η απόδοση*. Ορίζεται ως ο λόγος του πραγματοποιηθέντος κέρδους προς το επενδυμένο κεφάλαιο. Το κριτήριο της απόδοσης είναι ένα από τα πλέον σημαντικά γιατί καθορίζει και τους υποστόχους που θα τεθούν, για παράδειγμα στόχους σχετικά με τα κόστη των πρώτων υλών. Πρόκειται για κριτήριο στενά συνυφασμένο με την έννοια του ρίσκου, καθορίζοντας και την συμπεριφορά των αποφασιζόντων απέναντι σε αυτό. Έργα με μεγάλη απόδοση είναι συνήθως αυτά που περικλείουν το μεγαλύτερο ρίσκο.

2. *Η προσαρμοστηκότητα*. Οι μονάδες υγείας πρέπει να αντιδρούν αποτελεσματικά και άμεσα στις αλλαγές του περιβάλλοντος. Η εκπλήρωση της αποστολής να καλύπτουν αδιάκοπα τις ιατρικές ανάγκες των πολιτών, δεν πρέπει να βάλλεται από την ανισορροπία και την αστάθεια του περιβάλλοντος και για να επιτευχθεί αυτό είναι απαραίτητος ο συστηματικός σχεδιασμός της δομής της μονάδας αλλά και των απειλών που αντιμετωπίζει.

3. *Η ποιότητα.* Πρέπει να είναι συνεχής η αναζήτηση προϊόντων και υπηρεσιών καλύτερης ποιότητας, όπως για παράδειγμα η συντήρηση του ιατρικού εξοπλισμού. Συχνά οι εναλλακτικές επιλογές καθορίζουν διαφορετικά κόστη επηρεάζοντας τους στόχους και τον προϋπολογισμό.

4. *Η μεγέθυνση.* Ο οργανισμός μπορεί να θέσει όρους ανάπτυξης, όπως για παράδειγμα η λειτουργία μίας ακόμα νοσοκομειακής πτέρυγας. Οι στόχοι αυτοί συχνά συνδέονται με την αναζήτηση του βέλτιστου μεγέθους, που επιτρέπει στη μονάδα να επιβιώνει και να εξελίσσεται, χωρίς οι υπηρεσίες που παρέχει να στερούνται ποιότητας.

4.2 Γενικά χαρακτηριστικά του Συστήματος Υγείας

Ως σύστημα υγείας ορίζεται το *σύνολο των υγειονομικών μονάδων οι οποίες βρίσκονται σε συνεχή συνεργασία και λειτουργική αλληλεξάρτηση με σκοπό τη διατήρηση και προαγωγή της υγείας του πληθυσμού*. Παρά τις διαφορές που μπορεί να εμφανίζουν (μέγεθος, τοπικότητα παροχής υπηρεσιών κ.α.), οι μονάδες ιατρικής περίθαλψης που απαρτίζουν το Σύστημα Υγείας παρουσιάζουν ισχυρές ομοιότητες. Οι ομοιότητες αυτές συνθέτουν τα κύρια γνωρίσματα του Συστήματος Υγείας, τα οποία σύμφωνα με τους Σούλη, Σαρρή και Θεοδώρου είναι [22] :

1. **Διαθεσιμότητα των υπηρεσιών υγείας**, δηλαδή η δυνατότητα του συστήματος να προσφέρει τις υπηρεσίες του στον πληθυσμό χωρίς εμπόδια και χρονικούς περιορισμούς.

2. **Προσπελασιμότητα των υπηρεσιών υγείας**. Κάθε άτομο, οποιασδήποτε κοινωνικοοικονομικής θέσης, πρέπει να έχει τη δυνατότητα να χρησιμοποιήσει τις υπηρεσίες υγείας. Αυτό προϋποθέτει ισότιμη κατανομή των πόρων και υπηρεσιών υγείας και πάντα σύμφωνα με τις ανάγκες υγείας του πληθυσμού.

3. **Συνέχεια στη προσφορά υπηρεσιών υγείας**. Η προσφορά υπηρεσιών υγείας προς τον πληθυσμό δεν περιορίζεται μόνο στο στάδιο της θεραπευτικής αντιμετώπισης μια ασθένειας αλλά επίσης καλύπτει τα στάδια πριν και μετά την εμφάνιση της νόσου.

4. **Ισότητα ή ίσες ευκαιρίες στη χρήση των υπηρεσιών**. Η ισότητα στη χρήση υπηρεσιών υγείας επιδέχεται δυο εννοιολογικούς προσδιορισμούς. Ο ένας αφορά την ίση μεταχείριση μεταξύ ίσων (οριζόντια ισότητα), όπου μόνον όταν οι χρήστες των υπηρεσιών είναι ίσοι, επιτυγχάνεται ισότητα. Ο δεύτερος αφορά στην άνιση μεταχείριση μη ίσων ατόμων (κάθετη ισότητα). Σε αυτήν την περίπτωση υπάρχει ανομοιογένεια στην ικανοποίηση των αναγκών υγείας και το αποτέλεσμα είναι αυξανόμενη ανισότητα.

5. **Το οργανωτικό επίκεντρο του συστήματος**. Κάθε σύστημα υγείας, στη διαδρομή του στον χώρο και στον χρόνο, δίνει ιδιαίτερο βάρος στην ανάπτυξη ενός συγκεκριμένου τύπου υπηρεσιών υγείας, ο οποίος λειτουργεί ως επίκεντρο γύρω από τον οποίο αναπτύσσεται το σύστημα υγείας στο σύνολό του. Άλλα συστήματα έχουν ως επίκεντρο το νοσοκομείο της δευτεροβάθμιας περίθαλψης (νοσοκομειακό σύστημα) και άλλα οργανώνονται και διαρθρώνονται με επίκεντρο την πρωτοβάθμια φροντίδα υγείας. Κατά αντιστοιχία τα συστήματα με επίκεντρο το νοσοκομείο δίνουν έμφαση στη θεραπευτική

αντιμετώπιση της ασθένειας, ενώ τα συστήματα με επίκεντρο την πρωτοβάθμια περίθαλψη δίνουν ιδιαίτερο βάρος στην πρόληψη της ασθένειας και στην αποκατάσταση μετά τη θεραπεία.

4.3 Ο Ψηφιακός Μετασχηματισμός του Συστήματος Υγείας

Η ραγδαία εξέλιξη της τεχνολογίας και η ενσωμάτωση της τελευταίας ως βασικού εργαλείου διεκπεραίωσης διαδικασιών σε κάθε τομέα, έχει επιφέρει επαναστατικά αποτελέσματα αλλάζοντας ριζικά τον τρόπο με τον οποίο ο άνθρωπος αντιλαμβάνεται και αντιδρά. Οι προσπάθειες ένταξης των τεχνολογικών επιτευγμάτων στον τομέα της υγείας, τόσο για να προάγουν την έρευνα όσο και για απλοποιήσουν τη φύση των τακτικών επαναλαμβανόμενων διαδικασιών, αντανακλούσαν την ανάγκη για ευρύτερη κοινωνική αλλαγή. Ιδιαίτερα στο υγειονομικό σύστημα, οι προσπάθειες αυτές εντατικοποιήθηκαν οδηγούμενες από την απαίτηση για αυξημένη απόδοση, εξάλειψη των λαθών και βελτίωση ποιότητας στην παροχή υπηρεσιών.

Συγκρινοντάς την με άλλους τομείς, θα μπορούσε κανείς να πει ότι η ψηφιοποίηση του συστήματος υγείας είναι σχετικά πρόσφατο επίτευγμα, με το ρυθμό αλλαγής που σημειώνεται τις τελευταίες δεκαετίες να είναι ταχύτερος από ποτέ. Πέρα από την εύκολα εννοούμενη χρήση του ψηφιακού κόσμου για αποτελεσματικότερη αποθήκευση και διαχείριση πληρφοριών, τα τελευταία χρόνια τα πλεονεκτήματα από πιθανές εφαρμογές της τεχνολογίας στον τομέα της υγείας συνεχίζουν να αυξάνονται, με τους ερευνητές να κάνουν λόγο για τηλεϊατρική και ¨έξυπνα νοσοκομεία¨.

4.3.1 Ο ηλεκτρονικός φάκελος των ασθενών

Το πρώτο σύστημα ηλεκτρονικού φακέλου για την καταγραφή δεδομένων ασθενών δημιουργήθηκε το 1961, από τον Dr. Lawrence L. Weed. Το σύστημα αυτό λεγόταν Problem Oriented Medical Information System (Promise) και ο σχεδιασμός του στόχευε στην μείωση των γραφειοκρατικών πρακτικών και την απλοποίηση της αποθήκευσης και επεξεργασίας του ιατρικού ιστορικού [23].

Σήμερα, η μορφή του ηλεκτρονικού φακέλου είναι εντελώς διαφορετική, περιλαμβάνοντας τεχνολογίες αιχμής όπως και Big Data Analytics, και τα αρχεία αυτά μπορούν να διακριθούν σε δύο κατηγορίες, τα **ηλεκτρονικά αρχεία υγείας** (electronic health records -**EHRs**) και τα **αρχεία υγείας ασθενή** (patient health records -**PHRs**). Τα ηλεκτρονικά αρχεία υγείας (EHRs) αποτελούν μία συστηματική συλλογή δεδομένων των πολιτών, από το ιατρικό τους ιστορικό μέχρι οικονομικές πληροφορίες που τους αφορούν. Μέσω αυτών οι υπεύθυνοι μπορούν να οργανώσουν το είδος και τις υπηρεσίες που πρέπει να παρέχουν στον εν λόγω ασθενή, καταγράφοντας τα δεδομένα, συγκρίνοντάς τα με αντίστοιχα αρχεία και εκτιμώντας έτσι τα αποτελέσματα που αναμένονται. Τα αρχεία υγείας ασθενή (PHRs) περιέχουν τις ίδιες πληροφορίες (διάγνωση, δοσολογία, οικογενειακό ιστορικό κ.α.) μόνο που είναι σχεδιασμένα για να τα διαχειρίζονται και να τα ενημερώνουν οι ασθενείς. Τα αρχεία αυτά αποτελούν βασικούς πυλώνες πάνω στους οποίους δομείται το σύστημα της ηλεκτρονικής υγείας (eHealth), που εξετάζεται στην επόμενη υποπαράγραφο, και η επίδραση τους

στο σύστημα της δημόσιας υγείας μέσα από διαφορετικά παραδείγματα χρήσης φαίνεται στο Σχήμα 4.1.

Σχήμα 4.1: *Παραδείγματα χρησιμότητας των EHR, PHR, Πηγή: SPHINX D2.4*

Τα οφέλη που συνοδεύουν αυτή την αλλαγή στον τρόπο καταγραφής, αποθήκευσης και επεξεργασίας της πληροφορίας είναι ποιοτικά και ποσοτικά και αφορούν εκτός από τους ασθενείς, τις ίδιες τις μονάδες που υποστηρίζουν τέτοια συστήματα αλλά και το κράτος.

- **Ασθενείς** : Οι ασθενείς απολαμβάνουν πρόσβαση στα δεδομένα τους συνολικά, αίροντας χρονικούς ή τοπικούς περιορισμούς. Οι πληροφορίες τους, όντας ψηφιακά καταχωρημένες, κοινοποιούνται πολύ απλά σε κάποιον που τις χρειάζεται, ακόμα και αν πρόκειται για διασυνοριακές συναλλαγές. Τα ποσοστά ακρίβειας των διαγνώσεων αυξάνονται και οι ασθενείς έτσι θεραπεύονται αποτελεσματικότερα.

- **Μονάδες Υγείας**: Οι μονάδες υγείας επωφελούνται από την άμεση ανταλλαγή δεδομένων μεταξύ του ιατρικού προσωπικού. Η διατομεακή προσέγγιση της πληροφορίας και η απρόσκοπτη επικοινωνία μεταξύ των ειδημόνων αυξάνει την επίδοση των ιατρών και μειώνει την πιθανότητα λάθους. Επίσης η συνεργασία αυτή εξοικονομεί πόρους και χρόνο από το ιατρικό και διοικητικό προσωπικό. Ο συντονισμός του κλάδου της ιατρικής περίθαλψης και η εφαρμογή των μεθοδολογιών με στόχο τη λήψη αποφάσεων γίνονται ευκολότερα τα τελευταία χρόνια χάρη στην ηλεκτρονική διαχείρηση των πληροφοριών.

- **Κράτος**: Συλλέγοντας τις πληροφορίες αυτές, το κράτος διαθέτει στατιστικά νούμερα και τάσεις σχετικά με την υγεία του πληθυσμού τα οποία μπορεί να χρησιμοποιήσει με στόχο τη βελτίωση του γενικού βιοτικού επιπέδου.

Τα τελευταία χρόνια παρατηρείται η αύξηση της αυτοματοποιημένης επεξεργασίας των δεδομένων με την εφαρμογή τεχνολογιών Big Data Analytics συνδυασμένων με λύσεις τεχνητής νοημοσύνης. Ο συνδυασμός αυτός είναι πολλά υποσχόμενος στην κατεύθυνση της προαγωγής της κλινικής έρευνας. Η επεξεργασία και η ανάλυση τεράστιου όγκου δεδομένων προσεγγίζονται ολιστικά, με τους επιστήμονες να εκμεταλλεύονται τη δυνατότητα συνδυαστικής ανάλυσης για την παρατήρηση μοτίβων σχετικών με ασθένειες.

Αναλυτικότερα τα Big Data Analytics επιτρέπουν την (Deloitte, 2020) :

- επεξεργασία ιστορικών δεδομένων με σκοπό την πρόβλεψη μελλοντικών αποτελεσμάτων προς αξιοποίηση κατά τη διαδικασία της έρευνας,

- επεξεργασία, συνδυαστική ανάλυση και ένταξη στη διαδικασία της έρευνας μεγάλου όγκου δεδομένων από πολλαπλές πηγές, όπως δημογραφικές πληροφορίες διάγνωσης, φαρμακευτικές αγωγές, θεραπευτικά πρωτόκολλα, εργαστηριακές εξετάσεις και κλινικές σημειώσεις από ηλεκτρονικούς φακέλους υγείας,
- επεξεργασία δεδομένων για τον εντοπισμό ομάδων ασθενών που μοιράζονται κοινά χαρακτηριστικά με στόχο την ακριβέστερη διενέργεια κλινικών δοκιμών κατά την εξέταση συγκεκριμένων παραγόντων,
- αποτελεσματικότερη διαχείριση χρόνιων ασθενειών.

Οι χρόνιες ασθένειες είναι το ταχύτερα αναπτυσσόμενο και πιο δαπανηρό πρόβλημα το οποίο αντιμετωπίζει ο κλάδος της υγείας σήμερα. Η αξιοποίηση των Big Data Analytics συνεισφέρουν στην κατανόηση του ασθενή όσο το δυνατόν περισσότερο, στοχεύοντας στην αναγνώριση των προειδοποιητικών σημαδιών κάποιας σοβαρής ασθένειας σε αρκετά πρώιμο στάδιο, έτσι ώστε η θεραπεία να είναι πιο απλή και λιγότερο δαπανηρή. Τα Big Data Analytics συνεισφέρουν στη δυνατότητα καλύτερης κατανόησης μοτίβων και τάσεων των χρόνιων ασθενειών προκειμένου να αναλαμβάνεται δράση με βάση τις πραγματικές ανάγκες του πληθυσμού που πάσχει από χρόνιες μη μεταδοτικές ασθένειες.

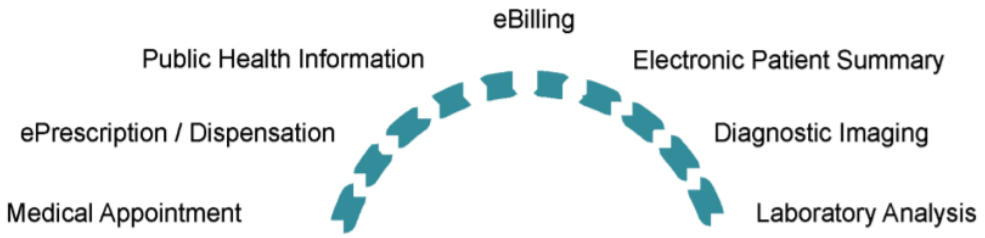
Παρά τα πλεονεκτήματα που συνεπάγονται από την ενσωμάτωση των τεχνολογιών αυτών στις ιατρικές πρακτικές, τίθενται πολύ σοβαρά ζητήματα κυβερνοασφάλειας. Η προσπάθεια διατήρησης της ασφάλειας των συστημάτων του τομέα Υγείας, αποτελεί σημαντικό διακύβευμα τόσο σε κρατικό όσο και σε παγκόσμιο επίπεδο.

4.3.2 Ηλεκτρονική Υγεία - e-Health

Οι μονάδες Υγείας υιοθετούν σταδιακά νέες τεχνολογίες με στόχο να παρέχουν τις υπηρεσίες τους διαδικτυακά σε ένα διεθνές πλαίσιο. Στις υπηρεσίες αυτές, που απλοποιούν σημαντικά την αλληλεπίδραση των ασθενών με τις μονάδες του Συστήματος Υγείας, συγκαταλέγονται η ηλεκτρονική συνταγογράφηση (ePrescription), η ηλεκτρονική σύνοψη πληροφοριών ασθενούς (Electronic patient summary), η ηλεκτρονική έκδοση παραπεμπτικών (eReferrals), η ηλεκτρονική πληρωμή υπηρεσιών υγείας (eBilling), οι εικονικές συνεδρίες (Virtual consultations) και πολλές άλλες [24]. Παραδείγματα των υπηρεσιών φαίνονται στο Σχήμα 4.3. Το σημαντικότερο πλεονέκτημα μετά την απλοποίηση των διαδικασιών είναι ότι ο εκμοντερνισμός του συστήματος Υγείας ανταποκρίνεται στις ανάγκες για εξατομικευμένη και ανθρωποκεντρική θεραπεία.

Οι εφαρμογές ηλεκτρονικής υγείας προσφέρουν τη δυνατότητα για μια απρόσκοπτη σχέση μεταξύ ασθενών και επαγγελματιών υγείας, και προσφέρει στους παρόχους μια συνεχή ροή δεδομένων ασθενών σε πραγματικό χρόνο. Μέσω αυτής αξιολογούνται οι ανάγκες του κάθε περιστατικού, και ο ασθενής κατευθύνεται στο πεδίο ιατρικής φροντίδας που κρίνεται σχετικό.

Για να είναι αυτά δυνατά τα παραπάνω, οι οργανισμοί που εφαρμόζουν τις υπηρεσίες Ηλεκτρονικής Υγείας χρησιμοποιούν εργαλεία βασισμένα σε εξωτερικές οντότητες όπως τεχνολογίες διαδικτύου (IP και web services) και ανοιχτά πρότυπα (open standards πχ HL7)), όπου οι έλεγχοι ασφάλειας δύσκολα ενισχύονται και υλοποιούνται. Η ύπαρξη ευπαθειών



Σχήμα 4.2: *Παραδείγματα εφαρμογών e-Health, Πηγή: SPHINX D2.4*

και αδύναμων σημείων στο ηλεκτρονικό σύστημα ενισχύει τις ανησυχίες για τους πιθανούς κινδύνους που το απειλούν, την ακεραιότητά του και την υποκλοπή ευαίσθητων απόρρητων πληροφοριών. Τα συστήματα προστασίας και τα σημεία ελέγχου της ασφάλειας που θα οριστούν, πρέπει να ελαχιστοποιούν το ρίσκο που αφορά την πραγματοποίηση κυβερνοεπιθέσεων.

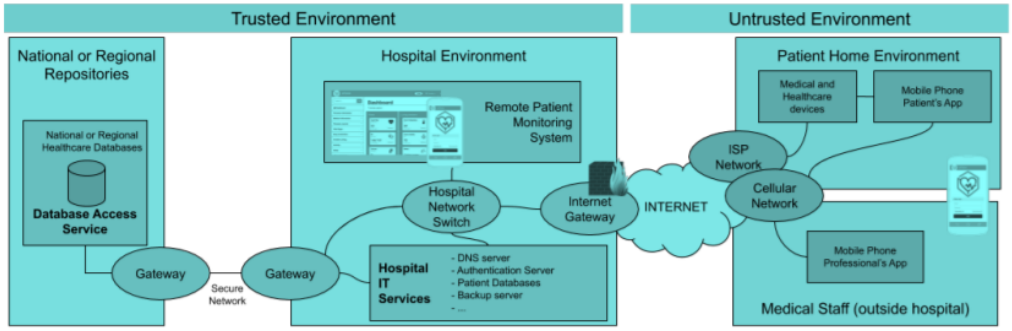
4.3.3 Κινητή Υγεία - m-Health

Η εξέλιξη της τεχνολογίας των πληροφοριών έχει αναδείξει άλλη μία μορφή ηλεκτρονικής υγείας, την κινητή υγεία (mobile health). Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ), m-Health είναι «*η άσκηση της Ιατρικής και των πρακτικών δημόσιας υγείας μέσω έξυπνων κινητών συσκευών, όπως κινητά τηλέφωνα (smartphones) και tablets, προσωπικών ψηφιακών βοηθών (PDAs) και άλλων ασύρματων συσκευών*». Η κινητή υγεία, στοχεύει στην παροχή υπηρεσιών μέσω ιατρικών συσκευών απομακρυσμένης πρόσβασης (remote access), χωρίς δηλαδή να απαιτείται ο ασθενής και ο ιατρός να βρίσκονται στον ίδιο χώρο. Αυτό είναι εφικτό χάρη στις τεχνολογίες στις οποίες βασίζεται ο κλάδος, κυρίως στο Διαδίκτυο των πραγμάτων, IoT και συγκεκριμένα στο Internet of Medical Things, IoMT, καθώς και σε εφαρμογές συνδεδεμένες με πληροφοριακά συστήματα του κλάδου υγείας. Διευκολύνεται η ανταλλαγή πληροφοριών και βελτιώνεται σημαντικά η εμπειρία του ασθενή και η φροντίδα που του παρέχεται, καθώς η παρακολούθηση της κατάστασής του γίνεται και εκτός των πλαισίων των εκάστοτε μονάδων υγείας. Μέσα από φορητές συσκευές, όπως εμφυτεύματα που παρακολουθούν την καρδιακή λειτουργία (heart monitoring implants) ή αντλίες έγχυσης (infusion pumps), το ιατρικό προσωπικό αποκτά ανά πάσα στιγμή την εικόνα του ασθενούς μέσα από τον πλήρη ιατρικό φάκελο ασθενή, αποτελέσματα ιατρικών εξετάσεων αλλά και συνεχή ροή ζωτικών στοιχείων του ασθενούς που συγκεντρώνονται με τη βοήθεια wearables. Κάποιες από αυτές τις συσκευές μόνο αποστέλλουν πληροφορίες μέσω ασύρματων συνδέσεων, ενώ άλλες και μπορούν και να λάβουν. Ένα παράδειγμα της πρώτης κατηγορίας είναι οι βηματοδότες, ενώ στην δεύτερη κατηγορία υπάγονται συσκευές όπως οι αντλίες έγχυσης. Σύμφωνα με τις εκτιμήσεις των ειδικών, μέχρι το 2025 οι φορητές συσκευές που χρησιμοποιούνται στον τομέα της υγείας θα ξεπερνούν τα 25 δισεκατομμύρια, ενώ το κόστος αυτών των λύσεων θα αγγίζει την τάξη των 3 τρισεκατομμυρίων.

Παρατηρείται ιδιαίτερο ενδιαφέρον από την πλευρά των ερευνητών για την αποτίμηση της συμβολής της m-Health στην αντιμετώπιση χρόνιων προβλημάτων [25], και πολλές με-

λέτες έχουν αφιερωθεί στο σκοπό αυτό. Το χαμηλό κόστος, τόσο για τους ασθενείς όσο και για τις ίδιες τις μονάδες, καθώς και η προσβασιμότητα σε πληθυσμούς απομακρυσμένων περιοχών, σε ευαίσθητες ομάδες πληθυσμού και σε χρόνια πάσχοντες, καθιστούν την κινητή υγεία προτιμητέα επιλογή. Η λήψη και ανάλυση δεδομένων σε πραγματικό χρόνο, καθώς και η προσιτότητα που χαρακτηρίζει αυτόν τον τρόπο επικοινωνίας έχει επιφέρει μεγάλη βελτίωση στην διάγνωση, την παρακολούθηση και την παροχή ιατρικών οδηγιών σχετικά με τα χρόνια νοσήματα, τα οποία αποτελούν αιτία θανάτου για 40 εκατομμύρια ανθρώπους ετησίως, αριθμός που ισοδυναμεί με το 70% των θανάτων σε παγκόσμιο επίπεδο.

Οι φορητές συσκευές που χρησιμοποιούνται στα πλαίσια ιατρικής περίθαλψης αναμφισβήτητα εισάγουν στον τομέα πολλά θετικά στοιχεία, συνοδεύονται όμως και από πολλούς κινδύνους. Είναι συχνά ευάλωτες σε ιούς και κακόβουλο λογισμικό που μπορεί να προκαλέσουν την αποτυχία λειτουργίας διαφόρων συσκευών που είτε λαμβάνουν είτε μεταδίδουν ιατρικά δεδομένα, αλλά και την διαρροή ευαίσθητων πληροφοριών των ασθενών. Ακόμη, η χρήση προσωπικών συσκευών (πχ για εγκατάσταση εφαρμογών m - Health) που δεν ανήκουν, επομένως δεν είναι και υπό τον έλεγχο των μονάδων υγείας εισάγει τον κίνδυνο αυτές να κλαπούν απειλώντας τη διατήρηση του απορρήτου της πληροφορίας. Καθώς όλες αυτές οι συσκευές αλληλοσυνδέονται στο ευρύτερο πλαίσιο ενός ψηφιακού συστήματος υγείας, οι απειλές για την διαφύλαξη της πληροφορίας γιγαντώνονται, και πρέπει να ληφθούν πολύ σοβαρά υπόψη από τους υπεύθυνους.



Σχήμα 4.3: *Το σύστημα της κινητής υγείας και οι κίνδυνοι που αντιμετωπίζει eHealth, Πηγή: SPHINX D2.4*

Μέρος II

Πρακτικό Μέρος

Κεφάλαιο 5

Μοντελοποίηση Σεναρίων Ρίσκου με χρήση του GIRA model

Στα προηγούμενα κεφάλαια τέθηκε το απαραίτητο θεωρητικό υπόβαθρο και μελετήθηκε η αναγκαιότητα ανάπτυξης ενός πλάνου Διαχείρισης Ρίσκου σε μονάδες του Συστήματος Υγείας. Σε αυτό το κεφάλαιο γίνεται εφαρμογή του μοντέλου GIRA, υβριδικής μεθόδου Εκτίμησης Ρίσκου, που παρουσιάστηκε στην παράγραφο 2.5.4. Στόχος της παρούσας εργασίας είναι η προσομοίωση χρήσης των μεθοδολογιών Εκτίμησης Ρίσκου ως εργαλείων υποστήριξης λήψης αποφάσεων και όχι η αναγνώριση όλων των απειλών και όλων των ευαισθησιών που παρουσιάζονται στο Σύστημα Υγείας. Ως εκ τούτου αποφασίστηκε η εφαρμογή της μεθόδου GIRA να γίνει στην τοπολογία ενός ακτινολογικού ιατρείου. **Η μαθηματική ανάλυση του μοντέλου γίνεται στο Παράρτημα Α΄.** Παρακάτω παρατίθενται τα χαρακτηριστικά της τοπολογίας του ιατρείου και του ανθρωπίνου δυναμικού από το οποίο απαρτίζεται.

Όσον αφορά στο ανθρώπινο δυναμικό, στο συγκεκριμένο ιατρείο εργάζονται :

- 2 γιατροί,
- 3 νοσοκόμες,
- 2 γραμματείς (Διοικητικό προσωπικό),
- Υπεύθυνος διαχείρισης συστήματος (Τεχνικό προσωπικό).

Τα Σχήματα 5.1 και 5.2 περιλαμβάνουν τα χαρακτηριστικά του εσωτερικού και εξωτερικού χώρου του ιατρείου που κρίθηκαν χρήσιμα για την ανάλυση καθώς και τις λεπτομέρειες δικτύου :

Δίκτυο	
Server 1	Ιστοσελίδα ιατρείου/ τοπική μνήμη για άλλους υπολογιστές
Server 2	Υποστήριξη ιατρικού εξοπλισμού
Πρόσβαση στο τοπικό δίκτυο	Γραφείο γραμματέως, γραφεία ιατρών
	Unused cable lobby

Σχήμα 5.1: *Χαρακτηριστικά δικτύου ακτινολογικού ιατρείου*

Τοποθεσία	
Αθήνα, κέντρο	Διαμέρισμα 1ου ορόφου
Χώροι	
Χώρος υποδοχής	Γραφείο γραμματέως: - Υπολογιστές - Φυσικά αρχεία
	Μπάνιο
4 Δωμάτια ασθενών	Ιατρικές πρώτες ύλες και προμήθειες
	Απομακρυσμένη παρακολούθηση ασθενών
2 Γραφεία ιατρών	Υπολογιστές
	Φυσικά αρχεία με δεδομένα ασθενών
Χώρος ανάπαυσης νοσοκόμων	Προσωπικά αντικείμενα νοσοκόμων
Δωμάτιο server	Εξοπλισμός Server
Χώρος στάθμευσης στο πίσω μέρος της πολυκατοικίας	Κουτιά παροχής ηλεκτρικού ρεύματος στο πίσω μέρος της πολυκατοικίας
Διάδρομος που συνδέει όλα τα δωμάτια	
Κήπος περιμετρικά του ιατρείου	

Σχήμα 5.2: *Τοπολογία ακτινολογικού ιατρείου*

5.1 Περίπτωση Χρήσης 1: Πυρκαγιά στο ιατρείο

Στο Σχήμα 5.3 φαίνονται τα χαρακτηριστικά του πρώτου σεναρίου χρήσης:

Εύρος (Scope)	
Εύρος επίδρασης (Application Scenario)	**Διαχείριση Εγκαταστάσεων**
Επίθεση (Attack)	
Τύπος Απειλής (Threat Type)	**Μη ανταγωνιστική- Φυσική καταστροφή- Ανθρώπινο Σφάλμα (Human Error)**
Πηγή/Υποκείμενο Απειλής (Threat Actor)	-
Στόχευση Επίθεσης (Attack Vector)	**Physical and environmental security**
Κρίσιμα Στοιχεία του τομέα Υγείας (Critical Healthcare Assets)	
Στοιχεία που επηρεάζονται (Affected assets)	**Εγκαταστάσεις, Εξοπλισμός, Ιατρικά δεδομένα**
Κρισιμότητα στοιχείων που επηρεάζονται (Criticality of affected assets)	**Πολύ κρίσιμα**

Σχήμα 5.3: *UC1: Περιγραφή Χαρακτηριστικών Σεναρίου*

1.Κόμβος έκθεσης σε απειλή (Threat exposure Node) :

Το ιατρείο βρίσκεται στον πρώτο όροφο μίας πολυκατοικίας στο κέντρο της Αθήνας. Λόγω πυρακτωμένης επιφάνειας στην κουζίνα που ξέχασαν οι ένοικοι, το διαμέρισμα που βρίσκεται

πάνω από το ιατρείο πιάνει φωτιά. Θα θεωρήσουμε ότι η πιθανότητα να γίνει αντιληπτή εγκαίρως η πυρκαγιά είναι 25%, διαφορετικά εξαπλώνεται στα υπόλοιπα διαμερίσματα της πολυκατοικίας με πιθανότητα 75%. Σε αυτό το σημείο πρέπει να σημειώσουμε ότι η παραπάνω πιθανότητα δεν είναι προφανώς στατική, αλλά της ανατίθεται τιμή με σκοπό να γίνει πιο κατανοητή η εφαρμογή της μεθόδου.

Σχήμα 5.4: *UC1: Έκθεση σε Απειλή*

2.Κόμβος μέτρων αντιμετώπισης απειλών (Incident Response Node) :

Σχήμα 5.5: *UC1: Μέτρα Αντιμετώπισης Απειλής*

Για να αντιμετωπίσουν τον κίνδυνο πυρκαγιάς (Incident response), οι υπεύθυνοι του ιατρείου μπορούν να εγκαταστήσουν είτε αισθητήρες και συναγερμό πυρανίχνευσης, είτε σύστημα πυρόσβεσης. Φυσικά έχουν την επιλογή να συνδυάσουν τις δύο παραπάνω λύσεις είτε να μην κάνουν τίποτα.

Ο κόμβος με τις αντιδράσεις για την αντιμετώπιση της απειλής πυρκαγιάς θα έχει 4 πιθανές καταστάσεις. Οι δείκτες IR αναφέρονται στις 4 εναλλακτικές δράσεις - Incident responses:

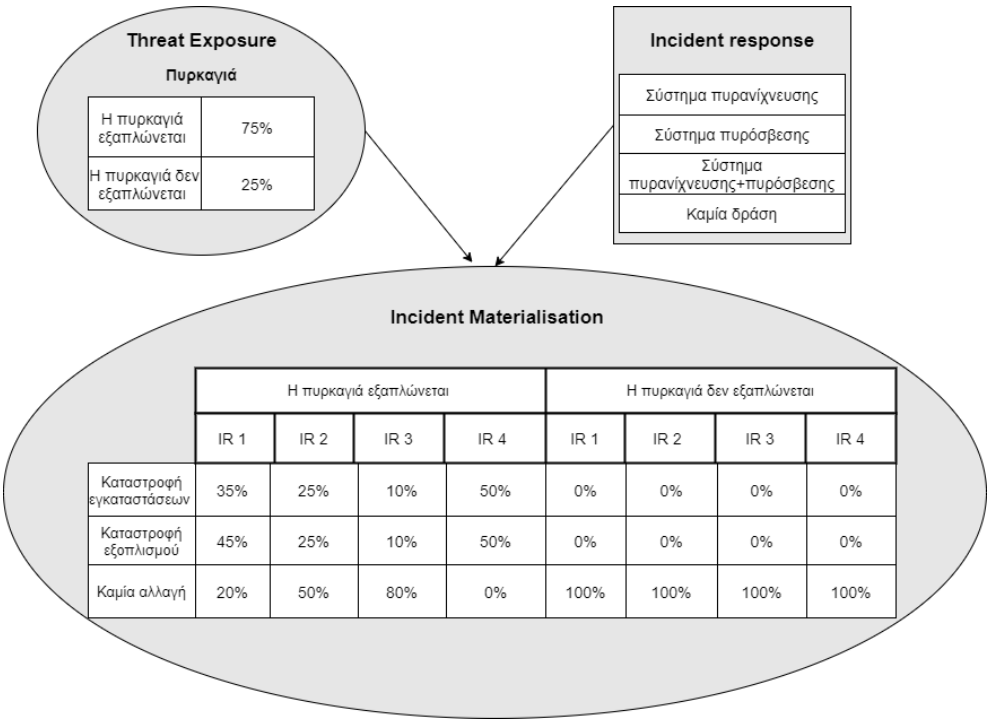
- IR1: Σύστημα πυρανίχνευσης
- IR2: Σύστημα πυρόσβεσης
- IR3: Σύστημα πυρανίχνευσης και πυρόσβεσης
- IR4: Καμία δράση

3.Κόμβος πραγματοποίησης κινδύνου (Incident Materialisation Node) :

Λαμβάνοντας υπόψη τα μέτρα που μπορούν να ληφθούν για να μετριαστεί ή να εξαλειφθεί η πιθανότητα πυρκαγιάς, προκύπτουν 3 διακριτά σενάρια. Τα σενάρια αυτά αφορούν τον βαθμό στον οποίο η πυρκαγιά θα επηρεάσει το ιατρείο:

- (Πλήρης ή μερική) καταστροφή εγκαταστάσεων
- Καταστροφή ευαίσθητου ιατρικού εξοπλισμού
- Καμία αλλαγή

Σημείωση: Ο παρακάτω πίνακας δίνει την πιθανότητα να πραγματοποιηθούν τα ενδεχόμενα καταστροφής εγκαταστάσεων, καταστροφής εξοπλισμού ή καμίας αλλαγής, δεδομένου ότι η πυρκαγιά έχει εξαπλωθεί και τα μέτρα αντιμετώπισης έχουν ληφθεί. Πρόκειται δηλαδή για δεσμευμένες πιθανότητες, οι οποίες υπολογίζονται με βάση τον τύπο του Bayes ως εξής:



	Η πυρκαγιά εξαπλώνεται				Η πυρκαγιά δεν εξαπλώνεται			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Καταστροφή εγκαταστάσεων	35%	25%	10%	50%	0%	0%	0%	0%
Καταστροφή εξοπλισμού	45%	25%	10%	50%	0%	0%	0%	0%
Καμία αλλαγή	20%	50%	80%	0%	100%	100%	100%	100%

Σχήμα 5.6: *UC1: Πραγματοποίηση Κινδύνου*

4.Κόμβος Συνεπειών στο Σύστημα υπό Διαχείριση (Consequences in the Managed System Node) :

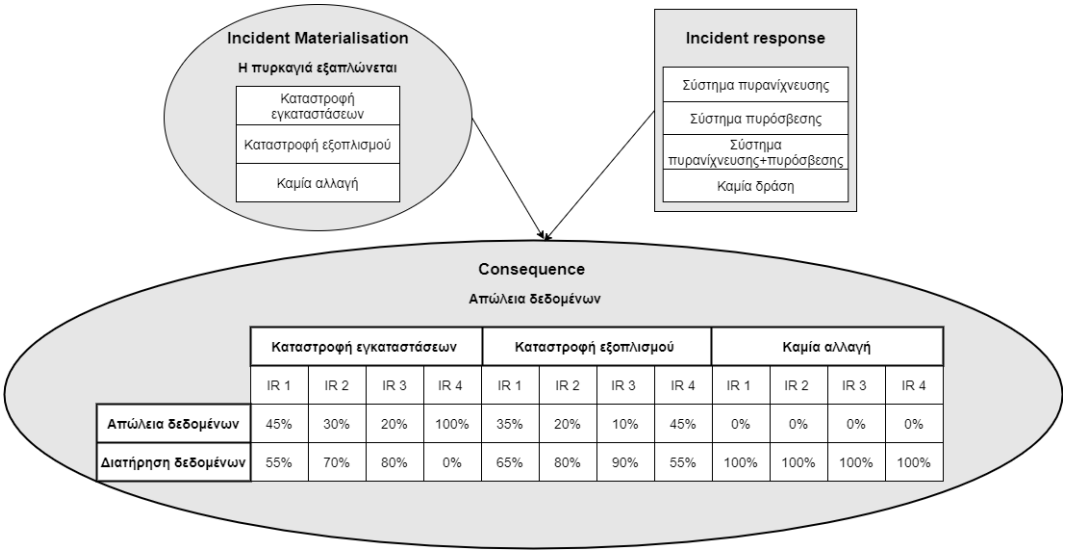
Ο κίνδυνος που προσπαθούμε να μετριάσουμε αφορά το εάν θα ξεσπάσει πυρκαγιά στο ιατρείο, καταστρέφοντας είτε τις εγκαταστάσεις είτε τον εξοπλισμό. Εκτός όμως από τα παραπάνω, σε περίπτωση πραγματοποίησης του κινδύνου που μελετάμε, θα πρέπει να ληφθούν υπόψη όλες οι πιθανές συνέπειες που θα έχει αυτό στο σύστημά μας:

- σωματική βλάβη ασθενών ή προσωπικού,
- απώλεια σημαντικών πληροφοριών όπως το ιστορικό των ασθενών και τα προσωπικά τους δεδομένα.

Τα παραπάνω ενδεχόμενα είναι ανεξάρτητα γι' αυτό και αναπαρίστανται στο διάγραμμα από κόμβους που δεν επικοινωνούν μεταξύ τους. Οι καταστάσεις κάθε κόμβου υπαγορεύονται από το βαθμό σοβαρότητας των συνεπειών.

Σημειώνουμε ότι στα παρακάτω διαγράμματα, οι πιθανότητες που παρουσιάζονται είναι δεσμευμένες. Για παράδειγμα, το 0,25 της πρώτης στήλης δεν αφορά την πιθανότητα να τραυματιστεί κάποιος, αλλά την πιθανότητα να τραυματιστεί δεδομένου ότι έχει εγκατασταθεί σύστημα πυρανίχνευσης.

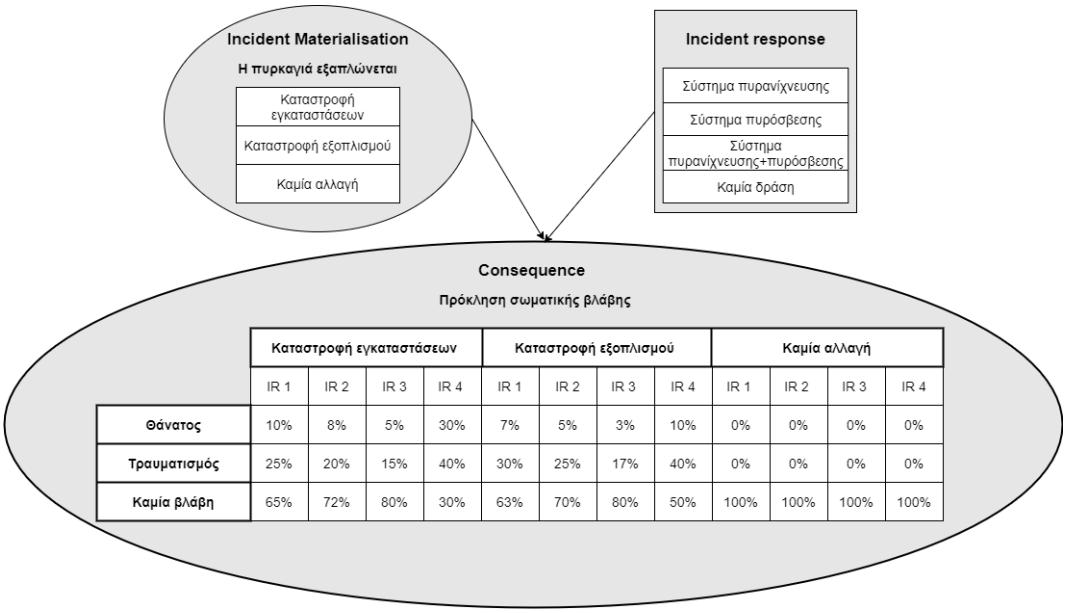
Η πιθανότητα **απώλειας δεδομένων** μοντελοποιείται ως εξής:



	Καταστροφή εγκαταστάσεων				Καταστροφή εξοπλισμού				Καμία αλλαγή			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Απώλεια δεδομένων	45%	30%	20%	100%	35%	20%	10%	45%	0%	0%	0%	0%
Διατήρηση δεδομένων	55%	70%	80%	0%	65%	80%	90%	55%	100%	100%	100%	100%

Σχήμα 5.7: *UC1: Απώλεια Δεδομένων*

Η πιθανότητα πρόκλησης **σωματικής βλάβης** σε ασθενείς ή ιατρικό προσωπικό μοντελοποιείται ως εξής:



	Καταστροφή εγκαταστάσεων				Καταστροφή εξοπλισμού				Καμία αλλαγή			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Θάνατος	10%	8%	5%	30%	7%	5%	3%	10%	0%	0%	0%	0%
Τραυματισμός	25%	20%	15%	40%	30%	25%	17%	40%	0%	0%	0%	0%
Καμία βλάβη	65%	72%	80%	30%	63%	70%	80%	50%	100%	100%	100%	100%

Σχήμα 5.8: *UC1: Πρόκληση Σωματικής Βλάβης*

5.Κόμβος Στοιχείων υπό προστασία (Asset status Node) :

Οι υπεύθυνοι του ιατρείου διαφημίζουν την αξιοπιστία και την διαρκή παροχή των υπηρεσιών τους. Επομένως ενδιαφέρονται για τη συνεχή λειτουργία του ιατρείου και τη διατήρηση της καλής φήμης. Προσπαθούν να μετριάσουν τα ρίσκα και τους κινδύνους που αντιμετωπίζουν, με γνώμονα την προστασία των παραπάνω δύο χαρακτηριστικών.

Σχήμα 5.9: *UC1: Στοιχεία υπό προστασία*

6.Κόμβος Επίπτωσης στα Στοιχεία υπό προστασία (Asset status Node) :

Συνέπειες της πυρκαγιάς στη φήμη του ιατρείου: Οι υπεύθυνοι του ιατρείου γνωρίζουν ότι, στην περίπτωση που εξαιτίας της πυρκαγιάς προκληθεί σωματική βλάβη σε κάποιον, θα πρέπει να λογοδοτήσουν για την έλλειψη τόσο μέτρων πρόληψης όσο και αντιμετώπισης μίας τέτοιας κρίσης. Ακόμη, η μη ψηφιοποίηση των δεδομένων των ασθενών και η διατήρησή τους σε φακέλους, μπορεί να έχει ως αποτέλεσμα την πλήρη απώλειά τους. Σε μία τέτοια περίπτωση οι ασθενείς θα πρέπει να επαναλάβουν εξετάσεις ώστε να αναπληρωθεί μέρος των χαμένων αρχείων, γεγονός που τους προκαλεί δυσαρέσκεια.

Συνέπειες της πυρκαγιάς στη λειτουργία του ιατρείου: Οι υπεύθυνοι του ιατρείου θα χρειαστούν κάποιες μέρες ή και εβδομάδες μέχρι να προετοιμαστούν για την επαναλειτουργία του. Αυτή η συνέπεια είναι προφανής σε περίπτωση που είναι αναγκαία η επισκευή των εγκαταστάσεων. Αλλά ακόμα και στην περίπτωση που η φωτιά δεν προκαλέσει υλικές ζημιές στο ιατρείο, μία πτώση τάσης ή διακοπή του ρεύματος μπορεί να είναι αρκετή ώστε να απορρυθμίσει ή να καταστήσει αδύνατη τη λειτουργία ευαίσθητων ιατρικών μηχανημάτων όπως ο μαγνητικός τομογράφος. Τότε η επιλογή, η παραγγελία και η εγκατάσταση του νέου εξοπλισμού μπορεί να διαρκέσει εβδομάδες.

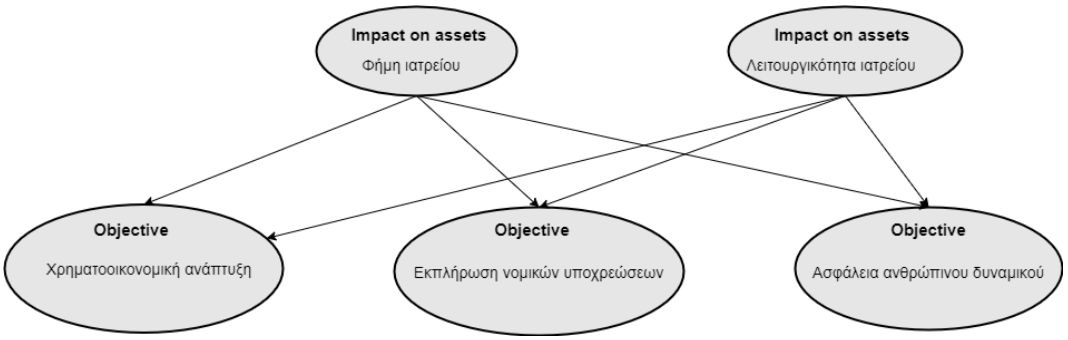
7.Κόμβος Στόχων (Objective Node) :

Ο κόμβος τελικών στόχων συνοψίζει όλα τα στοιχεία που είναι σημαντικά για τους υπεύθυνους του ιατρείου. Τα στοιχεία αυτά θα μπορούσαν να θεωρηθούν και δείκτες επιτυχίας του ιατρείου ως παρόχου υγείας που ανήκει στον ιδιωτικό τομέα. Οι μετρικές απόδοσης, των οποίων η διαγραμματική παρουσίαση των στόχων δίνεται στο Σχήμα 5.10, είναι :

- Η ασφάλεια και η υγεία του ανθρώπινου δυναμικού (ασθενείς και προσωπικό)
- Η χρηματοοικονομική ανάπτυξη
- Η εκπλήρωση των νομικών υποχρεώσεων

8.Κόμβος Αξιολόγησης Κινδύνου (Risk Evaluation Node) :

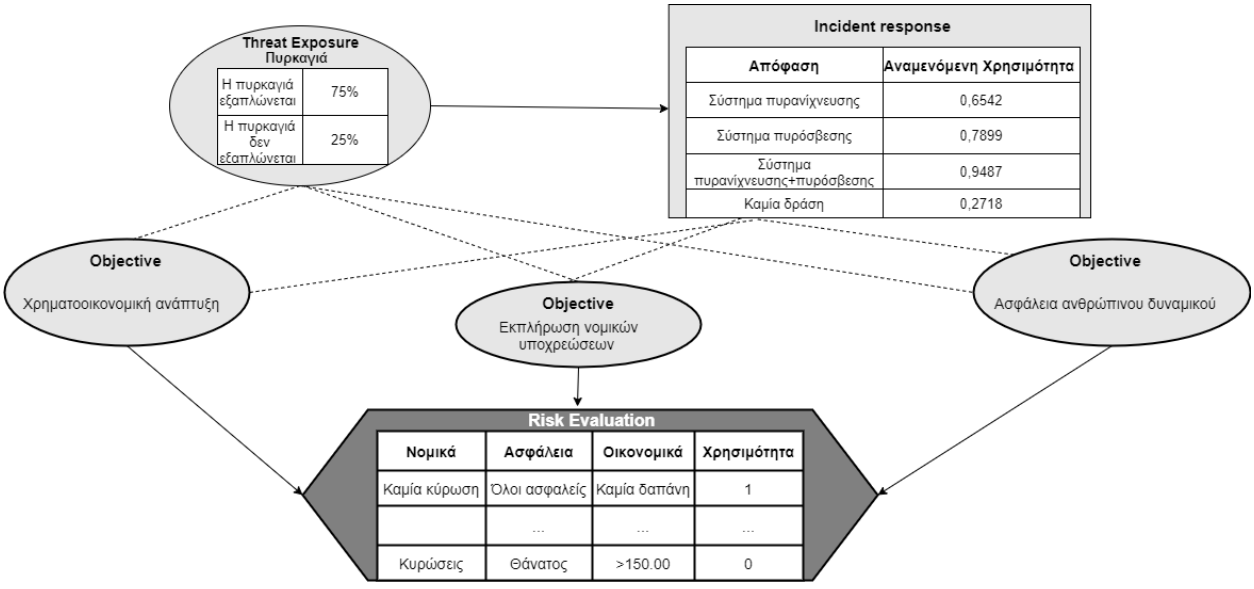
Μετά την ολοκληρωμένη μοντελοποίηση του σεναρίου, την ανίχνευση των απειλών και της πιθανότητας αυτές να υλοποιηθούν, αλλά και την μελέτη εναλλακτικών τρόπων δράσης απέναντι σε αυτές (Incident responses), οι υπεύθυνοι του ιατρείου είναι σε θέση να αξιολογήσουν το ρίσκο. Στόχος είναι να επιλέξουν εκείνη την εναλλακτική που ελαχιστοποιεί τον κίνδυνο η πυρκαγιά να προκαλέσει καταστροφές, με γνώμονα πάντα τους στόχους που



Σχήμα 5.10: *UC1: Στόχοι*

έχουν τεθεί στο πλαίσιο της επαγγελματικής ηθικής του ιατρείου. Σε αυτή τη φάση της ανάλυσης δεν αρκεί λοιπόν να επιλέξουμε την εναλλακτική που ελαχιστοποιεί το **ρίσκο**. Σημαντικό επίσης είναι το **κόστος**, καθώς και ο **χρονικός ορίζοντας** υλοποίησης της εκάστοτε λύσης. Οι παραπάνω συντελεστές, αποτελούν κριτήρια που θα επηρεάσουν την επιλογή των υπευθύνων. Οι αποφασίζοντες, στην προσπάθειά τους να εκτιμήσουν τα κριτήρια και την ικανοποίησή τους, συχνά οδηγούνται σε αντικρουόμενα αποτελέσματα. Για παράδειγμα, θα μπορούσε η στρατηγική που ελαχιστοποιεί το ρίσκο, να είναι εκείνη που μεγιστοποιεί το κόστος. Έτσι προκύπτει η αναγκαιότητα σύνθεσης των κριτηρίων με **Πολυκριτηριακή Ανάλυση Αποφάσεων**.

Η ταξινόμηση των εναλλακτικών γίνεται μέσω της εφαρμογής της πολυκριτηριακής μεθόδου **MAUT**, η θεωρία της οποίας παρατίθεται στο Κεφάλαιο 2. Στη συνέχεια, οι υπεύθυνοι του ιατρείου αποδίδουν χρησιμότητες στα σενάρια που αφορούν τον βαθμό επίτευξης των στόχων, θέτοντας χρησιμότητα 1 στο προτιμότερο σενάριο, και 0 στο λιγότερο προτιμητέο. Στα υπόλοιπα σενάρια ανατίθενται τιμές μεταξύ του 0 και του 1, συνεπείς όμως προς την ήδη υπάρχουσα ταξινόμηση. Στο επόμενο και τελικό βήμα ανατίθενται χρησιμότητες στα εναλλακτικά μέτρα αντιμετώπισης και επιλέγεται αυτό που εγγυάται τα καλύτερα αποτελέσματα.



Σχήμα 5.11: *UC1: Αξιολόγηση Κινδύνου*

5.2 Περίπτωση Χρήσης 2 : Υποκλοπή δεδομένων ασθενών μέσω Keylogging hardware

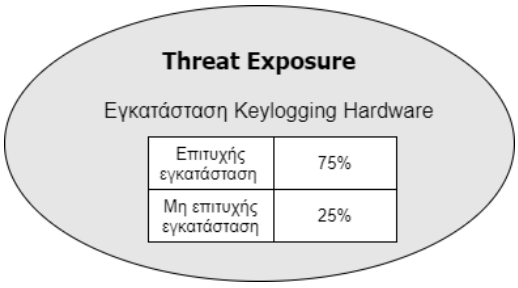
Στο Σχήμα 5.12 φαίνονται τα χαρακτηριστικά του σεναρίου χρήσης:

Εύρος (Scope)	
Εύρος επίδρασης (Application Scenario)	**Φυσική αλληλεπίδραση με IT assets**
Επίθεση (Attack)	
Τύπος Απειλής (Threat Type)	**Ανταγωνιστική/ Κακόβουλη- Malware**
Πηγή/Υποκείμενο Απειλής (Threat Actor)	**Κακόβουλος εξωτερικός χρήστης**
Στόχευση Επίθεσης (Attack Vector)	**Physical and technical security**
Κρίσιμα Στοιχεία του τομέα Υγείας (Critical Healthcare Assets)	
Στοιχεία που επηρεάζονται (Affected assets)	**Ιατρικά δεδομένα**
Κρισιμότητα στοιχείων που επηρεάζονται (Criticality of affected assets)	**Πολύ κρίσιμα**

Σχήμα 5.12: *UC2: Περιγραφή Χαρακτηριστικών Σεναρίου*

1.Κόμβος έκθεσης σε απειλή (Threat exposure Node) :

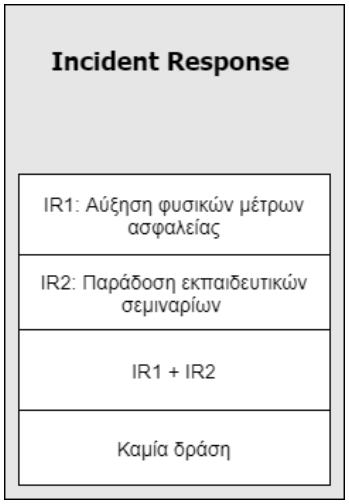
Στο χώρο υποδοχής του ιατρείου βρίσκεται το γραφείο της γραμματέως. Ο δράστης Χ, κλείνει ραντεβού για να κάνει εξετάσεις στο ιατρείο. Καταφθάνει στο ιατρείο αρκετά νωρίτερα και περιμένει να φύγει η γραμματέας για λίγο από το χώρο. Όταν αυτό συμβαίνει, ο δράστης βρίσκει ευκαιρία να τοποθετήσει στον υπολογιστή της, Keylogging Hardware. Όπως αναφέρθηκε στην παράγραφο 2.2.3,το Keylogging Hardware υπάγεται στην ευρύτερη κατηγορία των κατασκοπευτικών προγραμμάτων (spyware). Πρόκειται για μια δυσδιάκριτη συσκευή που αποθηκεύει όλους τους χαρακτήρες που πληκτρολογούνται και δεν ανιχνεύεται από το λογισμικό. Ο δράστης επιστρέφει κάποιες μέρες αργότερα στο ιατρείο για να πάρει τα αποτελέσματα και με την ίδια τεχνική παίρνει και τη συσκευή. Μέσω των πληκτρολογημένων χαρακτήρων καταφέρνει να βρει τα credentials (usernames passwords) και μπαίνει στο ηλεκτρονικό σύστημα του ιατρείου, έχοντας πρόσβαση σε δεδομένα ασθενών, τραπεζικές συναλλαγές του ιατρείου κ.α.



Σχήμα 5.13: *UC2: Έκθεση σε Απειλή*

2.Κόμβος μέτρων αντιμετώπισης απειλών (Incident Response Node) :

Όπως ήδη αναφέρθηκε στην παράγραφο 2.2.3, μια συσκευή keylogger δεν είναι ανιχνεύσιμη από κανένα λογισμικό καθώς είναι έτσι φτιαγμένη ώστε να μην εξαρτάται από το λειτουργικό σύστημα του υπολογιστή και να μην αλληλεπιδρά με τα προγράμματά του.



Σχήμα 5.14: *UC2: Μέτρα Αντιμετώπισης Απειλής*

Αυτό σημαίνει ότι δεν μπορούμε να επωφεληθούμε από τεχνικά μέτρα ασφαλείας για την προστασία των δεδομένων από την απειλή της συγκεκριμένης επίθεσης. Οι εναλλακτικές δράσεις στις οποίες κατέληξαν οι υπεύθυνοι είναι δύο, και ανήκουν στην κατηγορία μέτρων για τον περιορισμό γενικά των κινδύνων από επιθέσεις φυσικής παρουσίας.

- Συνεχής επίβλεψη των επαγγελματικών χώρων, κυρίως του χώρου αναμονής, είτε έπειτα από συνεννόηση των εργαζομένων ώστε να μην μένει ο χώρος χωρίς φύλαξη, είτε με την πρόσληψη ειδικού φρουρού (security).

- Σεμινάρια ενημέρωσης του προσωπικού ώστε να ενισχυθεί η φυσική και τεχνική ασφάλεια. Πιο συγκεκριμένα, ένας ενημερωμένος υπάλληλος θα μπορούσε πολύ εύκολα να αντιληφθεί την ύπαρξη του keylogger που τοποθετείται μεταξύ πληκτρολογίου και υπολογιστή.

3.Κόμβος πραγματοποίησης κινδύνου (Incident Materialisation Node) :

Έχοντας εγκαταστήσει το Keylogging Hardware, ο δράστης δεν μπορεί να αποκτήσει έλεγχο του υπολογιστή, αποκτά όμως πρόσβαση σε σημαντικές πληροφορίες. Λαμβάνοντας υπόψη τα μέτρα αντίδρασης, και το γεγονός ότι δεν υπάρχουν τεχνικά τείχη προστασίας από την συγκεκριμένη απειλή, προκύπτουν 3 διακριτά σενάρια.

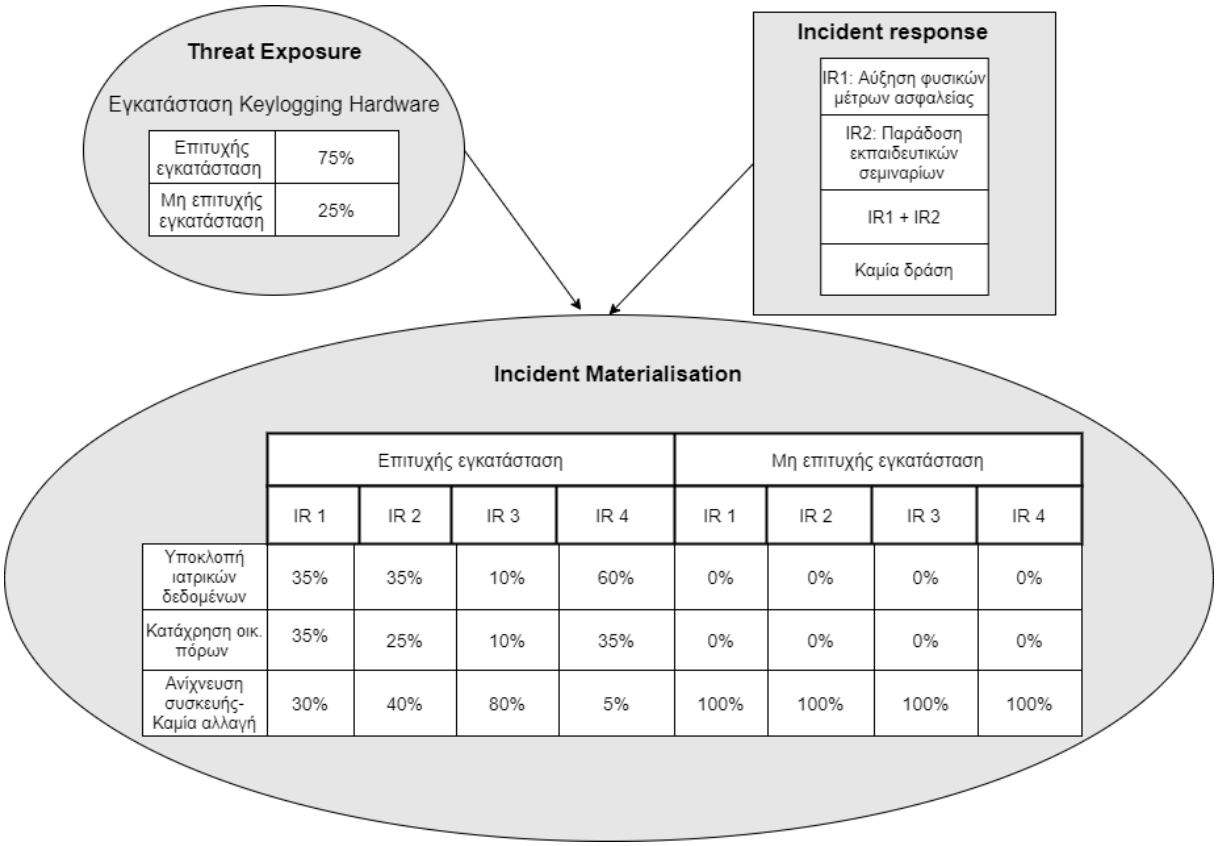
- Υποκλοπή ιατρικών δεδομένων.

- Κατάχρηση οικονομικών πόρων μέσω απόκτησης πρόσβασης σε τραπεζικούς λογαριασμούς.

- Ανίχνευση συσκευής / καμία αλλαγή στην ακεραιότητα των δεδομένων.

Στο σημείο αυτό αξίζει να σημειωθεί ότι με τη χρήση Keylogging Software αντί Hardware, ο δράστης θα μπορούσε πάλι να υποκλέψει ευαίσθητες πληροφορίες, και οι συνέπειες της πραγματοποίησης της απειλής θα ήταν οι ίδιες. Αυτό που θα άλλαζε θα ήταν τα μέτρα αντιμετώπισης για την αποφυγή του κινδύνου, καθώς το keylogging λογισμικό μπορεί να ανιχνευθεί και να αφαιρεθεί από anti-spyware λογισμικό. Η επιλογή του σεναρίου αυτού έγινε για να υποδείξει ότι η ασφάλεια των πληροφοριών δεν επιτυγχάνεται μόνο με τεχνικές αλλά και φυσικές μεθόδους.

Τα σενάρια αυτά μαζί με τις πιθανότητες πραγματοποίησής τους παρουσιάζονται στο Σχήμα 5.15.



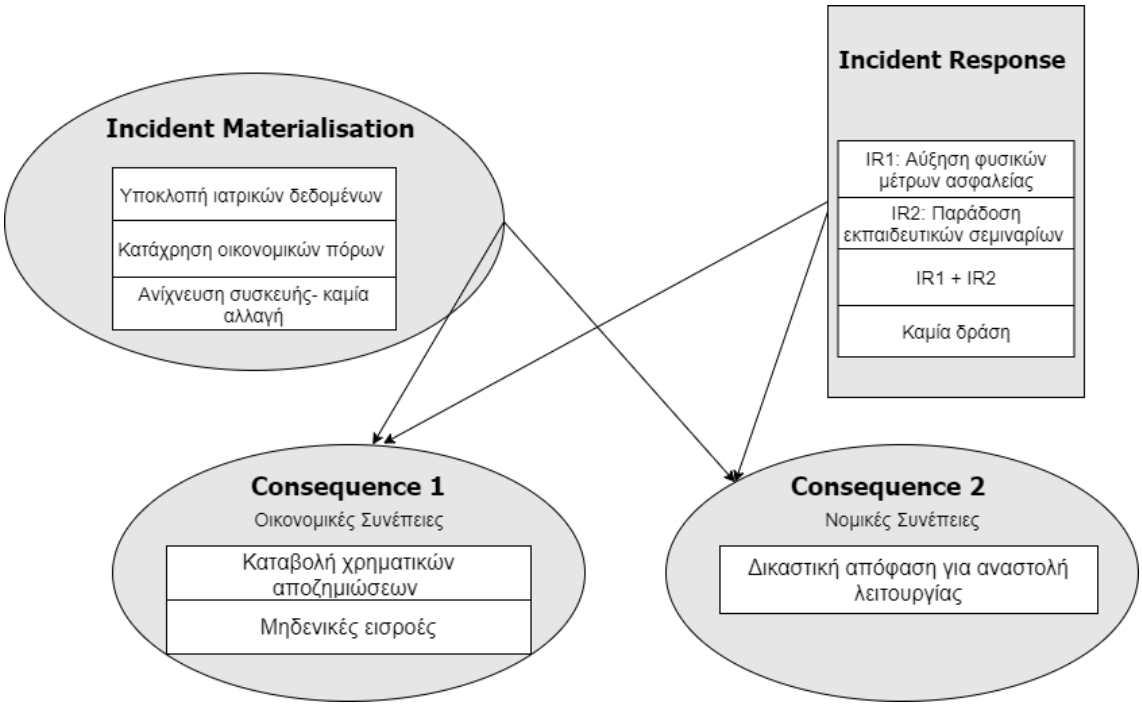
Σχήμα 5.15: *UC2: Πραγματοποίηση Κινδύνου*

4.Κόμβος Συνεπειών στο Σύστημα υπό Διαχείριση (Consequences in the Managed System Node) :

Εξαιτίας της υποκλοπής, πολλοί από τους ασθενείς του ιατρείου κατέθεσαν μήνυση εναντίον του, για παραβίαση προσωπικών δεδομένων. Αυτό είχε ως αποτέλεσμα, να ανασταλεί προσωρινά η λειτουργία του ιατρείου, λόγω ασυνέπειας στην εκπλήρωση των νομικών υποχρεώσεών του, δηλαδή της διαφύλαξης του απορρήτου των προσωπικών πληροφοριών. Οι συνέπειες λοιπόν της πραγματοποιημένης επίθεσης είναι :

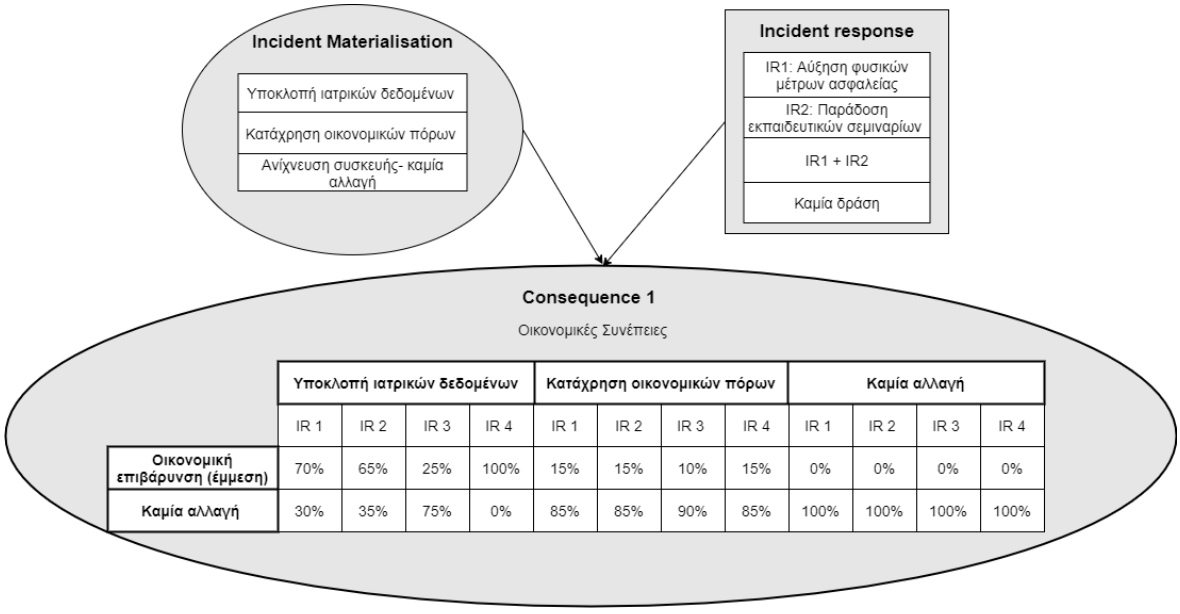
- Προσωρινή αναστολή της λειτουργίας του ιατρείου σύμφωνα με δικαστική απόφαση,
- Καταβολή χρηματικών αποζημιώσεων στους ασθενείς,
- Μηδενικές εισροές εξαιτίας της παύσης λειτουργίας.

Οι δύο τελευταίες συνέπειες είναι μεταξύ τους ανεξάρτητες, αλλά αφορούν και οι δύο στην οικονομική κατάσταση του ιατρείου. Θα μπορούσαν να μοντελοποιηθούν σε ξεχωριστά διαγράμματα, αντίστοιχα με την Περίπτωση Χρήσης 1, αλλά οι επιμέρους επιπτώσεις αθροίζονται εφόσον αφορούν το ίδιο στοιχείο του ιατρείου, τα οικονομικά του. Αυτό υποδεικνύει ότι το μοντέλο που εφαρμόζουμε είναι **αθροιστικό** ως προς τις συνέπειες του κινδύνου, όπως αυτό παρουσιάζεται και στο Κεφάλαιο 2, στο Σχήμα 2.8. Οι νομικές συνέπειες ως ανεξάρτητες με τις οικονομικές σχεδιάζονται σε ξεχωριστό κόμβο, όπως φαίνεται στο Σχήμα 5.16.



Σχήμα 5.16: *UC2:Συνέπειες στο Σύστημα*

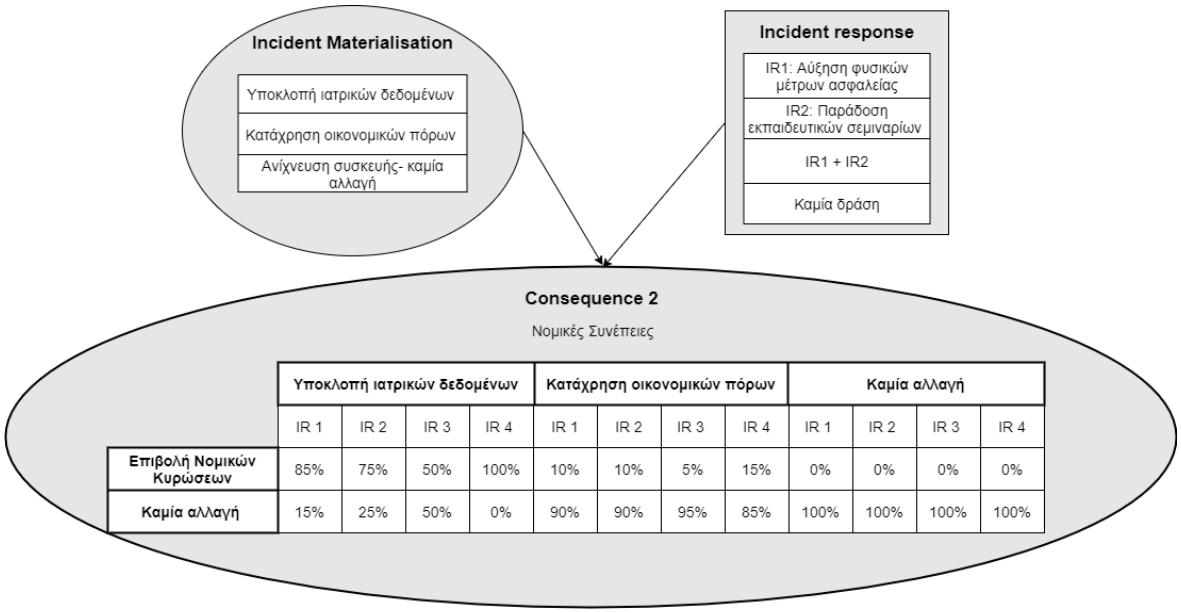
Πιο συγκεκριμένα, οι οικονομικές συνέπειες που προκαλούνται έμμεσα (το διάγραμμα δεν αφορά το χρηματικό ποσό που μπορεί να κλέψει ο δράστης, αλλά την οικονομική επιβάρυνση που συνεπάγεται η επίθεση) από την πιθανότητα πραγματοποίησης της απειλής μοντελοποιούνται όπως φαίνεται στο Σχήμα 5.17 :



	Υποκλοπή ιατρικών δεδομένων				Κατάχρηση οικονομικών πόρων				Καμία αλλαγή			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Οικονομική επιβάρυνση (έμμεση)	70%	65%	25%	100%	15%	15%	10%	15%	0%	0%	0%	0%
Καμία αλλαγή	30%	35%	75%	0%	85%	85%	90%	85%	100%	100%	100%	100%

Σχήμα 5.17: *UC2:Οικονομικές Συνέπειες στο Σύστημα*

Αντίστοιχα, οι νομικές συνέπειες μοντελοποιούνται σύμφωνα με το Σχήμα 5.18 :



	Υποκλοπή ιατρικών δεδομένων				Κατάχρηση οικονομικών πόρων				Καμία αλλαγή			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Επιβολή Νομικών Κυρώσεων	85%	75%	50%	100%	10%	10%	5%	15%	0%	0%	0%	0%
Καμία αλλαγή	15%	25%	50%	0%	90%	90%	95%	85%	100%	100%	100%	100%

Σχήμα 5.18: *UC2:Νομικές Συνέπειες στο Σύστημα*

5.Κόμβος Στοιχείων υπό προστασία (Asset status Node) :

Τα στοιχεία υπό προστασία, εξαρτώνται μόνο από τις προτεραιότητες που έχει θέσει ένας οργανισμός, καθορίζονται στα αρχικά στάδια και δεν αλλάζουν για τα διαφορετικά σενάρια κινδύνου. Οπότε σε πλήρη αναλογία με την προηγούμενη περίπτωση χρήσης, αυτά που επιδιώκουν οι αποφασίζοντες είναι :

- Η συνεχής λειτουργία ιατρείου.
- Η διατήρηση καλής φήμης.

6.Κόμβος Επίπτωσης στα Στοιχεία υπό προστασία (Asset status Node) :

Συνέπειες της επίθεσης στη φήμη του ιατρείου

Η φήμη του ιατρείου εξαρτάται από την προστασία των προσωπικών δεδομένων των ασθενών και την ακεραιότητα αυτών. Σε περίπτωση που πραγματοποιηθεί επιτυχημένη επίθεση κατά του ιατρείου, η φήμη του θα επηρεαστεί αρνητικά σε τέτοιο βαθμό που ίσως είναι δύσκολο να αποκατασταθεί.

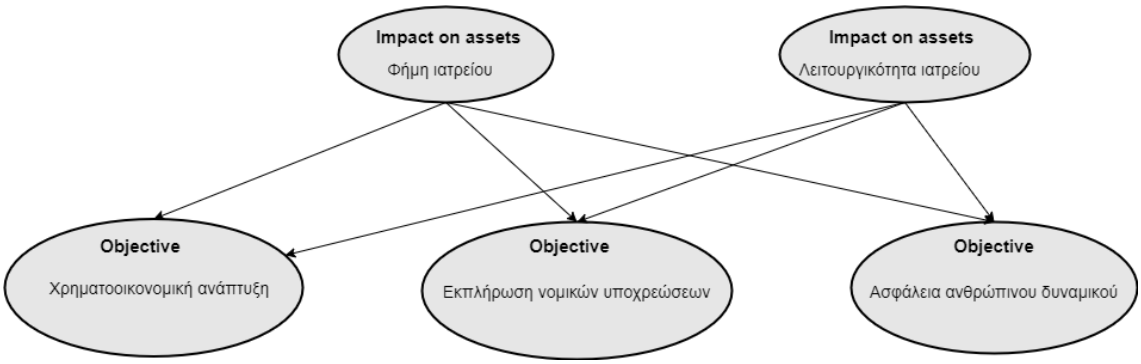
Συνέπειες της επίθεσης στη λειτουργία του ιατρείου

Εάν πραγματοποιηθεί η επίθεση και κλαπούν τα προσωπικά δεδομένα ασθενών, απειλείται η συνέχιση λειτουργίας του ιατρείου. Σε περίπτωση που οι ασθενείς καταθέσουν μηνύσεις εναντίον του, είναι πιθανή η νομική επιβολή της αναστολής λειτουργίας για ένα διάστημα. Ακόμη και αν αυτό δεν συμβεί, οι υπεύθυνοι του ιατρείου θα χρειαστούν κάποιες μέρες για να αναδιοργανώσουν το προσωπικό και τα πληροφοριακά συστήματα, κατά τη διάρκεια των οποίων το ιατρείο δεν θα είναι ανοιχτό.

7.Κόμβος Στόχων (Objective Node) :

Οι στόχοι του ιατρείου είναι αυτοί που παρουσιάστηκαν στην Περίπτωση Χρήσης 1:

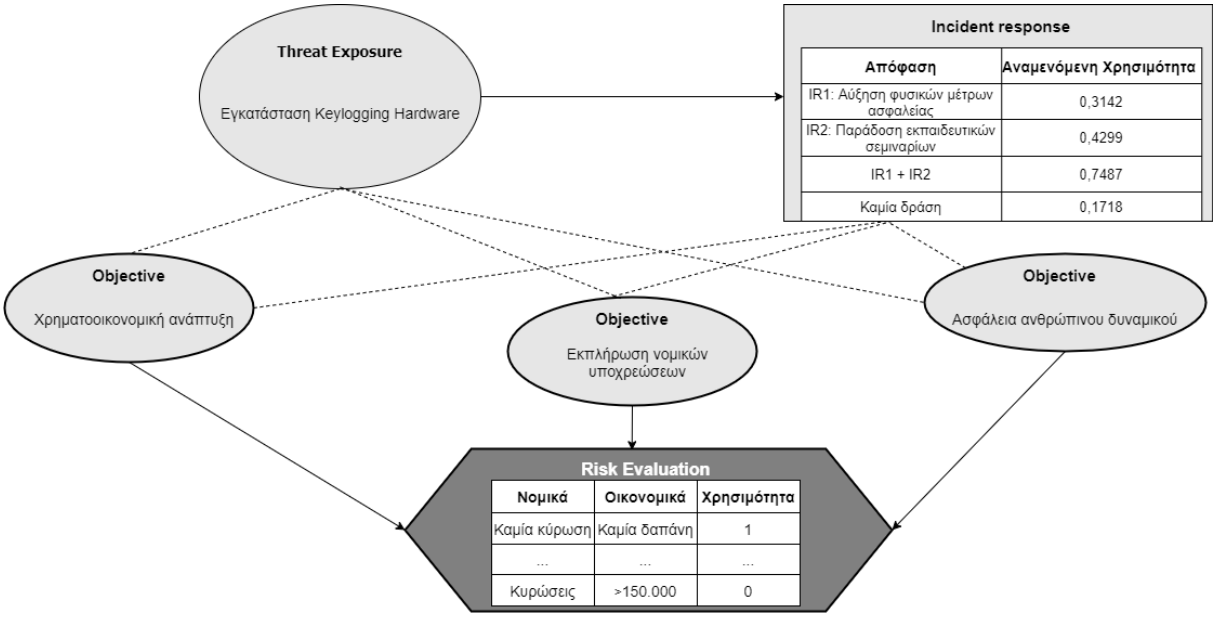
- Η ασφάλεια και η υγεία του ανθρώπινου δυναμικού (ασθενείς και προσωπικό)
- Η χρηματοοικονομική ανάπτυξη
- Η εκπλήρωση των νομικών υποχρεώσεων



Σχήμα 5.19: *UC2: Στόχοι*

8.Κόμβος Αξιολόγησης Κινδύνου (Risk Evaluation Node) :

Με την ολοκλήρωση της διαδικασίας, οι αποφασίζοντες έχουν σκιαγραφήσει το περιβάλλον του προβλήματος απόφασης. Στην ουσία έχουν αποτιμήσει την πιθανότητα υλοποίησης της συγκεκριμένης επίθεσης σε σχέση με τις δυσκολίες που αυτή θα εισάγει στην προσπάθεια επίτευξης των τελικών στόχων. Με την υλοποίηση μίας μεθόδου πολυκριτήριας ανάλυσης, (έστω MAUT), είναι σε θέση να επιλέξουν την εναλλακτική εκείνη για την οποία μεγιστοποιείται η αναμενόμενη χρησιμότητα.



Σχήμα 5.20: *UC2: Αξιολόγηση Κινδύνου*

5.3 Περίπτωση Χρήσης 3 : Εγκατάσταση κακόβουλου λογισμικού (malware) στους υπολογιστές του ιατρείου

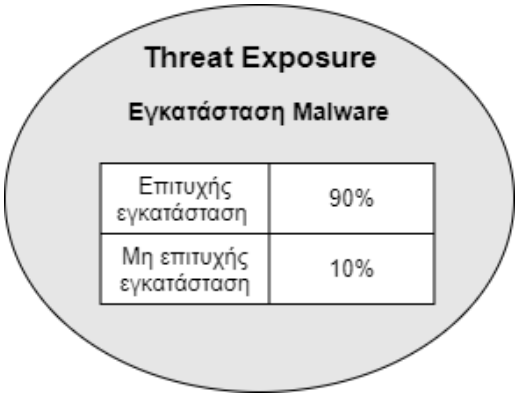
Στο Σχήμα 5.21 φαίνονται τα χαρακτηριστικά του σεναρίου χρήσης:

Εύρος (Scope)	
Εύρος επίδρασης (Application Scenario)	**Τεχνική αλληλεπίδραση με IT assets**
Επίθεση (Attack)	
Τύπος Απειλής (Threat Type)	**Ανταγωνιστική/ Κακόβουλη- Malware**
Πηγή/Υποκείμενο Απειλής (Threat Actor)	**Κακόβουλος εξωτερικός χρήστης**
Στόχευση Επίθεσης (Attack Vector)	**Technical security**
Κρίσιμα Στοιχεία του τομέα Υγείας (Critical Healthcare Assets)	
Στοιχεία που επηρεάζονται (Affected assets)	**Ιατρικά δεδομένα**
Κρισιμότητα στοιχείων που επηρεάζονται (Criticality of affected assets)	**Πολύ κρίσιμα**

Σχήμα 5.21: *UC3: Περιγραφή Χαρακτηριστικών Σεναρίου*

1.Κόμβος έκθεσης σε απειλή (Threat exposure Node) :

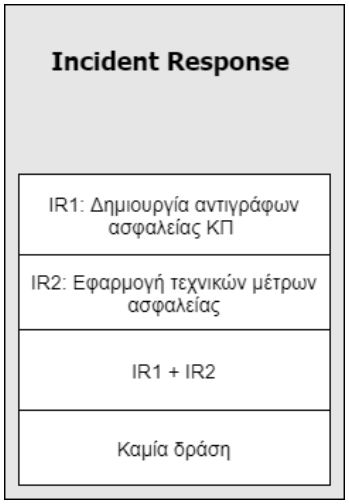
Σε αυτό το σενάριο, ο δράστης προσλαμβάνεται από μία τρομοκρατική οργάνωση για να επιτεθεί, μεταξύ άλλων, και στο ιατρείο υπό διαχείριση. Ο δράστης στέλνει εκατοντάδες e-mail με κακόβουλο λογισμικό (rootkit malware), σε διάφορα κέντρα υγείας και ιατρεία. Ένας γιατρός, ανοίγει το e-mail το οποίο εγκαθιστά στον υπολογιστή του το κακόβουλο λογισμικό. Αν και ο υπολογιστής έχει εγκατεστημένο antivirus λογισμικό, αυτό δεν κατάφερε να ανιχνεύσει και συνεπώς να μπλοκάρει το rootkit malware, εξαιτίας των εξελιγμένων του χαρακτηριστικών (χαμηλό φορτίο CPU και σπάνια ανεβάζει δεδομένα). Έτσι ο δράστης, μπορεί να παρακολουθεί και να ελέγχει τον συγκεκριμένο υπολογιστή, έχοντας πρόσβαση σε ευαίσθητα δεδομένα του ιατρείου και των ασθενών.



Σχήμα 5.22: *UC3: Έκθεση σε Απειλή*

2.Κόμβος μέτρων αντιμετώπισης απειλών (Incident Response Node) :

Όπως ήδη αναφέρθηκε στην παράγραφο 2.2.3, το κακόβουλο λογισμικό (malware) είναι ένας από τους σημαντικότερους κινδύνους που αντιμετωπίζεται στον ψηφιακό κόσμο.



Σχήμα 5.23: *UC3: Μέτρα Αντιμετώπισης Απειλής*

Οι υπεύθυνοι του ιατρείου ξέρουν ότι είναι αδύνατο να θωρακίσουν σε απόλυτο βαθμό τα πληροφοριακά τους συστήματα ενάντια στις απειλές, παρόλα αυτά έχουν καταλήξει σε ένα πλάνο δράσεων που καθιστά τα συστήματα σε μεγάλο βαθμό ¨κυβερνο-ασφαλή¨ :

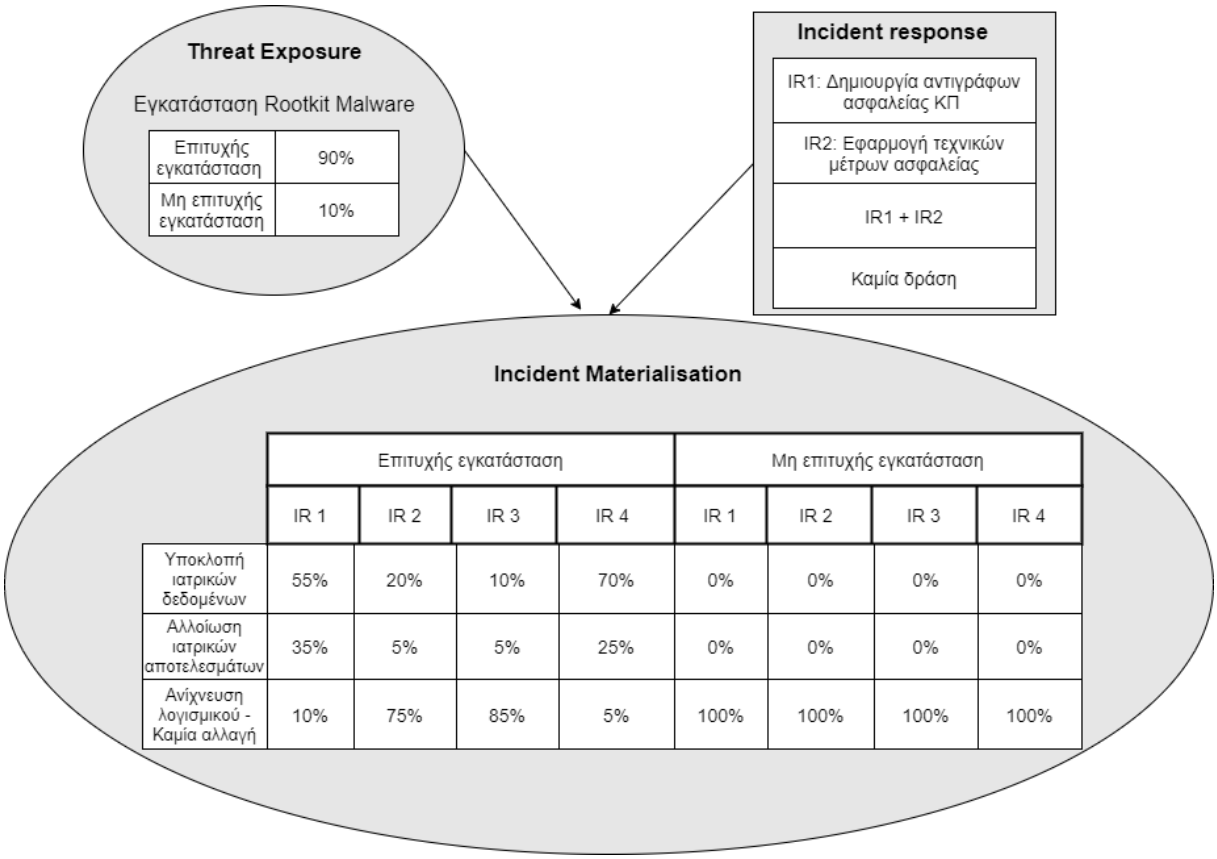
- Συστηματική δημιουργία αντιγράφων ασφαλείας κρίσιμων πληροφοριών (σε εξωτερικές συσκευές, υπηρεσίες cloud κ.α.).
- Εφαρμογή τεχνικών μέτρων ασφαλείας, συγκεκριμένα :
  * Χρήση Firewall, είτε σε μορφή hardware συσκευής, είτε προγράμματος λογισμικού, το οποίο αποκλείει τη μη εξουσιοδοτημένη αποστολή δεδομένων προς τον υπολογιστή (βέβαια δεν μπορεί να τον προστατέψει εάν ο ίδιος ο χρήστης ζητήσει δεδομένα από κακόβουλη πηγή).
  * Συστηματική ενημέρωση για καινούρια software patches και εγκατάστασή τους.
  * Εγκατάσταση antimalware λογισμικού.

3.Κόμβος πραγματοποίησης κινδύνου (Incident Materialisation Node) :

Με την εγκατάσταση του rootkit malware, ο δράστης έχει τον έλεγχο του υπολογιστή και αποκτά πρόσβαση σε απόρρητες πληροφορίες. Λαμβάνοντας υπόψη τους πιθανούς τρόπους αντίδρασης, προκύπτουν 3 διακριτά σενάρια σχετικά με την πραγματοποίηση της απειλής :

- Υποκλοπή ιατρικών δεδομένων: Ο δράστης έχει πρόσβαση σε ευαίσθητες πληροφορίες ασθενών, τις οποίες μπορεί να επεξεργαστεί και να χρησιμοποιήσει με κακόβουλα κίνητρα.
- Αλλοίωση ιατρικών αποτελεσμάτων: Σε αντίθεση με το προηγούμενο σενάριο χρήσης, ο δράστης μέσω του εγκατεστημένου rootkit malware, έχει τον έλεγχο του υπολογιστή του γιατρού, που σημαίνει ότι μπορεί να παραποιήσει εξετάσεις ασθενών είτε για να βλάψει απευθείας τους ίδιους, είτε την φήμη του ιατρείου.
- Ανίχνευση λογισμικού / καμία αλλαγή στην ακεραιότητα των δεδομένων.

Τα σενάρια αυτά μαζί με τις πιθανότητες πραγματοποίησής τους παρουσιάζονται στο Σχήμα 5.24.



Σχήμα 5.24: *UC3: Πραγματοποίηση Κινδύνου*

4.Κόμβος Συνεπειών στο Σύστημα υπό Διαχείριση (Consequences in the Managed System Node) :

Οι συνέπειες στο σύστημα λόγω της πραγματοποιημένης επίθεσης είναι :

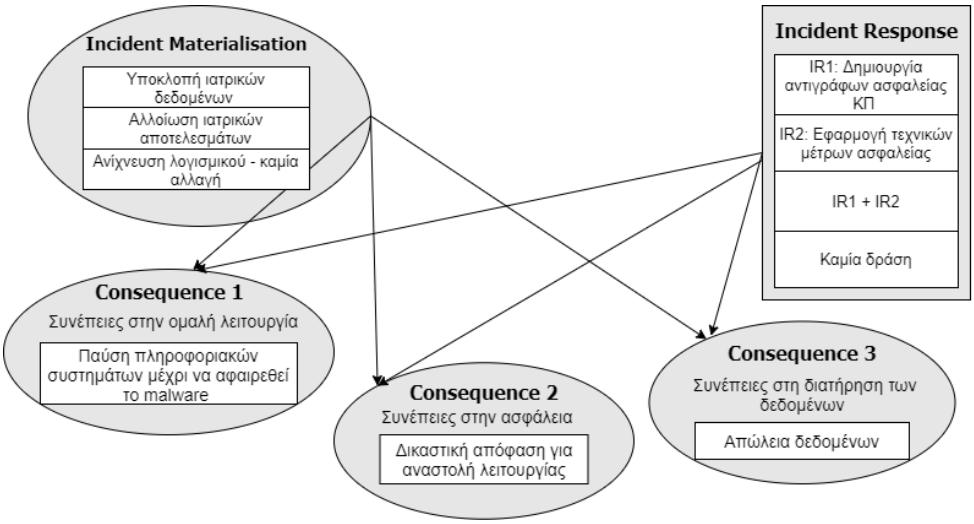
- προσωρινή παύση των πληροφοριακών συστημάτων του ιατρείου μέχρι να απομακρυνθεί το κακόβουλο λογισμικό, που πιθανώς συνεπάγεται και την παύση λειτουργίας του μέχρι να ολοκληρωθούν οι ενέργειες.

- απώλεια δεδομένων των ασθενών.

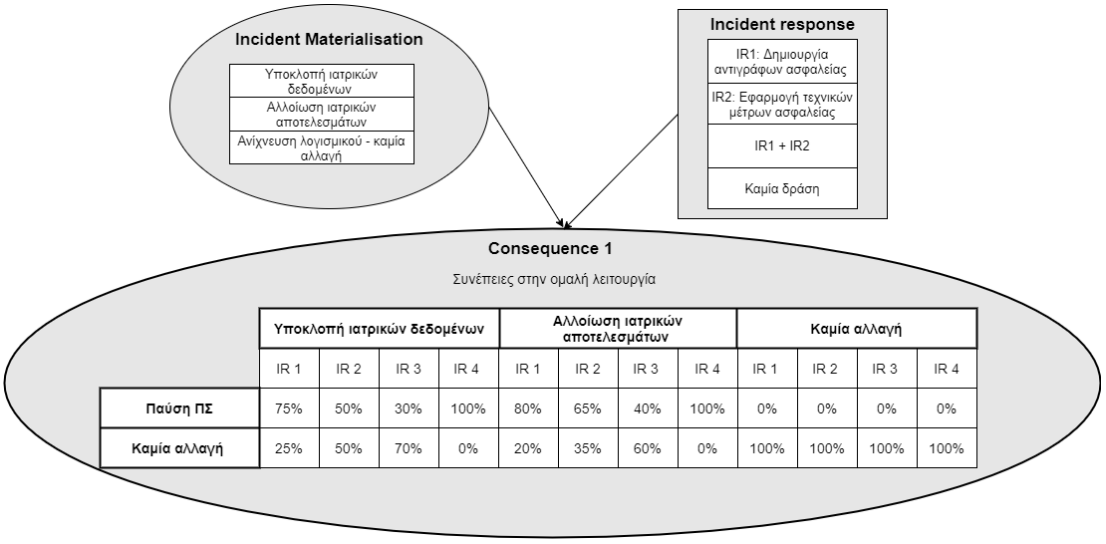
- βλάβη ασθενή εξαιτίας λανθασμένης διάγνωσης.

Οι συνέπειες αυτές είναι μεταξύ τους ανεξάρτητες, επομένως μοντελοποιούνται σε ξεχωριστούς κόμβους, όπως φαίνεται στο Σχήμα 5.25.

Στο σχήμα 5.26, 5.27 και 5.28 αντίστοιχα, γίνεται ανάλυση των συνεπειών που αφορούν στην αναστολή της λειτουργίας των πληροφοριακών συστημάτων, στην απώλεια δεδομένων και στην διακινδύνευση της ασφάλειας των ασθενών αντίστοιχα.

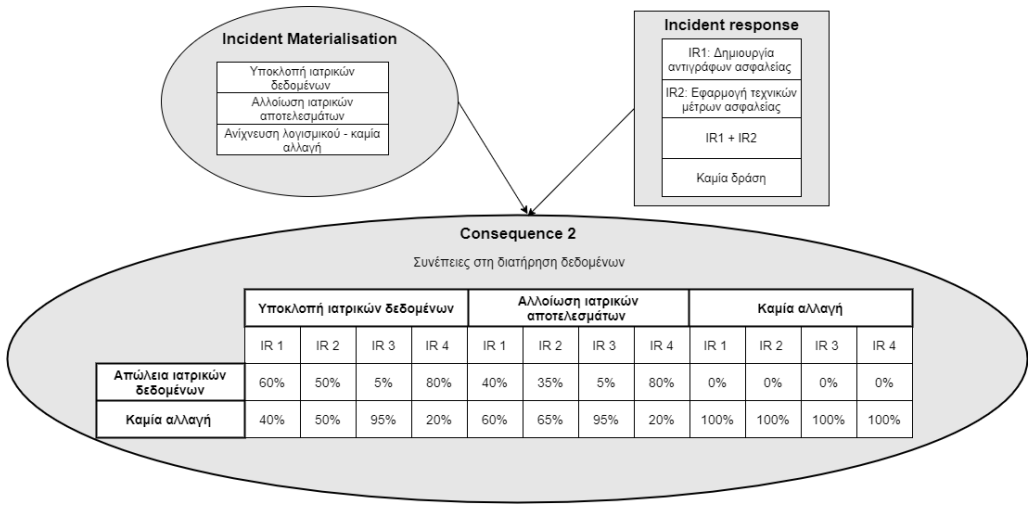


Σχήμα 5.25: *UC3:Συνέπειες στο Σύστημα*



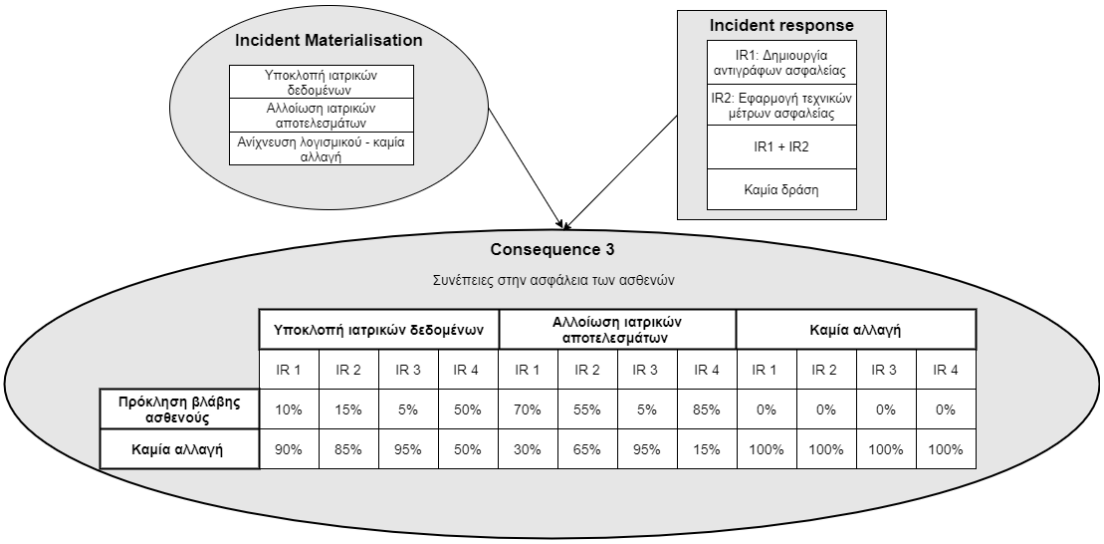
	Υποκλοπή ιατρικών δεδομένων				Αλλοίωση ιατρικών αποτελεσμάτων				Καμία αλλαγή			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Παύση ΠΣ	75%	50%	30%	100%	80%	65%	40%	100%	0%	0%	0%	0%
Καμία αλλαγή	25%	50%	70%	0%	20%	35%	60%	0%	100%	100%	100%	100%

Σχήμα 5.26: *UC3: Προσωρινή παύση πληροφοριακών συστημάτων*



	Υποκλοπή ιατρικών δεδομένων				Αλλοίωση ιατρικών αποτελεσμάτων				Καμία αλλαγή			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Απώλεια ιατρικών δεδομένων	60%	50%	5%	80%	40%	35%	5%	80%	0%	0%	0%	0%
Καμία αλλαγή	40%	50%	95%	20%	60%	65%	95%	20%	100%	100%	100%	100%

Σχήμα 5.27: *UC3: Απώλεια δεδομένων*



	Υποκλοπή ιατρικών δεδομένων				Αλλοίωση ιατρικών αποτελεσμάτων				Καμία αλλαγή			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Πρόκληση βλάβης ασθενούς	10%	15%	5%	50%	70%	55%	5%	85%	0%	0%	0%	0%
Καμία αλλαγή	90%	85%	95%	50%	30%	65%	95%	15%	100%	100%	100%	100%

Σχήμα 5.28: *UC3: Διακινδύνευση ασφάλειας ασθενών*

5.Κόμβος Στοιχείων υπό προστασία (Asset status Node) :

Τα στοιχεία υπό προστασία, εξαρτώνται μόνο από τις προτεραιότητες που έχει θέσει ένας οργανισμός, καθορίζονται στα αρχικά στάδια και δεν αλλάζουν για τα διαφορετικά σενάρια κινδύνου. Οπότε σε πλήρη αναλογία με την προηγούμενη περίπτωση χρήσης, αυτά που επιδιώκουν οι αποφασίζοντες είναι :

- Η συνεχής λειτουργία ιατρείου.
- Η διατήρηση καλής φήμης.

6.Κόμβος Επίπτωσης στα Στοιχεία υπό προστασία (Asset status Node) :

Συνέπειες της επίθεσης στη φήμη του ιατρείου

Η φήμη του ιατρείου μπορεί να επηρεαστεί ανεπανόρθωτα από την πραγματοποίηση της επίθεσης, εξαιτίας της αδυναμίας να προστατεύσει τα δεδομένα και την κατάσταση των ασθενών.

Συνέπειες της επίθεσης στη λειτουργία του ιατρείου

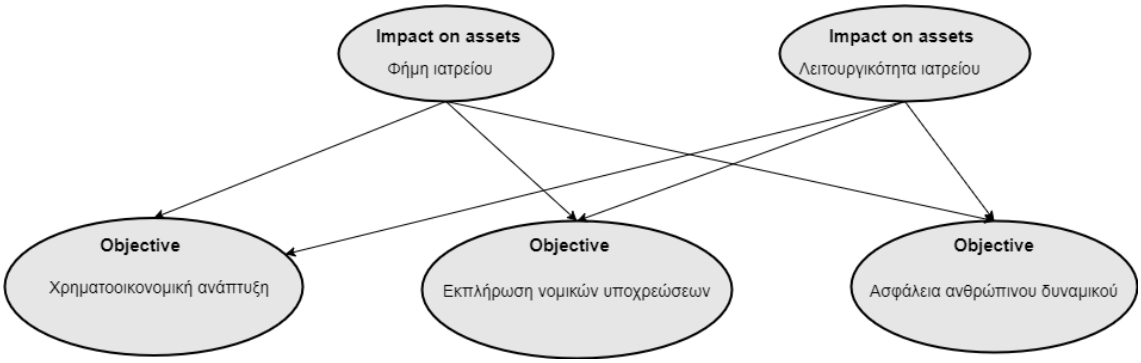
Η εγκατάσταση του κακόβουλου λογισμικού, αφού γίνει αντιληπτή, πρέπει να αντιμετωπιστεί με τη χρήση ειδικών προγραμμάτων ασφαλείας που θα αφαιρέσουν το malware. Για να γίνει αυτό, ίσως χρειαστεί να τεθεί σε παύση η λειτουργία των υπολογιστών και των υπολοίπων μηχανημάτων του ιατρείου, γεγονός που καθιστά το ιατρείο μη λειτουργικό.

7.Κόμβος Στόχων (Objective Node) :

Οι στόχοι του ιατρείου είναι αυτοί που παρουσιάστηκαν στην Περίπτωση Χρήσης 1:

- Η ασφάλεια και η υγεία του ανθρώπινου δυναμικού (ασθενείς και προσωπικό)
- Η χρηματοοικονομική ανάπτυξη

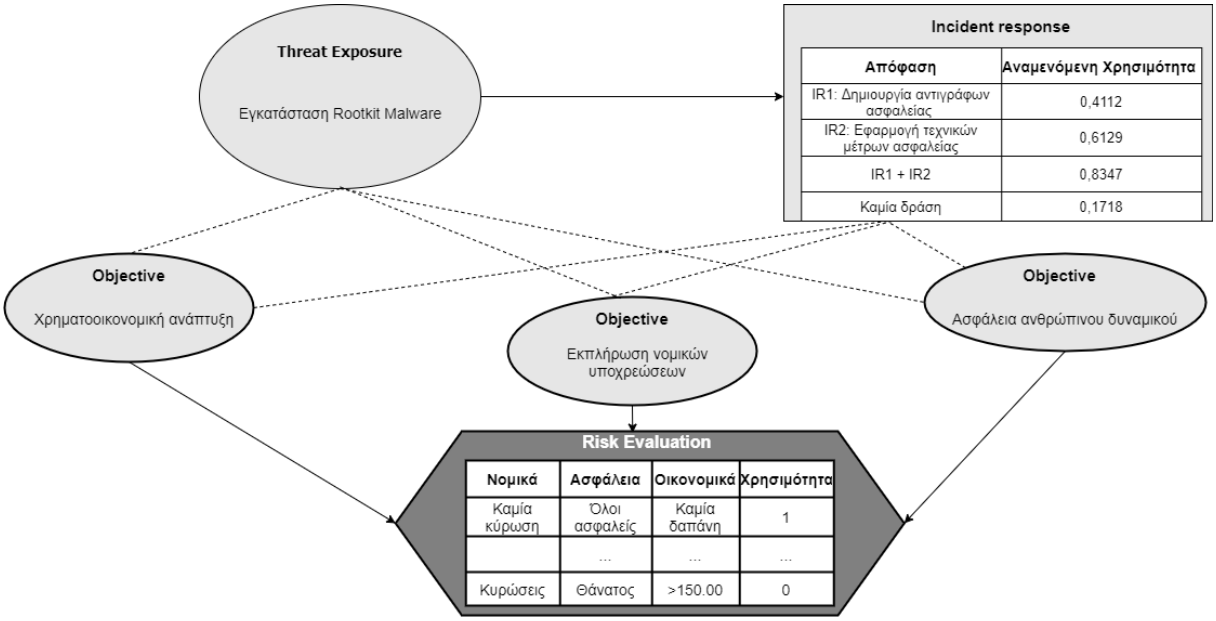
- Η εκπλήρωση των νομικών υποχρεώσεων



Σχήμα 5.29: *UC3: Στόχοι*

8.Κόμβος Αξιολόγησης Κινδύνου (Risk Evaluation Node) :

Με την ολοκλήρωση της διαδικασίας, οι αποφασίζοντες είναι σε θέση να επιλέξουν την εναλλακτική εκείνη για την οποία μεγιστοποιείται η αναμενόμενη χρησιμότητα, όπως φαίνεται στο Σχήμα 5.30



Σχήμα 5.30: *UC3: Αξιολόγηση Κινδύνου*

Μέρος III

Επίλογος

Κεφάλαιο 6

Συμπεράσματα

Σκοπός της παρούσας εργασίας ήταν η μελέτη των κλάδων **Διαχείρισης** και **Εκτίμησης Ρίσκου**, η αναγνώριση των παραγόντων που επιβάλλουν την **εφαρμογή του σε μονάδες του Συστήματος Υγείας** και η **μοντελοποίηση σεναρίων ρίσκου** σε αυτές με χρήση του μοντέλου GIRA. Τα παραδείγματα σεναρίων ρίσκου χρησιμοποιούνται για να υποδείξουν στους αποφασίζοντες, με ποιό τρόπο η αναγνώριση και ο υπολογισμός των πιθανών επιπτώσεων που προκύπτουν από την πραγματοποίηση μίας ενδεχόμενης απειλής, λειτουργούν ως εργαλείο για να ενισχυθούν τα αδύναμα σημεία του οργανισμού.

Στην παρούσα εργασία μελετήθηκαν τα διαφορετικά χαρακτηριστικά του κινδύνου και προτάθηκαν διαφορετικές ταξινομήσεις και τεχνικές εκτίμησης αυτού, που επιλέγονται από τους οργανισμούς με βάση τις ιδιότητες των διαθέσιμων δεδομένων και το επιθυμητό επίπεδο λεπτομέρειας της ανάλυσης . Οι οργανισμοί πλέον, καλούνται να προσαρμοστούν στην ιδιάζουσα πολυπλοκότητα ώστε να είναι σε θέση να αντιμετωπίσουν τις απειλές. Με άλλα λόγια, η αποτελεσματική μείωση της έκθεσης στον κίνδυνο, βασίζεται στην απλοποιημένη αλλά επαρκή αναπαράσταση του περιβάλλοντος μέσα στο οποίο δραστηριοποιούνται, καθώς και την επιλογή των κατάλληλων μεθόδων που επιτρέπουν την απαραίτητη ευελιξία. Ιδιαίτερα όσον αφορά τις **μονάδες του Συστήματος Υγείας**, το οποίο αποτελεί μία από τις Κρίσιμες Υποδομές του κράτους, οι λόγοι που καθιστούν αναγκαία την εδραίωση ενός πλάνου Διαχείρισης Ρίσκου, είναι προφανείς. Συμπληρωματικά όμως, η επιλογή μεθόδων πρέπει να είναι τέτοια ώστε, εκτός από το να μοντελοποιεί ικανοποιητικά τον κίνδυνο, να ικανοποιεί τις γενικές επιδιώξεις του οργανισμού.

Μέσα από την μελέτη και την σύγκριση διαφορετικών μεθόδων, επιλέχθηκε το μοντέλο GIRA. Το μοντέλο αυτό προτείνει το **συνδυασμό** του κλάδου **Διαχείρισης/Εκτίμησης Ρίσκου** με αυτόν την **Πολυκριτήριας Ανάλυσης Αποφάσεων**, με κοινό στόχο την επιτυχημένη δόμηση των προβλημάτων απόφασης που εμπεριέχουν τον παράγοντα του κινδύνου. Συγκεκριμένα :

1. **Επιτυγχάνεται η διεξοδική ανάλυση του περιβάλλοντός του κινδύνου, λαμβάνοντας υπόψην τα πιθανά Incident Responses και όλους τους πιθανούς συνδυασμούς μεταξύ αυτών** : Ο κίνδυνος αναλύεται περαιτέρω, και εξετάζονται οι διαφορετικές εναλλακτικές για την αντιμετώπισή του και το πώς αυτές ελαχιστοποιούν το ρίσκο. Το GIRA παρέχει μία ολιστική αλλά συστηματοποιημένη θεώρηση του περιβάλλοντος του κινδύνου σε αντίθεση με τις υπόλοιπες 3 μεθόδους που μελετήθηκαν γιατί:

- Στην περίπτωση της **μήτρας κινδύνου** και της **Fault Tree Analysis** τα μέτρα αντιμετώπισης του κινδύνου δεν λαμβάνονται υπόψη. Στη μήτρα κινδύνου, το επίπεδο επικινδυνότητας καθορίζεται μονοσήμαντα χωρίς να αποτυπώνονται και να αναλύονται διεξοδικά πληροφορίες που αφορούν ένα συγκεκριμένο πρόβλημα απόφασης. Στην Fault Tree Analysis μελετώνται τα αίτια που προκάλεσαν την εμφάνιση του κινδύνου, αλλά όχι το πώς, από τη στιγμή που εμφανίστηκε, οι συνέπειες του θα μπορούσαν να περιοριστούν.
- Στα **δέντρα αποφάσεων** ενώ λαμβάνονται υπόψη τα διαφορετικά μέτρα αντίδρασης και ο συνδυασμός τους, μοντελοποιούνται τα αρνητικά σενάρια που προκύπτουν ως συνέπειες της πραγματοποίησης του κινδύνου, αλλά όχι οι επιπτώσεις αυτών των σεναρίων εντός και εκτός του συστήματος υπό μελέτη.

2. **Οι εναλλακτικές δεν αξιολογούνται με μόνο κριτήριο την ελαχιστοποίηση του ρίσκου :** Με στόχο να αντανακλά την πραγματικότητα πιο ρεαλιστικά το GIRA model ενσωματώνει στο τέλος της διαδικασίας μία μέθοδο Πολυκριτήριας Ανάλυσης Αποφάσεων, επιτρέποντας έτσι στους αποφασίζοντες να επιλέξουν την εναλλακτική που υπόσχεται ελαχιστοποίηση του κινδύνου ενώ ταυτόχρονα ικανοποιεί και τις γενικές τους επιδιώξεις. Αυτό είναι και το χαρακτηριστικό που το αναδεικνύει ως ι**δανική για τις μονάδες του Συστήματος Υγείας επιλογή**, καθώς κάθε **στρατηγική** που επιλέγεται από αυτές πρέπει να **διασφαλίζει πρωτίστως την ασφάλεια των ασθενών και παράλληλα να πληροί κοινωνικές, νομικές , οικονομικές και περιβαλλοντικές προϋποθέσεις**.

3. **Η μοντελοποίηση του κινδύνου αφορά την τρέχουσα κατάσταση του συστήματος :** Σε αντίθεση με τις παραδοσιακές μεθόδους εκτίμησης ρίσκου, το μοντέλο είναι έτσι σχεδιασμένο (ανήκει στην κατηγορία των δικτύων Bayes, ώστε να παράγει τις σχετικές με τον κίνδυνο πληροφορίες, **κατά τη διάρκεια** του αρνητικού συμβάντος. Όταν προκύπτει η πραγματοποίηση του κινδύνου, δηλαδή όταν η αρχική πιθανότητα έκθεσης στον κίνδυνο γίνει ίση με 1, ενεργοποιείται αυτόματα η διαδικασία υπολογισμού βάσει των ήδη καθορισμένων ¨μονοπατιών¨.

4. **Παρουσιάζει ασθενή εξάρτηση από την παρουσία ειδικών αναλυτών :** Δεδομένου ότι το δίκτυο κόμβων που αναπαριστά το σύστημα σύστημα και οι σχέσεις μεταξύ των κόμβων έχουν ορισθεί, η μοντελοποίηση μίας νέας απειλής που αντιστοιχεί στην ίδια τοπολογία δικτύου γίνεται αυτόματα (το μόνο που πρέπει να ενημερωθεί είναι τα Incident Responses και η πιθανότητα να αντιμετωπίσουν τον κίνδυνο). Ακόμη και η περίπτωση προσθήκης κάποιου νέου κόμβου δεν απαιτεί ιδιαίτερη υπολογιστική πολυπλοκότητα αφού η γενίκευση των σχέσεων, δηλαδή η επέκταση του δικτύου, γίνεται αυτόματα βάσει των ήδη υπαρχουσών. Χάρη σε αυτή την αυτοματοποίηση οι αποφάσεις που καλούνται να λάβουν οι αποφασίζοντες είναι ημι- δομημένες και συχνά πλήρως δομημένες (ορισμός στο κεφάλαιο 2).

Με την ολοκλήρωση της εφαρμογής του μοντέλου GIRA, οι αποφασίζοντες που έχουν στόχο την προστασία των μονάδων Υγείας, μπορούν να έχουν αναγνωρίσει τα αδύναμα σημεία που επιτρέπουν την υλοποίηση της απειλής και να έχουν κατανοήσει τη σχέση αυτών με τις

γενικές επιδιώξεις τους. Έτσι, αποκτούν μία ξεκάθαρη εποπτεία του προβλήματος και είναι σε θέση να ιεραρχήσουν τις διαφορετικές δράσεις για μετριασμό της επικινδυνότητας με βάση τις προτεραιότητές τους.

Παραρτήματα

Παράρτημα Α΄

Επεξήγηση Μαθηματικών Σχέσεων του μοντέλου GIRA

Στο παράρτημα αυτό γίνεται επεξήγηση του τρόπου υπολογισμού των δεσμευμένων πιθανοτήτων που ορίζονται στο κεφάλαιο 2 και προκύπτουν στα σενάρια χρήσης που παρουσιάζονται στο κεφάλαιο 5.

Α΄.1 Αρχικές Πιθανότητες

Χάριν ευκολίας, και για λόγους συμβατότητας με την εργασία του Κεφαλαίου 5,παρακάτω αναλύεται η γενική περίπτωση ενός σεναρίου χρήσης ανάλογου με τα UC1,UC2, UC3.

Στο γενικό σενάριο το σύστημα βάλλεται από μία απειλή, έστω E (πχ εγκατάσταση μαλωαρε) . Αν η $P(E)$ συμβολίζει την πιθανότητα να υλοποιηθεί η απειλή, τότε η $P(E')$ αναπαριστά την πιθανότητα να μην υλοποιηθεί και ισχύει $P(E)+P(E')=1$. *Χωρίς βλάβη της γενικότητας* υποθέτουμε ότι οι αποφασίζοντες για να αντιμετωπίσουν την απειλή E, μπορούν να εφαρμόσουν 2 διακριτά μέτρα αντιμετώπισης, από τα οποία προκύπτουν 4 πιθανές εναλλακτικές στρατηγικές αντιμετώπισης:

- IR1 : εφαρμογή πρώτου μέτρου (πχ δημιουργία αντιγράφων ασφαλείας),
- IR2 : εφαρμογή δεύτερου μέτρου (πχ εφαρμογή τεχνικών μέτρων ασφαλείας),
- IR3 : εφαρμογή και των δύο μέτρων ταυτόχρονα (πχ δημιουργία αντιγράφων ασφαλείας και εφαρμογή τεχνικών μέτρων ασφαλείας),
- IR4 : καμία δράση.

Ορίζουμε τις πιθανότητες:

- P(E1) : η πιθανότητα η απειλή να πραγματοποιηθεί ενώ έχει εφαρμοστεί το IR1
- P(E'1) : η πιθανότητα η απειλή να μην πραγματοποιηθεί ενώ έχει εφαρμοστεί το IR1
- P(E2) : η πιθανότητα η απειλή να πραγματοποιηθεί ενώ έχει εφαρμοστεί το IR2
- ...

Πρέπει να σημειωθεί ότι τα παραπάνω ενδεχόμενα αφορούν στην πραγματικότητα,την γενική **απόδοση** των αντίστοιχων μέτρων εφαρμογής στην αντιμετώπιση ανάλογων κινδύνων. Οι πιθανότητες που αντιστοιχούν στα ενδεχόμενα μπορούν να αποκτηθούν από **ιστορικά δεδομένα**, **στατιστικά στοιχεία**, **δείκτες απόδοσης** κ.α.

Για παράδειγμα, η P(E2) στο σενάριο χρήσης 3, δηλαδή η πιθανότητα να προσβληθεί ο υπολογιστής από κακόβουλο λογισμικό ενώ έχει εγκατασταθεί anti- malware λογισμικό, μπορεί να προκύψει αν συμβουλευτούμε τους δείκτες απόδοσης του anti- malware λογισμικού. Για την P(E4) που αντιστοιχεί στο να πραγματοποιηθεί η απειλή ενώ δεν έχει εφαρμοστεί κανένα μέτρο αντιμετώπισης, ισχύει P(E4) = P(E), δηλαδή ισούται με την αρχική πιθανότητα απειλής.

Α΄.2 Πραγματοποίηση Κινδύνου - Incident Materialisation : Υπολογισμός πιθανοτήτων

Έστω, επίσης χωρίς βλάβη της γενικότητας, ότι αν πραγματοποιηθεί ο κίνδυνος προκύπτουν 3 διακριτά σενάρια αρνητικής ενδεχομενικότητας για το σύστημα και οι αντίστοιχες πιθανότητες :

- Σενάριο H1 με πιθανότητα πραγματοποίησης P(H1), (πχ υποκλοπή ιατρικών δεδομένων),
- Σενάριο H2 με πιθανότητα πραγματοποίησης P(H2), (πχ αλλοίωση ιατρικών αποτελεσμάτων),
- Σενάριο H3 με πιθανότητα πραγματοποίησης P(H3), (πχ καμία αλλαγή).

Οι τιμές των P(H1), P(H2), P(H3) (που αντιπροσωπεύουν τα αρνητικά σενάρια H1, H2, H3 ανεξάρτητα της πραγματοποίησης της αρχικής απειλής) πρέπει να είναι διαθέσιμες στην αρχή της διαδικασίας. Μία καλή πηγή είναι ιστορικά δεδομένα ή στατιστικά.

Το GIRA model είναι σχεδιασμένο έτσι ώστε να λαμβάνει υπόψη τα μέτρα αντιμετώπισης του κινδύνου που μπορούν να ληφθούν πριν την πραγματοποίηση της απειλής. Οι πιθανότητες που προκύπτουν στον υπολογισμό των αρνητικών επιπτώσεων από την πραγματοποίηση ενός κινδύνου είναι **δεσμευμένες**, δηλαδή αφορούν το ενδεχόμενο να προκληθουν αρνητικές συνέπειες στο σύστημα δεδομένου ότι έχουν ληφθεί μέτρα για την πρόληψή του.

Η $P(H \mid E1)$ δηλαδή εκφράζει την πιθανότητα να συμβεί το σενάριο H, δεδομένου ότι η απειλή πραγματοποιήθηκε και είχε εφαρμοστεί το μέτρο πρόληψης IR1. Για παράδειγμα θα μπορούσαμε να υπολογίσουμε την πιθανότητα να κλαπούν ιατρικά δεδομένα ασθενών, δεδομένου ότι έχει πραγματοποιηθεί κυβερνοεπίθεση και οι υπεύθυνοι του ιατρείου δεν είχαν λάβει κανένα μέτρο προστασίας (IR4). Έτσι προκύπτουν συνολικά 24 διαφορετικές περιπτώσεις με τις αντίστοιχες πιθανότητες (3 σενάρια επιπτώσεων × 4 εναλλακτικές μέτρων αντιμετώπισης × 2 - πραγματοποίηση απειλής ή μη) :

- A11 : σενάριο H1 + E1, με πιθανότητα P(A11)
- A12 : σενάριο H1 + E2, με πιθανότητα P(A12)

- ....

Συνολικά, οι δεσμευμένες πιθανότητες φαίνονται στο σχήμα Α΄.1 :

Incident Materialisation

	Πραγματοποίηση Απειλής				Μη πραγματοποίηση απειλής			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Σενάριο 1	P(H1|E1)	P(H1|E2)	P(H1|E3)	P(H1|E4)	P(H1|E'1)	P(H1|E'2)	P(H1|E'3)	P(H1|E'4)
Σενάριο 2	P(H2|E1)	P(H2|E2)	P(H2|E3)	P(H2|E4)	P(H2|E'1)	P(H2|E'2)	P(H2|E'3)	P(H2|E'4)
Σενάριο 3	P(H3|E1)	P(H3|E2)	P(H3|E3)	P(H3|E4)	P(H3|E'1)	P(H3|E'2)	P(H3|E'3)	P(H3|E'4)

Σχήμα Α΄.1: *Πίνακας δεσμευμένων πιθανοτήτων GIRA model*

Στην πρακτική εφαρμογή της μεθόδου στο κεφάλαιο 5, όλες οι πιθανότητες τα συμβούν αρνητικά σενάρια, δεδομένου ότι η απειλή δεν έχει υλοποιηθεί, λαμβάνουν την τιμή 0. Αυτό που πρέπει να υπολογιστεί στο στάδιο πραγματοποίησης κινδύνου (incident materialisation) είναι η $P(H1 \mid E1)$ **=** $P(A11)$ και οι πιθανότητες όλων των αντίστοιχων ενδεχομένων ώστε να περάσουν ως **είσοδοι στο επόμενο στάδιο υπολογισμού**. Ο υπολογισμός της πιθανότητας γίνεται ως εξής:

$$P(H1 \mid E1) = \frac{P(E1 \mid H1)\,P(H1)}{P(E1)} \tag{Α΄.1}$$

όπου για την $P(E1 \mid H1)$ ισχύει:

$$P(E1 \mid H1) = \frac{P(E1 \cap H1)}{P(H1)} \tag{Α΄.2}$$

Όπως τα ίδια τα ενδεχόμενα E1 και H1 έτσι και η τομή αυτών, $E1 \cap H1$, προκύπτει από ιστορικά δεδομένα και είναι διαθέσιμη πριν την ανάλυση.

Όταν υπολογιστούν οι πιθανότητες όλων των ενδεχομένων που αφορούν το H1, δηλαδή οι πιθανότητες που αντιστοιχούν στην πρώτη γραμμή του διαγράμματος που φαίνεται στο σχήμα Α΄.1, αυτές πρέπει να επαληθεύουν τη σχέση :

$$P(H1\,) = P(H1 \mid E1) + P(H1 \mid E2) + \ldots + P(H1 \mid E'1) + \ldots + P(H1 \mid E'4) \tag{Α΄.3}$$

Αντίστοιχα γίνεται ο υπολογισμός και για την πιθανότητα των υπόλοιπων δύο σεναρίων H2, H3.

Α΄.3 Συνέπειες στο Σύστημα Υπο Διαχείριση - Consequences in the Managed System : Υπολογισμός πιθανοτήτων

Στο προηγούμενο στάδιο, υπολογίστηκαν οι πιθανότητες της μορφής P(H1.M1) = P(A11), οι οποίες λαμβάνονται ως είσοδοι στο στάδιο υπολογισμού της πιθανότητας, τα αρνητικά σενάρια Η, να έχουν ως αποτέλεσμα περαιτέρω συνέπειες στο σύστημα. Σε αντίθεση με τα διαφορετικά σενάρια πραγματοποίησης του κινδύνου, επειδή οι συνέπειες είναι ανεξάρτητες και μοντελοποιούνται σε διαφορετικούς κόμβους, κάθε συνέπεια μελετάται ξεχωριστά και μας αφορούν μόνο δύο ενδεχόμενα:

- CO η συνέπεια πραγματοποιείται με πιθανότητα P(CO)
- CO', η συνέπεια δεν πραγματοποιείται, με πιθανότητα P(CO') = 1 - P(CO).

Η συνέπεια μπορεί να προκύψει με 12 διακριτούς τρόπους: Έτσι προκύπτουν συνολικά 24 διαφορετικές περιπτώσεις με τις αντίστοιχες πιθανότητες (2 πραγματοποίηση συνέπειας ή μη× 3 σενάρια επιπτώσεων× 4 εναλλακτικές μέτρων αντιμετώπισης) :

- η συνέπεια CO πραγματοποιείται + H1 + IP1, με πιθανότητα $P(CO \mid A11)$
- η συνέπεια CO πραγματοποιείται + H1 + IP2, με πιθανότητα$P(CO \mid A12)$
- ....

Οι δεσμευμένες πιθανότητες των συνεπειών φαίνονται στο σχήμα Α΄.2 :

Consequence

	H1				H2				H3			
	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4	IR 1	IR 2	IR 3	IR 4
Εμφάνιση Συνέπειας	P(CO|A11)	P(CO|A12)	P(CO|A13)	P(CO|A14)	P(CO|A21)	P(CO|A22)	P(CO|A13)	P(CO|A24)	P(CO|A31)	P(CO|A32)	P(CO|A33)	P(CO|A34)
Μη εμφάνιση	P(CO'|A11)	P(CO'|A12)	P(CO'|A13)	P(CO'|A14)	P(CO'|A21)	P(CO'|A22)	P(CO'|A13)	P(CO'|A24)	P(CO'|A31)	P(CO'|A32)	P(CO'|A33)	P(CO'|A34)

Σχήμα Α΄.2: *Πίνακας δεσμευμένων πιθανοτήτων συνεπειών GIRA model*

Η τιμή της P(CO) (που αντιπροσωπεύει την συνέπεια CO ανεξάρτητα της πραγματοποίησης της αρχικής απειλής) πρέπει να είναι διαθέσιμη στην αρχή της διαδικασίας. Μία καλή πηγή είναι ιστορικά δεδομένα ή στατιστικά.

Ο υπολογισμός των πιθανοτήτων γίνεται ως εξής:

$$P(CO \mid A11) = \frac{P(A11 \mid CO)\,P(CO)}{P(A11)} \qquad (\text{Α΄.4})$$

Όταν υπολογιστούν οι πιθανότητες όλων των ενδεχομένων που αφορούν την συνέπεια CO, δηλαδή οι πιθανότητες που αντιστοιχούν στην πρώτη γραμμή του διαγράμματος που φαίνεται στο σχήμα Α΄.2, αυτές πρέπει να επαληθεύουν τη σχέση :

$$P(CO) = P(CO \mid A11)+P(CO \mid A12)+...+P(CO \mid A21)+...++P(CO \mid A31)+...+P(CO \mid A34) \quad (A'.5)$$

Στη συνέχεια οι αποφασίζοντες αξιολογούν την μοντελοποιημένη επικινδυνότητα, με βάση τα στοιχεία του οργανισμού που επιθυμούν να προστατεύσουν και τις γενικές τους επιδιώξεις.

Βιβλιογραφία

[1] Μ. Μιχαλόπουλος και Ε. Γρηγορούδης και Κ. Ζοπουνίδης. *Στρατηγική των Επιχειρήσεων*. Κλειδάριθμος, Αθήνα, 1η έκδοση, 2007.

[2] Mouna Jouinia, Latifa Ben Arfa Rabaia και Anis Ben Aissab. *Classification of security threats in information systems*. *5th International Conference on Ambient Systems, Networks and Technologies*, Hasselt, Belgium, 2014.

[3] Daniel T. Kuehl. *From Cyberspace to Cyberpower: Defining the Problem*. *In Cyberpower and National Security*, University of Nebraska Press, 2009.

[4] Refsdal Atle, Solhaug Bjørnar και Stolen Ketil. *Cyber-Risk Management*. Springer International Publishing, Springer, 1η έκδοση, 2015.

[5] Aeiad Elamin. *Ανάλυση Οικονομικών Επιπτώσεων Κυβερνοεπίθεσης σε Διεθνείς Οργανισμούς και Επιχειρήσεις Μέθοδοι Προστασίας Προσωπικών Δεδομένων*. Μεταπτυχιακή διπλωματική εργασία, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης Δ.Π.Μ.Σ : Διοίκηση Επιχειρήσεων Πληροφοριακά Συστήματα, 2020.

[6] Baudilio Tomé Muguruza. *Προκλήσεις για μια αποτελεσματική ευωσιακή πολιτική για την κυβερνοασφάλεια*. *Ευρωπαϊκό Ελεγκτικό Συνέδριο*, Λουξεμβούργο, 2019.

[7] Ponemon Institute. *2018 Cost of Data Breach Study: Impact of Business Continuity Management*. Report 1, Research Department, Michigan, 2018.

[8] ENISA. *ENISA Threat Landscape Report 2018*. ENISA 1.0, European Union Agency For Network and Information Security, ETL, 2019.

[9] Ι.Σίσκος. *Μουτέλα Αποφάσεων*. Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 1η έκδοση, 2008.

[10] Brandas Claudiu. *Contributions to Conception, Design and Development of Decision Support Systems*. Διδακτορική Διατριβή, "Babeș - Bolyai" University, Cluj-Napoca, 2007.

[11] ISO. *Risk management — Risk assessment techniques*. ISO 31010, International Organization for Standardization, Geneva, Switzerland, 2009.

[12] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar και Mohamed Cheriet. *Taxonomy of information security risk assessment (ISRA)*. *Natural Sciences and Engineering Research Council of Canada Research Chair on Sustainable Smart Eco-Cloud*, Canada, 2015.

[13] Martin Stamer Ralf Fiedler. *Multidimensional, Integrated, risk assessment framework and dynamic, collaborative risk management tools for critical information infrastructures*. Report 7.3, MITIGATE Project, Horizon 2020 Programme, 2018.

[14] Aitor Couce-Vieira, David Rios Insua και Siv Hilde Houmb. *GIRA: a general model for incident risk analysis*. Report 10.1080/13669877.2017.1372509, Journal of Risk Research, Journal of Risk Research, 2017.

[15] Ι. Κολέτσος και Δ. Στογιάννης. *Εισαγωγή στην Επιχειρησιακή 'Ερευνα*. Εκδόσεις Συμεών, Αθήνα, 3η έκδοση, 2017.

[16] Aitor Couce Vieira. *Decision Models for Cybersecurity Risk Analysis*. Διδακτορική Διατριβή, Universidad Rey Juan Carlos, 2019.

[17] Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών. *Ολιστική Προστασία Κρίσιμων Υποδομών: Ανθεκτικότητα και Προστασία Διασυνδέσεων, Ενδελεχής Επιτελική Σύνοψη* . Report 020616, Οικονομικό Πανεπιστήμιο Αθηνών, Αθήνα, Ελλάδα, 2016.

[18] Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών. *Ολιστική Προστασία Κρίσιμων Υποδομών: Ολιστική Προστασία Κρίσιμων Υποδομών, Μέρος Α' Καταγραφή Εθνικών Κρίσιμων Υποδομών Και Διασυνδέσεων* . Report 1, Οικονομικό Πανεπιστήμιο Αθηνών, Αθήνα, Ελλάδα, 2016.

[19] Frederic Petit, Duane Verner, David Brannegan, David Brannegan, David Dickinson, Karen Guziel, Rebecca Haffenden, Julia Phillips και James P. Peerenboom. *Analysis of Critical Infrastructure Dependencies and Interdependencies*. Report ΑΝΛ/ΓΣΣ-15/4, Argonne National Laboratory, Argonne, Illinois, 2015.

[20] George Stergiopoulos. *Securing critical infrastructures at software and interdependency levels*. Διδακτορική Διατριβή, Οικονομικό Πανεπιστήμιο Αθηνών. Τμήμα Πληροφορικής, 2015.

[21] Halima Ibrahim Kure και Shareeful Islam. *Assets focus risk management framework for critical infrastructure cybersecurity risk management*. Report 2398-3396, School of Architecture, Computing, and Engineering, University of East London, London, UK, 2019.

[22] Θεοδώρου Μ . και Σαρρής Μ . και Σούλης Σ. . *Συστήματα Υγείας*. Εκδόσεις Παπαζήση, Αθήνα, 1η έκδοση, 2001.

[23] Ian Stine, Mason Rice, Stephen Dunlap και John Pecarina. *A cyber risk scoring system for medical devices*. Report ΑΔ1054765, Department of Electrical and Computer Engineering, Air Force Institute of Technology, Ohio, USA, 2017.

[24] SPHINX partners. *A Universal Cyber Security Toolkit for Health-Care Industry,D2.4 - Use Cases Definition and Requirements Document, v1.00*. Report 826183, National Technical University of Athens, Athens, 2019.

[25] Α. Σπυριδάκη και Ι. Αντωνάκος και Ι. Αποστολάκης και Ι. Τούντας. *Εφαρμογές της «κινητής υγείας» (mobile health) στα χρόνια νοσήματα και διερεύνηση της αποτελεσματικότητάς τους*. Report 11-05-3992, Athens Medical Society, Αθήνα, 2018.