Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Ανάπτυξη Μεθοδολογιών για τις Τεχνοοικονομικές Πλευρές, των Συστημάτων Information and Communications Technology (ICT)

Φώτιος Καράμπελας

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Ιούνιος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ανάπτυξη Μεθοδολογιών για τις Τεχνοοικονομικές Πλευρές, των Συστημάτων Information and Communications Technology (ICT)

ΦΩΤΙΟΣ ΚΑΡΑΜΠΕΛΑΣ

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Ιούνιος 2018

ΛΕΥΚΗ ΣΕΛΙΔΑ

“If you can't measure it, you can't improve it.”
- Lord Kelvin

ΠΕΡΙΛΗΨΗ

Από την πρώτη στιγμή που εμφανίστηκαν οι υπολογιστές και τα συστήματα Πληροφορικής, η νέα τεχνολογία παρουσιάστηκε σαν ένα θαύμα, μία τεχνολογία που θα άλλαζε τον κόσμο, η 5η Τεχνολογική Επανάσταση. Ήταν απόλυτα λογικό οι Οργανισμοί να θεωρήσουν ότι η χρήση τους θα περιόριζε άμεσα το κόστος των επιχειρήσεων και θα αύξανε κατακόρυφα το κέρδος τους. Αν και η ανάπτυξη των τεχνολογιών αυτών, μπορεί να βελτιώσει αισθητά την αποδοτική λειτουργία ενός τέτοιου συστήματος, δεν είναι σαφές στους οργανισμούς, ο βαθμός επένδυσης σε αυτά, για τη μείωση του κόστους και την αύξηση της απόδοσης, κάθε φορά.

Όταν στην εξίσωση εισέρχεται και η Ασφάλεια, τότε ο προβληματισμός μεγαλώνει. Η απάντηση που πρέπει να απαντήσουν οι ειδικοί είναι απλή αλλά με διττή σημασία: Τι οικονομικά οφέλη έχει ένας Οργανισμός και πόση επένδυση είναι αρκετή στα συστήματα ασφαλείας ώστε να αντιμετωπιστούν σε μεγάλο βαθμό όλοι οι κίνδυνοι που απειλούν τα συστήματα τους.

Με την εκτενή βιβλιογραφική ανασκόπηση και μελέτη των περισσότερων οικονομικών μοντέλων και αναλύοντας τα συμπεράσματα διαπιστώθηκε, ότι οι Οργανισμοί παγκοσμίως βλέπουν την επένδυση στα συστήματα ασφαλείας, ανεξάρτητα από την οικονομική τους πτυχή. Ενώ διαπιστώνεται πλήθος οικονομικών προτάσεων, είναι ακόμη πολύ δύσκολο να υπολογιστεί ο βέλτιστος βαθμός επένδυσης διότι στα οικονομικά μοντέλα δεν υπολογίζονται μεγέθη που δεν αποφέρουν άμεσα έσοδα στους Οργανισμούς.

Η λύση που δίνεται σε αυτήν την Διατριβή είναι η δημιουργία ενός μεθοδολογικού πλαισίου που θα λαμβάνει υπόψη όλους τους προβληματισμούς και θα είναι ικανό να υπολογίσει όλες τις επιπτώσεις μετά από μία επίθεση στα συστήματα ενός Οργανισμού που δεν είναι άμεσα μετρήσιμες και θα χρησιμοποιεί την τεχνική εκτίμησης του ρίσκου VaR προσαρμοσμένη στις ανάγκες της Διατριβής.

Λέξεις Κλειδιά

Ασφάλεια, Οικονομικά της Κυβερνοασφάλειας, Διαχείριση Κινδύνου, Επιστροφή της Επένδυσης στην Ασφάλεια, Αξία σε Κίνδυνο, Συστήματα Τ.Π.Ε

SUMMARY

From the very first time that computers and computer systems emerged, the new technology was presented as a miracle, a technology that would change the world, the 5th Technological Revolution. It was entirely sensible for organizations to believe that their use would directly reduce business costs and increase profits. Although the development of these technologies can substantially improve the efficient operation of such a system, it is not clear to organizations, the degree of investment in them, to reduce costs and increase performance at the same time.

When in the equation Security is added, then the concern grows. The answer that experts have to answer is simple but twofold: What economic benefits does an organization have and how much investment is enough in security systems to be able to a large extent to encounter all the dangers that threaten their systems.

With the extensive bibliographic review and study of most economic models and analyzing the findings, it was found that organizations worldwide view investment in security systems, regardless of their economic aspect. While there are numerous financial models, it is still very difficult to calculate the optimal degree of investment because the economic models do not calculate figures that do not generate direct revenue to the Organizations.

The solution given in this thesis, is the creation of a methodological framework that will take into account all the concerns and will be able to calculate all the consequences after an attack on the systems of an organization which are not directly measurable and will use the method of VaR adjusted to the needs of the thesis.

Keywords

Security, Cyber-Security Economics, Risk Management, Return on Security Investment, Value at Risk, ICT Systems

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέπων καθηγητή μου κύριο Νικόλαο Σκλάβο για την υποστήριξη, την πολύτιμη βοήθειά του, την καθοδήγηση που μου προσέφερε καθώς και την άριστη συνεργασία που είχαμε κατά τη διάρκεια της εκπόνησης της πτυχιακής μου εργασίας.

Επίσης θα ήθελα να ευχαριστήσω και όλους τους καθηγητές που είχα τα τρία χρόνια των σπουδών μου στο Ανοιχτό Πανεπιστήμιο Κύπρου, για την υπομονή τους, τη βοήθειά τους και την προσπάθεια για την μετάδοση των γνώσεων τους, η οποία ήταν και θα είναι πολύτιμη για τη ζωή μου.

Δεν θα μπορούσα να μην ευχαριστήσω τους συναδέρφους μου στην δουλειά και ήδη κατόχους τίτλων Μεταπτυχιακών σπουδών, Νικόλαο Μακαρώνη και Ειρήνη Χαντζίδου για τις πολύτιμες συμβουλές τους στον τρόπο εκπόνησης της παρούσας Διατριβής.

Ιδιαίτερη αναφορά για να του εκφράσω τις ευχαριστίες μου θα κάνω στον Αλέξανδρο Θυμιανίδη, για την πολύτιμη βοήθεια και επεξήγηση όλων των οικονομικών όρων που χρησιμοποιήθηκαν σε αυτήν την Διατριβή.

Τέλος θα ήθελα να ευχαριστήσω την σύζυγό μου Αθανασία Παπαδημητρίου για την στήριξη των προσπαθειών μου και για την υπομονή που έδειξε κατά τις ώρες μελέτης.

Περιεχόμενα

Κατάσταση Εικόνων

Κατάσταση Πινάκων

Κεφάλαιο 1

Εισαγωγή

1.1 Η νέα ψηφιακή εποχή

Ο 20ος αιώνας ήταν η απαρχή της 5ης τεχνολογικής επανάστασης, της μεγαλύτερης μετά από αυτήν της βιομηχανικής επανάστασης. Η δημιουργία του πρώτου υπολογιστή και η γέννηση μιας νέας επιστήμης, της Πληροφορικής, επέφερε μεγάλες ανακαλύψεις δίνοντας μία νέα ώθηση στην ανάπτυξη πολλών και καινοτόμων εφαρμογών.

Η ανάπτυξη της νέας επιστήμης επηρέασε σημαντικούς επιστημονικούς κλάδους και κυρίως άλλαξε την καθημερινότητα του ανθρώπου. Διάφοροι τομείς της, όπως η Οικονομία, η Υγεία, η Παιδεία και η Ασφάλεια άλλαξαν ριζικά. Επιπρόσθετα τα σύγχρονα συστήματα Πληροφορικής και Επικοινωνιών και οι ανάλογες εφαρμογές τους , αντιμετωπίζοντας με διαφορετικό τρόπο τα προβλήματα, βελτίωσαν το βιοτικό επίπεδο του ανθρώπου και άλλαξαν σημαντικά τις σύγχρονες κοινωνίες.

Στην Ψηφιακή Εποχή οι τηλεπικοινωνίες είναι ο κύριος μοχλός για τη μετάβαση του σημερινού κόσμου από το βιομηχανικό παρελθόν στην κοινωνία της γνώσης. Η μετάβαση αυτή σημαίνει ότι, για πρώτη φορά στην ιστορία της ανθρωπότητας, οι πρώτες ύλες παύουν να αποτελούν τον ακρογωνιαίο λίθο της παραγωγικής διαδικασίας και ότι η οικονομία βασίζεται λιγότερο στα εργατικά χέρια και περισσότερο στις υπηρεσίες. Όμως, η ανάπτυξη των υπηρεσιών βασίζεται στην καινοτομία, στη διαρκή παραγωγή νέων κλάδων οι οποίοι απαντούν στις πολύπλοκες ανάγκες των σύγχρονων κοινωνιών. Δεν είναι λοιπόν τυχαίο το γεγονός ότι η γνώση αποτελεί, στο εξής, τη βασική πλουτοπαραγωγική πηγή της παγκόσμιας οικονομίας.

Αυτή η γνώση όμως, με την μορφή της Πληροφορίας, έχει μεγάλη αξία και πρέπει να προστατευτεί Η νέα Τεχνολογία επέφερε τεράστιες αλλαγές όχι μόνο στην καθημερινότητα του ανθρώπου αλλά επίσης στις συναλλαγές και στην λειτουργία των επιχειρήσεων. Η δημιουργία και η κατανομή των σύγχρονων Συστημάτων, αύξησε την πολυπλοκότητα τους και τα έκανε πιο ευάλωτα σε κινδύνους. Η προστασία της Πληροφορίας λοιπόν και κατά επέκταση και των Συστημάτων που την διαχειρίζονται και την διανέμουν, είναι πολύ σημαντική τόσο για τους καθημερινούς χρήστες όσο και για τους Οργανισμούς που έχουν επενδύσει σημαντικά ποσά για την Ασφάλεια τους.

1.2 Στόχος της Διατριβής-Ερευνητικά Ερωτήματα

Σε αυτή τη διατριβή, θα μελετηθούν και θα αναλυθούν οι τεχνικές προσεγγίσεις της οικονομίας, στα συστήματα ICT. Θα προταθούν βέλτιστες και εναλλακτικές λύσεις, έτσι ώστε να εκτιμηθεί το κόστος εξοικονόμησης, λόγω της ανάπτυξης των συστημάτων ICT. Θα μελετηθεί κατά πόσο η επένδυση από τους Οργανισμούς σε συστήματα ασφαλείας είναι επωφελής για αυτούς ενώ το κυριότερο ερώτημα που θα προσπαθήσει να απαντήσει είναι αυτό που απασχολεί όλο και περισσότερους ερευνητές:

Πόση επένδυση στην Ασφάλεια είναι αρκετή για έναν Οργανισμό;

Τα ερευνητικά ερωτήματα που πρέπει να απαντηθούν για να ικανοποιηθούν οι στόχοι της παρούσας της Διατριβής είναι:

H1: Ποια είναι τα τεχνοοικονομικά οφέλη των Οργανισμών από την χρήση των Συστημάτων Information and Communications Technology (ICT);

H2: Είναι τα υπάρχοντα οικονομικά μοντέλα ικανά και αρκετά για να περιγράψουν την επιστροφή της επένδυσης σε συστήματα ασφαλείας από έναν Οργανισμό;

H3: Ποιος πρέπει να είναι ο βαθμός επένδυσης από έναν Οργανισμό στα Συστήματα Information and Communications Technology (ICT) για την αύξηση της απόδοσης ώστε να είναι επικερδής;

1.3 Η Δομή της Διατριβής

Σε αυτό το τμήμα παρουσιάζεται αναλυτικά η δομή της Διατριβής, η οποί αποτελείται από έξι (6) Κεφάλαια και την Βιβλιογραφία που χρησιμοποιήθηκε.

Το πρώτο Κεφάλαιο αποτελεί και την εισαγωγή της παρούσας Διατριβής. Περιγράφεται η νέα Ψηφιακή Εποχή και οι αλλαγές που έχει αποφέρει στην καθημερινότητα και σε όλες τις πτυχές της ζωής αλλά και στις επιχειρήσεις. Αναφέρονται οι στόχοι της Διατριβής και τα ερευνητικά ερωτήματα, ενώ περιγράφεται και η δομή και τα περιεχόμενα των Κεφαλαίων.

Το δεύτερο Κεφάλαιο με τίτλο «Βασικοί Ορισμοί», περιλαμβάνει όλους τους απαραίτητους και θεμελιώδεις Ορισμούς για την κατανόηση των Πληροφοριακών Συστημάτων και Επικοινωνίας. Περιγράφονται αναλυτικά τα οφέλη που έχουν οι Οργανισμοί από την χρήση των Συστημάτων Τ.Π.Ε, ενώ κατόπιν αναλύονται οι θεμελιώδεις ορισμοί για την Ασφάλεια της Πληροφορίας. Επιπρόσθετα αναλύονται οι απειλές και ευπάθειες αυτών των Συστημάτων και κατηγοριοποιούνται οι απειλές των. Τέλος γίνεται μία αναφορά στην έννοια του Κινδύνου και στις Κρίσιμες Πληροφοριακές Υποδομές, (Critical Information Infrastructures).

Το τρίτο Κεφάλαιο με τίτλο «Συστήματα και Επιχειρήσεις» περιλαμβάνει μία ιστορική αναδρομή για την χρήση των συστημάτων Τ.Π.Ε, παρουσιάζονται σύγχρονα στατιστικά στοιχεία για την χρήση τους στις επιχειρήσεις, ενώ αναλύεται διεξοδικά η αρχιτεκτονική τους, η συνεισφορά τους στην οικονομική ανάπτυξη και τέλος τα οφέλη από την χρήση τους στην αύξηση της απόδοσης ενός Οργανισμού.

Στο τέταρτο Κεφάλαιο με τίτλο «Τα Οικονομικά της Κυβερνοασφάλειας» μετά από μία σύντομη εισαγωγή για να τονιστεί ο παγκόσμιος προβληματισμός για τον βαθμό της επένδυσης σε συστήματα Τ.Π.Ε και συστήματα Ασφαλείας, παρουσιάζονται αρχικά τα κόστη που αντιμετωπίζει ένας Οργανισμός από την χρήση αυτών των Συστημάτων ή μετά από μία κυβερνοεπίθεση. Κατόπιν αναλύονται και αξιολογούνται τα περισσότερα μοντέλα για τον υπολογισμό του κόστους παρουσιάζοντας τις δυνατότητες, τα πλεονεκτήματα και τα μειονεκτήματα τους. Στο τέλος περιγράφονται και κάποιες από τις τεχνικές εκτίμησης του Κινδύνου (Risk).

Στο πέμπτο Κεφάλαιο, το πιο σημαντικό της παρούσας Διατριβής, παρουσιάζεται η σχεδίαση ενός μεθοδολογικού πλαισίου για την εύρεση του βέλτιστου βαθμού επένδυσης στα συστήματα Τ.Π.Ε. Το πλαίσιο αυτό είναι συνδυασμός των υπαρχόντων οικονομικών μοντέλων, λαμβάνοντας υπόψη τα κόστη και όλες τις συνέπειες που αντιμετωπίζει ένας Οργανισμός μετά από μία επίθεση. Γίνεται προσπάθεια με ένα υπάρχων γραμμικό οικονομικό μοντέλο, να υπολογιστεί το κόστος από διάφορα μη-μετρήσιμα ποιοτικά μεγέθη, όπως είναι η φήμη ενός Οργανισμού ή η ζημιά από την μείωση της παραγωγής. Επίσης χρησιμοποιείται η μέθοδος VaR προσαρμοσμένη στις ανάγκες της Διατριβής για εκτίμηση και ποσοτικοποίηση του κινδύνου στα συστήματα ασφαλείας από μελλοντικές επιθέσεις και κατά επέκταση τις απώλειες και ζημιές στην καθαρή θέση ενός Οργανισμού για ένα συγκεκριμένο χρονικό διάστημα. Προτείνεται ο συνδυασμός της με την μέθοδο της ιστορικής προσομοίωσης ή με την μέθοδο Monte Carlo, ενώ τέλος γίνεται η Αξιολόγηση της επένδυσης με την Καθαρά Παρούσα Αξία συνδυασμένη με τον δείκτη του Εσωτερικού Βαθμού Απόδοσης για μεγαλύτερα χρονικά διαστήματα.

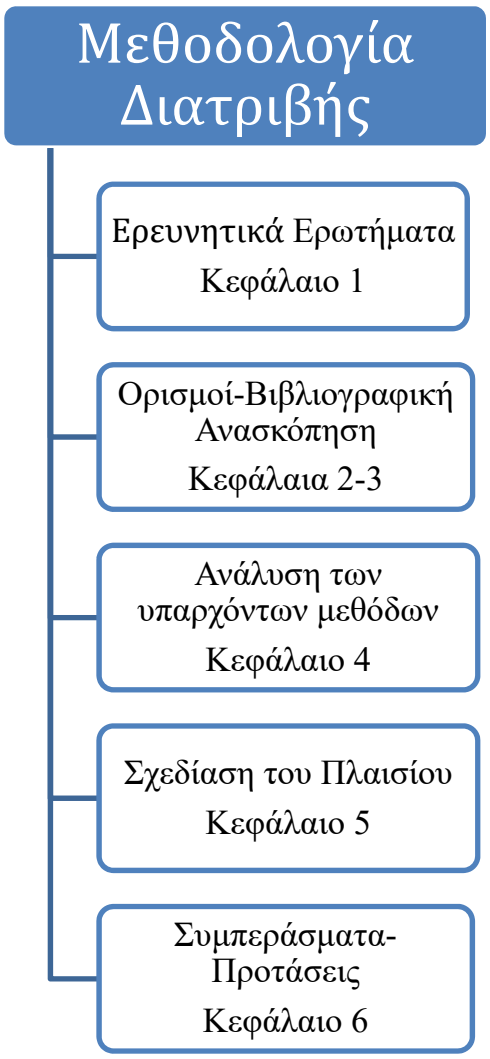
Στο έκτο και τελευταίο Κεφάλαιο παρουσιάζονται τα Συμπεράσματα αυτής της Διατριβής, οι αδυναμίες της που μπορούν με μία εντελεχής έρευνα να επιβεβαιωθούν και η ανάγκη για περαιτέρω έρευνα στα Οικονομικά των συστημάτων Τ.Π.Ε

1.4 Μεθοδολογία

Στο παρακάτω σχήμα παρουσιάζεται ο τρόπος με τον οποίο συγγράφηκε η παρούσα Διατριβή και τα βήματα που ακολουθήθηκαν. Συγκεκριμένα στο παρόν κεφάλαιο παρουσιάστηκαν τα ερευνητικά ερωτήματα και ο στόχος της Διατριβής. Κατόπιν με μία σύντομη βιβλιογραφική ανασκόπηση παρουσιάστηκαν και αναλύθηκαν οι κυριότερες μέθοδοι για την αξιολόγηση μίας επένδυσης. Κατόπιν σχεδιάστηκε ένα μεθοδολογικό πλαίσιο για την πρόταση αυτής της Διατριβής, μία πρόταση που αποτελεί έναν συνδυασμό αυτών των παραπάνω μεθόδων.

Σκοπός δεν ήταν φυσικά να δημιουργηθεί μία νέα μέθοδος για την Αξιολόγηση μίας επένδυσης στην Ασφάλεια. **Κύριος σκοπός ήταν μία πρόταση που θα συμπεριλάμβανε όλα τα πλεονεκτήματα των υπαρχόντων μεθόδων δημιουργώντας ένα μεθοδολογικό πλαίσιο που θα μπορούσε να το χρησιμοποιήσει οποιοσδήποτε Οργανισμός ανεξαρτήτου μεγέθους και προϋπολογισμού.**

Αυτό που δεν έγινε και αποτελεί ίσως τον στόχο μίας μελλοντικής μελέτης είναι η επικύρωση αυτής της μεθόδου, είτε μελετώντας τα πραγματικά στοιχεία μίας εταιρείας (case study) όπως η επένδυση σε συστήματα Τ.Π.Ε και Ασφαλείας και η απόδοση αυτής της Επένδυσης μετά από κάποια επίθεση. Σε περίπτωση μάλιστα και εξεύρεσης πραγματικών δεδομένων, θα μπορούσε να γίνει μία στατιστική ανάλυση που θα έδινε ακριβώς τα πραγματικά μεγέθη που χρησιμοποιούνται στο Κεφάλαιο 5.



Κεφάλαιο 2
Βασικοί Ορισμοί

2.1 Εισαγωγή

Σε αυτό το κεφάλαιο, ορίζονται οι κύριες έννοιες των αναγκαίων εννοιών για τα Πληροφοριακά Συστήματα, για τις τεχνολογίες Πληροφοριών και Επικοινωνίας και όλες τις ορολογίες που αφορούν την Ασφάλεια των. Στη συνέχεια περιγράφεται η μεθοδολογία Εκτίμησης Επικινδυνότητας και οι τρέχουσες προσεγγίσεις σε σχέση με αυτή. Ακολουθεί η εννοιολογική θεμελίωση της περιοχής των Κρίσιμων (Πληροφοριακών και Επικοινωνιακών) Υποδομών (ICT Infrastructure). Οι ορισμοί αυτοί είναι το αναγκαίο θεωρητικό υπόβαθρο για αυτήν την Διατριβή και για τα αποτελέσματα που θα προκύψουν στα πλαίσια της ερευνητικής αυτής προσπάθειας.

2.2 Πληροφοριακά Συστήματα

Πληροφοριακό σύστημα (Information System) ονομάζεται ένα σύνολο διαδικασιών, ανθρώπινου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, που προορίζεται για τη συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση πληροφοριών. Επίσης τεχνικά μπορεί να οριστεί ως ένα σύνολο αλληλοσχετιζόμενων στοιχείων, τα οποία συλλέγουν ή ανακτούν, επεξεργάζονται, αποθηκεύουν και διανέμουν πληροφορίες που υποστηρίζουν τη λήψη αποφάσεων και τον έλεγχο σε έναν οργανισμό, ενώ βοηθούν τους διευθυντές και τους εργαζόμενους σε αυτόν να αναλύουν τα προβλήματα και να δημιουργούν νέα προϊόντα (Laudon & Laudon, 2011: 15). Τα Πληροφοριακά Συστήματα αποτελούνται από:

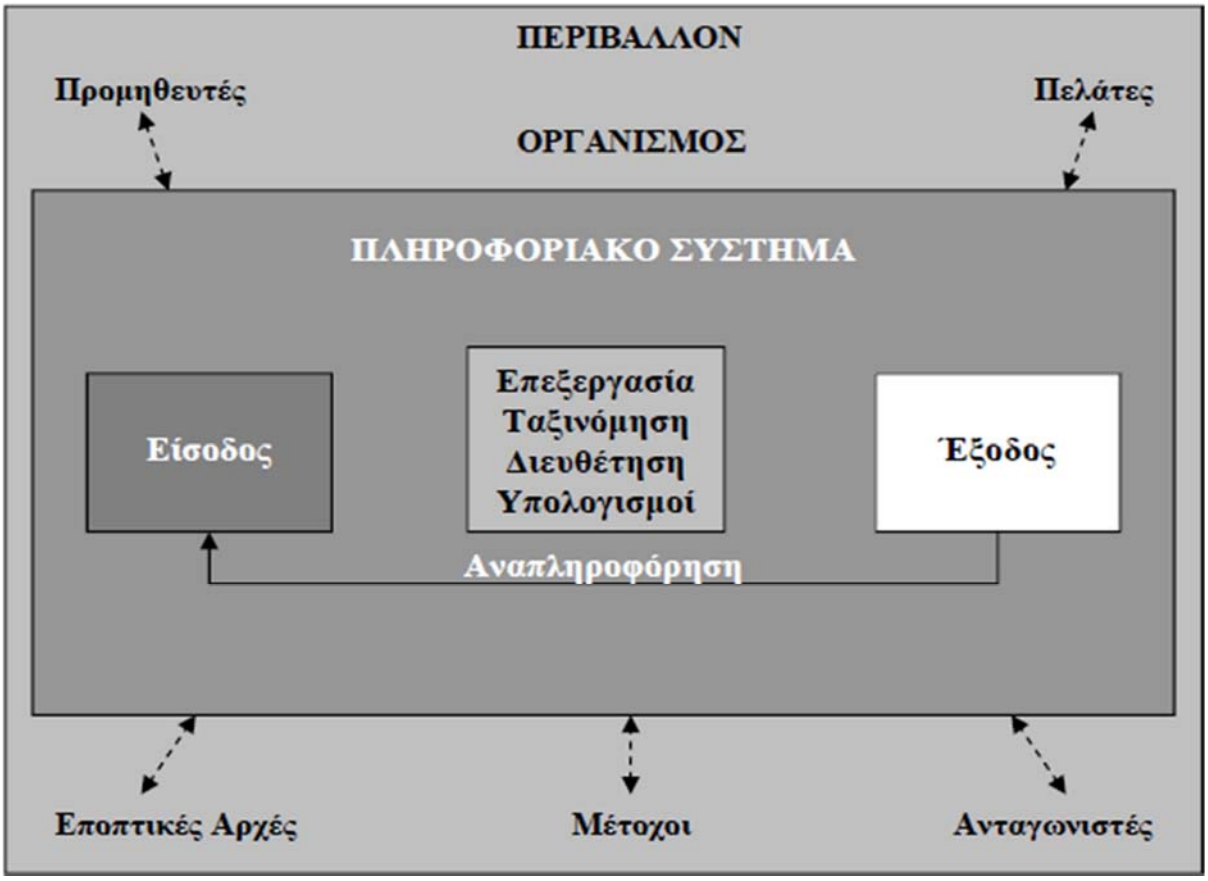
- Εισροές (Inputs): η συλλογή και η απόκτηση ακατέργαστων δεδομένων που μπορεί να προέρχονται από το εσωτερικό ή εξωτερικό περιβάλλον ενός Οργανισμού όπως είναι τα δεδομένα, οι εντολές και οι πληροφορίες.

- Επεξεργασία που αφορά την μετατροπή, τον χειρισμό και την ανάλυση των ακατέργαστων δεδομένων. Από αυτήν την επεξεργασία προκύπτουν οι πληροφορίες.

- Εκροές (Outputs): η διανομή και η διάχυση των επεξεργασμένων πληροφοριών στα άτομα στις δραστηριότητες που θα τις χρησιμοποιήσουν όπως είναι οι αναφορές και οι υπολογισμοί.

- Μηχανισμούς ανατροφοδότησης (feedback) που ελέγχουν την συνολική λειτουργία και είναι η εκροή του συστήματος που επιστρέφει στον Οργανισμό για να τον βοηθήσει, μέσα από μία διαδικασία ελέγχου, στην αξιολόγηση και την διόρθωση των εισροών.

- Το Περιβάλλον μέσα στο οποίο λειτουργεί.



Εικόνα 1: Το Πληροφοριακό Σύστημα και οι Λειτουργίες του (Πηγή: Laudon & Laudon, 2011:17)

2.2.1 Συστατικά Μέρη

Ένα Πληροφοριακό Σύστημα αποτελείται από διαφορετικά μέρη τα οποία αποτελούν και τα διακριτά του χαρακτηριστικά. Τα έξι διαφορετικά στοιχεία που πρέπει να ενωθούν για να αποτελέσουν το Πληροφοριακό Σύστημα είναι (Turban & Volonino, 2011: 9):

- Υλικό (Hardware): Ο όρος αυτός αναφέρεται ξεκάθαρα στις συσκευές ενός Π.Σ και πιο συγκεκριμένα στον υπολογιστή και στα διάφορα μέσα υποστήριξης του όπως μέσα αποθήκευσης, οθόνες, πληκτρολόγια κτλ.

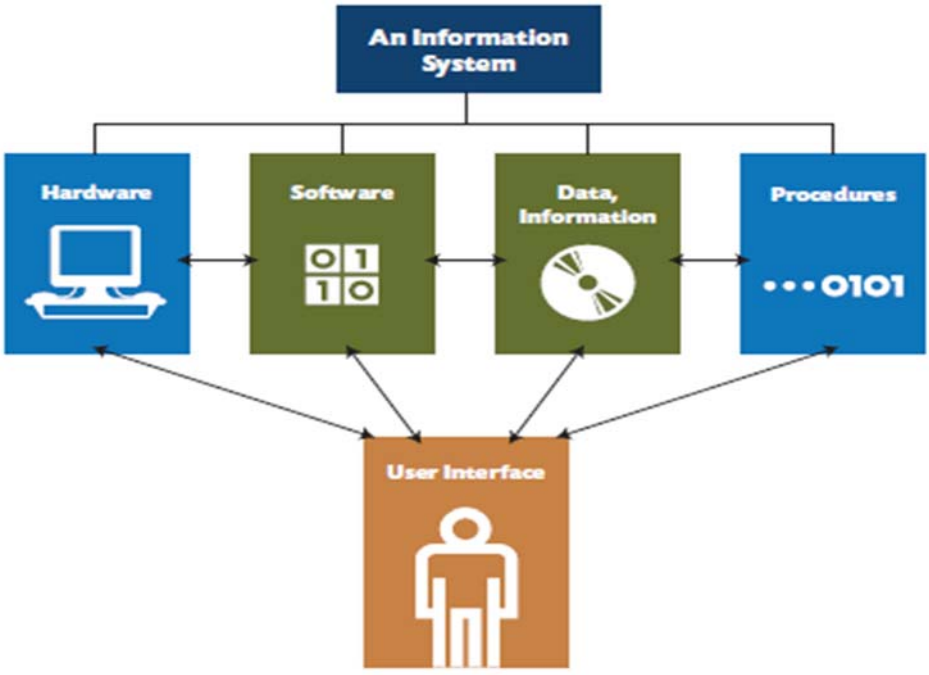
- Λογισμικό (Software): Το σύνολο των προγραμμάτων ή εφαρμογών που επεξεργάζονται δεδομένα (data) ή εισροές όπως οι φωνητικές εντολές.

- Δεδομένα (Data): Είναι τα διάφορα γεγονότα που χρησιμοποιούνται από τα προγράμματα για να δημιουργήσουν χρήσιμη πληροφορία και αν είναι απαραίτητο αποθηκεύονται σε μία βάση δεδομένων ή άλλα αποθηκευτικά μέσα.

- Διαδικασίες (Procedures): Είναι οι οδηγίες που δείχνουν τον τρόπο συνεργασίας όλων των συστατικών του Π.Σ για την επεξεργασία των πληροφοριών.

- Άνθρωποι (People): Ο ανθρώπινος παράγοντας είναι και ο πιο σημαντικός για την λειτουργία του Π.Σ. Σαν ορισμός περιλαμβάνει όχι μόνο τους χρήστες του εν λόγω συστήματος αλλά και τους ανθρώπους που εξυπηρετούν το υλικό, διατηρούν τα δεδομένα και υποστηρίζουν το δίκτυο.

- Δίκτυο (Network): Το σύστημα που επιτρέπει σε δύο ή περισσότερους υπολογιστές να συνδέονται και να χρησιμοποιούν τους ίδιους πόρους.



Εικόνα 2: Τα συστατικά Μέρη ενός Πληροφοριακού Συστήματος (Πηγή: Turan & Volonino: 9)

2.2.2 Πληροφοριακά Συστήματα και Οργανισμός

Όλες οι παραπάνω έννοιες είναι σημαντικές για την κατανόηση ενός Π.Σ, πρέπει όμως να αναχθούν στην λειτουργία ενός Οργανισμού για την καλύτερη προσέγγιση του θέματος. Καταρχήν, σε όλη την Διατριβή θα χρησιμοποιείται εφεξής ο όρος Τ.Π.Ε (Τεχνολογίες Πληροφορικής και Επικοινωνίας) που έχει αντικαταστήσει διεθνώς την Πληροφορική και αποτελεί μετάφραση του όρου ICT (Information and Communication Technologies).

Γιατί όμως οι σύγχρονες επιχειρήσεις χρησιμοποιούν όλο και περισσότερα συστήματα με Τ.Π.Ε; Τι είναι αυτά που προσφέρουν στον Οργανισμό; Γενικότερα η ανάπτυξη αυτών των Συστημάτων επέφερε μεγάλες αλλαγές και οι κυριότεροι λόγοι ανάπτυξης τους σε έναν Οργανισμό είναι οι παρακάτω:

- Μείωση του ανθρώπινου δυναμικού, συνεπώς αύξηση του προσδοκώμενου κέρδους.
- Γενικότερη αύξηση των εσόδων και μείωση του κόστους.
- Για να γίνει περισσότερο αποδοτικός.
- Για να παραμείνει ανταγωνιστικός και να αποκτήσει πλεονέκτημα έναντι των ανταγωνιστών του.
- Για να είναι καινοτόμος

Επιπλέον οι δυνατότητες που παρέχουν τα Π.Σ σε έναν Οργανισμό είναι πολλές και συμβάλλουν θετικά σε κάθε πτυχή του. Συγκεκριμένα:

- Παρέχουν μία γρήγορη και πιο ορθολογική χαμηλού κόστους επικοινωνία μέσα αλλά και μεταξύ των Οργανισμών.
- Επιτρέπουν την γρήγορη και φθηνή πρόσβαση σε μεγάλο πλήθος πληροφοριών.
- Αυτοματοποιούν τις επιχειρηματικές διαδικασίες.
- Αυξάνουν την αποτελεσματικότητα και την αποδοτικότητα της ομαδικής εργασίας.
- Αποθηκεύουν μεγάλο όγκο πληροφοριών σε ένα εύκολα προσβάσιμο και σχετικά μικρό χώρο.

- Μπορούν να υποστηρίζουν τις πρωτοποριακές εφαρμογές.

2.3 Ασφάλεια Πληροφορίας (Information Security)

Ακόμη και σήμερα δεν υπάρχει ένας κοινά αποδεκτός ορισμός της Ασφάλειας Πληροφοριών. Σε άλλες περιπτώσεις αναφέρονται σε ασφάλεια Πληροφοριακών Συστημάτων, σε άλλες σε ασφάλεια επιχειρήσεων, σε ψηφιακή ασφάλεια ή απλά σε ασφάλεια. Για την συγκεκριμένη διατριβή, ο ορισμός που αναφέρεται στο ISO 27002 βοηθά στην κατανόηση όλων αυτών των κοινωνικό-οικονομικών πτυχών που θέλουμε να μελετήσουμε.

Συγκεκριμένα σύμφωνα με το Πρότυπο ISO 27002, *«η Ασφάλεια Πληροφοριών προστατεύει τα πληροφοριακά αγαθά από μία μεγάλη γκάμα απειλών με σκοπό να εξασφαλίσει την διάρκεια μίας επιχείρησης, να ελαχιστοποιήσει το επιχειρησιακό ρίσκο αλλά και να μεγιστοποιήσει την επιστροφή της επένδυσης (ROI, που θα εξετάσουμε σε παρακάτω κεφάλαιο) και τις επιχειρηματικές ευκαιρίες».*

Με άλλα λόγια, οι δύο κύριοι Αντικειμενικοί Σκοποί της Ασφάλειας είναι:

- Η συνέχιση της λειτουργίας μίας επιχείρησης με την όσο το δυνατόν ελαχιστοποίηση των καταστροφών που θα προκύψουν από συμβάντα ή από ρήγματα στο επικοινωνιακό και πληροφοριακό δίκτυο της και
- Η μεγιστοποίηση της επιστροφής της επένδυσης (Return On Investment/ROI).

Είναι όμως χρήσιμο να ορίσουμε και την έννοια της Ασφάλειας στα Συστήματα Τ.Π.Ε (ICT Security) που είναι η ασφάλεια της τεχνολογικής υποδομής των Π.Σ, συμπεριλαμβανομένων και των επικοινωνιακών υποσυστημάτων του. Είναι εμφανές ότι με αυτόν τον ορισμό δίνεται μεγαλύτερη έμφαση στους τεχνικούς παράγοντες στης Ασφάλειας των Τ.Π.Ε

2.3.1 Γενικοί ορισμοί

Στόχος λοιπόν της Ασφάλειας σε ένα Πληροφορικό Σύστημα ή για να το εξειδικεύσουμε στις Τ.Π.Ε είναι η προστασία των πληροφοριών και ειδικότερα η προστασία των Υπολογιστικών Συστημάτων (Computer Security) και η προστασία των Επικοινωνιών (Communication

Security). Στόχος της είναι τόσο η προστασία των υπολογιστικών πόρων του συστήματος από μη εξουσιοδοτημένη χρήση όσο και η προστασία των δεδομένων.

Η διαφύλαξη των πόρων και η προστασία των δεδομένων στηρίζονται πάνω στις τρεις (3) θεμελιώδεις ιδιότητες της Ασφάλειας που είναι το γνωστό τρίπτυχο CIA.

- Εμπιστευτικότητα (**C**onfidentiality) που αφορά την προστασία της πληροφορίας από μη-εξουσιοδοτημένη αποκάλυψη.
- Ακεραιότητα (**I**ntegrity) που αναφέρεται στην προστασία της πληροφορίας από την μη-εξουσιοδοτημένη τροποποίηση της και
- Διαθεσιμότητα (**A**vailability) που αφορά την εξασφάλιση της εξουσιοδοτημένης πρόσβασης στην πληροφορία χωρίς παρεμπόδιση ή καθυστέρηση.

Υπάρχουν φυσικά και άλλες βασικές ιδιότητες που εφαρμόζονται στην ασφάλεια των Τ.Π.Ε όπως είναι η Αυθεντικότητα (Authentication), η Εξουσιοδότηση (Authorization), η Πιστοποίηση Ταυτότητας (Identification) και η αδυναμία Αποποίησης (Non-Repudiation). Βασικές έννοιες της Ασφάλειας είναι επιγραμματικά οι παρακάτω (Μαυρίδης, 2015: 18):

- Αγαθό (asset) ορίζεται κάθε αντικείμενο (πόροι συστήματος, δεδομένα κτλ) που έχει αξία (value) για έναν Οργανισμό ή έναν ιδιοκτήτη (owner) και αξίζει να προστατευτεί.
- Αξία (value) είναι η σπουδαιότητα ενός αγαθού εκφρασμένη με οικονομικούς όρους.
- Ζημία (harm) είναι ο περιορισμός της αξίας ενός αγαθού.
- Επίπτωση (impact) είναι η δυσμενής τροποποίηση στο επίπεδο των επιχειρησιακών στόχων ενός Οργανισμού (οικονομικές απώλειες, παρεμπόδιση λειτουργίας, απώλεια καλής φήμης).
- Επικινδυνότητα (Risk) είναι η πιθανότητα ή το ενδεχόμενο μια δεδομένη απειλή να εκμεταλλευτεί αδυναμίες ενός αγαθού ή μιας ομάδας αγαθών και να προκαλέσει ζημία σε έναν οργανισμό.
- Εκτίμηση Επικινδυνότητας (Risk assessment) είναι ο προσδιορισμός της αξίας των αγαθών, ο εντοπισμός των ενδεχόμενων απειλών και ευπαθειών και ο εντοπισμός των μέτρων ασφαλείας. Επίσης η Εκτίμηση Επικινδυνότητας προσδιορίζει τις πιθανές

επιπτώσεις και ιεραρχεί τους κινδύνους με βάση κριτήρια αξιολόγησης που θέτει το περιβάλλον εφαρμογής.

2.3.2 Απειλές Πληροφοριακών Συστημάτων

Απειλή (threat) είναι μία πιθανή κατάσταση που μπορεί να προκαλέσει ζημία σε έναν Οργανισμό ή ένα Πληροφοριακό Σύστημα. Οι απειλές αυτές μπορούν να κατηγοριοποιηθούν ως εξής:

- Φυσικές Απειλές που προκύπτουν από το περιβάλλον που λειτουργούν (φωτιές, πλημμύρες, σεισμοί κτλ.)
- Απειλές τεχνικών βλαβών λόγω της φύσης των συστημάτων (διακοπή ηλεκτροδότησης, αστοχία λογισμικού, βλάβη εξυπηρετητή κτλ.)
- Ανθρώπινες απειλές που μπορεί να είναι σκόπιμες όταν προκύπτουν από εσκεμμένες κακόβουλες ενέργειες (κλοπή υλικού, μη-εξουσιοδοτημένη χρήση) ή ακούσιες (λάθη χρηστών, λάθη συντήρησης υλικού κτλ.)

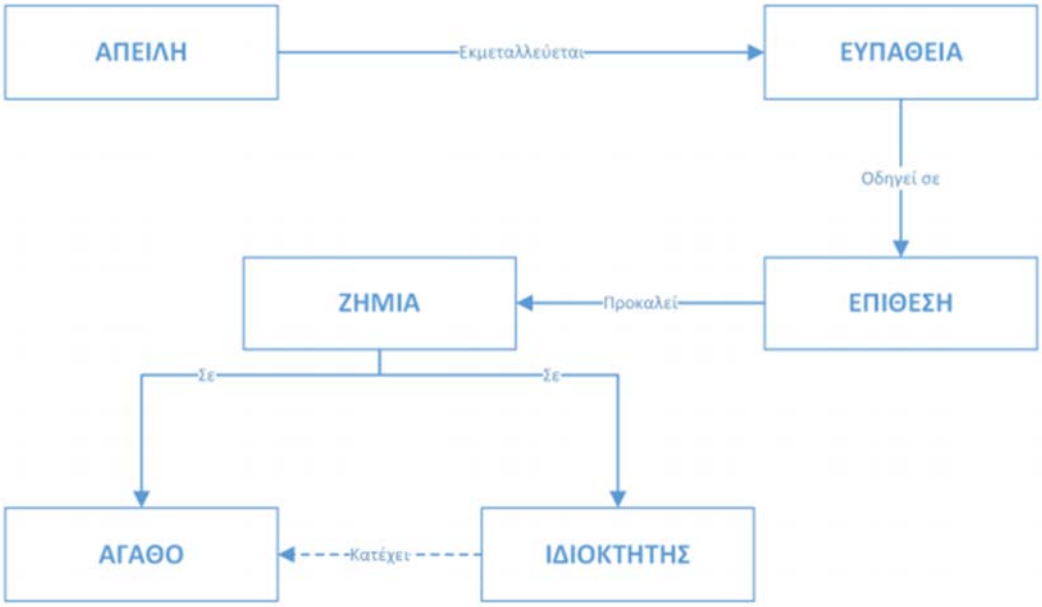
2.3.3 Ευπάθειες Πληροφοριακών Συστημάτων

Ευπάθεια (vulnerability) είναι μία αδυναμία/ευπάθεια ενός αγαθού ή ενός μέτρου ασφαλείας που μπορεί να εκμεταλλευτεί μία απειλή. Οι ευπάθειες αφορούν μια αδυναμία στις ρυθμίσεις ή τη διαχείριση του πληροφοριακού συστήματος ή ένα ευάλωτο σημείο σε ένα υποσύστημα ασφάλειας. Οι ευπάθειες μπορούν να κατηγοριοποιηθούν ως εξής (Μαυρίδης, 2015):

- Ευπάθειες υλικού (προβληματική κατασκευή, λανθασμένες ρυθμίσεις).
- Ευπάθειες λογισμικού (λανθασμένες ρυθμίσεις, έλλειψη τεκμηρίωσης εφαρμογών κτλ.).
- Ευπάθειες δικτύου (χρήση μη προστατευόμενων δημόσιων δικτύων, αποστολή πληροφοριών χωρίς κρυπτογράφηση).
- Ευπάθειες επικοινωνιών (κατασκευαστικές αδυναμίες, δυσλειτουργίες δικτυακών συνδέσεων).
- Φυσικές ευπάθειες (λόγω κατασκευής του κτηρίου, λόγω του χώρου όπου λειτουργεί ένα σύστημα).

- Ανθρώπινες ευπάθειες που είναι και από τις πιο επικίνδυνες.

Η συσχέτιση των βασικών εννοιών που περιγράφηκαν παραπάνω είναι αυτή που φαίνεται στην παρακάτω εικόνα.



Εικόνα 3: Συσχέτιση Βασικών Εννοιών (Πηγή: Μαυρίδης, 2015: 20)

2.3.4 Κατηγορίες επιθέσεων

Επίθεση (attack) είναι κάθε προσπάθεια για μη-εξουσιοδοτημένη πρόσβαση ή μη εξουσιοδοτημένη χρήση ενός αγαθού και κάθε προσπάθεια για την καταστροφή, τροποποίηση, κλοπή ή απενεργοποίηση του. Μπορούν να κατηγοριοποιηθούν ως εξής (Μαυρίδης, 2015: 21):

- Πλαστοπροσωπία (masquerading): Συμβαίνει όταν ένας μη εξουσιοδοτημένος χρήστης προσποιείται ότι είναι ένας νόμιμος χρήστης του Συστήματος για να αποκτήσει πρόσβαση σε αυτό ή για να αποκτήσει περισσότερα προνόμια από αυτά που είναι εξουσιοδοτημένος.

- Παθητική και ενεργή παρακολούθηση (active and passive tapping): Συμβαίνει όταν ο επιτιθέμενος αποκτά πρόσβαση στη διακίνηση δεδομένων και είτε τα τροποποιεί και εισάγει τα δικά του δεδομένα (ενεργή παρακολούθηση), είτε τα καταγράφει με σκοπό τη μετέπειτα ανάλυσή τους (παθητική παρακολούθηση).

- Αποποίηση (repudiation): Συμβαίνει όταν μια νόμιμα εξουσιοδοτημένη οντότητα αποποιείται τη συμμετοχή της σε μια ενέργεια (π.χ. αποστολή ενός μηνύματος) στο σύστημα ή ότι τροποποίησε δεδομένα.

- Άρνηση Εξυπηρέτησης (denial of service): Συμβαίνει όταν ο εισβολέας προκαλεί υπερβολική κατανάλωση ή δέσμευση πόρων προκειμένου να παρεμποδίσει την ομαλή λειτουργία συστήματος και την διαθεσιμότητα της υπηρεσίας.

- Κατανεμημένη επίθεση άρνησης εξυπηρέτησης (Distributed Denial of Service): Σχεδόν ίδια με την DOS, με τη διαφορά ότι ο εισβολέας έχει εγκαταστήσει το κακόβουλο λογισμικό σε δεκάδες συστήματα και τα οποία χρησιμοποιεί για να τα κατευθύνει προς συγκεκριμένο στόχο.

- Επανεκπομπή μηνυμάτων (replay): Είναι μία μορφή επίθεσης δικτύου στην οποία ο επιτιθέμενος συνδυάζει παθητική παρακολούθηση με καταγραφή μηνυμάτων και μεταγενέστερη επανεκπομπή (playback) τους (π.χ. κρυπτογραφημένα συνθηματικά).

- Ανάλυση επικοινωνίας (traffic analysis): Πρόκειται για μορφή παθητικής παρακολούθησης (ακόμη και κρυπτογραφημένων δεδομένων), με σκοπό την ανάλυση της κυκλοφορίας/διακίνησης δεδομένων. Η στατιστική και μόνο ανάλυση της επικοινωνίας, χωρίς απαραίτητα να γίνεται ανάγνωση των ίδιων των δεδομένων, μπορεί να οδηγήσει σε χρήσιμα συμπεράσματα για την επόμενη επίθεση.

- Κακόβουλο λογισμικό (malware): Λογισμικό του οποίου ο επιτιθέμενος επιδιώκει την εκτέλεση από νόμιμα εξουσιοδοτημένες οντότητες με σκοπό την εξαπόλυση πρόσθετων επιμέρους επιθέσεων. Είναι ένας γενικός όρος που περιλαμβάνει διάφορους τύπους απειλών όπως viruses, Trojan horses, worms, spyware, rootkits, botnets κτλ.

- Μη-εξουσιοδοτημένη τροποποίηση (unauthorized modification): Η κακόβουλη τροποποίηση των δεδομένων ενός συστήματος.

- Πλαστογράφηση (spoofing): Συμβαίνει όταν ένας εισβολέας αποκτά παράνομη πρόσβαση σε ένα Σύστημα χρησιμοποιώντας πλαστές πληροφορίες και διακρίνεται σε IP, ARP, Web και DNS Spoofing.

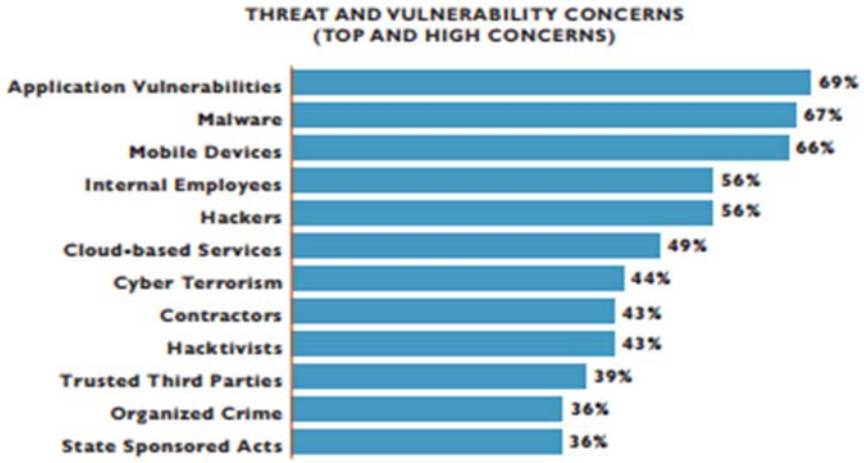
Γενικότερα, έχουν αναπτυχθεί πολλά μοντέλα για την κατηγοριοποίηση των απειλών. Ένα από αυτά είναι και ίσως το πιο γνωστό, είναι το STRIDE της Microsoft που εκτός από την κατηγοριοποίηση των απειλών, περιλαμβάνει και τρόπους για τον περιορισμό ή μετριασμό

(mitigation) του κινδύνου. Το STRIDE περιλαμβάνει έξι (6) κατηγορίες απειλών από αυτές που αναλύθηκαν παραπάνω και που είναι οι εξής:

- **S**poofing (Πλαστογράφηση)
- **T**ampering (Παρακολούθηση)
- **R**epudiation (Αποποίηση)
- **I**nformation disclosure (Αποκάλυψη Πληροφορίας)
- **D**enial of Service (Άρνηση Υπηρεσίας)
- **E**levation of Privilege (Απόκτηση *παράνομων* προνομίων χωρίς εξουσιοδότηση)

Το STRIDE βέβαια δημιουργήθηκε κυρίως για τον σχεδιασμό του λογισμικού. Σκοπός του δηλαδή είναι να βοηθήσει τους ειδικούς να σχεδιάσουν λογισμικό έχοντας αναγνωρίσει τους κινδύνους αλλά και τις απειλές που θα αντιμετωπίσουν. Με την χρήση του αναγνωρίζεις τα πιθανά προβλήματα ώστε κατόπιν να αναπτύξεις τους μηχανισμούς. Επίσης το πιο σημαντικό χαρακτηριστικό του είναι ότι βρίσκει τις απειλές, από ένα σημείο και μετά δηλαδή δεν έχει σημασία η κατηγοριοποίηση τους αλλά μόνο ο τρόπος που θα τις αντιμετωπίσεις.

Πάντως από έρευνα που έγινε από το Ponemon Institute για τις απειλές στην ασφάλεια των Οργανισμών, οι πιο σημαντικές από αυτές τις απειλές και οι πιο συχνές έχουν αποδειχτεί ότι είναι οι ευπάθειες των εφαρμογών (69%) και το κακόβουλο λογισμικό (67%).



Εικόνα 4. Απειλές στην Ασφάλεια των Οργανισμών (Πηγή: Global Information Security Workforce Study, 2013: 6)

Επιπρόσθετα οι κυριότεροι λόγοι για τους οποίους οι Οργανισμοί προσπαθούν να προστατεύσουν τα αγαθά τους και να αντιμετωπίσουν τους κινδύνους, όπως φαίνεται και στην παρακάτω εικόνα είναι (Global Information Security Workforce Study, 2013):

- Η προστασία της φήμης τους (83%)
- Η αποφυγή παραβιάσεων των νόμων και των κανονισμών (75%)
- Η μείωση του χρονικού διαστήματος (downtime) που θα είναι εκτός οι υπηρεσίες που προσφέρουν στους πελάτες τους (74%)
- Η προστασία της ιδιωτικής ζωής των πελατών τους (71%)
- Η αποφυγή κλοπής της πνευματικής της ιδιοκτησίας (58%)

Εικόνα 5. Προτεραιότητες Οργανισμών (Πηγή: Global Information Security Workforce Study, 2013, σελ.7)

2.3.5 Μέτρα Ασφαλείας

Τα Μέτρα Ασφαλείας (Security controls) ή Αντίμετρα (countermeasures), αφορούν όλες τις διαδικασίες, τις τεχνικές, τις ενέργειες και τις συσκευές που έχουν ως πρωταρχικό σκοπό να περιορίσουν τις ευπάθειες και τις απειλές του πληροφοριακού συστήματος. Ουσιαστικά σκοπός τους είναι η διασφάλιση του τρίπτυχου CIA που διασφαλίζει τις ικανότητες και λειτουργίες ενός Οργανισμού, μέσω της μείωσης της έκθεσης σε κίνδυνο για τα συστήματα, του περιορισμού της πιθανότητας επίθεσης και της μείωσης των κινδύνων.

Διακρίνονται σε τέσσερις μεγάλες κατηγορίες:

- Πρόληψη: τα αντίμετρα αυτά προσπαθούν να μειώσουν τον κίνδυνο από τις απειλές κατά των Π.Σ.

- Διασφάλιση: εργαλεία, έλεγχοι και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των παρόντων αντιμέτρων.

- Ανίχνευση: προγράμματα και τεχνικές για την έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών ασφαλείας.

- Επαναφορά: διαδικασίες που στοχεύουν στην γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον έπειτα από ρήξη ασφαλείας.

2.3.6 Κυβερνοασφάλεια

Η Κυβερνοασφάλεια ορίζεται ως όλες οι οργανωμένες ενέργειες οι οποίες απαιτούνται για να εξασφαλιστούν οι Πληροφορίες από κάθε κίνδυνο ή ρίσκο σε όλες του τις μορφές (ηλεκτρονικές ή φυσικές), καθώς και για να διασφαλιστούν τα συστήματα και τα δίκτυα, μέσω των οποίων γίνεται η αποθήκευση, η ανάκτηση, η επεξεργασία και η μεταφορά τους, συμπεριλαμβανομένων των ενεργειών που πρέπει να γίνονται, ώστε να προφυλάσσονται από εγκληματικές ενέργειες, δολιοφθορές, κατασκοπεία, ατυχήματα και αστοχίες.

Στους κινδύνους αυτούς περιλαμβάνονται και αυτοί που αφορούν την μείωση της εμπιστοσύνης και των παροχών μίας επιχείρησης προς τους πελάτες της και οι οποίοι αν δεν αντιμετωπιστούν επιτυχώς, είναι πολύ πιθανόν να επηρεάσουν σημαντικά την σχέση της με αυτούς, παραβιάζοντας την προστασία της ταυτότητας και της ιδιωτικής τους ζωής.

2.3.7 Η έννοια του Κινδύνου

Η έννοια του ρίσκου/Κινδύνου (Risk) έχει πολλές και διαφορετικές εφαρμογές σε όλες τις πτυχές της ζωής, στις επιστήμες αλλά και στις επιχειρήσεις, ενώ χρησιμοποιείται και με πολλούς τρόπους.

Ως Κίνδυνο λοιπόν, ορίζουμε την μεταβλητότητα των απροσδόκητων ενδεχομένων. Ρίσκο είναι επίσης το αποτέλεσμα της αβεβαιότητας σχετικά με τους στόχους που έχουν τεθεί.[1] Το αποτέλεσμα αυτό είναι μία απόκλιση από αυτό που αναμενόταν (θετική και/ή αρνητική). Αποτελείται από δύο συστατικά: την έκθεση και την αβεβαιότητα (Holton 2004). Γενικά είμαστε εκτεθειμένοι σε καταστάσεις που έχουν υλικές συνέπειες για εμάς, ενώ η έννοια της αβεβαιότητας ορίζεται ως η πιθανότητα να υπάρχουν δύο πιθανές εκβάσεις ενός περιστατικού ή μίας κατάστασης. Υπολογίζεται ως συνάρτηση τριών παραγόντων, των απειλών που αυτά αντιμετωπίζουν, των ευπαθειών τους και των επιπτώσεων που θα υπάρξουν από την πραγματοποίηση των απειλών.

Η έννοια του κινδύνου συνδέεται με την ποσοτικοποίηση της αβεβαιότητας. Στον επιστημονικό και οικονομικό χώρο, ο κίνδυνος εκφράζεται σε όρους πιθανότητας εμφάνισης των δυσμενών συμβάντων. Σε άλλους χώρους, όπως την αξιολόγηση του πολιτικού κινδύνου, ο κίνδυνος μπορεί να είναι ποιοτικός ή υποκειμενικός. Γενικά, υπάρχουν πολλά είδη κινδύνου, όπως είναι ο πολιτικός, ο οικονομικός, ο επιχειρησιακός, ο κίνδυνος ασφαλείας κτλ.

Σύμφωνα με τον Holton, ο επιχειρησιακός κίνδυνος σε μία συγκεκριμένη κατάσταση υπάρχει όταν υφίσταται αβεβαιότητα και αντιληπτή έκθεση σχετικά με μελλοντική κατάσταση που θα αποφέρει επιπτώσεις για ένα αντικείμενο. Ουσιαστικά είναι ο συνδυασμός της πιθανότητας να γίνει ένα ανεπιθύμητο γεγονός, με την επίπτωση (impact) που θα επιφέρει πάνω σε μία αξία.

Για να υφίσταται ο επιχειρησιακός κίνδυνος, πρέπει πρώτα να αναγνωρίζεται από έναν Οργανισμό. Για να μπορέσουν να τον αξιολογήσουν, είναι πολύ βασικό να γνωρίζουν από που προέρχεται και πως αυτό δημιουργείται. Μπορεί να δημιουργηθεί είτε από τον ανθρώπινο παράγοντα, είτε να προέλθει από απρόβλεπτους παράγοντες όπως τα φυσικά φαινόμενα (καιρός, σεισμοί).

Μία άλλη προσέγγιση στον ορισμό του, είναι ότι Επιχειρησιακός Κίνδυνος (operational risk), είναι ο Κίνδυνος απώλειας που προέρχεται από ανεπαρκής εσωτερικές διαδικασίες (internal processes), από ανθρώπους (people), από συστήματα λειτουργίας (systems) και εξωτερικές διαδικασίες (external risks).[2]

[1] ISO 31000. Risk Management and Guidelines.
[2] Basel Committee on Banking Supervision (2006). «International Convergence of Capital Measurement and Capital Standards-A Revised Framework».

Υπάρχουν διάφοροι τρόποι μέτρησης του Κινδύνου και της αβεβαιότητας των συστημάτων και των δικτύων. Προκειμένου να κατανοήσουμε τις έννοιες τους, πρέπει να είμαστε σε θέση να μετρήσουμε τα αποτελέσματα των εννοιών αυτών. Η Εκτίμηση Επικινδυνότητας (Risk assessment) προσδιορίζει την αξία των αγαθών, εντοπίζει τις ενδεχόμενες απειλές και ευπάθειες, εντοπίζει υπάρχοντα μέτρα ασφαλείας και πως αυτά επηρεάζουν την επικινδυνότητα, προσδιορίζει τις πιθανές επιπτώσεις και ιεραρχεί τους κινδύνους με βάση κριτήρια αξιολόγησης που θέτει το περιβάλλον εφαρμογής.

Η διαχείριση του Κινδύνου (Risk Management), παρέχει ένα πλαίσιο για την αξιολόγηση των ευκαιριών για κέρδος, καθώς επίσης και τη μέτρηση των απειλών για απώλειες. Με άλλα λόγια, η διαχείριση Κινδύνου είναι οι συντονισμένες δράσεις για να κατευθύνουν και να ελέγχουν έναν Οργανισμό σε ότι αφορά τον Κίνδυνο. Χωρίς τη μέτρηση του Κινδύνου, δε γίνονται αντιληπτό ποιες εναλλακτικές αποφάσεις πρέπει να ληφθούν για τη μείωση και την αντιμετώπιση του. Για αυτό απαιτείται μία ανάλυση κόστους που υπολογίζει τον παράγοντα της αβεβαιότητας.

Η αποτελεσματική διαχείριση λοιπόν του Κινδύνου που διέπουν τους κινδύνους στα συστήματα μίας επιχείρησης, προσπαθεί να βρει την χρυσή τομή μεταξύ κόστους και ωφέλειας τους ώστε αυτή η επένδυση να είναι συμφέρουσα και ωφέλιμη προς την επιχείρηση.[3] Για αυτό είναι ωφέλιμο πάντα για μία επιχείρηση, ανεξάρτητα του μεγέθους της, να καθορίσει τις προτεραιότητες της και να καθορίσει το ρίσκο που πρέπει να πάρει για μία επένδυση σε συστήματα Τ.Π.Ε, γνωρίζοντας ότι πιθανόν να μην έχει τα επιθυμητά αποτελέσματα στον βαθμό που θα ήθελε.

Στην παρούσα Διατριβή θα χρησιμοποιήσουμε τον ορισμό που αφορά τον λειτουργικό Κίνδυνο (Operational Risk) για έναν Οργανισμό γιατί μπορεί να απεικονίσει καλύτερα τους Κινδύνους που απειλούν ένα Π.Σ. Κίνδυνος λοιπόν σε ένα Π.Σ ορίζεται ως η αρνητική επίπτωση από την εκμετάλλευση μίας ευπάθειας λαμβάνοντας υπόψη την πιθανότητα και την διάσταση του γεγονότος αλλά και της ικανότητας και επάρκειας των ελέγχων ασφαλείας (Stoneburner et al. 2002:23). Συνεπώς ο Κίνδυνος μπορεί να οριστεί με την παρακάτω εξίσωση:

$$\boldsymbol{Κίνδυνος = Απειλή\ \chi\ Ευπάθεια\ \chi\ Κόστος}$$

[3] NIST Special Document 800-39 (2011) «Measuring Information Security Risk».

Όπου απειλή είναι η πιθανότητα να εμφανιστεί μία απειλή, ευπάθεια είναι η πιθανότητα επιτυχούς εκμετάλλευσης της από την απειλή και κόστος είναι η επίπτωση που πρόκειται να επιφέρει.

2.4 Κρίσιμες Υποδομές (ICT Infrastructure)

Στις περισσότερες προσεγγίσεις, οι κρίσιμες υποδομές συμπεριλαμβάνουν υλικά και πληροφοριακά αγαθά (assets), δίκτυα, υπηρεσίες και εγκαταστάσεις που αν καταστραφούν ή υποβαθμιστούν, θα έχουν αρνητικό αντίκτυπο στην Εθνική Ασφάλεια, την οικονομική και κοινωνική ευημερία ενός έθνους, αλλά και στην αποτελεσματική λειτουργία της Κυβέρνησης ενός κράτους (Brunner & Suter, 2008:36). Κύριο χαρακτηριστικό αυτών αποτελεί το γεγονός ότι όλες οι κρίσιμες υποδομές χρησιμοποιούν ευρέως και εξαρτώνται σε ισχυρό βαθμό από τις τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ). Σαν κρίσιμοι τομείς που πρέπει να προστατευτούν ορίζονται οι παρακάτω (Hyslop, 2004:10):

- Οικονομίας (Finance)
- Ενέργειας και πόροι (Energy and Resources)
- Παροχής τροφίμων (Food Supply)
- Υγείας (Health)
- Κυβερνητικές Υπηρεσίες (Government Services)
- Νόμος και τάξη (Law and Order)
- Βιομηχανίας (Manufacturing)
- Εθνικών συμβόλων (National Icons)
- Μεταφορών (Transports)
- Νερού (Water)
- Αποβλήτων (Waste water)
- Εκπαίδευση (Education)

- Πνευματική Ιδιοκτησία (Intellectual Property)

Επιπρόσθετα οι Κρίσιμες Υποδομές διακρίνονται σε τέσσερα (4) επίπεδα (Adar & Wuchner 2005: 5):

- Το Επιχειρηματικό/Στρατηγικό (business/strategic), το οποίο περιλαμβάνει την κεντρική επιχειρησιακή διαδικασία
- Το Οργανωτικό (organizational), το οποίο περιλαμβάνει τις διαδικασίες και την ανθρώπινη συμπεριφορά.
- Του Κυβερνοχώρου (Cyber Space), το οποίο σχετίζεται με τα δεδομένα και τα επικοινωνιακά και πληροφοριακά συστήματα και τέλος
- Το Φυσικό, όπου συναντάμε τις φυσικές συσκευές της κάθε υποδομής.

Στο σχετικό πλάνο για την προστασία κρίσιμων υποδομών των Η.Π.Α. [DHS, 2009] γίνεται ειδική αναφορά σε κυβερνουποδομές (Cyber Infrastructures). Αυτές περιλαμβάνουν ηλεκτρονικά, πληροφοριακά και επικοινωνιακά συστήματα, καθώς και την πληροφορία που εμπεριέχεται σε αυτά. Υπολογιστικά συστήματα καθώς και δίκτυα, όπως το διαδίκτυο, αποτελούν μέρος των κρίσιμων υποδομών.

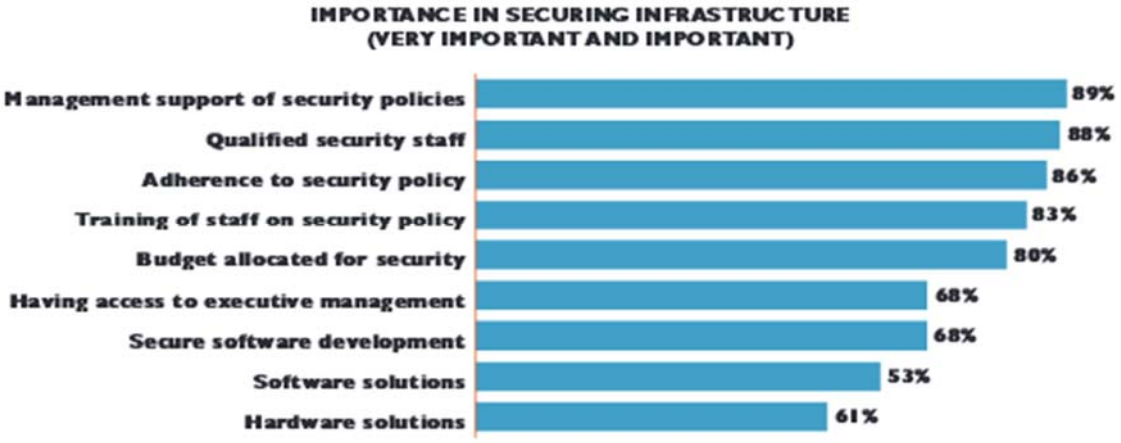
Η Προστασία Κρίσιμων Πληροφοριακών Υποδομών (Critical Information Infrastructure Protection-CIIP) αναφέρεται αποκλειστικά στην ασφάλεια και την προστασία των συνδέσεων και των λύσεων ΤΠΕ ανάμεσα στους διαφορετικούς τομείς υποδομών. Η προστασία των φυσικών στοιχείων των υποδομών (Critical Infrastructure Protection- CIP) διασφαλίζεται μέσα από ξεχωριστό οργανωτικό πλαίσιο και η μεταστροφή αυτή συνέβη κυρίως μετά τα γεγονότα της 11η Σεπτεμβρίου 2001, όπου υπήρξε μια μεταστροφή από την κλασσική έννοια της πληροφοριακής απειλής, η οποία παραπέμπει έντονα στην ασφάλεια πληροφοριών. Ειδικά στις Η.Π.Α., εστιάστηκε η προσοχή κυρίως σε δομικές απειλές, οι οποίες προκύπτουν μη τυχαία αλλά εσκεμμένα, με την αντιτρομοκρατική στρατηγική να παίζει κυρίαρχο ρόλο.

Γενικά, μια κρίσιμη πληροφοριακή και επικοινωνιακή υποδομή αποτελεί μέρος της εθνικής πληροφοριακής υποδομής η οποία είναι απαραίτητη για την παροχή κρίσιμων υπηρεσιών. Αποτελεί σε μεγάλο βαθμό μέρος του κρίσιμου τομέα των ΤΠΕ και περιλαμβάνει συστατικά όπως τηλεπικοινωνίες, υπολογιστές, λογισμικό, το διαδίκτυο, δορυφόρους, οπτικές ίνες κλπ. Ο όρος χρησιμοποιείται επίσης για το σύνολο των διασυνδεόμενων υπολογιστών και δικτύων και

των κρίσιμων ροών πληροφορίας μεταξύ τους. Ακριβώς λόγω αυτού του ρόλου διασύνδεσης υποδομών και καθώς αποτελούν και νέους δυνατούς στόχους, οι κρίσιμες πληροφοριακές υποδομές παίζουν σημαντικό ρόλο στην προστασία των κρίσιμων υποδομών γενικότερα. Μπορούν, λοιπόν, να θεωρηθούν ως η ραχοκοκαλιά των κρίσιμων υποδομών, δεδομένου ότι η απρόσκοπτη ανταλλαγή δεδομένων είναι απαραίτητη για τη λειτουργία των υποδομών και των αντίστοιχων υπηρεσιών τους.

Τέλος Οι Οργανισμοί θεωρούν πολύ σημαντική για την προστασία των Υποδομών τους (Global Information Security Workforce Study, 2013):

- Την υποστήριξη και τις πολιτικές ασφαλείας (89%)
- Την ποιότητα του εξειδικευμένου προσωπικού στην ασφάλεια (88%)
- Την προσήλωση στην πολιτική ασφαλείας (86%) και
- Την εκπαίδευση του προσωπικού στην ασφάλεια (83%).



Εικόνα 6. Σπουδαιότητα στην Προστασία των Κρίσιμων Υποδομών (Πηγή: Global Information Security Workforce Study, 2013: 10)

Κεφάλαιο 3
Συστήματα και Επιχειρήσεις

3.1 Εισαγωγή

Οι τεχνοοικονομικές πλευρές των συστημάτων Information and Communications Technology (ICT), αποτελούν ένα από τα πιο σημαντικά θέματα, στις εφαρμογές των επιστημών πληροφορικής. Μια κοινή άποψη, για τα συστήματα ICT, βασίζεται σε τεχνοοικονομικά μέτρα. Τα πρωτόκολλα επικοινωνίας, τα δίκτυα, οι υποδομές σε υλικό και οι εφαρμογές σε λογισμικό εφαρμόζονται σε κάθε πλαίσιο πληροφοριών ενός σύγχρονου οργανισμού.

Η ταχεία τεχνολογική εξέλιξη στην παραγωγή των μικροεπεξεργαστών και η συνεχιζόμενη μείωση του κόστους των υπολογιστών και όλων των σχετιζόμενων Συστημάτων Πληροφορικής και Επικοινωνίας, επέτρεψε τους σύγχρονους Οργανισμούς να κάνουν μεγάλες επενδύσεις για την αγορά τέτοιων Συστημάτων. Οι τεχνολογίες αυτές όμως, όπως και κάθε νέα τεχνολογία, απαιτούν χρόνο για να αναπτυχθούν, να ωριμάσουν και να αποφέρουν τα οφέλη που αναμένει ένας Οργανισμός.

Πριν όμως προχωρήσουμε με την επίδραση των Συστημάτων Τ.Π.Ε σε μία επιχείρηση, είναι απαραίτητο να δούμε συνοπτικά κάποιους ορισμούς που θα μας βοηθήσουν στην εύρεση αυτής της σχέσης μεταξύ των.

Απόδοση (Firm Efficiency)

Η εταιρική απόδοση είναι μια έννοια που εξηγεί την επιτυχία μιας επιχείρησης. Περιγράφει βασικά την απόδοση μίας επιχείρησης σε μία συγκεκριμένη χρονική περίοδο. Με την μέτρηση της απόδοσης μια επιχείρηση μπορεί να συγκρίνει τις επιδόσεις της σε διαφορετικές χρονικές περιόδους και, κατά συνέπεια, οι επιδόσεις διαφορετικών επιχειρήσεων μπορούν επίσης να συγκριθούν μεταξύ τους. Δύο διαφορετικές κατηγορίες μέτρησης της απόδοσης υπάρχουν: μία χρησιμοποιώντας οικονομικές μεθόδους και μία χωρίς την χρήση τους.

Καινοτομία (Innovation)

Η Καινοτομία είναι η μετατροπή μίας ιδέας σε εμπορεύσιμο προϊόν ή υπηρεσία. Η καινοτομία εμφανίζεται κυρίως σε οργανισμούς όπου υπάρχουν διαφορετικές γνώσεις που συνδυάζονται μεταξύ τους. Η καινοτομία δημιουργεί νέες δυνατότητες χρησιμοποιώντας αυτούς τους συνδυασμούς. Επομένως τα δύο σημαντικά κλειδιά φαίνεται να είναι η προσβασιμότητα στην κατάλληλη γνώση και εύρεση ο σωστός συνδυασμός των συνόλων γνώσης (Bessant et al., 2005). Δεδομένου ότι η καινοτομία αφορά κυρίως τη συνιστώσα της γνώσης, η διαχείριση αυτής της γνώσης καθίσταται εξαιρετικά σημαντική για την επιτυχή καινοτομία. Η τεχνολογία (ΤΠΕ) μπορεί να διαδραματίσει ζωτικό ρόλο στην ενίσχυση της καινοτομίας σε μια επιχείρηση.

3.2 Ιστορικό

Η αλματώδης τεχνολογική ανάπτυξη τις τελευταίες δεκαετίες των τεχνολογιών IT (Information Technology) ήταν εκπληκτική τόσο σε ταχύτητα όσο και σε γεωγραφική κάλυψη. Πλέον οι τεχνολογίες αυτές βρίσκονται σε κάθε σπίτι, σε κάθε δημόσιο και ιδιωτικό Οργανισμό. Ποιο ήταν όμως το σημείο καμπής για αυτήν την τεχνολογική επανάσταση; Αρκετοί μελετητές ορίζουν ως την απαρχή της Πέμπτης Τεχνολογικής Επανάστασης το 1971 με την κατασκευή του πρώτου μικροεπεξεργαστή (4004 microprocessor που χρησιμοποιήθηκε για την κατασκευή του πρώτου ηλεκτρονικού υπολογιστή για το σπίτι) από την Intel στην Καλιφόρνια των Η.Π.Α (Perez 2010:18, Freeman & Louca, 2001). Από το 1971 και μέχρι σήμερα ο κόσμος μας γνωρίζει μία τεράστια ανάπτυξη και μετασχηματίζεται τόσο κοινωνικά όσο και οικονομικά.

Οι τεχνολογίες και τα συστήματα Τ.Π.Ε, δεν είναι τίποτα παρά μία επέκταση της Τεχνολογίας Πληροφοριών με την ενσωμάτωση των τηλεπικοινωνιών (τηλεφωνικές γραμμές και ασύρματες επικοινωνίες). Όταν όμως αναφερόμαστε σε Τ.Π.Ε, εστιάζουμε κυρίως στην έννοια της Επικοινωνίας. Ο όρος Τ.Π.Ε λοιπόν περιλαμβάνει το υλικό, το λογισμικό, τα δίκτυα και τα μέσα ενημέρωσης για την συλλογή, αποθήκευση, επεξεργασία, εκπομπή και παρουσίαση της Πληροφορίας (σε μορφή ήχου/video ή σε μορφή δεδομένων) και άλλων συσχετιζόμενων υπηρεσιών (World Bank., 2014).

Σε μία ευρύτερη έννοια θα μπορούσαμε να πούμε ότι τα συστήματα Τ.Π.Ε είναι οι τεχνολογίες που χρησιμοποιούν ηλεκτρονικά μέσα για να εξυπηρετήσουν τον άνθρωπο διανέμοντας και

αποθηκεύοντας κάθε μορφή πληροφορίας και γνώσης. Χωρίς να διαχωρίζουμε αν ο όρος Τ.Π.Ε αναφέρεται σε συσκευές ή εφαρμογές, πάντα δίνουμε μία έμφαση στο ότι τα συστήματα αυτά υποστηρίζουν διάφορες τεχνοοικονομικές δραστηριότητες. Για αυτό τον λόγο υποστηρίζεται ότι οι Τ.Π.Ε μπορούν να ταξινομηθούν και ως μία μορφή Τεχνολογίας Γενικού σκοπού (General Purpose Technology, GPT), όπως είναι το αυτοκίνητο το ηλεκτρικό ρεύμα, τεχνολογίες δηλαδή που μπορούν να επηρεάσουν την κοινωνία και την οικονομία σε εθνικό ή παγκόσμιο επίπεδο (Jovanovic & Rousseau 2005:1184). Οι επιπτώσεις από την χρήση τους είναι τεράστιες και μπορούν να αλλάξουν τον τρόπο ζωής μας, τον τρόπο που σκεφτόμαστε και δουλεύουμε αλλά και τον τρόπο που επικοινωνούμε με τον συνάνθρωπο μας.

Τα τελευταία χρόνια και παρόλο την παγκόσμια οικονομική ύφεση, παρατηρείται μία σημαντική ενίσχυση για την παγκόσμια αγορά συστημάτων Τ.Π.Ε η οποία προέρχεται, κατά κύριο λόγο, από το γεγονός ότι έχει γίνει κατανοητό πόσο απαραίτητος είναι ο ψηφιακός μετασχηματισμός τόσο του δημόσιου, όσο και του ιδιωτικού τομέα. Παράλληλα, οι σύγχρονες τάσεις που συνδέονται με το "3rd Platform" (3η Πλατφόρμα) και αφορούν το Mobility (συσκευές, εφαρμογές, υπηρεσίες), το Cloud Computing (ιδιωτικό, δημόσιο, υβριδικό), τα Big Data - Analytics και τα Social Networks, εισέρχονται σε μία επόμενη φάση εξέλιξης, ενώ πλέον ετοιμαζόμαστε για την "4th Platform" (4η Πλατφόρμα), όπου κυρίαρχο ρόλο παίζουν οι εφαρμογές Επαυξημένης και Εικονικής Πραγματικότητας (Augmented/ Virtual Reality).[4]

Επιπρόσθετα, παρατηρείται το φαινόμενο της αυτοματοποίησης όλων των διαδικασιών, όπως και του ενισχυμένου ρόλου των smartphones. Στις τάσεις που θα παίξουν καθοριστικό ρόλο τα επόμενα χρόνια, περιλαμβάνονται ακόμη το Internet of Things (IoT), το 3D Printing, η Ρομποτική, τα Wearables, οι Λύσεις Ασφάλειας επόμενης γενιάς και τα Γνωστικά Συστήματα (Cognitive Systems).

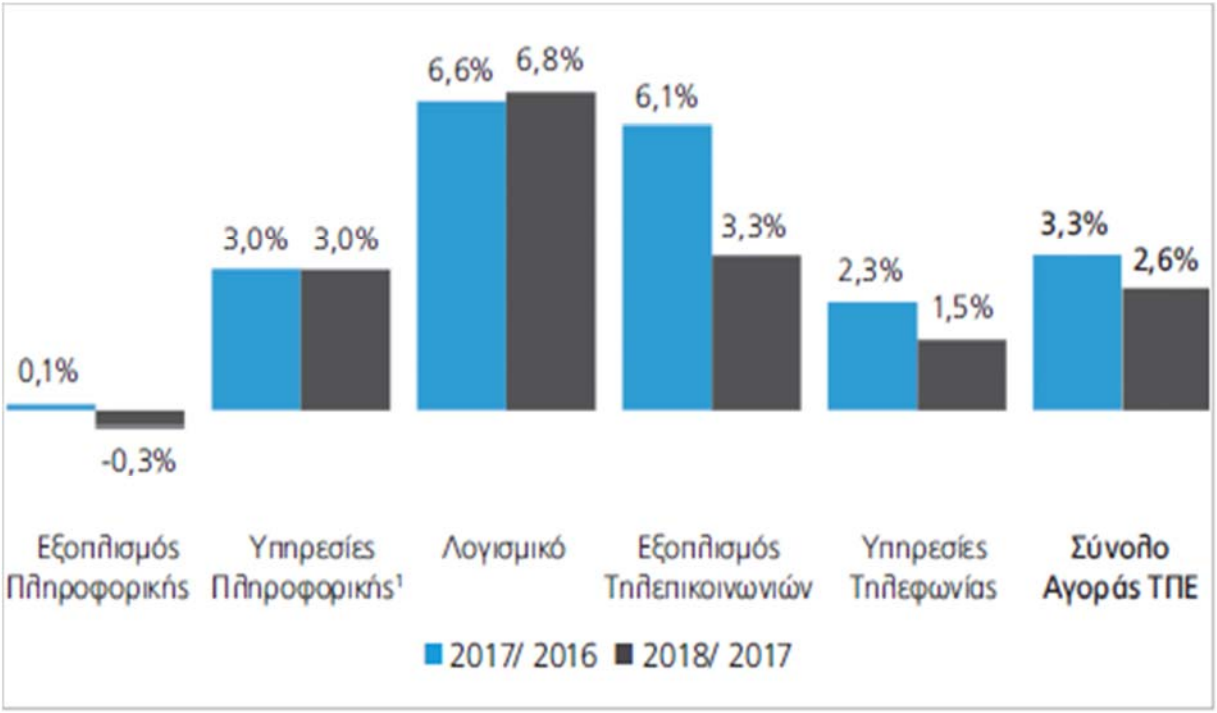
3.2.1 Στατιστικά Στοιχεία

Το 2016 η αξία της παγκόσμιας αγοράς ΤΠΕ αυξήθηκε κατά 3,2% σε σχέση με το 2015 και διαμορφώθηκε σε €3,084 τρις. Ο κλάδος θα συνεχίσει να κινείται ανοδικά και το 2017, καταγράφοντας αύξηση 3,3%, με την αξία της αγοράς να τοποθετείται στα €3,187 τρις. Τόσο ο τομέας Πληροφορικής, όσο και ο τομέας Τηλεπικοινωνιών, που συνιστούν τους δύο επιμέρους

[4] ICT MARKET REPORT 2017/ 2018. 2017.Τεύχος 13. «ΈΡΕΥΝΑ ΓΙΑ ΤΗΝ ΑΓΟΡΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΉΣ & ΕΠΙΚΟΙΝΩΝΙΏΝ 2017/ 2018»

πυλώνες του κλάδου ΤΠΕ, ενισχύθηκαν το 2016, με το πρόσημο να αναμένεται θετικό και για το 2017.

Συγκεκριμένα, η αξία της παγκόσμιας αγοράς Πληροφορικής αυξήθηκε 2,6% το 2016, φθάνοντας το €1,32 τρις. Για το 2017, αναμένεται ότι ο τομέας θα ενισχυθεί περαιτέρω κατά 3,4%, με την αξία της αγοράς να φθάνει στα €1,365 τρις. Η παγκόσμια αγορά Τηλεπικοινωνιών κατάφερε, το 2016, να βελτιώσει τις επιδόσεις της σε σχέση με ένα χρόνο νωρίτερα, ενώ αυξητική είναι η τάση και για το 2017. Η αξία της αγοράς, σε παγκόσμιο επίπεδο, διευρύνθηκε το 2016 κατά 3,7% και διαμορφώθηκε σε €1,763 τρις. Για το 2017, η αγορά θα κινηθεί επίσης ανοδικά, κατά 3,3%, με την αξία της αγοράς να ανέρχεται στα €1,822 τρις.



Εικόνα 7: Αξία Παγκόσμιας Αγοράς Τ.Π.Ε ανά κλάδο. (Πηγή: ΕΙΤΟ, επεξεργασία ΣΕΠΕ, 9/2017, σελ.4)

Η ανοδική τάση, που παρατηρείται στην παγκόσμια αγορά ΤΠΕ, παρά τη διεθνή οικονομική κρίση, δείχνει τη σημασία που έχουν αποκτήσει οι ψηφιακές τεχνολογίες, για όλους τους οικονομικούς κλάδους, τις επιχειρήσεις αλλά και τους οικιακούς καταναλωτές και επιβεβαιώνει την άποψη ότι έχουμε εισέλθει σε μία ψηφιακή εποχή.

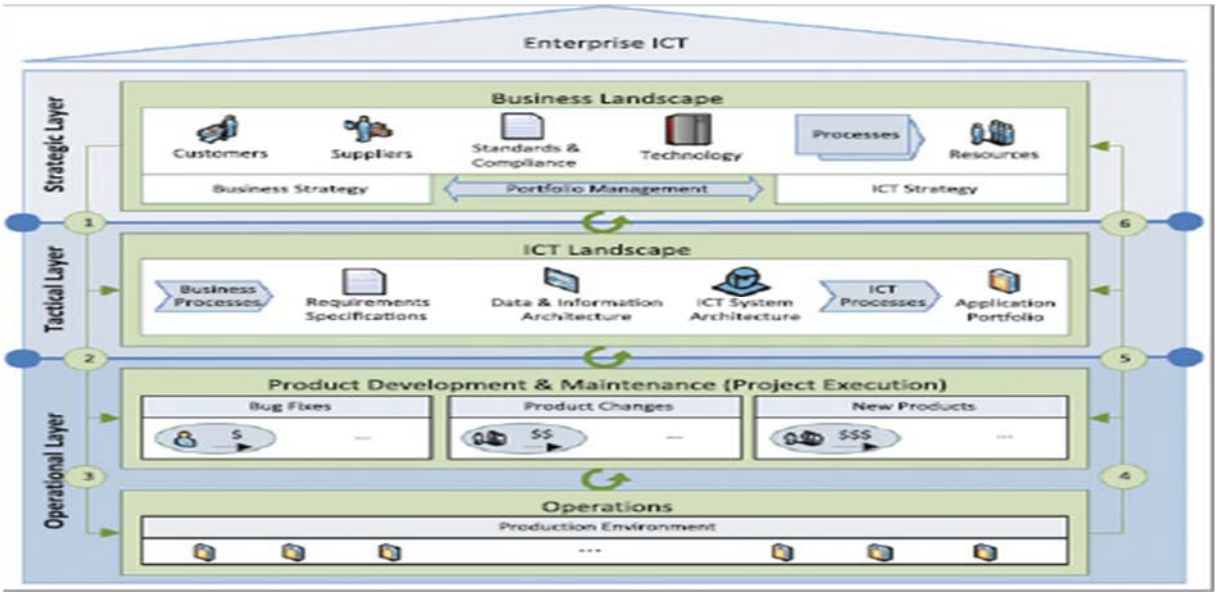
3.3 Αρχιτεκτονική των Επιχειρήσεων Τ.Π.Ε

Οι επιχειρήσεις την σημερινή εποχή εξαρτώνται σε μεγάλο βαθμό στα Συστήματα Τ.Π.Ε που όχι μόνο παρέχουν πληροφορίες στους χρήστες τους αλλά παίζουν και ένα πολύ σημαντικό ρόλο στην λήψη αποφάσεων. Σύμφωνα με τον Φιτσιλή (2015:33) «*η αρχιτεκτονική ενός πληροφοριακού συστήματος αποτελεί τη γέφυρα μεταξύ των επιχειρηματικών και των τεχνικών απαιτήσεων, η οποία επιτυγχάνεται με την καταγραφή και αντιστοίχιση των περιπτώσεων χρήσης του συστήματος με τις τεχνικές λύσεις που τις υλοποιούν».*

Στα πλαίσια λοιπόν του Οργανισμού, οι πληροφορίες που περιλαμβάνονται σε ένα Π.Σ υποστηρίζουν την λήψη αποφάσεων και τον έλεγχο μέσα σε αυτόν. Επιπλέον είναι η Τεχνολογία της Πληροφορίας και Επικοινωνίας (ΤΠΕ) που ένας Οργανισμός χρησιμοποιεί αλλά και ο τρόπος που οι άνθρωποι αλληλεπιδρούν με αυτήν την τεχνολογία για την υποστήριξη των επιχειρηματικών διαδικασιών.

Οι εισροές περιλαμβάνουν τα πρωτογενή δεδομένα που συλλέγονται μέσα στον Οργανισμό ή από το εξωτερικό του περιβάλλον. Όλα αυτά τα πρωτογενή δεδομένα μέσω της επεξεργασίας (processing) μετατρέπονται σε μία πιο κατανοητή μορφή και κατόπιν οι επεξεργασμένες αυτές πληροφορίες από τις εκροές μεταφέρονται στους ανθρώπους ή στις δραστηριότητες που θα τις χρησιμοποιήσουν. Αυτές οι πληροφορίες είναι απαραίτητες μέσα στον Οργανισμό για την λήψη αποφάσεων, τον έλεγχο των λειτουργιών αλλά και για την παραγωγή νέων προϊόντων ή υπηρεσιών.

Μία επιχείρηση Τ.Π.Ε περιλαμβάνει τρία (3) στρώματα: το στρατηγικό, το τακτικό και το επιχειρησιακό επίπεδο (Wieczorek et al, 2014:33). Το στρατηγικό επίπεδο περιλαμβάνει όλες τις στρατηγικές για την επιχείρηση και τις Τ.Π.Ε, τα πρότυπα και τους κανονισμούς για την συμμόρφωση με τους διεθνείς νόμους, τις τεχνολογικές τάσεις αλλά και τις διαδικασίες που εφαρμόζονται σε μία επιχείρηση. Στο τακτικό επίπεδο εφαρμόζονται οι στρατηγικές του στρατηγικού επιπέδου και περιέχονται όλα τα συστήματα Τ.Π.Ε, ο σχεδιασμός, η συντήρηση και η παρακολούθηση τους. Στο επιχειρησιακό επίπεδο γίνεται η χρήση των συστημάτων Τ.Π.Ε ενώ σε αυτό περιλαμβάνεται και η υποστήριξη του πελάτη της επιχείρησης.



Εικόνα 8. Αρχιτεκτονική Επιχείρησης Τ.Π.Ε (Πηγή: Wieczorek et al.. 2014:33)

Υπάρχουν πολλά είδη Πληροφοριακών Συστημάτων που μπορούν να χρησιμοποιηθούν σε έναν Οργανισμό ανάλογα με τις ανάγκες αλλά και τις οικονομικές δυνατότητες του. Με βάση το ιεραρχικό επίπεδο που υποστηρίζουν σε έναν Οργανισμό/Επιχείρηση διακρίνονται στις παρακάτω τρεις (3) κατηγορίες (Laudon & Laudon, 2011):

- **Στο Εκτελεστικό επίπεδο που ένας Οργανισμός χρησιμοποιεί Συστήματα Επεξεργασίας Συναλλαγών (Transaction Processing Systems-TPS)** που υποστηρίζουν τις βασικές δραστηριότητες και συναλλαγές μίας επιχείρησης (πωλήσεις, εισπράξεις, μισθοδοσία).

- **Στο Διοικητικό επίπεδο που ένας Οργανισμός χρησιμοποιεί Πληροφοριακά Συστήματα Διοίκησης (Management Information Systems-MIS) και Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems-DSS)**, που εξυπηρετούν τον έλεγχο και την λήψη αποφάσεων στο μεσαίο επίπεδο της επιχείρησης.

- **Στο Στρατηγικό επίπεδο που ένας Οργανισμός χρησιμοποιεί Συστήματα Υποστήριξης Διοίκησης (Executive Control Systems-ESS)** που εξετάζουν τα στρατηγικά ζητήματα μίας επιχείρησης σε σχέση με το εξωτερικό περιβάλλον. Περιλαμβάνουν τις στρατηγικές για την επιχείρηση και τις Τ.Π.Ε

Σε πολλές μελέτες στους τύπους αυτούς περιλαμβάνονται και τα Συστήματα Επιπέδου Γνώσης που αναφέρονται κυρίως στο εξειδικευμένο προσωπικό ενός Οργανισμού και βοηθούν μία επιχείρηση στην αφομοίωση της νέας επιχειρηματικής γνώσης.

Οι τέσσερις διαφορετικές κατηγορίες Πληροφοριακών Συστημάτων που αναφέρθηκαν παραπάνω είναι (Laudon and Laudon 2011:45):

- **Συστήματα Επεξεργασίας Συναλλαγών (Transaction Processing Systems/TPS).** Τα συστήματα αυτά που απευθύνονται κυρίως στα κατώτερα στελέχη, σε καθημερινή βάση πραγματοποιούν και ελέγχουν όλες τις απαραίτητες συναλλαγές που χρειάζεται μία επιχείρηση για να λειτουργήσει (πωλήσεις, παραγγελίες, ισοζύγια πελατών, κατάσταση αποθεμάτων). Παρακολουθούν επίσης όλες τις εσωτερικές λειτουργίες της επιχείρησης αλλά και τη σχέση της με το εξωτερικό περιβάλλον. Παραδείγματα TPS αποτελούν η μαζική επεξεργασία δοσοληψιών (batch processing), η επεξεργασία σε πραγματικό χρόνο (real-time processing), ο διαμοιρασμός χρόνου (timesharing) και η επεξεργασία δοσοληψιών (transaction processing) (Φυτσιλής 2014:8).

- **Πληροφοριακά Συστήματα Διοίκησης (Management Information Systems/MIS).** Εξυπηρετούν το διοικητικό επίπεδο μίας επιχείρησης παρέχοντας τις απαραίτητες αναφορές για την απόδοση της (π.χ. ανάλυση της παραγωγής, συγκεντρωτικές καταστάσεις εσόδων-εξόδων, δημιουργία στατιστικών προβλέψεων και τάσεων). Πρωταρχικός τους σκοπός είναι η επεξεργασία δεδομένων για την εξαγωγή πληροφοριών. Χρησιμοποιούνται επίσης για τον έλεγχο της επιχείρησης αλλά και για να προβλέψουν την μελλοντική της απόδοση (πχ πρόβλεψη πωλήσεων).

- **Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems/DSS).** Εξυπηρετούν και αυτά το διοικητικό επίπεδο και επικεντρώνονται κυρίως σε θέματα/προβλήματα που είναι μοναδικά και αλλάζουν διαρκώς και οι διαδικασίες για την επίλυση τους δεν είναι προκαθορισμένες σε αντίθεση με τα συστήματα MIS. Χρησιμοποιούνται κυρίως για τον προγραμματισμό, την μελέτη εναλλακτικών λύσεων και την λήψη αποφάσεων και τις περισσότερες φορές περιλαμβάνουν μεθοδολογίες βέλτιστων αποφάσεων (προγραμματισμός παραγωγής, σχεδιασμός πολιτικής μάρκετινγκ).

- **Συστήματα Υποστήριξης Διοίκησης ή Υποστήριξης Ανώτερων Στελεχών (Executive Support Systems).** Χρησιμοποιούνται στο στρατηγικό επίπεδο από τα ανώτερα στελέχη μιας επιχείρησης και καλύπτουν όλο το εύρος μιας επιχείρησης και παρακολουθούν όλους τους κρίσιμους δείκτες της. Επιπρόσθετα, χρησιμοποιούνται για την λήψη αποφάσεων που δεν μπορούν να ληφθούν στα προηγούμενα επίπεδα (τι στόχους έχει η επιχείρηση για τα επόμενα χρόνια, τι προϊόντα θα παράγει σε βάθος

χρόνου). Ένα άλλο χαρακτηριστικό τους είναι η ποικιλία προβολής των πληροφοριών, για παράδειγμα σε μορφή γραφικών παραστάσεων, σε μορφή πινάκων ή σε μορφή αναφορών κειμένου.

Σαφώς με την εξέλιξη της τεχνολογίας αλλά και των επιχειρήσεων, έχουν αναπτυχθεί και επιπλέον Πληροφοριακά Συστήματα που εξυπηρετούν τα διάφορα επίπεδα σε έναν Οργανισμό αλλά και τις διαφορετικές του ανάγκες, όπως τα:

- ERP [(Enterprise Resource Planning) που αποτελείται από ένα σύνολο εφαρμογών λογισμικού που ενσωματώνουν πληροφορίες και διαδικασίες από διάφορες λειτουργίες της επιχείρησης],

- Συστήματα Αυτοματισμού Γραφείου (Office Automation Systems-OAS) και Συστήματα Διαχείρισης Γνώσης (Knowledge Work Systems-KMS) που βοηθούν μία επιχείρηση στο γνωστικό της επίπεδο. Ουσιαστικά τα συστήματα KMS βοηθούν τους εργαζομένους στην επιχείρηση να δημιουργήσουν γνώση και να την ενσωματώσουν σε αυτήν, ενώ τα συστήματα OAS διαχειρίζονται αρχεία κειμένων και προγραμματίζουν μέσω ηλεκτρονικού ημερολογίου.

- CRM Customer Relationship Management -CRM) που έχει σαν στόχο την συλλογή πληροφοριών που βοηθούν στο διοικητικό προσωπικό μιας εταιρείας στο να διαχειριστεί με τον καλύτερο δυνατό τρόπο τις σχέσεις της με τους πελάτες της.

- Τα Έμπειρα Συστήματα (Expert Systems-ES) που αποτελούν μία ειδική κατηγορία συστημάτων και είναι σχεδιασμένα και μπορούν να εκτελεστούν από επαγγελματίες μέσα σε πολύ μικρό χρονικό διάστημα. Ουσιαστικά αποτυπώνουν τις γνώσεις πεπειραμένων εργαζομένων με την μορφή ενός συνόλου κανόνων.

Η θεμελιώδης βάση όλης αυτής της Αρχιτεκτονικής αποτελείται από τέσσερα (4) διαφορετικά συστατικά (Wieczorek et al., 2014:31):

- Τους Ανθρώπους που απαρτίζουν την επιχείρηση (εργαζομένους, managers, μετόχους), που ουσιαστικά δημιουργούν ένα σύστημα που αποτελεί το μυαλό της επιχείρησης.

- Τις Διαδικασίες που δημιουργούν την σχέση μεταξύ της τεχνολογίας και των ανθρώπων.

- Τα Προϊόντα που είναι αυτά που κατασκευάζει και προσφέρει η επιχείρηση και τέλος

- Τα έργα και το χαρτοφυλάκιο που περιλαμβάνουν τους στόχους της επιχείρησης που περιορίζονται όμως μέσα σε έναν προϋπολογισμό.

3.4 Συστήματα και Οικονομική Ανάπτυξη

Η οικονομική ανάπτυξη είναι ένα σημαντικό πεδίο της θεωρίας των μακροοικονομικών. Μία από τις εγκυρότερες θεωρίες που έχουν αναπτυχθεί σχετικά είναι το μοντέλο του Robert Solow. Το μοντέλο αυτό ποσοτικοποιεί την ανάπτυξη ως γινόμενο τεσσάρων παραγόντων: της παραγωγικότητας, του κεφαλαίου, της αύξησης του πληθυσμού και της τεχνολογικής προόδου.[5] Νεότερες μελέτες έδειξαν ότι η τεχνολογική πρόοδος είναι η κύρια αιτία της οικονομικής ανάπτυξης (Grossman and Helpman, 1991) με τις τεχνολογίες Τ.Π.Ε στο επίκεντρο αυτών. Οι τεχνολογίες αυτές δημιούργησαν νέες αγορές, - προσωπικοί υπολογιστές, λογισμικό και υπηρεσίες που βασίζονται στις ΤΠΕ - με αποτέλεσμα να σημειωθεί επανάσταση στις παραγωγικές μεθόδους σε πολλές βιομηχανίες και να αναπτυχθεί ο τομέας των υπηρεσιών (Επιτροπή των Ευρωπαϊκών Κοινοτήτων, 2003: 4). Οι καινοτομίες αυτές και κυρίως ο προσωπικός υπολογιστής ή το internet και η συνεχιζόμενη μείωση των τιμών τους, έφερε την παγκόσμια αποδοχή αυτών των συστημάτων.

Αρχικά και στις πρώτες σχετικά μελέτες για την επίπτωση της χρήσης των συστημάτων Τ.Π.Ε αναφέρθηκαν αρνητικά ή καθόλου σημαντικά αποτελέσματα (Oliner & Sichel 1994:285, Jorgenson & Stiroh 1995:45) και αυτό το γεγονός είχε ήδη ωθήσει τον Robert Solow να μιλήσει από το καλοκαίρι του 1987 για το «παράδοξο της παραγωγικότητας». Συγκεκριμένα ανέφερε ότι *μπορείς να δεις παντού τους ηλεκτρονικούς υπολογιστές εκτός από τους στατιστικούς δείκτες της παραγωγικότητας*.

Συγκεκριμένα και ενώ στα αρχικά στάδια της εμφάνισης των υπολογιστών, οι εταιρείες επένδυσαν τεράστια κεφάλαια στις Τ.Π.Ε (τις δύο πρώτες δεκαετίες κυρίως σε Τ.Π), η παραγωγικότητα εμφάνιζε αρνητικές μετρήσεις αντί για θετικές. Το παράδοξο αυτό αναλύθηκε

[5] https://el.wikipedia.org/wiki/Οικονομική_ανάπτυξη#Ιστορικό_της_έννοιας

σε πάρα πολλές μελέτες και πέρασε από πέντε (5) διαφορετικά στάδια (Macdonald et al. 2000 :3-4):

- Πάντα μετά από μία μεγάλη εφεύρεση υπάρχει πολύ μεγάλη αναμονή για τις καινοτομίες που μπορεί να επιφέρει. Στο αρχικό στάδιο πολλοί πίστευαν ότι τα συστήματα Τ.Π.Ε μπορούσαν να αντικαταστήσουν πλήρως την ανθρώπινη εργασία μειώνοντας τα συνολικά έξοδα μίας επιχείρησης. Επίσης υπήρχε η αντίληψη ότι η αύξηση της παραγωγικότητας θα οφειλόταν κυρίως στην επίδραση της νέας τεχνολογίας.

- Προς τα τέλη της δεκαετίας του 1970, φάνηκε ξεκάθαρα ότι οι επιπτώσεις δεν ήταν αυτές που αναμενόταν. Ωστόσο οι εταιρείες συνέχιζαν να επενδύουν τεράστια ποσά, για την εποχή, για την αγορά συστημάτων πληροφορικής, χωρίς να προσπαθήσουν να αξιολογήσουν αυτά τα συστήματα ή να ελέγξουν αν η επένδυση ήταν κερδοφόρα.

- Στο τρίτο στάδιο, υπήρχε η αντίληψη ότι παραγωγικότητα δεν συνδέονταν άμεσα με την νέα τεχνολογία, ενώ οι εταιρείες προσπάθησαν να χρησιμοποιήσουν τα συστήματα Τ.Π.Ε για να αποκτήσουν στρατηγικό πλεονέκτημα στην αγορά έναντι των ανταγωνιστών τους.

- Κάπου στα τέλη της δεκαετίας του 1980, οι εταιρείες ξεκίνησαν να επενδύουν σε συστήματα Τ.Π διοίκησης (Management Information Systems/MIS), κυρίως συστήματα επιτήρησης και ελέγχου που δεν αναμένονταν να είναι πλήρως παραγωγικά.

- Τις τελευταίες δύο (2) δεκαετίες οι περισσότερες επενδύσεις γίνονται σε συστήματα επικοινωνίας.

Οι αναλυτές προκειμένου να εξηγήσουν τους αριθμούς για το παράδοξο της παραγωγικότητας, επισήμαναν πως είτε τα συμβατικά στατιστικά στοιχεία δεν μετρούσαν σωστά την πραγματική αξία της καινοτομίας, είτε ότι η φαινομενική εξέλιξη της καινοτομίας ήταν στην πραγματικότητα μια ψευδαίσθηση. Προς τα μέσα της δεκαετίας του 1990 απομονώθηκαν τέσσερα (4) πιθανά αίτια για την επεξήγηση του παράδοξου (Brynjolfsson E. 1993:71):

- Λανθασμένες μετρήσεις στις εισροές και εκροές των Οργανισμών

- Καθυστέρηση στην μέτρηση των ωφελειών που επέφερε η νέα τεχνολογία καθώς ήταν δύσκολο στην αρχή να μετρηθούν αυτές οι επιπτώσεις.

- Η ανακατανομή των κερδών από τα συστήματα Τ.Π.Ε σε άλλες δραστηριότητες ενός Οργανισμού με αποτέλεσμα να μην φαίνεται αν η νέα τεχνολογία είναι κερδοφόρα.

- Κακή διαχείριση της νέας τεχνολογίας.

Η εικόνα όμως αυτή άρχιζε να αλλάζει όταν ξεκίνησαν να μετριούνται στοιχεία σε μικροοικονομικό επίπεδο, στις ίδιες τις επιχειρήσεις. Κοινή διαπίστωση των ερευνητών είναι ότι η πληροφορική έχει θετική και σημαντική επίδραση στην παραγωγικότητα, ενώ πρέπει να εξεταστεί αναλυτικά το τι συμβαίνει στην ίδια την επιχείρηση. Παρατηρήθηκε ότι όμοιες επιχειρήσεις με παρόμοια ποσά επένδυσης στα συστήματα Τ.Π παρουσίαζαν διαφορετικές επιδόσεις. Επίσης μετρήθηκαν και αναλύθηκαν τα μακροπρόθεσμα οφέλη της πληροφορικής που είναι κατά πολύ μεγαλύτερα από τα βραχυπρόθεσμα. Έτσι η προσοχή εστιάσθηκε στις οργανωτικές αλλαγές, που πρέπει να συνοδεύουν μία επένδυση σε συστήματα Τ.Π.Ε και που είναι αναμενόμενο να απαιτούν περισσότερο χρόνο για υλοποίηση και απόδοση.

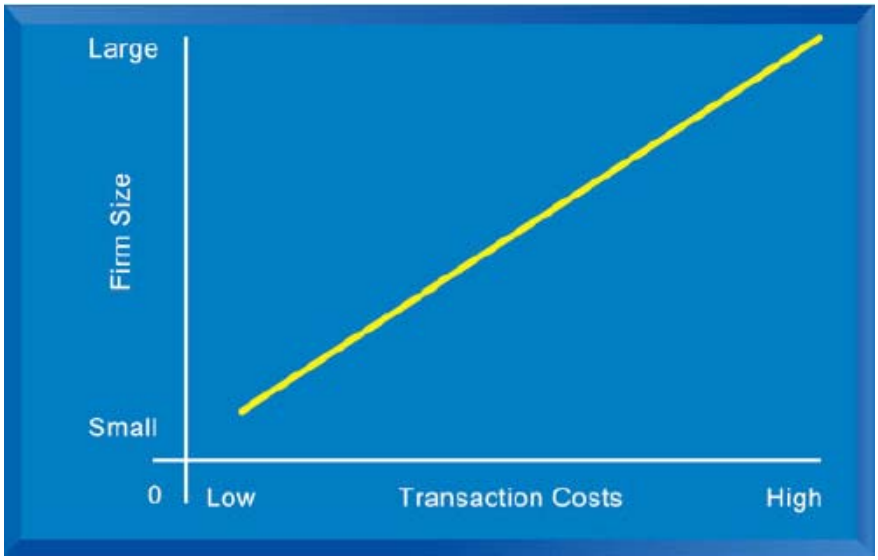
Σταδιακά δημιουργήθηκε η εικόνα ότι τα συστήματα Τ.Π.Ε δεν αυξάνουν την παραγωγικότητα αυτόματα αλλά αποτελούν αναπόσπαστο μέρος ενός ευρύτερου συστήματος οργανωτικών αλλαγών μέσα σε μία επιχείρηση (Brynjolfsson & Hitt., 2000:45). Στην ίδια εξάλλου μελέτη, οι Brynjolfsson και Hitt μελετώντας περιπτώσεις εταιρειών και χρησιμοποιώντας οικονομικά στοιχεία, κατέληξαν ότι τα συστήματα Τ.Π.Ε συνεισφέρουν πολύ περισσότερο από ότι πιστευόταν έως τότε, με την συνδρομή τους στην αλλαγή των επιχειρησιακών διαδικασιών, στην αλλαγή των απαιτούμενων προσόντων και δεξιοτήτων των εργαζομένων και στην αλλαγή των επιχειρησιακών δομών των ίδιων των Οργανισμών.

Εκτός όμως από την μικροοικονομική θεωρία όπου οι νέες τεχνολογίες και ειδικότερα οι Τ.Π.Ε θεωρούνται ως συντελεστές της παραγωγής που υποκαθιστούν το κεφάλαιο και την εργασία, υπάρχουν δύο ακόμη προσεγγίσεις για την επίδραση των πληροφοριακών συστημάτων στις επιχειρήσεις που απλά θα αναφερθούν σε αυτήν την μεταπτυχιακή διατριβή. Αυτές είναι η θεωρία κόστους συναλλαγών (transaction cost theory) και η θεωρία των αντιπροσώπων (agency theory) (Laudon & Laudon, 2011:89).

Η θεωρία του κόστους συναλλαγών θεωρεί την επιχείρηση ως μία δομή και αναφέρεται στο κόστος που απαιτείται για την παροχή κάποιου αγαθού ή υπηρεσίας μέσω της αγοράς αντί να παρέχεται από την ίδια την επιχείρηση ή γενικότερα στο κόστος που προκύπτει για την πραγματοποίηση μίας οικονομικής συναλλαγής. Η θεωρία του

κόστους συναλλαγών προϋποθέτει ότι οι επιχειρήσεις προσπαθούν αφενός να ελαχιστοποιήσουν το κόστος ανταλλαγής πόρων με το εξωτερικό τους περιβάλλον και αφετέρου προσπαθούν να μειώσουν το γραφειοκρατικό κόστος μέσα στην επιχείρηση. Σύμφωνα λοιπόν με την θεωρία αυτή, οι επιχειρήσεις υπάρχουν επειδή μπορούν να διεξάγουν συναλλαγές/δοσοληψίες εσωτερικά με πιο φθηνό τρόπο από ότι με εσωτερικές επιχειρήσεις στην αγορά, ουσιαστικά δηλαδή όταν διευρύνονται. Στην επιχείρηση έρχεται κόστος όταν εισέρχεται σε μία αγορά την οποία δεν έχει η ίδια δημιουργήσει. Αυτό είναι το κόστος συναλλαγών, το κόστος που υφίσταται μια επιχείρηση όταν αγοράζει από την αγορά αυτά που δεν μπορεί να παράγει η ίδια.

Τα πληροφοριακά συστήματα βοηθούν στη μείωση του κόστους συμμετοχής σε μία αγορά (κόστους συναλλαγών) κάνοντας ελκυστική τη δραστηριοποίηση σε αυτήν, χωρίς να αυξηθεί το μέγεθος του Οργανισμού όπως φαίνεται και στην παρακάτω εικόνα.



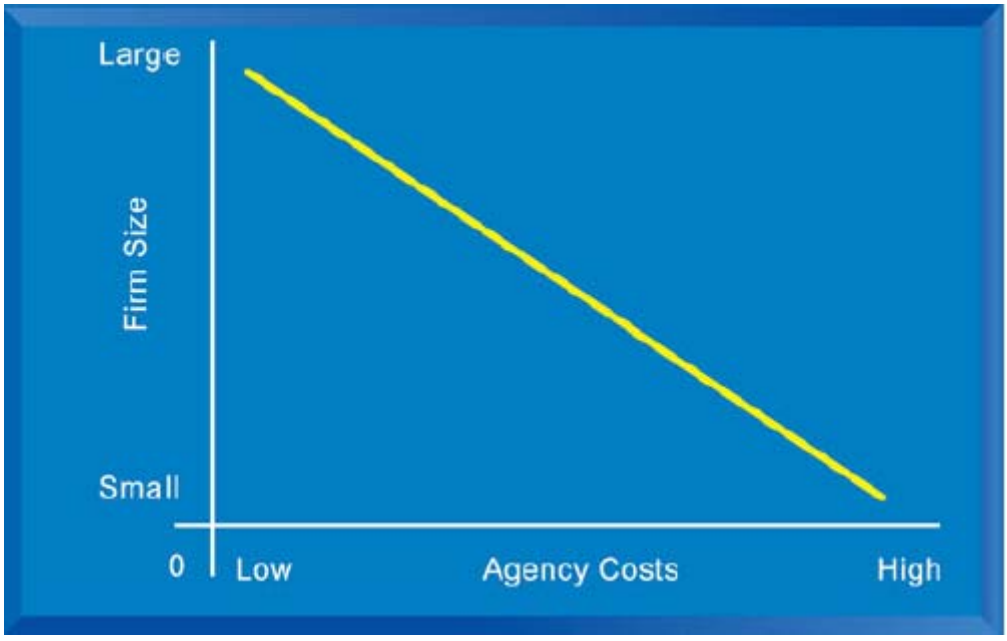
Εικόνα 9. Κόστος Συναλλαγών και Μέγεθος Οργανισμού (Πηγή: Laudon and Laudon, σελ.90)

Από την πλευρά της θεωρίας της αντιπροσώπευσης η οποία αρχικά εδραιώθηκε από το έργο του Adam Smith (1776) και στη συνέχεια στους σύγχρονους καιρούς από αυτό των Berle και Means (1933), η επιχείρηση είναι ένα πλέγμα από συμβάσεις ανάμεσα σε ενδιαφερόμενα άτομα και όχι μία οντότητα ενοποιημένη που ζητά μεγιστοποίηση κέρδους. Η θεωρία της αντιπροσώπευσης αναφέρεται στη σχέση που υπάρχει μεταξύ δύο μερών σε μία επιχείρηση, αφενός δηλαδή του κυρίου (principal) ή αλλιώς εντολέα και αφετέρου του αντιπροσώπου (agent) ή αλλιώς εντολοδόχου. Συγκεκριμένα, με τη

θεωρία αντιπροσώπευσης προσδιορίζεται η σχέση όπου ο εντολέας αναθέτει συγκεκριμένη εργασία και συγκεκριμένες αρμοδιότητες και εξουσίες, μέσα στα πλαίσια δράσης μιας οικονομικής οντότητας, στον αντιπρόσωπο.

Όταν προκύπτει σχέση αντιπροσώπευσης στις επιχειρήσεις, προκύπτει μία τάση για αύξηση του κόστους αντιπροσώπευσης (Agency costs). Ως κόστος αντιπροσώπευσης ορίζεται ως το κόστος που πραγματοποιείται προκειμένου να διατηρηθεί μία αποτελεσματική σχέση αντιπροσώπευσης, δηλαδή προκειμένου να μμειωθεί το δυνητικό χάσμα που υπάρχει, είτε σε πληροφοριακό επίπεδο είτε σε επίπεδο δράσης της διοίκησης, μεταξύ του εντολέα και του εντολοδόχου. Πρωταρχικός σκοπός αυτής της θεωρίας αντιπροσώπευσης είναι η διατήρηση και η ενίσχυση της αξίας και η προστασία των μετόχων και ως εκ τούτου η εταιρική δομή διαμορφώνεται σε πλαίσια για την εξυπηρέτηση αυτού του σκοπού.

Για να το εξειδικεύσουμε στην χρήση των συστημάτων Τ.Π.Ε, οι αντιπρόσωποι (εργαζόμενοι) μιας επιχείρησης χρειάζονται επίβλεψη προκειμένου να υλοποιούν τους στόχους της. **Όσο μεγαλώνει η επιχείρηση, το κόστος αντιπροσώπευσης και συντονισμού των αντιπροσώπων αυξάνει με την τεχνολογία των Πληροφοριών να μειώνει το κόστος αντιπροσώπευσης διευκολύνοντας την επίβλεψη και τον έλεγχο των εργαζομένων.**



Εικόνα 10. Κόστος Αντιπροσώπευσης και Μέγεθος Οργανισμού (Πηγή: Laudon and Laudon, σελ. 91)

Σαν συμπέρασμα πρέπει να καταλάβουμε ότι η φύση της συγκεκριμένης τεχνολογίας είναι τέτοια ώστε να μην μπορεί απλά να θεωρηθεί ως μία επένδυση κεφαλαίου, αλλά ως αναπόσπαστο κομμάτι του επιχειρηματικού σχεδιασμού και των λειτουργιών. Τα χαρακτηριστικά που ξεχωρίζουν τη θέση της Τ.Π είναι η δυνατότητά της να δημιουργεί νέες ευκαιρίες και να αλλάζει τον τρόπο διεξαγωγής των εργασιών καθώς και οι αλλαγές που επιφέρει στην οργανωτική δομή. Η αξιολόγηση των επενδύσεων θα πρέπει να λαμβάνει υπόψη αυτή τη διαφορετική διάσταση και τα έμμεσα αποτελέσματα, όπως τις αλλαγές στις μισθολογικές δομές, στο ρόλο της διοίκησης και στην παραδοσιακή διάκριση μεταξύ των λειτουργιών που είναι δύσκολο να αποδοθούν απόλυτα σε χρηματικούς όρους.

3.5 Συστήματα Τ.Π.Ε και Καινοτομία

Όπως αναφέρθηκε και στην προηγούμενη ενότητα, το παράδοξο της παραγωγικότητας έχει πλέον ξεθωριάσει και η εστίαση έχει μετατοπιστεί στη δύναμη και τον παράγοντα που επηρεάζει τις Τ.Π.Ε και την παραγωγικότητα, παρά στην ύπαρξη κάποιας σχέσης. Προκειμένου να εξηγηθεί αυτή η σχέση καλύτερα, πρέπει να εισαχθεί ένας νέος παράγοντας μεταξύ Τ.Π.Ε και παραγωγικότητας που είναι η καινοτομία. Η καινοτομία έχει αποκτήσει τεράστια σημασία τις τελευταίες δεκαετίες.

Πριν λίγα χρόνια η καινοτομία περιοριζόταν στην καινοτομία των προϊόντων και δεν συνεπαγόταν καν όλους τους τομείς της βιομηχανίας. Πλέον η καινοτομία δεν περιορίζεται σε ένα προϊόν ή σε λίγους τομείς της βιομηχανίας καθώς είναι πολύ συνηθισμένο να θεωρούμε και την υπηρεσία (service) ως ένα προϊόν. Έτσι, η καινοτομία των προϊόντων εφαρμόζεται επίσης στον τομέα των υπηρεσιών.

Η καινοτομία προϊόντων αφορά είτε την δημιουργία ενός νέου προϊόντος είτε την βελτίωση της ποιότητας του. Η τεχνολογία Τ.Π.Ε βελτιώνει την ποιότητα των προϊόντων (Tarafdar & Gordon 2007) και ενισχύει έτσι την καινοτομία. Επιπλέον, ένα από τα αποτελέσματα της εφαρμογής της τεχνολογίας Τ.Π.Ε είναι και η καινοτομία (Tarafdar & Gordon 2007). Στις μέρες μας αποτελεί αναμφισβήτητο γεγονός ότι η καινοτομία μπορεί να επιφέρει επανάσταση στις οργανωτικές δομές και γενικά στους επιμέρους κλάδους των επιχειρήσεων.

3.6 Οφέλη στην Απόδοση ενός Οργανισμού

Διάφορες μελέτες έχουν δείξει τις επιπτώσεις που έχει η χρήση Συστημάτων ICT στην απόδοση ενός Οργανισμού. Όσο περισσότερο επενδύουν οι εταιρείες σε αυτά, τόσο καλύτερη και πιο δυνατή θέση θα κατέχουν στην αγορά (Ho et al., 2011) ενώ οι επιχειρήσεις με την χρήση τους μπορούν να αυξήσουν την απόδοση τους. (Noor & Apadore, 2014)

Τα οφέλη από κάθε επένδυση σε αυτά τα συστήματα θα πρέπει να εξεταστούν στο γενικότερο πλαίσιο της οργανωτικής δομής μιας επιχείρησης διότι σπάνια μειώνουν το κόστος. Η βασική αξία της επένδυσης έγκειται στο ότι αλλάζει τη διάρθρωση κόστους ενός οργανισμού έτσι ώστε να αυξάνονται οι πωλήσεις ή το παραγόμενο προϊόν χωρίς να αυξάνεται το προσωπικό. Τα μη-ποσοτικά όμως αποτιμώμενα οφέλη συνήθως παραλείπονται από τις μελέτες σκοπιμότητας διότι είναι δύσκολο να αξιολογηθούν με τις οικονομικές τεχνικές αξιολόγησης και δεν είναι βέβαιο ή δεν μπορούν να έχουν προφανή βραχυχρόνια απόδοση. Τα οφέλη αυτά είναι: η καλύτερη εξυπηρέτηση και ικανοποίηση του πελάτη, τα υψηλότερα επίπεδα επαγγελματικής ικανοποίησης, η υψηλότερη και καλύτερη ποιότητα προϊόντων, οι προηγμένες εσωτερικές και εξωτερικές επικοινωνίες μέσα στην επιχείρηση, η απόκτηση ανταγωνιστικού πλεονεκτήματος έναντι άλλων επιχειρήσεων και οι προηγμένες σχέσεις με προμηθευτές.

Τα άμεσα οφέλη, όπως αύξηση παραγωγικότητας λόγω της βελτίωσης στην απόδοση και στις αποδοτικότερες εργασιακές σχέσεις, μείωση κόστους, μετατόπιση κόστους και αύξηση εισοδήματος, εμφανίζονται γρήγορα και είναι σχετικά εύκολο να προσδιοριστούν. Τα έμμεσα οφέλη, όπως μείωση επιχειρηματικού κινδύνου (λόγω της μείωσης του κινδύνου των λαθών), επέκταση επιχειρηματικής δραστηριότητας (λόγω της δημιουργίας νέων ευκαιριών και της απόκτησης ανταγωνιστικού πλεονεκτήματος) και επιβίωση, συμβαίνουν σε μακρύτερες χρονικές περιόδους και είναι δυσκολότερο να συσχετιστούν με τις επενδύσεις σε Τ.Π.Ε.

Κεφάλαιο 4

Τα Οικονομικά της Κυβερνοασφάλειας

4.1 Επενδύοντας στην Ασφάλεια

Εκτεθειμένες σε ολοένα και πιο εξελιγμένες μορφές κυβερνοεπιθέσεων βρίσκονται, σήμερα, οι επιχειρήσεις σε παγκόσμιο επίπεδο. Τα ευρήματα δείχνουν ότι το 56% των εταιρειών πραγματοποιούν ή σχεδιάζουν αλλαγές στη στρατηγική τους, λόγω των αυξημένων επιπτώσεων των κυβερνοαπειλών, των κινδύνων και των τρωτών σημείων των επιχειρήσεων. Επιπλέον η ταχύτητα του ρυθμού συνδεσιμότητας μέσα στους παγκόσμιους οργανισμούς, η οποία ενισχύεται από την ανάπτυξη του Internet of Things (IoT), αφήνει τις επιχειρήσεις ακόμη πιο εκτεθειμένες στις ολοένα και πιο εξελιγμένες μορφές κυβερνοεπιθέσεων. Ένα από τα μεγαλύτερα θέματα λοιπόν που αντιμετωπίζουν οι Οργανισμοί, είναι το πως θα προστατευτούν από όλες αυτές τις κυβερνοαπειλές, ειδικότερα αν σκεφτούμε ότι το εύρος και το είδος αυτών των επιθέσεων είναι άγνωστα.

Η Ασφάλεια φυσικά πρέπει να συμβάλει άμεσα στην επιτυχία ενός Οργανισμού και όχι να αποτελεί εμπόδιο ή να την επιβαρύνει με μεγάλο κόστος. Για τον λόγο αυτό η Ασφάλεια πρέπει να αντιμετωπίζεται ως μία επένδυση από μία επιχείρηση και όχι ως μία ανώφελη δαπάνη. Για τον λόγο αυτό έχουν αναπτυχθεί διάφορα μοντέλα για την ορθή λήψη αποφάσεων και την προστασία των πληροφοριακών αγαθών σε έναν Οργανισμό, ενώ έχουν εκπονηθεί και πάρα πολλές μελέτες για τον σκοπό αυτό

Λαμβάνοντας υπόψη και την σημασία της προστασίας ενός Οργανισμού από επιθέσεις, τόσο για την συνέχεια των δραστηριοτήτων της όσο κυρίως για την ίδια της την επιβίωση, το κύριο ερώτημα που τίθεται είναι το εξής:

Πόσο πρέπει να επενδύσει ένας Οργανισμός για όλες τις δραστηριότητες που αφορούν την Κυβερνοασφάλεια του;

Το ερώτημα μπορεί να φαίνεται απλό αλλά καθόλου εύκολο να απαντηθεί για πολλούς και διάφορους λόγους. Καταρχήν πρωτεύων παράγοντας για να παραχθεί αξία από την Ασφάλεια είναι να γνωρίζουμε ότι οι τεχνολογικές επενδύσεις προστατεύουν τα κατάλληλα αγαθά, κατόπιν πρέπει να εκτιμηθεί σωστά η αξία των αγαθών που πρέπει να προστατευτούν και τα οφέλη που φέρνουν στην επιχείρηση. Επιπλέον, να εκτιμηθεί σωστά το κόστος της επιπλέον επένδυσης που πρέπει να γίνει σε συστήματα ασφαλείας και να αξιολογηθεί αυτή η επένδυση. Αν το κόστος της επένδυσης ξεπερνά τα οικονομικά οφέλη της, τότε η επένδυση αυτή δεν πρέπει να γίνει. Με απλά λόγια ένας Οργανισμός πρέπει να αποφανθεί αν το κόστος της επένδυσης στην Κυβερνοασφάλεια είναι επικερδής ή όχι.

Βέβαια η αποτίμηση του κόστους και η εύρεση της βέλτιστης επένδυσης έχει αποδειχτεί ένα πολύ δύσκολο αντικείμενο. Το πρόβλημα εντοπίζεται ακριβώς στην ίδια την φύση της Ασφάλειας. Η Ασφάλεια δεν είναι μία επένδυση που μπορείς να υπολογίσεις ακριβώς τα κέρδη και τα οφέλη της γιατί δεν παράγει κέρδος αλλά αποτρέπει την απώλεια τους. Πιο συγκεκριμένα ο ειδικός της Ασφάλειας που θα υπολογίσει τον προϋπολογισμό της σε μία επιχείρηση, δεν δύναται να δικαιολογήσει αυτό το ποσό γιατί δεν μπορεί να αποδώσει κέρδος στην επιχείρηση. Δεν μπορεί να ισχυριστεί ότι η αγορά ενός πιο ακριβού firewall για το δίκτυο θα αποφέρει κάποιο μεγαλύτερο κέρδος για την επιχείρηση, γιατί ακριβώς δεν θα φέρει κάποιο κέρδος. Μπορεί όμως να αποφανθεί αν η αγορά του firewall μπορεί να αποτρέψει περισσότερες επιθέσεις ή όχι.

Τίθεται όμως το ερώτημα αν οι Οργανισμοί δίνουν αυτήν την πρέπουσα σημασία στην Ασφάλεια τους. Η παγκόσμια οικονομική κρίση μετά το 2008, έφερε τις επιχειρήσεις και ιδιαίτερα αυτές τις υποδομές που χρησιμοποιούν συστήματα Τ.Π.Ε αντιμέτωπες με αύξηση των εξόδων και κίνδυνο χρεωκοπίας. Η λύση ήταν η άμεση αναπροσαρμογή των επιχειρηματικών σχεδίων τους και η περικοπή των εξόδων τους που δεν είχε όμως άμεσο αντίκτυπο στην παραγωγή τους (Chronopoulos et al 2017:1). Οι επιτιθέμενοι αντίθετα δεν αντιμετώπισαν κάποιο ανάλογο πρόβλημα. Άλλωστε με πολύ λίγα χρήματα και τα κατάλληλα εργαλεία μπορούν να προκαλέσουν ζημιές εκατομμυρίων, ενώ βρίσκονται πάντα ένα βήμα πιο μπροστά από τους αμυντικούς μηχανισμούς χρησιμοποιώντας όλο και περισσότερο την Κοινωνική Μηχανική (Social Engineering).

Για αυτόν τον λόγο η Κυβερνοασφάλεια δεν είναι μία μόνο αμυντική επιλογή αλλά και μία στρατηγική απόφαση για τους Οργανισμούς, που μπορεί να παίξει πολύ σημαντικό ρόλο στην απόκτηση πλεονεκτήματος στον ανταγωνισμό έναντι άλλων Οργανισμών. Για αυτόν τον λόγο πλέον και δίνουν όλο και μεγαλύτερη αξία στις επενδυτικές τους αποφάσεις όσον αφορά την Ασφάλεια. Οι Οργανισμοί πλέον βλέπουν την ανάγκη να θέσουν προτεραιότητες στον τρόπο που θα αμυνθούν, λαμβάνοντας υπόψη τις απειλές από τις οποίες κινδυνεύουν περισσότερο και τις ευπάθειες των συστημάτων που χρησιμοποιούν ώστε να μειώσουν όσο είναι δυνατόν τις αδυναμίες τους (Chronopoulos et al 2017:2).

Για αυτόν τον λόγο, έχουν αναπτυχθεί δύο διαφορετικές προσεγγίσεις στην επένδυση από τους Οργανισμούς (Friendman 2011:8). Η πρώτη προσέγγιση σχετίζεται πιο πολύ με την αντίδραση σε μία επίθεση. Πολλοί Οργανισμοί επενδύουν σε συστήματα επανάκτησης των πληροφοριών ή επιδιόρθωσης των συστημάτων τους μόνο έπειτα από μία επίθεση, υπολογίζοντας επίσης και το κόστος από την απώλεια της φήμης τους αλλά και από πιθανά έξοδα νομικής φύσεως, προσέγγιση που για κάποιους ερευνητές φαίνεται λογική και βέλτιστη κοινωνικά (Grossklags et al. 2008:08)

Η δεύτερη προσέγγιση αφορά μία αέναη προσπάθεια να σταματήσεις κάθε επίθεση, επενδύοντας διαρκώς σε συστήματα. Όπως προαναφέρθηκε όμως, δεν είναι δυνατόν Οι Οργανισμοί να γνωρίζουν ακριβώς, το εύρος και το είδος των επιθέσεων, οπότε και το εύρος της επένδυσης είναι δύσκολο να εκτιμηθεί. Ωστόσο τα περιστατικά ασφαλείας και οι παραβιάσεις συνεχώς αυξάνονται, γεγονός που δείχνει μία λάθος εκτίμηση στην επένδυση στην Ασφάλεια αλλά και λάθος υπολογισμούς στο κόστος και τα οφέλη που μπορεί να αποφέρει. Επιπρόσθετα η συνεχής επένδυση σε συστήματα ασφαλείας και αναβαθμίσεις των ήδη υπαρχόντων για να εξαλείψει ένας Οργανισμός τις ευπάθειες του, μπορεί να οδηγήσει σε μία υπερβολική επένδυση που δεν θα είναι συμφέρουσα για αυτόν.

Λαμβάνοντας υπόψη τις αβεβαιότητες που αφορούν τις παραβιάσεις του κυβερνοχώρου και τις προσπάθειες για την πρόληψη τέτοιων παραβιάσεων, υπάρχει και μία τρίτη προσέγγιση (Gordon et al., 2003:2). Η επιλογή αυτή προτείνει μία συντηρητική και λογική στρατηγική: πρώτα επενδύεις ένα αρχικό και σχετικά μικρό μέρος του διαθέσιμου προϋπολογισμού για την ασφάλεια των συστημάτων σου και κατόπιν περιμένεις την παραβίαση ώστε να επενδύσεις το υπόλοιπο ποσό. Με αυτήν

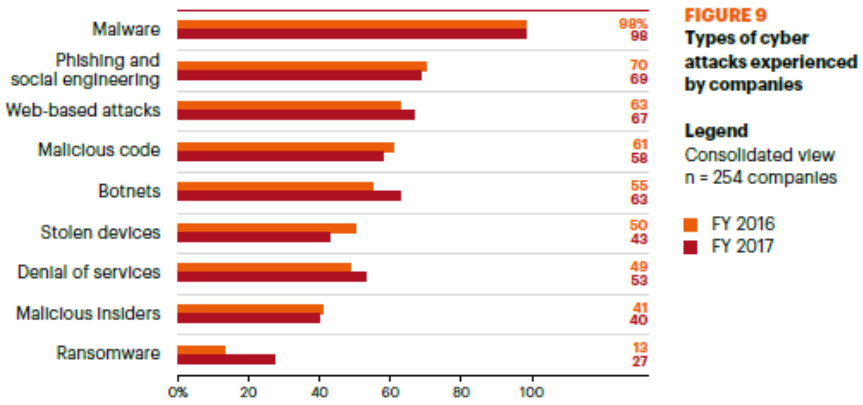
την προσέγγιση, οι Οργανισμοί θα χρησιμοποιήσουν τις παραβιάσεις στα συστήματα τους, ως καθοριστικό παράγοντα της πραγματικής τους επένδυσης για την ασφάλεια στον κυβερνοχώρο.

Το ερώτημα λοιπόν που τίθεται και είναι το αντικείμενο του προβληματισμού παγκοσμίως είναι: *Πόση επένδυση στην Ασφάλεια είναι αρκετή;*

Η αναζήτηση αυτής της βέλτιστης επένδυσης είναι και αυτό που θα μας απασχολήσει στο υπόλοιπο της Διατριβής. Πριν ξεκινήσουμε με την βιβλιογραφική ανασκόπηση και την ανάλυση των κυριότερων οικονομικών μοντέλων που σχετίζονται με την επένδυση στην Ασφάλεια, θα προχωρήσουμε με κάποια στατιστικά στοιχεία που δείχνουν ακριβώς το μέγεθος αυτό του παγκόσμιου προβληματισμού.

4.2 Το κόστος του Κυβερνοεγκλήματος

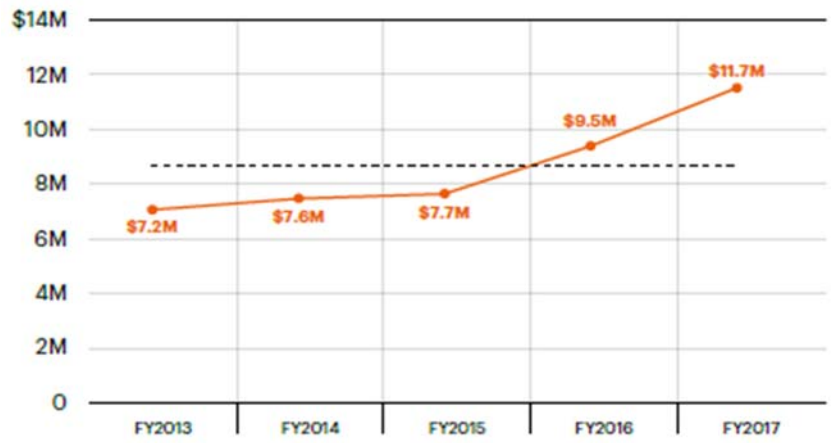
Οι ραγδαίες αλλαγές στην τεχνολογία, η παγκόσμια δικτύωση καθώς και η αυξανόμενη αξίας της άμεσης και έγκυρης πληροφόρησης επέφεραν μεγάλο προβληματισμό στους Οργανισμούς παγκοσμίως. Τα τελευταία χρόνια έχουν εμφανιστεί πολλαπλές απειλές στα δίκτυα επικοινωνίας, ειδικά με την μεγάλη αύξηση της χρήσης του διαδικτύου από τους πολίτες. Παρατηρείται πλέον, σε παγκόσμιο επίπεδο, το γεγονός ότι όχι μόνο αυξάνεται η συχνότητα των επιθέσεων στον κυβερνοχώρο, αλλά επίσης και η πολυπλοκότητα των επιθέσεων αυτών. Οι επιθέσεις Ransomware έχουν σχεδόν διπλασιαστεί μέσα σε ένα μόνο χρόνο, σχεδόν όλοι οι Οργανισμοί αντιμετώπισαν επιθέσεις με κακόβουλο λογισμικό (malware), ενώ οι επιθέσεις εξαπάτησης των χρηστών (phishing) έφτασαν στο 69% όπως φαίνεται και παρακάτω [6].



Εικόνα 11. Τύποι επιθέσεων το 2017 (Πηγή: Ponemon Institute, Cost Of Cybercrime Study, 2017, σελ.23)

[6] Ponemon Institute (2017). Cost of Cyberware Study

Ειδικότερα, το 2017 οι επιτυχημένες επιθέσεις και τα ρήγματα (security breaches) στην ασφάλεια των Οργανισμών παγκοσμίως αυξήθηκαν κατά 27% (κατά μ.ό. από 102 ρήγματα ανά Οργανισμό αυξήθηκε στα 130) με περιστατικά όπως τα WannaCry και Petya να είναι τα σημαντικότερα (Ponemon Institute, Cost of Cybercrime, 2017, σελ.3). Το κόστος αυτό είναι αυξανόμενο τα τελευταία 5 χρόνια και ανέρχεται περίπου στα $11.7 εκατομμύρια ανά περιστατικό.



Εικόνα 12. Κόστος ανά περιστατικό (Πηγή: Ponemon Institute, Cost Of Cybercrime Study, 2017, σελ.12)

Επιπρόσθετα το 2017 η Kaspersky δημοσίευσε την έκθεση της για το κόστος των Κυβερνοεπιθέσεων και τις επιπτώσεις που επιφέρουν σε μία εταιρεία (Kaspersky 2017): η έρευνα έγινε με μορφή ερωτηματολογίου για την ασφάλεια και τις υποδομές σε 5.500 εταιρείες σε 26 χώρες του κόσμου και σίγουρα τα αποτελέσματα είναι εντυπωσιακά:

- Περίπου το 90% των επιχειρήσεων παραδέχτηκε ότι αντιμετώπισε τουλάχιστον ένα περιστατικό ασφαλείας.
- Περίπου το 46% των επιχειρήσεων ανέφερε την απώλεια ευαίσθητων δεδομένων.
- Το κόστος για να επαναφέρουν τα συστήματα είναι κατά μ.ο. $551.000 για μεγάλες επιχειρήσεις και $38.000 για τις μεσαίες και μικρές επιχειρήσεις (μία αύξηση της τάξης του 146% σε σχέση με το 2015).
- Οι πιο ακριβές περιπτώσεις επαναφοράς προήλθαν από απάτη των υπαλλήλων αλλά και από την κατασκοπεία., ενώ οι πιο επικίνδυνες απειλές που αντιμετώπισαν ήταν το

κακόβουλο λογισμικό (malware), οι επιθέσεις ψαρέματος (phishing) και η τυχαία αποκάλυψη πληροφοριών από τους υπαλλήλους των εταιρειών.

Οι τρεις (3) κυριότερες συνέπειες αυτών των περιστατικών είναι η αδυναμία πρόσβασης στις πληροφορίες της επιχείρησης, η προσωρινή απώλεια της ικανότητας της εταιρείας να κάνει εμπορικές συναλλαγές αλλά και η ζημιά στην εικόνα και την φήμη της.

Τα προαναφερόμενα νούμερα όμως αφορούν μόνο τα άμεσα ποσά που πρέπει να πληρώσει μία εταιρεία (π.χ. απώλεια συμβολαίων, πληρωμή των ειδικών ασφαλείας για την αποκατάσταση, χρόνος επαναφοράς του δικτύου της), ενώ το επιπλέον ποσό που πρέπει να ξοδέψει μία μεγάλη επιχείρηση είναι περίπου $69.000 για έμμεσες επιπτώσεις (επιπλέον εκπαίδευση του προσωπικού, πρόσληψη υπαλλήλων, αναβάθμιση των υποδομών της κτλ.) που περιορίζεται στα $8.000 για μία μεσαία ή μικρή επιχείρηση.

4.3 Το κόστος της Ασφάλειας

Καταρχήν πρέπει να διαχωρίσουμε το κόστος από την χρήση των συστημάτων Τ.Π.Ε με το κόστος που προκύπτει από μία επίθεση στον Οργανισμό παρόλο που και αυτό δεν είναι τελείως ακριβές. Αρχικά ένας Οργανισμός όταν σχεδιάζει το σύστημα Ασφαλείας του πρέπει να υπολογίσει τρία διαφορετικά κόστη όσον αφορά τα συστήματα Τ.Π.Ε και ασφαλείας που πρέπει να προμηθευτεί (Beissel 2016:129):

- Το κόστος της απόφασης (decision making costs)
- Το κόστος του Σχεδιασμού (planning costs) και
- Το κόστος της αρχικής Επένδυσης (initial investment costs)

Κατόπιν πρέπει να υπολογίσει το κόστος από την χρήση και την συντήρηση αυτών των συστημάτων. Συγκεκριμένα πρέπει να υπολογίσει:

- Το λειτουργικό κόστος (operation costs)
- Το κόστος Συντήρησης (maintenance costs) και
- Το κόστος Ευκαιρίας (initial investment costs) που αφορά την απώλεια από τις επενδυτικές ευκαιρίες που προκύπτουν σε έναν Οργανισμό και δεν μπορεί να

εκμεταλλευτεί καθώς τα χρήματα από την Ασφάλεια δεν μπορούν να επενδυθούν ξανά σε κάποιον άλλον τομέα της επιχείρησης.

Το επόμενο βήμα είναι να υπολογιστεί το κόστος μετά από κάποια επίθεση στα συστήματα του Οργανισμού. Σύμφωνα με την CISCO οι Οργανισμοί αντιμετωπίζουν τρεις (3) διαφορετικές οικονομικές επιδράσεις μετά από ένα συμβάν ασφαλείας (security breach):

- Την έμμεση οικονομική επίδραση (Immediate Economic Impact) που αφορά το κόστος επισκευής και αντικατάστασης των συστημάτων που έχουν υποστεί ζημία αλλά και το κόστος από την διακοπή στις επιχειρηματικές λειτουργίες και στην ροή χρημάτων της επιχείρησης.

- Την βραχυπρόθεσμη οικονομική επίδραση (Short-term Economic Impact) που αφορά το κόστος από την απώλεια πελατών και από την αρνητική επίδραση στην φήμη της εταιρείας.

- Την μακροπρόθεσμη οικονομική επίδραση (Long-term Economic Impact).

Είναι όμως απαραίτητο να διαχωρίσουμε αυτές τις οικονομικές επιπτώσεις σε κάτι πιο απτό, να δούμε ποιες ακριβώς είναι και πως επιδρούν σε έναν Οργανισμό. Επειδή είναι δύσκολο να υπολογιστούν σε ακριβή μεγέθη για πολλούς και διάφορους λόγους (ανεπαρκή στοιχεία, αδυναμία υπολογισμού διάφορων μεγεθών, μη δημοσιοποίηση στοιχείων από τις εταιρείες), τουλάχιστον μπορούμε να τοποθετήσουμε αυτές τις επιπτώσεις σε ένα γενικότερο πλαίσιο.

Οι οικονομικές επιπτώσεις λοιπόν μπορούν να χωριστούν σε άμεσες ή απτές (tangible costs) και έμμεσες ή αλλιώς άυλες (intangible costs) και οι κατηγορίες που προκύπτουν είναι οι εξής:

Κόστος Επισκευής. Άμεσο κόστος που αφορά το κόστος επισκευής για την επιστροφή ενός Συστήματος στην αρχική του κατάσταση. Αποτελείται από το κόστος της εργασίας και το κόστος της αγοράς των υλικών. Όσον αφορά την αγορά των υλικών είναι πολύ εύκολο να προϋπολογιστεί λαμβάνοντας υπόψη βέβαια και πιθανή ανατίμηση μέσα σε ένα χρονικό διάστημα. Το κόστος της εργασίας εξαρτάται από τον ωριαίο μισθό του ειδικού που θα επισκευάσει το υλικό και τον χρόνο που θα χρειαστεί για αυτήν την επισκευή. Ακόμη και ο χρόνος όμως είναι σχετικός. Άλλο χρόνο θα χρειαστεί ο ειδικός για την επανεγκατάσταση ενός Λειτουργικού Συστήματος και άλλον για την επανεγκατάσταση μίας εφαρμογής. Σε αυτήν την κατηγορία δεν περιλαμβάνεται το κόστος από την επισκευή ενός συστήματος από τους ίδιους τους υπαλλήλους της επιχείρησης αλλά μόνο από τους ειδικούς. Στην συγκεκριμένη περίπτωση

μιλάμε για κόστος από την απασχόληση των υπαλλήλων και την απώλεια παραγωγικότητας στο συγκεκριμένο χρονικό διάστημα.

Κόστος από την απώλεια της Παραγωγικότητας: Στην συγκεκριμένη κατηγορία μιλάμε για την απώλεια χρόνου για την αντιμετώπιση ενός κακόβουλου λογισμικού ή spam και την συνεπαγόμενη μείωση της παραγωγικότητας για το συγκεκριμένο χρονικό διάστημα. Το κόστος από την διαγραφή spam μπορεί να φαίνεται μικρό αλλά σε έρευνα που πραγματοποιήθηκε, ένας εργαζόμενος σε μία επιχείρηση στις Η.Π.Α, κατά μέσο όρο χρειάζεται 16 δευτερόλεπτα για να αναγνωρίσει και να διαγράψει ένα spam mail, ξοδεύει 5,6 λεπτά ανά ημέρα για να σβήσει όλα τα ενοχλητικά spam που κοστίζει 712$ ανά εργαζόμενο το χρόνο, με συνολικό κόστος 70 δις $ το χρόνο για όλες τις επιχειρήσεις (Nucleus Research, 2007). Αν ανάγουμε αυτόν το νούμερο στις μέρες εργασίας σε έναν χρόνο και στον αριθμό των εργαζομένων της επιχείρησης, μπορούμε να πάρουμε ένα εκτιμώμενο κόστος για την πτώση της παραγωγικότητας. Ο υπολογισμός αυτός είναι δυσκολότερος στην περίπτωση που το spam περιέχει μέσα ένα κακόβουλο λογισμικό καθώς πρέπει να υπολογιστεί ο αριθμός των εργαζομένων που επηρεάστηκαν και το μέγεθος της ζημίας που επέφεραν στα μηχανήματα τους.

Κόστος από την απώλεια εσόδων: Σχετίζεται άμεσα με την προηγούμενη κατηγορία. Όμως η απώλεια παραγωγικότητας σε ένα συγκεκριμένο χρονικό διάστημα είναι πιθανόν να αποφέρει αύξηση της τιμής των διατιθέμενων προϊόντων της επιχείρησης. Αντίθετα η απώλεια εισόδων σχετίζεται με το χρονικό διάστημα που δεν θα χρησιμοποιούνται οι υπηρεσίες του Οργανισμού λόγω π.χ. ενός κακόβουλου λογισμικού ή μίας DDOS επίθεσης. Ειδικά σε μία εταιρεία που ασχολείται με το ηλεκτρονικό εμπόριο και εξαρτάται άμεσα από τα συστήματα Τ.Π.Ε, το κόστος αυτό αυξάνεται κατά πολύ. Φυσικά το τελευταίο εξαρτάται και από την συμπεριφορά των καταναλωτών. Διαφορετική είναι η περίπτωση που ο καταναλωτής θα επανέλθει αργότερα για να αγοράσει ένα προϊόν ή μία υπηρεσία, διαφορετικό αν στο συγκεκριμένο χρονικό διάστημα στραφεί σε έναν άλλο ανταγωνιστή της και το αγοράσει από αυτήν.

Κόστος από την απώλεια δεδομένων: Αφορά το κόστος από την απώλεια δεδομένων μετά από μία επίθεση που δεν μπορούν να ανακτηθούν. Το ακριβές ποσό είναι δύσκολο να υπολογιστεί γιατί αφορά τον χρόνο και το κόστος συλλογής αλλά και το πόσο αξίζουν αυτά τα δεδομένα για τον Οργανισμό.

Κόστος από την Οικονομική Απάτη που σχετίζεται άμεσα με τις ηλεκτρονικές αγορές και την χρήση πιστωτικών καρτών που επιφέρουν μία άμεση αρνητική επίδραση στην επιχείρηση.

Κόστος από την αρνητική φήμη που αποκτά μία επιχείρηση όταν συμβεί ένα περιστατικό ασφαλείας. Το κόστος αυτό δεν είναι άμεσα εμφανές αλλά σίγουρα αποφέρει απώλεια εσόδων σε αυτήν από την απώλεια πιθανών νέων πελατών. Επίσης σε αυτήν την κατηγορία πρέπει να υπολογιστούν και πιθανά έξοδα για επιπλέον διαφήμιση που θα αποκαταστήσει το όνομα της επιχείρησης.

Κόστος από υιοθέτηση επιπλέον μέτρων ασφαλείας: Αφορά άμεσα έξοδα για την αντιμετώπιση των επιπτώσεων από ένα περιστατικό ασφαλείας. Σε αυτήν την κατηγορία μπορούν να συμπεριληφθούν και μέτρα για την αντιμετώπιση μελλοντικών απειλών που είναι έμμεσα έξοδα όπως επίσης και τα έξοδα για την εκπαίδευση του προσωπικού.

Κόστος για την βελτίωση της Υποδομής, σε περίπτωση που απαιτηθεί κατασκευή ή αγορά νέων συστημάτων για την συνολική αύξηση της ασφάλειας της επιχείρησης.

Κόστος από την πιο αργή υιοθέτηση της τεχνολογίας και των συστημάτων Τ.Π.Ε. Φυσικά πρόκειται για έμμεσο κόστος καθώς αφορά την απώλεια εμπιστοσύνης σε προϊόντα ή υπηρεσίες που σχετίζονται αυτά. Το συγκεκριμένο κόστος είναι και πολύ δύσκολο να εκτιμηθεί.

Κόστος από την απώλεια πελατείας και το οποίο οδηγεί στην απώλεια εσόδων. Το μέγεθος της απώλειας εξαρτάται από το είδος του Οργανισμού που θα υποστεί μία επίθεση.

Νομικό Κόστος το οποίο θα αφορά επίλυση διενέξεων με φυσικά πρόσωπα που υπέστησαν απώλειες αλλά και τις εποπτικές αρχές. Το κόστος αυτό πρέπει να υπολογιστεί για μεγάλο χρονικό διάστημα, όσο δηλαδή θα διαρκέσει η ενδεχόμενη δικαστική διαμάχη.

4.4 Αξιολόγηση των Επενδύσεων στην Ασφάλεια

Το ζήτημα της λήψης και αξιολόγησης των επενδύσεων, είναι ένα σοβαρό οικονομικό πρόβλημα που απαιτεί ορθολογισμό και αποτελεσματικότητα στην οργάνωση του, ενώ αποτελεί αντικείμενο ευρείας μελέτης. Καθώς οι Οργανισμοί σήμερα, αντιμετωπίζουν συνεχώς νέες και μεγαλύτερες προκλήσεις, που τους επιβάλλουν την αύξηση της αποδοτικότητας των λειτουργιών και των υπηρεσιών που προσφέρουν στους πελάτες τους, η λήψη της κατάλληλης επενδυτικής απόφασης είναι κρίσιμη.

Η αξιολόγηση επενδύσεων σε μία επιχείρηση είναι ένα πολύ σημαντικό στάδιο για την επιλογή ή την απόρριψη μιας επένδυσης. Για να εξασφαλιστεί η μέγιστη δυνατή ωφέλεια, ελαχιστοποιώντας το κόστος και εξαλείφοντας τους κίνδυνους που θα προκύψουν, θα πρέπει να προηγηθεί μια αξιολόγηση. Αν όμως η αξιολόγηση σε μία επιχείρηση είναι δύσκολη, η αξιολόγηση της επένδυσης σε Τ.Π.Ε είναι κάτι παραπάνω από απαιτητική. Σκοπός της είναι να κατανοήσουν περισσότερο οι Οργανισμοί το πώς οι Τ.Π.Ε συνεισφέρουν στην απόδοση του. Το αποτέλεσμα που προκύπτει, καθορίζεται έπειτα από την συνολική εκτίμηση του κόστους και των ωφελειών, τόσο των άμεσα ποσοτικών μεγεθών (tangible) όσο και των μη-ποσοτικών ή ποιοτικών μεγεθών (intangible).

Οι συνηθέστερες μέθοδοι για την αξιολόγηση της επένδυσης είναι η Απόδοση της επένδυσης (ROI), η περίοδος Επανείσπραξης (PBP), η Καθαρή Παρούσα Αξία (NVP) και ο Εσωτερικός Συντελεστής Απόδοσης (IRR).

Παρόλα αυτά πρέπει να αναφερθεί ότι όλοι αυτοί οι κλασικοί χρηματοοικονομικές μέθοδοι έχουν κατά καιρούς συγκεντρώσει τα πυρά των ειδικών, καθότι έχουν πολύ περιορισμένη προοπτική αντίληψη των πραγμάτων, δεν περιλαμβάνουν μη οικονομικά μεγέθη στην ανάλυση, ενώ δίνουν υπέρ το δέον έμφαση στα βραχυπρόθεσμα αποτελέσματα (Adler, 2000). Επιπρόσθετα η πρόβλεψη ή αποτίμηση όλων των συντελεστών που προσδιορίζουν το κόστος και τις ωφέλειες, αποτελεί μία εξαιρετικά δύσκολη διαδικασία με πολλά εμπόδια (Andersen et al. 2000:59).

4.4.1 Η Απόδοση της Επένδυσης (ROI)

Η μέθοδος Απόδοσης Επενδύσεων (Return On Investment – ROI) ή αλλιώς η μέθοδος Du Pont (από το όνομα της εταιρείας που υλοποιήθηκε για πρώτη φορά), είναι από τις πιο γνωστές μεθόδους αποτίμησης των οικονομικών επιπτώσεων των επενδύσεων.

Η μεθοδολογία ROI αποτελεί το μέσο για να διαπιστωθεί εάν μια επένδυση συνεισφέρει ή όχι στον οργανισμό, καθώς αυτό που κάνει είναι να εξετάζει εάν τα οφέλη από το πρόγραμμα, εκφρασμένα σε αξία, ξεπερνούν τα κόστη. Ο οργανισμός μπορεί να συγκρίνει τη συνεισφορά διαφόρων επενδύσεων μεταξύ τους και να εκτελεί μόνο τις επικερδείς. Η απόδοση της επένδυσης δίνεται από τον παρακάτω τύπο και το αποτέλεσμα εκφράζεται ως ποσοστό:

$$\textbf{ROI} = \frac{Κέρδος\ επένδυσης - Κόστος\ επένδυσης}{Κόστος\ επένδυσης}\%$$

Εάν η επένδυση δεν έχει θετικό πρόσημο ή αν υπάρχουν άλλες επενδύσεις με υψηλότερη απόδοση, τότε η επένδυση δεν θα πρέπει να αναληφθεί. Η μέθοδος αυτή είναι αποτελεσματική όταν τα κέρδη και το κόστος της επένδυσης είναι γνωστά, όμως σε σύνθετες επιχειρήσεις δεν είναι πάντα εύκολο να καθοριστούν συγκεκριμένα μεγέθη όπως αυξημένα κέρδη και συγκεκριμένα κόστη, συνεπώς η μέθοδος ROI δεν είναι πάντα αξιόπιστη για την επιλογή επενδύσεων και αποφάσεων. [7]

Όταν η επένδυση διαρκεί μόνο ένα έτος , ο υπολογισμός του ROI είναι σχετικά απλός. Στην περίπτωση όμως που η επένδυση που διαρκεί περισσότερο από ένα έτος, υπάρχουν τρεις (3) διαφορετικοί τρόποι υπολογισμού που φαίνονται παρακάτω:

- Να υπολογιστεί το ROI στο σύνολο της περιόδου των ετών που διαρκεί η επένδυση.
- Το σύνολο των εσόδων και των εξόδων, να διανεμηθεί σε κάθε έτος ισόποσα, να υπολογιστεί το ROI για κάθε έτος ξεχωριστά και στο τέλος να αθροιστούν όλα τα ROI, δίνοντας ένα τελικό αποτέλεσμα που θα κρίνει την επένδυση.
- Υπολογίζει τα έσοδα και τα έξοδα κάθε έτους , ωστόσο, ο υπολογισμός γίνεται με βάση τις σωρευτικές τους ταμειακές ροές, δηλαδή, η σωρευτική απόδοση για ένα χρόνο ισούται με το άθροισμα του τρέχοντος έτους και τα προηγούμενα χρόνια (Botchkarer & Andru. 2011:250)

Αυτό είναι όμως και το κυριότερο πρόβλημα με την μέθοδο ROI, το γεγονός ότι δεν περιλαμβάνει στην εξίσωση τον χρόνο (Gonzalez et al. 2014:3) και υπολογίζει μόνο ένα μέγεθος (Andersen et al. 2000:60). Διαφορετική αξία έχει το χρήμα σε ένα χρόνο, διαφορετική μετά από αρκετά χρόνια, οπότε και η επιστροφή της Επένδυσης θα είναι διαφορετική και σίγουρα πιο πολύτιμη σε πιο βραχύ χρονικό διάστημα (αν αφορά το ίδιο αποτέλεσμα). Επιπρόσθετα το ROI δεν είναι εύκολο να υπολογιστεί διότι, τα οφέλη ή κέρδη από την επένδυση και το κόστος για κάθε χρόνο ποικίλουν. Τέλος η μέθοδος αυτή δεν μπορεί να συνδυάσει διαφορετικά προγράμματα επενδύσεων σε διαφορετικά χρονικά διαστήματα.

[7] Business Encyclopedia, «Return on Investment (ROI) defined and calculated, with examples, usage, and comparison to other financial metrics». Online at https://www.business-case-analysis.com/return-on-investment.html

4.4.2 Το Μοντέλο Gordon and Loeb

Είναι ίσως το δημοφιλέστερο οικονομικό μοντέλο που χρησιμοποιείται για να αναλύσει την βέλτιστη δυνατή επένδυση στην Ασφάλεια της Πληροφορίας. Ένας Οργανισμός πριν αποφασίσει να το χρησιμοποιήσει χρειάζεται να απαντήσει σε τρεις (3) διαφορετικές ερωτήσεις:

- Πόσο αξίζουν τα δεδομένα που πρέπει να προστατέψει;
- Πόσα από αυτά βρίσκονται σε κίνδυνο και
- Ποια είναι η πιθανότητα μία επίθεση σε αυτά να είναι επιτυχής;

Σε αντίθεση με άλλα μοντέλα ανάλυσης της επικινδυνότητας, το πληροφοριακό αγαθό δεν είναι απαραίτητο να προστατευτεί με μία δαπανηρή επένδυση από την στιγμή που υπάρχει ένα σημείο δαπάνης και μετά στο οποίο η επένδυση για την Ασφάλεια των Πληροφοριακών αγαθών κρίνεται ασύμφορη. Στην ουσία η βέλτιστη δαπάνη για την προστασία ενός πληροφοριακού αγαθού δεν είναι πάντοτε ανάλογη της αξίας του.

Οι Gordon και Loeb λοιπόν, στο οικονομικό τους μοντέλο έδειξαν ότι *η βέλτιστη δαπάνη για την Ασφάλεια των Πληροφοριακών Συστημάτων δεν πρέπει να ξεπερνάει το 37% (για την ακρίβεια 36,8% λόγω του* $\frac{1}{e}$ *) της πιθανής οικονομικής απώλειας που μπορεί να προκύψει από ένα περιστατικό ασφαλείας (*Gordon & Loeb, 2002:440).

Επιπρόσθετα οι Gordon και Loeb δεν στοχεύουν ακριβώς στην προστασία του τρίπτυχου CIA, αλλά δημιουργούν ένα μοντέλο που εξετάζει συγκεκριμένα το πώς η ευπάθεια των πληροφοριών και η πιθανότητα απωλειών λόγω της ευπάθειας αυτής, επηρεάζει το βέλτιστο ποσό των πόρων που θα έπρεπε να αφιερωθεί στην εξασφάλιση αυτών των πληροφοριών, δηλαδή του ποσού που πρέπει να διατεθεί για την προστασία αυτών των πληροφοριών.

<u>Ανάλυση</u>

Ας ξεκινήσουμε όμως με την ανάλυση αυτού του μοντέλου για να καταδείξουμε τα κύρια στοιχεία του και κατόπιν να αναλύσουμε τις κριτικές και τους προβληματισμούς που απορρέουν από αυτό. Οι κύριες υποθέσεις που έκαναν οι δύο μαθηματικοί είναι οι εξής:

- Όλες οι πληροφορίες και τα πληροφοριακά αγαθά σε έναν Οργανισμό υπόκεινται σε κίνδυνο. Κάθε αγαθό, κάθε πληροφορία, κάθε σύστημα κινδυνεύουν από κυβερνοεπίθεση. Δεν υπάρχει Οργανισμός που δεν θα υποστεί κάποια μορφή κυβερνοεπίθεσης, άλλωστε σύμφωνα με το Ponemon Institute η πιθανότητα αυτή είναι 22% για ένα διάστημα 24 μηνών. Αυτή η ευπάθεια λοιπών των πληροφοριακών αγαθών ορίζεται ως v στο υπό εξέταση μοντέλο και μάλιστα ισχύει $0 \leq v \leq 1$. Μπορούμε να πούμε λοιπόν ότι ως v ορίζεται η πιθανότητα να συμβεί οποιαδήποτε κυβερνοεπίθεση κάτω από συγκεκριμένες συνθήκες.

- Αν ή μάλλον όταν συμβεί η επίθεση σε ένα πληροφοριακό αγαθό, η αξία του αντιπροσωπεύει την πιθανή οικονομική απώλεια η οποία ορίζεται σαν **L** και που στο συγκεκριμένο μοντέλο θεωρείται σταθερή για ένα συγκεκριμένο set αγαθών, π.χ. η λίστα των πελατών της εταιρείας.

- Σαν **t** ορίζεται η πιθανότητα μίας επιχειρούμενης παραβίασης στο συγκεκριμένο set αγαθών, η οποία ονομάζεται πιθανότητα απειλής.

- Είναι λογικό ότι το **v*L** αντιπροσωπεύει και ισούται με την αναμενόμενη απώλεια πριν από μία οποιαδήποτε οικονομική επένδυση στην ασφάλεια του Οργανισμού.

- Η οικονομική επένδυση **z** που θα κάνει ένας Οργανισμός θα μειώσει και την πιθανότητα **v** να συμβεί ένα ρήγμα στην ασφάλεια του Οργανισμού. Το **s (z,v)** λοιπόν ορίζεται ως η πιθανότητα να προκύψει οποιοδήποτε ρήγμα στην ασφάλεια και είναι συνάρτηση των δύο τυχαίων μεταβλητών, της επένδυσης σε συστήματα ασφαλείας και της πιθανότητας μίας απειλής να προκαλέσει μία επιτυχημένη επίθεση. Μάλιστα σύμφωνα με τους μαθηματικούς τύπους, ισχύει ότι όσο περισσότερο επενδύεις στην ασφάλεια, τόσο περισσότερο μειώνεις την πιθανότητα να προκύψει ένα ρήγμα αλλά ποτέ δεν θα φτάσεις να την εξαφανίσεις τελείως.

Αξιολόγηση

Η συγκεκριμένη πρόταση είναι σαφώς ενδιαφέρουσα, ξεκινάει όμως με πολλές υποθέσεις. Η κυριότερη από αυτές, θεωρεί ότι ο Οργανισμός που θα υποστεί την επίθεση δεν θα πάρει κάποιο επιπρόσθετο μέτρο για να την εξαλείψει. Επιπρόσθετα λόγω των μαθηματικών πράξεων που γίνονται στο μοντέλο, αποδεικνύεται ότι όσο περισσότερο επενδύεις στην Κυβερνοασφάλεια, τα οφέλη από αυτήν την αύξηση, αν και θετικά, μειώνονται συνεχώς. Κάποια δεδομένη στιγμή λοιπόν, θα χρειαστεί ο Οργανισμός να επενδύσει ένα επιπλέον ποσό για την ασφάλεια του.

Η θεώρηση ότι δεν μπορείς να εξαλείψεις τελείως τον κίνδυνο από μία απειλή είναι μεν σωστή, στην πραγματικότητα όμως θα μπορούσες υπό συγκεκριμένες συνθήκες να εξαλείψεις τον κίνδυνο από μία συγκεκριμένη επίθεση.

4.4.3 Καθαρή Παρούσα Αξία (NPV)

Η μέθοδος της Καθαρής Παρούσας Αξίας (Net Present Value) είναι η πιο διαδεδομένη μέθοδος αξιολόγησης των επενδύσεων και χρησιμοποιείται από την πλειοψηφία των επιχειρήσεων. Είναι μία μέθοδος αξιολόγησης των επενδύσεων η οποία χρησιμοποιεί όλες τις χρηματικές ροές μιας επένδυσης, λαμβάνοντας όμως υπόψη τη χρονική αξία του χρήματος. Αποτελεί μια τυποποιημένη μέθοδο που χρησιμοποιεί την έννοια της χρονικής αξίας του χρήματος για την εκτίμηση μακροπρόθεσμων επενδύσεων. Η χρονική αξία του χρήματος στα χρηματοοικονομικά, υπαγορεύει ότι ο χρόνος έχει επιπτώσεις στην αξία των ταμειακών ροών. Η χρονική αξία του χρήματος, βασίζεται στην υπόθεση ότι τα σημερινά κέρδη έχουν μεγαλύτερη αξία από τα κέρδη που θα έχει ένας οργανισμός σε έναν χρόνο. Ουσιαστικά δίνεται από τον τύπο:

$$\boldsymbol{Καθαρή\ Παρούσα\ Αξία} = Παρούσα\ Αξία - Κόστος\ Επένδυσης$$

Με την Καθαρά Παρούσα Αξία λοιπόν, φέρνουμε σε παρούσες αξίες τις καθαρές χρηματικές ροές, δηλαδή τα έσοδα και έξοδα του Οργανισμού και τα συγκρίνουμε με το κόστος κεφαλαίων που χρησιμοποιήθηκαν για μια επένδυση (Παπαδάμου και Συριόπουλος 2015:57). Τα μελλοντικά έσοδα και έξοδα του οργανισμού μειώνονται με βάση το επιτόκιο που επικρατεί στην αγορά, για να υπολογιστεί η παρούσα αξία τους.

Με βάση τον τύπο λοιπόν αν η παρούσα αξία των εσόδων είναι μεγαλύτερη από το κόστος της επένδυσης, τότε η Καθαρά Παρούσα Αξία θα είναι θετική που σημαίνει ότι η επένδυση κρίνεται κερδοφόρα. Αντίστροφα αν λοιπόν αν η παρούσα αξία των εσόδων είναι μικρότερη από το κόστος της επένδυσης, τότε η καθαρά παρούσα αξία θα είναι αρνητική που σημαίνει ότι η επένδυση κρίνεται μη κερδοφόρα ή αποφέρει ζημία στην επιχείρηση. Αν η Καθαρά Παρούσα Αξία μιας επένδυσης στην Κυβερνοασφάλεια είναι θετική, τότε και μόνο η επένδυση είναι επικερδής για τον οργανισμό.

Τα κυριότερα πλεονεκτήματα λοιπόν συνοψίζονται στο γεγονός ότι λαμβάνει υπόψη την χρονική αξία του χρήματος, η βάση της αναφοράς και ο χρόνος αναφοράς της ορίζονται στο παρόν, ενώ υποθέτει και την επανεπένδυση στο κόστος του κεφαλαίου.

Ο καθαρός υπολογισμός της για τις επενδύσεις δίνεται από τον παρακάτω τύπο:

$$\textbf{ΚΠΑ} = \sum_{t=1}^{N} \frac{\text{Ταμειακές Ροές}}{(1+r)^{\text{t}}} - \text{Αρχική Επένδυση}$$

Όπου t=χρονική περίοδος

N= χρονική διάρκεια της επένδυσης και r=Προεξοφλητικό επιτόκιο

Εφόσον το κόστος της Αρχικής Επένδυσης Χ δίνεται με ταμειακές ροές αναγόμενες σε χρόνο 0 δίνεται από τον τύπο:

$$\textbf{Χ} = \sum_{t=-m}^{0} \frac{\text{Ταμειακές Ροές}}{(1+r)^{\text{t}}}$$

Τότε και η Καθαρή Παρούσα Αξία μετασχηματίζεται ως εξής:

$$\textbf{ΚΠΑ} = \sum_{t=1}^{N} \frac{\text{Ταμειακές Ροές}}{(1+r)^{\text{t}}} - \sum_{t=-m}^{0} \frac{\text{Ταμειακές Ροές}}{(1+r)^{\text{t}}}$$

Στο σημείο αυτό πρέπει να αναφέρουμε ότι ο υπολογισμός των ταμειακών ροών ακολουθεί μια ανάλυση την οποία αναλαμβάνει το τμήμα χρηματοοικονομικής διοίκησης. Υπάρχει μια εκτενής ανάλυση των δεδομένων, αναλύεται ο προϋπολογισμός του έργου και χρησιμοποιούνται κοστολογικά δεδομένα από την πραγματοποίηση παρόμοιων έργων. Επιπλέον προσδιορίζεται το χρονοδιάγραμμα του έργου και ο χωρισμός των αντίστοιχων χρηματικών ροών, καθώς και η υπολειμματική του αξία (salvage value) δηλαδή τα έσοδα από την πώληση του πάγιου εξοπλισμού ή των κτισμάτων στο τέλος της λειτουργικής ζωής του έργου. Στον προσδιορισμό των ταμειακών ροών η διοίκηση υπολογίζει και τις δαπάνες που πραγματοποιεί η επιχείρηση κάθε έτος για το κόστος λειτουργίας (operating cost). Τέλος τα έσοδα που θα προκύψουν κατά την διάρκεια τις ωφέλιμης ζωής της επένδυσης υπόκεινται σε φορολογία με τον εκάστοτε φορολογικό συντελεστή. Βλέπουμε επομένως ότι η

σύνθεση των ταμειακών ροών και της εκτίμησης του κόστους ευκαιρίας κεφαλαίου, είναι μια πολύπλοκη και σύνθετη διαδικασία.

Αξιολόγηση

Αν και η μέθοδος αυτή υπολογίζει την χρονική αξία του χρήματος και λαμβάνει υπόψη την πραγματική χρονική στιγμή που πραγματοποιούνται οι ωφέλειες της επένδυσης , παρουσιάζει κάποια σημαντικά μειονεκτήματα. Πρώτον η ακρίβεια της μεθόδου της ΚΠΑ εξαρτάται άμεσα από την ακρίβεια εκτίμησης του κόστους κεφαλαίου, γεγονός που στην πράξη δύσκολα επιτυγχάνεται. Κατά συνέπεια, μόνο κατά προσέγγιση είναι δυνατόν να υπολογιστεί το πραγματικό κόστος των κεφαλαίων και επομένως η καθαρή παρούσα αξία. Επιπλέον παίρνει ως σταθερό το Προεξοφλητικό Επιτόκιο για όλη την διάρκεια της επένδυσης, γεγονός μη ρεαλιστικό για μακροχρόνιες επενδύσεις.

4.4.4 Εσωτερικός Βαθμός Απόδοσης (IRR)

Η μέθοδος του εσωτερικού βαθμού δείχνει την απόδοση ενός επενδυτικού προγράμματος και μοιάζει ισοδύναμη με την προηγούμενη. Αντί όμως να θεωρείται δεδομένο το κόστος του κεφαλαίου και να επιχειρείται η αναγωγή σε Καθαρά Παρούσα Αξία, αναζητείται το κόστος εκείνο που θα καθιστούσε μηδενική την Καθαρή Παρούσα Αξία της επένδυσης. Με άλλα λόγια ο εσωτερικός βαθμός απόδοσης είναι το προεξοφλητικό επιτόκιο το οποίο μηδενίζει την καθαρή παρούσα αξία της επένδυσης και υπολογίζεται εξισώνοντας την Παρούσα Αξία της αναμενόμενης καθαρής εισροής μετρητών με την παρούσα αξία της εκροής μετρητών. Δίνεται από τον τύπο:

$$\boldsymbol{CFo} = \sum_{\boldsymbol{t=1}}^{\boldsymbol{n}} \frac{\mathbf{CFt}}{(\mathbf{1} + \mathbf{IRR})^{\mathbf{t}}}$$

Όπου CFt η πρόσθετη ετήσια ταμειακή ροή (η ταμειακή ροή μπορεί να πάρει θετική ή αρνητική τιμή), μετά από φόρους του έτους t και t=0,1,2,...,n και IRR ο εσωτερικός βαθμός απόδοσης

Εάν ο εσωτερικός βαθμός απόδοσης είναι μεγαλύτερος ή ίσος με την απαιτούμενη απόδοση, η επένδυση γίνεται αποδεκτή γιατί σημαίνει ότι ακόμα και αν η επιχείρηση δανειστεί με επιτόκιο ίσο με τον εσωτερικό βαθμό απόδοσης, η επένδυση μπορεί να καλύψει τα δάνεια αλλά δεν θα

έχει επιπλέον κέρδη. Στην αντίθετη περίπτωση, η πρόταση απορρίπτεται. Το κριτήριο αποδοχής βασίζεται στην ακόλουθη άποψη: Εάν η επιχείρηση αποδεχτεί ένα πρόγραμμα με εσωτερικό βαθμό απόδοσης ο οποίος υπερβαίνει το κόστος των κεφαλαίων τα οποία χρησιμοποιήθηκαν για την χρηματοδότηση του συγκεκριμένου προγράμματος, το πλεόνασμα το οποίο απομένει μετά την αποπληρωμή των κεφαλαίων το καρπώνονται οι μέτοχοι της επιχείρησης.

Η μέθοδος του εσωτερικού επιτοκίου αποδόσεως είναι αλληλένδετη με αυτή της ΚΠΑ, γιατί η αποδοχή μιας επενδυτικής πρότασης σημαίνει θετική ΚΠΑ και άρα εσωτερικό βαθμό απόδοσης μεγαλύτερο από το επιτόκιο προεξόφλησης Δηλαδή ισχύει:

Όταν, ΚΠΑ > 0 θα έχουμε R > r,
Όταν, ΚΠΑ = 0 θα έχουμε R = r,
Όταν, ΚΠΑ < 0 θα έχουμε R < r,

<u>Αξιολόγηση</u>

Στα θετικά της μεθόδου του Εσωτερικού Βαθμού Αποδόσεως αναφέρεται το γεγονός ότι αυτή λαμβάνει υπόψη την χρονική αξία του χρήματος και στηρίζεται στην έννοια της προεξόφλησης (discounting) των καθαρών εισροών και εκροών της επένδυσης. Επίσης υποθέτει ότι οι καθαρές εισπράξεις κεφαλαίων που λαμβάνονται στην αρχή της ζωής της επένδυσης θα επενδυθούν ξανά με το ίδιο ποσοστό απόδοσης. Επιπρόσθετα επιτρέπει την αξιολόγηση της απόδοσης μιας επένδυσης σε σχέση με τον κίνδυνο που διατρέχει.

Αντίθετα ο Εσωτερικός Βαθμός Απόδοσης απαιτεί την ακριβή πρόβλεψη των μελλοντικών ταμειακών ροών, γεγονός δύσκολο, είναι δύσκολη στην εφαρμογή πολλαπλών επενδύσεων και αρκετές φορές μπορεί να δώσει λάθος αποτελέσματα διότι σε ορισμένες περιπτώσεις παρέχει πολλαπλές λύσεις, δηλαδή περισσότερα του ενός Εσωτερικούς Βαθμούς Απόδοσης που να εξισώνουν τις παρούσες αξίες εισροών και εκροών. Αυτό συμβαίνει όταν σε μια σειρά καθαρών εισροών μεσολαβήσουν ένα ή δύο χρόνια καθαρών εκροών.

4.4.5 Περίοδος Επανείσπραξης (PP)

Η περίοδος Επανείσπραξης (Payback Period), είναι μια μέθοδος αξιολόγησης επενδύσεων η οποία εξετάζει πόσος χρόνος θα απαιτηθεί για την ανάκτηση της αρχικής

επενδυτικής δαπάνης. Υπολογίζεται από τον παρακάτω τύπο, ενώ η καλύτερη επένδυση είναι αυτή με την μικρότερη περίοδο Επανείσπραξης.

$$\boldsymbol{Payback} = \frac{\text{investment}}{\text{annual cashflow}}$$

Αποτελεί μια από τις ευρύτερα χρησιμοποιούμενες μεθόδους αξιολόγησης και υπολογίζεται σε έτη ή σε μήνες. Ένας οργανισμός, κρίνει το χρονικό διάστημα που προκύπτει με βάση τις απαιτήσεις της διοίκησης, το σχεδιασμό που έχει γίνει αλλά και τις συνθήκες που επικρατούν σε αυτόν. Είναι αναγκαία μέθοδος όταν υπάρχουν μεγάλοι και ανυπολόγιστοι κίνδυνοι καθώς έχει μεγάλη ευκολία στους υπολογισμούς και κάνει χρήση καθαρών χρηματικών ροών. Η έννοια του κριτηρίου της περιόδου Επανείσπραξης είναι ανάλογη με την έννοια του νεκρού σημείου. Ενώ το νεκρό σημείο ορίζεται ως το σημείο της χρήσης πέρα από το οποίο η επιχείρηση πραγματοποιεί κέρδη, το κριτήριο της περιόδου Επανείσπραξης ορίζεται όπως ο αναγκαίος χρόνος κατά τον οποίο το άθροισμα των ταμειακών ροών ενός επενδυτικού έργου ισούται με την αρχική του δαπάνη.

Αξιολόγηση

Η περίοδος Επανείσπραξης παρέχει μια ένδειξη του κινδύνου και της ρευστότητας της επένδυσης. Όσο βραχύτερη είναι η περίοδος Επανείσπραξης, τόσο ασφαλέστερη είναι η επένδυση και μεγαλύτερη η ρευστότητά της. Σε επενδύσεις επομένως που η ρευστότητα έχει πρωταρχική σημασία, η μέθοδος επανάκτησης του κεφαλαίου είναι εξαιρετικά χρήσιμη.

Ωστόσο, η μέθοδος δε λαμβάνει υπόψη τη διασπορά των πιθανών καθαρών ταμειακών ροών και συνεπώς δεν αποτελεί επαρκή δείκτη του κινδύνου της επένδυσης. Τα μειονεκτήματα της συγκεκριμένης μεθόδου είναι ότι χρησιμοποιεί υποκειμενικά κριτήρια και αγνοεί τη χρονική αξία του χρήματος, ενώ δεν υπολογίζει και τα οφέλη πέρα από την περίοδο Επανείσπραξης συνεπώς δεν υπολογίζει την κερδοφορία. Ειδικότερα, τα κυριότερα μειονεκτήματα της μεθόδου είναι τα εξής:

- Αγνοεί τις καθαρές χρηματικές ροές της επένδυσης μετά την περίοδο επανάκτησης του κεφαλαίου που έχει ως αποτέλεσμα να ευνοούνται επενδυτικά σχέδια με αποδόσεις στο βραχυχρόνιο διάστημα, έστω και αν οι αποδόσεις αυτές δεν έχουν σημαντική διάρκεια

(Παπαδάμου και Συριόπουλος 2015:54). Αυτό είναι ένα πολύ σοβαρό μειονέκτημα γιατί ο καθορισμός της απαιτούμενης περιόδου Επανείσπραξης δεν βασίζεται σε ευρύτερους οικονομικούς παράγοντες, αλλά σε μία υποκειμενική εκτίμηση της ίδιας της επιχείρησης.

- Θεωρεί ότι οι αναμενόμενες χρηματορροές έχουν την ίδια αξία σήμερα, ανεξάρτητα από τον χρόνο που θα πραγματοποιηθούν. Επομένως η μέθοδος της περιόδου Επανείσπραξης δεν λαμβάνει υπόψη της τη χρονική αξία του χρήματος.

4.4.6 Η επενδυτική απόδοση της Ασφάλειας (ROSI)

Η μέθοδος της Απόδοσης Επενδύσεων ισχύει σε κάθε επένδυση, σε κάθε επιχείρηση. Με την ίδια λογική πρέπει να ισχύσει και στην Ασφάλεια που δεν αποτελεί εξαίρεση. Οι ειδικοί άλλωστε σε μία επιχείρηση, πριν καθορίσουν το ύψος του προϋπολογισμού και του ποσοστού που θα διατεθεί στην Ασφάλεια πρέπει να γνωρίζουν ακριβώς, τι θα ξοδέψουν, πόσο θα στοιχήσει η έλλειψη της και ποιες είναι οι πιο συμφέρουσες οικονομικά λύσεις (ENISA work program 2012:5).

Όταν εφαρμοστεί στην Ασφάλεια η μέθοδος μετασχηματίζεται σε ROSI (Return On Security Investment) και βοηθάει τους ειδικούς να απαντήσουν στις παρακάτω ερωτήσεις:

- Μήπως η επιχείρηση πληρώνει παραπάνω από ότι θα έπρεπε για την Ασφάλεια;
- Η έλλειψη Ασφάλειας τι αντίκτυπο θα έχει στην παραγωγικότητα της επιχείρησης;
- Πότε είναι αρκετή η Επένδυση στην Ασφάλεια και τέλος
- Η επένδυση αυτή είναι συμφέρουσα οικονομικά για την Επιχείρηση;

Ο δείκτης της ROSI βασίζεται στην σχέση ROI και είναι ο παρακάτω:

$$\boldsymbol{ROSI} = \frac{(\textbf{Risk Exposure} * \%\ \textbf{Risk Mitigation}) - \textbf{Solution Cost}}{\boldsymbol{Solution\ Cost}}$$

Αν για παράδειγμα μία εταιρεία υπολογίζει το συνολικό κόστος από ένα ιό που θα επηρεάσει το σύστημα της σε $50.000, την πιθανότητα να συμβεί αυτό μέσα σε ένα χρόνο 4 φορές και το κόστος αγοράς ενός antivirus που θα μετριάσει τον κίνδυνο κατά 75%, στα $20.000 τότε εφαρμόζοντας τον τύπο, προκύπτει ότι:

$$\boldsymbol{ROSI} = \frac{(\mathbf{50.000} * \mathbf{4} * \mathbf{75\%}) - \mathbf{20.000}}{\mathbf{20.000}} = \mathbf{650\%}$$

Από την στιγμή που ο τύπος μας δίνει θετικό αποτέλεσμα, η αγορά του συγκεκριμένου antivirus κρίνεται συμφέρουσα και επιβεβλημένη. Στην πράξη όμως τα πράγματα είναι πολύ διαφορετικά και ο υπολογισμός όλων αυτών των παραμέτρων είναι δύσκολος και σηκώνει πολλές ερμηνείες. Μία από αυτές τις μεθοδολογίες προτείνει διαφορετικά επίπεδα πιθανότητας και σοβαρότητας των περιστατικών που κατόπιν μεταφράζονται σε πιθανότητα εμφάνισης και άμεσο κόστος (Lockstep 2004:13-14).

Στην παρακάτω εικόνα φαίνεται αυτή η διαβάθμιση που ορίζεται στο συγκεκριμένο εγχειρίδιο, με την πιθανότητα να εκφράζεται σε εφτά (7) διαφορετικά επίπεδα και κατόπιν αυτό να ποσοτικοποιείται σε ποσοστό εμφάνισης.

Likelihood	Description from ACSI 33	p.a.
Negligible	Unlikely to occur	0.05[2]
Very Low	Likely to occur two/three times every five years	0.5
Low	Likely to occur once every year or less	1.0
Medium	Likely to occur once every six months or less	2.0
High	Likely to occur once per month or less	12.0
Very High	Likely to occur multiple times per month or less	50.0
Extreme	Likely to occur multiple times per day	500.0

Εικόνα 13. Πιθανότητα εμφάνισης, εκφρασμένη σε ποσοστό (Πηγή: Lockstep 2004, σελ.13)

Σε μία διαφορετική μεθοδολογία, οι παράμετροι αυτοί σχετίζονται είτε με το περιστατικό (συχνότητα εμφάνισης), είτε με την προστασία όπως είναι το κόστος, τα οφέλη και το ωφέλιμο ζωής ενός μέτρου που θα ληφθεί (Kosutic 2011).

Ο υπολογισμός της έκθεσης στον Κίνδυνο (Risk Exposure) προκύπτει από τον πολλαπλασιασμό του κόστος της ζημίας από ένα περιστατικό SLE (Single Loss Exposure) με μία προβλεπόμενη συχνότητα εμφάνισης ανά έτος ARO (Annual Rate of Occurrence). Από την πράξη αυτή προκύπτει η Ετήσια Έκθεση Απωλειών ALE (Annual Loss Exposure).

$$\textbf{Risk Exposure} = \boldsymbol{SLE} * \boldsymbol{ARO} = \boldsymbol{ALE}$$

Ο υπολογισμός του SLE είναι εξαιρετικά δύσκολος. Πολλές φορές ένα ανεπαίσθητο γεγονός και μία μικρή απώλεια από μία επίθεση σε μία μεγάλη επιχείρηση μπορεί να περάσει απαρατήρητο.

Επίσης έχει διαπιστωθεί ότι οι διάφοροι Οργανισμοί υπολογίζουν διαφορετικά το κόστος από ένα και μόνο περιστατικό. Επιπρόσθετα, μετά από ένα περιστατικό ασφαλείας και τον χρόνο που απαιτείται για να επανέρθει το Σύστημα στην προηγούμενη κατάσταση του, είναι πολύ δύσκολο να υπολογιστεί το κόστος από την απώλεια της παραγωγικότητας. Ειδικά σε έναν μεγάλο Οργανισμό με πολλούς εργαζομένους, το κόστος αυτό μπορεί να είναι πολύ μεγάλο και μπορεί να περιλαμβάνει όλα τα έξοδα, άμεσα και έμμεσα που αναφερθήκαμε παραπάνω.

Κατόπιν πρέπει να υπολογιστεί η συχνότητα εμφάνισης ή πιθανότητα να συμβεί ένα περιστατικό. Επίσης η συχνότητα εμφάνισης, είναι διαφορετική πριν εφαρμόσεις ένα μέτρο (π.χ. αγορά ενός antivirus) και διαφορετική όταν το εφαρμόσεις. Υπάρχει περίπτωση βέβαια αυτή η συχνότητα να είναι πάντα η ίδια (π.χ. η πιθανότητα να συμβεί μία πλημμύρα στην επιχείρηση).

Ο υπολογισμός της μετρίασης του Κινδύνου (Risk Mitigation) και του κέρδους που θα αποφέρει είναι φυσικά δύσκολος, γιατί η Ασφάλεια δεν δημιουργεί χειροπιαστό κέρδος στην επιχείρηση αλλά εμποδίζει την απώλεια κερδών από απειλές και επιθέσεις. Σε πολλές περιπτώσεις μία επιχείρηση δεν μπορεί να υπολογίσει την απώλεια που εμποδίστηκε από ένα σύστημα ασφαλείας που χρησιμοποιεί γιατί δεν μπορεί να γνωρίζει κάτι για αυτό. Δεν μπορεί για παράδειγμα να υπολογίσει αν το σύστημα της προσβλήθηκε λιγότερο γιατί ήταν πιο αποτελεσματικό το antivirus που χρησιμοποίησε ή γιατί έγιναν λιγότερες επιθέσεις.

Η λογική πάντως για τον υπολογισμό του Risk Mitigation είναι απλή: ένα σύστημα ασφαλείας σχεδιάζεται για να μετριάσει συγκεκριμένους κινδύνους και θεωρητικά η μετρίαση αυτή μπορεί να φτάσει στο 100%. Αν μπορεί να μετριάσει το 75% των κινδύνων τότε λέμε ότι το Risk Mitigation φτάνει στο 75%. Το θέμα είναι ότι μία συγκεκριμένη λύση ποτέ δεν λειτουργεί μόνη της αλλά εξαρτάται και από την αποτελεσματικότητα και άλλων συστημάτων ασφαλείας (π.χ χρήση ενός antivirus σε συνδυασμό με firewall). Επιπρόσθετα ένα σύστημα ασφαλείας δεν σχεδιάζεται ή καλύτερα ρυθμίζεται για να αποκόψει κάθε δυνατό κίνδυνο. Μία επιχείρηση για παράδειγμα δεν θα χρησιμοποιήσει ένα firewall για να κόψει όλη την εισερχόμενη κίνηση, διακινδυνεύει έτσι την μείωση της παραγωγικότητας.

Το πιο σημαντικό όμως ζήτημα είναι η αποτελεσματικότητα των συστημάτων ασφαλείας στην διάρκεια του χρόνου. Είναι δεδομένο ότι η αποτελεσματικότητα ενός συστήματος θα μειώνεται με την πάροδο του χρόνου, καθώς οι κυβερνοεγκληματίες θα βρουν τον τρόπο να το παρακάμψουν ή να το παραβιάσουν.

Ο υπολογισμός του κόστους της λύσης (cost solution) επίσης δεν είναι τόσο απλός. Το κόστος δεν αφορά μόνο την αγορά και την εφαρμογή ενός νέου συστήματος ασφαλείας, αλλά αφορά και

επιπλέον έξοδα που δεν φαίνονται, όπως το κόστος εγκατάστασης, το κόστος συντήρησης κτλ. Είναι επίσης το κόστος από μία πιθανή μείωση της παραγωγικότητας ή ακόμα και αύξηση της. Αν για παράδειγμα κάθε εργαζόμενος χρειάζεται συνεχώς να χρησιμοποιεί τους προσωπικούς του κωδικούς ασφαλείας για κάθε εφαρμογή που χρησιμοποιεί, τότε αυτό σημαίνει απώλεια χρόνου και απώλεια παραγωγικότητας που ισούται με επιπλέον κόστος από την χρήση του συστήματος. Αν όμως χρησιμοποιηθεί ένα σύστημα που θα μειώσει τον χρόνο που το Π.Σ μιας εταιρείας θα παραμένει εκτός (downtime), τότε αυτό το σύστημα ασφαλώς θα συνεισφέρει στην μείωση του κόστους της λύσης. Συνοπτικά για να υπολογίσεις αυτό το κόστος πρέπει να λάβεις υπόψη τους παρακάτω παράγοντες (Kosutic, 2011):

- Αξία αγοράς (υλικό, λογισμικό, κόστος εγκατάστασης).
- Υπολειπόμενη Αξία (το κόστος όταν πλέον δεν χρησιμοποιείται το μέτρο ασφαλείας).
- Αξία Συντήρησης (επιδιορθώσεις, service και κόστος των υπαλλήλων που το συντηρούν).

Αξιολόγηση

Ο υπολογισμός του ROSI είναι το αποτέλεσμα πολλών προσεγγίσεων και υποθέσεων. Το κόστος των περιστατικών ασφάλειας στον κυβερνοχώρο και η ετήσια εμφάνιση των περιστατικών είναι δύσκολο να εκτιμηθούν και οι προκύπτοντες αριθμοί μπορεί να είναι πολύ διαφορετικοί από ένα περιβάλλον σε άλλο. Επίσης όλες αυτές οι προσεγγίσεις συχνά υποκινούνται από την αντίληψή μας για τον κίνδυνο και ο υπολογισμός ROSI μπορεί εύκολα να χειριστεί για την εξυπηρέτηση του συμφέροντος του χρήστη ή για την αιτιολόγηση του ποσού που θα διατεθεί στον συνολικό προϋπολογισμό ενός Οργανισμού.

Για όλους αυτούς τους λόγους είναι απαραίτητη μία συνολική εκτίμηση της ασφάλειας των συστημάτων και ο υπολογισμός της μετρίασης του κινδύνου με διάφορους αλγόριθμους υπολογισμού. Τέτοιες πρακτικές έχουν εκδοθεί από διάφορους Οργανισμούς τυποποίησης όπως είναι ο NIST (National Institute of Standards in Security) και ο ISO (International Standards Organization).

4.5 Τεχνικές Εκτίμησης Κινδύνου

Κατά την Αξιολόγηση των επενδύσεων είναι απαραίτητο να εκτιμήσουμε τους παράγοντες που επηρεάζουν το επενδυτικό μας σχέδιο. Σε καθαρά οικονομικούς όρους,

εκτιμούμε το κόστος της επένδυσης, τα έσοδα ενός Οργανισμού, τα χρόνια λειτουργικής ζωής του έργου, την υπολειμματική αξία στο τέλος της περιόδου του έργου, τα λειτουργικά έξοδα στην διάρκεια ζωής του έργου και άλλους παράγοντες. Αν θελήσουμε να ανάγουμε αυτούς τους οικονομικούς όρους στην επένδυση στην ασφάλεια ενός Οργανισμού και στην επένδυση στα συστήματα Τ.Π.Ε, τότε αυτοί εξηγούνται ως εξής:

- Το κόστος της επένδυσης τόσο στην προμήθεια των συστημάτων Τ.Π.Ε όσο και στην προμήθεια των διάφορων συστημάτων ασφαλείας (safeguards).

- Στα λειτουργικά έξοδα συμπεριλαμβάνουμε το κόστος χρήσης των συστημάτων αλλά και το κόστος εκπαίδευσης του προσωπικού που θα τα χρησιμοποιήσει.

- Τα χρόνια λειτουργικής ζωής του έργου αναφέρονται στην χρονική διάρκεια που υπολογίζουμε την επένδυση μας και τέλος

- Η υπολειμματική αξία αφορά το κόστος των συστημάτων που έχουν απομείνει από την αρχική επένδυση και μετά το τέλος του έργου, υπολογίζοντας στην ζημιά ή φθορά που έχουν υποστεί τα συστήματα.

Για την μέτρηση του κινδύνου μίας επένδυσης χρησιμοποιούνται διάφορες τεχνικές από τους Οργανισμούς που για τους σκοπούς της παρούσας Διατριβής θα γίνει μία απλή αναφορά σε ορισμένους από αυτούς: στην χρησιμοποίηση των πιθανοτήτων, στην ανάλυση του κινδύνου με τα δέντρα αποφάσεων (decision trees), στην μέθοδο Delphi και στο μοντέλο της συμπεριφοράς (behavioral model). Παραλείπουμε προς το παρόν το επικρατέστερο μοντέλο μέτρησης του Κινδύνου σε Οργανισμούς που είναι η μέθοδος Monte Carlo[8] αλλά και την αξία σε κίνδυνο (VaR-Value at Risk) που θα χρησιμοποιηθούν στο προτεινόμενο πλαίσιο αυτής της Διατριβής στο επόμενο Κεφάλαιο.

4.5.1 Χρησιμοποίηση των Πιθανοτήτων

Για την μέτρηση κινδύνου μίας επένδυσης μία τεχνική είναι η κατανομή των πιθανοτήτων για όλα τα πιθανά αποτελέσματα της. Η εκτιμώμενη μέση τιμή μπορεί να χρησιμοποιηθεί για να εκφράσει την μέση αναμενόμενη απόδοση μίας επένδυσης, ενώ τον βαθμό του κινδύνου τον εκφράζει η τυπική απόκλιση σ.

[8] Σύμφωνα με το World Economic Forum (2015), Towards the Quantification of Cyber Threat, όπου παρουσιάζονται από τους Οργανισμούς όλοι οι προβληματισμοί τους απέναντι στις διαρκώς αυξανόμενες απειλές, ενώ παρατίθενται και οι διαφορετικοί μέθοδοι μέτρησης του Κινδύνου.

Αν για παράδειγμα ένας Οργανισμός υπολογίσει την Καθαρά Παρούσα Αξία μίας επένδυσης υπολογίζοντας όλα τα ποσοτικά μεγέθη της, η ΚΠΑ θα υπολογίζεται από τον τύπο:

$$\textbf{Μέση ΚΠΑ} = \sum_{i=1}^{n} \textbf{ΚΠΑ}_i$$

Ενώ η Τυπική Απόκλιση που θα δίνει και τον βαθμό κινδύνου από τον τύπο:

$$\sigma^2_{\text{ΚΠΑ}} = \sum_{\text{i=1}}^{\text{n}} (\boldsymbol{ΚΠΑ} - \boldsymbol{ΚΠΑ})$$

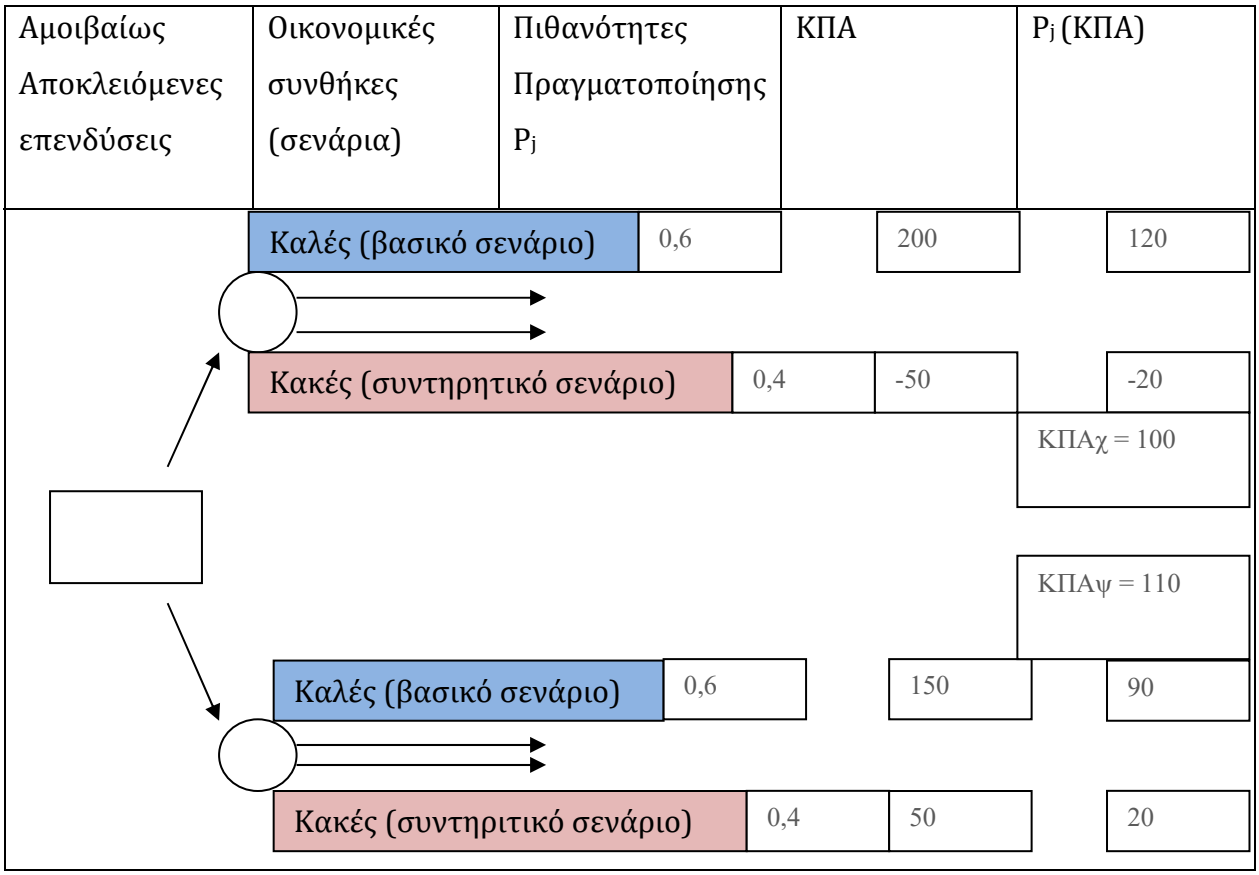
Επειδή είναι δύσκολη η κατανομή των πιθανοτήτων για τους βασικούς παράγοντες της επένδυσης λόγω υποκειμενικών κριτηρίων, στην πράξη μπορεί να γίνει με την μέθοδο προσομοίωσης Monte Carlo. Η μέθοδος Monte Carlo αποτελεί μοντέλο προσομοίωσης που μεταβάλλει όλους τους παράγοντες που επηρεάζουν βασικά χρηματοοικονομικά μεγέθη ταυτόχρονα σε ένα συγκεκριμένο εύρος τιμών ενώ παράλληλα καταγράφει τις αλλαγές που πραγματοποιούνται έτσι ώστε να εξαχθούν συμπεράσματα χρήσιμα για τις αποφάσεις μιας επιχείρησης στο μέλλον. Ουσιαστικά, εντοπίζει τις ευαισθησίες ενός επιχειρηματικού σχεδίου ή μιας επιχείρησης και παρουσιάζει πόσο κρίσιμες είναι τόσο για τη βιωσιμότητα όσο και για την επίτευξη κερδών. Έτσι, δίνει στον επιχειρηματία ή επενδυτή, τη δυνατότητα να αντιμετωπίσει αυτές τις ευαισθησίες και να λάβει καλύτερες επιχειρηματικές αποφάσεις.

4.5.2 Δέντρα αποφάσεων (decision trees)

Όταν τα προβλήματα απαιτούν την λήψη πληθώρας αποφάσεων αλλά και η πολυπλοκότητα των ενδεχομένων υπό ρίσκο αυξάνεται, τα δέντρα αποφάσεων προσφέρουν μια λύση μοντελοποίησης. Ουσιαστικά τα δένδρα αποφάσεων, είναι μια απλοποιημένη μορφή ενός πραγματικού προβλήματος, στην συγκεκριμένη περίπτωση μίας επένδυσης και περιλαμβάνουν τις κυριότερες ενέργειες και γεγονότα. Ουσιαστικά με την μέθοδο αυτή υπολογίζονται όλα τα πιθανά αποτελέσματα πριν από την ολοκλήρωση της αρχικής επένδυσης. Η επιλογή μεταξύ των διαθέσιμων επενδυτικών

αποφάσεων συνήθως γίνεται με τον προσδιορισμό των αποδόσεων, δηλαδή της ΚΠΑ που αναμένεται μετά από μία επένδυση.

Τα δέντρα αποφάσεων αποτελούν πολύτιμα εργαλεία για την αξιολόγηση της επένδυσης. Αν για παράδειγμα οι ταμειακές εισροές από μία επένδυση ξεπερνούν τις προβλεπόμενες, τότε μπορεί είτε να επεκταθεί η επένδυση είτε η ανάληψη μίας νέας επένδυσης. Στην αντίθετη περίπτωση, αν οι ταμειακές εισροές είναι μικρότερες του αναμενόμενου, τότε μπορεί η επένδυση ή να αναχρηματοδοτηθεί ή να εγκαταλειφτεί. Το μεγάλο τους μειονέκτημα ωστόσο είναι οι πολλές μεταβλητές που εισέρχονται στην ανάλυση, καθιστώντας την μέθοδο ιδιαίτερα πολύπλοκη.



Πίνακας 1. Σχηματική αναπαράσταση δέντρου αποφάσεων για την επιλογή μεταξύ επενδύσεων χ και ψ[9]

4.5.3 Μοντέλο συμπεριφοράς (behavioral modeling)

Η σχέση μεταξύ της τεχνολογίας και των ανθρώπων (άρα και την ανθρώπινης συμπεριφοράς) εισάγει συνεχώς πάγιους κινδύνους ασφαλείας δεδομένου ότι τα επίπεδα κατανόησης της ασφάλειας όσο και της ίδιας της τεχνολογίας που αξιοποιείται, μπορούν να διαφέρουν από άνθρωπο σε άνθρωπο. Είναι ένα μοντέλο που τονίζει την

[9] Όπως προτείνεται και αναλύεται από την Διδακτορική Διατριβή του Λούγκα Δ.(2009), σελ.27

σημασία της ανθρώπινης συμπεριφοράς κατά το σχεδιασμό, την ανάπτυξη και τη χρήση διαδικασιών ασφάλειας στον κυβερνοχώρο. Επεξηγεί ουσιαστικά το τρόπο με τον οποίο η επιστήμη συμπεριφοράς προσφέρει τη δυνατότητα για σημαντική αύξηση της αποτελεσματικότητας της ασφάλειας στον κυβερνοχώρο.

4.5.4 Μέθοδος Delphi

Η μέθοδος Delphi είναι μία ερευνητική μεθοδολογία που έχει τις ρίζες της στις ΗΠΑ και, από τη δεκαετία του '60 που εμφανίστηκε, έχει εφαρμοστεί σε πάρα πολλές περιπτώσεις όπου απαιτείται η συλλογή εξειδικευμένης γνώσης, ενώ χρησιμοποιείται ευρέως σε πλήθος επιστημονικών πεδίων, μεταξύ των οποίων και στην μέτρηση του Κινδύνου (Cyber Risk Measurement). Η μέθοδος σχεδιάστηκε για να υποστηρίξει την ανάπτυξη ενός ειλικρινούς διαλόγου μεταξύ ειδικών σε ένα ζήτημα, έχοντας ως κύρια χαρακτηριστικά της, την ανωνυμία των συμμετεχόντων και τη μεταξύ τους ανάδραση (feedback) (Gordon 2009).

Η βασική αρχή στην οποία στηρίζεται η φιλοσοφία της μεθόδου είναι ότι οι κρίσεις και τα συμπεράσματα που απορρέουν από μια ομάδα, είναι περισσότερο ασφαλείς από την ατομική κρίση σε ένα θέμα. Στόχος της μεθόδου είναι η συλλογή πληροφορίας και γνώσης κατανεμημένης σε πολλά άτομα με εξειδίκευση στο μελετώμενο αντικείμενο. Ακόμη περισσότερο, μέσα από την εφαρμογή της μεθόδου επιδιώκεται η πληροφορία που συλλέγεται να αποτελεί το προϊόν συναίνεσης μεταξύ των διαφορετικών απόψεων των συμμετεχόντων, ως αποτέλεσμα της ανάδρασης. Η επιδίωξη του στόχου αυτού υλοποιείται μέσα από μια δομημένη διαδικασία επικοινωνίας με τους συμμετέχοντες, που εξελίσσεται σε σειρά σταδίων - επαναλήψεων, με νέα κάθε φορά δεδομένα, τα οποία έχουν προκύψει από τα προηγούμενα βήματα.

Χρησιμοποιείται ευρέως όταν τα δεδομένα σε μία έρευνα είναι ανεπαρκή ή ακατάλληλα για να ερευνηθούν με άλλες ερευνητικές μεθόδους. Επίσης στην έρευνα δεν υπάρχουν γεωγραφικοί περιορισμοί καθώς οι συμμετέχοντες μπορούν να στέλνουν τις απαντήσεις τους online, ενώ δεν υπάρχει χρονικός περιορισμός. Έτσι το υπό εξέταση αντικείμενο έρευνας, εξετάζεται διεξοδικότερα.

Πάντως τα αποτελέσματα από την εφαρμογή της μεθόδου δεν έχουν ως στόχο την παραγωγή μίας στατιστικά σημαντικής πληροφορίας, καθώς αποτελούν πληροφορία από μικρό αριθμό ατόμων. Η αξία της μεθόδου έγκειται στις ιδέες που μπορεί να παραχθούν από την εφαρμογή της και ουσιαστικά είναι μία τεχνική που βοηθάει στην πρόβλεψη ή στην λήψη μίας απόφασης.

Κεφάλαιο 5

Μεθοδολογικό Πλαίσιο

5.1 Σχεδιασμός του Πλαισίου

Όπως αναλύθηκε στο προηγούμενο Κεφάλαιο, οι υπάρχουσες μέθοδοι υπολογισμού παρόλα τα προφανή πλεονεκτήματα τους, παρουσιάζουν πολλά μειονεκτήματα στην εξαγωγή ενός οριστικού συμπεράσματος για έναν Οργανισμό, για το αν η επένδυση σε συστήματα Τ.Π.Ε και συστήματα ασφαλείας είναι αρκετή και επικερδής.

Η μεθοδολογία της παρούσας έρευνας, για οργανισμούς που αντιμετωπίζουν προβλήματα ή επιθέσεις στα συστήματα ασφάλειας τους, είναι πολυεπίπεδη. Το κύριο πρόβλημα που παρουσιάζεται στις ερευνητικές ομάδες των συστημάτων ασφαλείας είναι πως τα δεδομένα που αντλούν από τις εταιρείες είναι ακανόνιστα δηλαδή, χωρίς συγκεκριμένη ροή (μηνιαία/ετήσια) και σε μερικές περιπτώσεις μη αξιόπιστα. Η αξιοπιστία έγκειται όχι μόνο στο γεγονός ότι πολλά από αυτά τα στοιχεία παρέχονται από εταιρείες (vendors) που διαφημίζουν προϊόντα ασφαλείας αλλά και στο γεγονός ότι πολλές φορές οι ίδιοι οι Οργανισμοί δεν αποκαλύπτουν τις επιθέσεις που έχουν δεχτεί αλλά και τις επιπτώσεις των. Επίσης ένα ακόμα πρόβλημα που παρουσιάζεται στην μέτρηση του κόστους των ζημιών που μπορεί να έχει μια εταιρεία είναι η δυσκολία στην κατηγοριοποίηση και ποσοτικοποίηση μη ποσοτικών μεγεθών, για παράδειγμα η ζημιά που μπορεί να υποστεί μια επιχείρηση στην φήμη της και στο όνομα της (Brand name).

Αυτή η Διατριβή προσπαθεί να αντιμετωπίσει αυτά τα προβλήματα με μεθόδους της σύγχρονης οικονομικής και επενδυτικής έρευνας. Συγκεκριμένα, προσπαθεί να ατομικεύσει την επένδυση στα συστήματα ασφαλείας και να αξιολογήσει την βιωσιμότητα της δημιουργώντας ένα μεθοδολογικό πλαίσιο (framework) για την απλούστευση της έρευνας και καλύτερη κατανόηση των αποτελεσμάτων.

Πάντα πρέπει να λαμβάνουμε υπόψη ότι οι επενδύσεις σε υποδομές ICT και συστήματα Ασφαλείας διαθέτουν κάποια ιδιαίτερα χαρακτηριστικά που όπως αναλύθηκαν και στα προηγούμενα Κεφάλαια, συνοψίζονται στα ακόλουθα (Milis & Mercken, 2003:96):

- Συνήθως τα αποτελέσματά τους εμφανίζονται μακροπρόθεσμα.
- Περιέχουν υψηλό ποσοστό κινδύνου και κυρίως
- Μεγάλο μερίδιο από τα οφέλη και τα έξοδα είναι ποιοτικά, μη απτά και δύσκολο να ποσοτικοποιηθούν.

Για όλους τους παραπάνω λόγους και δεδομένης της εκτεταμένης μελέτης των υπαρχόντων μοντέλων αλλά και της εκτεταμένης βιβλιογραφικής επισκόπησης, διαπιστώθηκε η έλλειψη ενός καθαρού τρόπου ή μεθόδου για να υπολογιστεί η επένδυση στα συστήματα Τ.Π.Ε και Ασφαλείας από έναν Οργανισμό.

Το προτεινόμενο μεθοδολογικό πλαίσιο προσπαθεί να υπολογίσει από την αρχή όλη την επένδυση σε αυτά τα συστήματα, να υπολογίσει το οικονομικό κόστος των επιπτώσεων των Κυβερνοεπιθέσεων σε έναν Οργανισμό, προτείνοντας μία διαφορετική λύση που θα χρησιμοποιεί τα κυριότερα πλεονεκτήματα όλων των μεθόδων αξιολόγησης που διερευνήθηκαν στο προηγούμενο Κεφάλαιο της παρούσας Διατριβής. Το πλαίσιο χωρίζεται σε τρία (3) σκέλη:

- την ποσοτικοποίηση των ποιοτικών παραμέτρων κόστους, για παράδειγμα το κόστος φήμης, το κόστος από την οικονομική απάτη και την μοντελοποίηση τους.
- Τον υπολογισμό του ρίσκου χρησιμοποιώντας μεθόδους όπως την Αξία σε Κίνδυνο (VaR) και την προσομοίωση Monte Carlo.
- την αξιολόγηση της επένδυσης με μεθόδους όπως η ROI και προσαρμοσμένη ΚΠΑ.

Ίσως το πιο σημαντικό κομμάτι της μεθοδολογίας αυτής της έρευνας είναι η εκτίμηση του κινδύνου με την μέθοδο Value at Risk (VaR), μία μεθοδολογία που χρησιμοποιείται με μεγάλη επιτυχία κυρίως στον χρηματοπιστωτικό τομέα για τον υπολογισμό των οικονομικών κινδύνων Ο σκοπός αυτού του τμήματος είναι να μπορέσουμε με την ποσοτικοποίηση του κινδύνου να προβλέψουμε τον μελλοντικό κίνδυνο και την ευαισθησία των συστημάτων ασφαλείας σε αυτόν, ενώ με την μεθοδολογία VaR, να αναλύσουμε υπό προϋποθέσεις τους κινδύνους για την ασφάλεια σε έναν Οργανισμό. Σε αυτό το σημείο αξίζει να αναφερθεί πως οι παραδοσιακές μέθοδοι μέτρησης του

κινδύνου αντιμετωπίζουν το πρόβλημα της μη κανονικής κατανομής στα δεδομένα των επιθέσεων σε συστήματα ασφαλείας. Ωστόσο η μεθοδολογία της παρούσας έρευνας κάνει μια προσπάθεια επίλυσης αυτού.

5.1.1 Ποσοτικοποίηση του Κινδύνου

Σύμφωνα με τον Holton όπως αναφέρθηκε και στο Κεφάλαιο 2, ο επιχειρησιακός κίνδυνος σε μία συγκεκριμένη κατάσταση υπάρχει όταν υφίσταται αβεβαιότητα και αντιληπτή έκθεση σχετικά με μελλοντική κατάσταση που θα αποφέρει επιπτώσεις για ένα αντικείμενο. Ουσιαστικά είναι ο συνδυασμός της πιθανότητας να γίνει ένα ανεπιθύμητο γεγονός, με την επίπτωση (impact) από αυτό το γεγονός. Τα στοιχεία που συνθέτουν τους Κινδύνους των Π.Σ είναι οι ευπάθειες τους, οι απειλές για την ασφάλεια του και τα μέτρα ασφαλείας ή αντίμετρα που παίρνει ένας Οργανισμός για την προστασία του Π.Σ και των αγαθών του. Η ανάλυση και το προτεινόμενο πλαίσιο επικεντρώνεται στους κινδύνους παραβιάσεων ασφαλείας και πρέπει να εξετάσουμε τόσο τη πιθανότητα να συμβεί μία παραβίαση όσο και στην ίδια την επίπτωση.

<u>Πιθανότητα</u>

Η πιθανότητα εξαρτάται από πολλούς παράγοντες και κυρίως από τον αριθμό των ευπαθειών που έχουν τα συστήματα που χρησιμοποιεί ο Οργανισμός, το είδος των αγαθών και το κίνητρο που έχει μία πηγή απειλής, η αποτελεσματικότητα των απειλών αλλά και από την αποτελεσματικότητα που έχουν τα αντίμετρα που χρησιμοποιούνται. Η πιθανότητα αυτή πρέπει να ποσοτικοποιηθεί σε συγκεκριμένο χρονικό διάστημα το οποίο δεν πρέπει να είναι μεγάλο, λαμβάνοντας υπόψη την τεχνολογία που χρησιμοποιούν οι πηγές απειλής και την συχνότητα που εμφανίζονται συνεχώς νέες και όλο πιο δύσκολες απειλές. Το χρονικό διάστημα ορίζεται στο ένα έτος καθώς σε αυτό το χρονικό διάστημα είναι δύσκολο να αλλάξει και η αξία των προστατευόμενων συστημάτων αλλά και συνήθως η οικονομική αξιολόγηση μίας επένδυσης ξεκινάει από το πρώτο έτος και επεκτείνεται μέχρι το τέλος του επενδυτικού διαστήματος.

Έτσι για το χρονικό διάστημα του ενός έτους δεν χρειάζεται να υπολογίσουμε την SLE (single loss expectancy), αλλά την πιθανότητα των απωλειών μέσα σε ένα έτος[10], που ίσως είναι και πιο εύκολο για έναν Οργανισμό από την στιγμή που με βάση τα στατιστικά στοιχεία που διατηρεί (και σαφώς μόνο ο ίδιος γνωρίζει, ένα από τα προβλήματα που αναφέραμε) θα μπορεί να

[10] Όπως προτείνεται και αναλύεται από την Διδακτορική Διατριβή του Πηρούνια Σ.(2012), σελ.204

υπολογίσει έναν εκτιμώμενο μέσο όρο απωλειών για ένα συγκεκριμένο χρονικό διάστημα. Σημειωτέο ότι όπως θα δούμε παρακάτω, αυτός ο αριθμός μπορεί να επεκταθεί και σε μεγαλύτερο χρονικό διάστημα (βλ. short/long term, Παρ. 5.5).

Κατόπιν παίρνουμε το μοντέλο Gordon & Loeb που αναλύσαμε στο προηγούμενο Κεφάλαιο όπου σαν **s (z,v)** ορίζεται ως η πιθανότητα να προκύψει οποιοδήποτε ρήγμα στην ασφάλεια που είναι συνάρτηση των δύο τυχαίων μεταβλητών, της επένδυσης σε συστήματα ασφαλείας και της πιθανότητας μίας απειλής να προκαλέσει μία επιτυχημένη επίθεση. Σε αυτόν προσθέτουμε και την αποτελεσματικότητα των αντιμέτρων που θα χρησιμοποιήσει ο Οργανισμός.

Επίπτωση

Η επίπτωση εξαρτάται σημαντικά από την αξία και την κρισιμότητα του αγαθού που θα δεχθεί την επίθεση για τον Οργανισμό. Το μέγεθος αυτής της επίπτωσης είναι ουσιαστικά ο βαθμός που θα επηρεαστεί η λειτουργία και η αποστολή του. Αν τα συστήματα που θα δεχτούν την επίθεση έχουν μικρή αξία, τότε συνεπακόλουθα ο κίνδυνος θα είναι χαμηλός ακόμα και αν η πιθανότητα να συμβεί η παραβίαση είναι μεγάλη. Άρα τα συστήματα με την μεγαλύτερη αξία για αυτόν, θα παρουσιάζουν και μεγαλύτερο Κίνδυνο που σημαίνει ότι ένας Οργανισμός πρέπει να θέτει προτεραιότητες για την προστασία τους. Επιπλέον το μέγεθος της επίπτωσης εξαρτάται σημαντικά και από τον βαθμό έκθεσης των συστημάτων στην απειλή και υπολογίζεται ως το ποσοστό από την αξία που θα απολεσθεί μετά από μία επιτυχημένη παραβίαση.

Υπολογισμός

Μια προτεινόμενη μέθοδο είναι του Annual Expectation Loss (ALE) του National Bureau of Standards (1979), που προτείνουν οι Sklavos και Souras (2005) στην έρευνα που δημοσίευσαν για οικονομικά μοντέλα στην ασφάλεια των ηλεκτρονικών συστημάτων. Συγκεκριμένα το πλαίσιο που προτείνουν ήταν η υλοποίηση μια στρατηγικής διαχείρισης ρίσκου ανάλογα με τις ανάγκες της επιχείρησης στο τμήμα των συστημάτων ασφαλείας. Ειδικότερα, ένα από τα μοντέλα στην μεθοδολογία που ακολουθούν είναι αυτό του ALE, που δείχνει στην εταιρεία την ετήσια αναμενόμενη ζημιά. Το μοντέλο είναι το εξής:

ALE = expected rate of loss x value of loss =ARO * SLE

$$\sum_{i=1}^{n} I(O_i)F_i$$

Όπου ($O_i, \ldots, O_n$) τα οποία είναι τα ζημιογόνα ενδεχόμενα που μπορούν να συμβούν στην χρονιά. Όπου I (O_i), το αποτέλεσμα των ζημιογόνων ενδεχομένων σε δολάρια. Όπου F_i, δηλώνουν την συχνότητα αυτών των ενδεχομένων.

Η μέθοδος αυτή συνοψίζει ουσιαστικά δύο (2) ποσοτικές παραμέτρους που μπορεί να διαφοροποιούνται μεταξύ τους σε έναν απλό αριθμό, την επίπτωση από τις ζημιές και την συχνότητα εμφάνιση τους. Σε αυτό ακριβώς το σημείο επισημαίνεται και το μεγάλο μειονέκτημα της. Συγκεκριμένα μπορεί να εμφανιστεί ένα ίδιο αποτέλεσμα και να μην ξεχωρίσει την διαφορά μεταξύ ενός γεγονότος με μικρή συχνότητα εμφάνισης αλλά μεγάλη επίπτωση και σε ένα άλλο γεγονός με μεγάλη συχνότητα εμφάνισης αλλά μικρή επίπτωση (Sklavos & Souras 2005:16).

Η τροποποίηση της με βάση αυτά που αναφέραμε παραπάνω και στα πλαίσια του προτεινόμενου πλαισίου, είναι η χρήση της πιθανότητας των απωλειών μέσα σε ένα έτος αντί της συχνότητας εμφάνισης.

Βέβαια για τους λόγους όμως που αναφέρθηκαν στο προηγούμενο Κεφάλαιο ο υπολογισμός του ALE είναι δύσκολος. Διαφορετικό είναι όταν συμβεί μία επίθεση και διαφορετικό αν μετά την επίθεση ο Οργανισμός έχει πάρει μέτρα για να αντιμετωπίσει αυτό το είδος των επιθέσεων. Στην περίπτωση αυτή προκύπτει ένα τροποποιημένο ALE (mALE/modified ALE) που σαφώς δίνει μικρότερο κόστος σε έναν Οργανισμό.

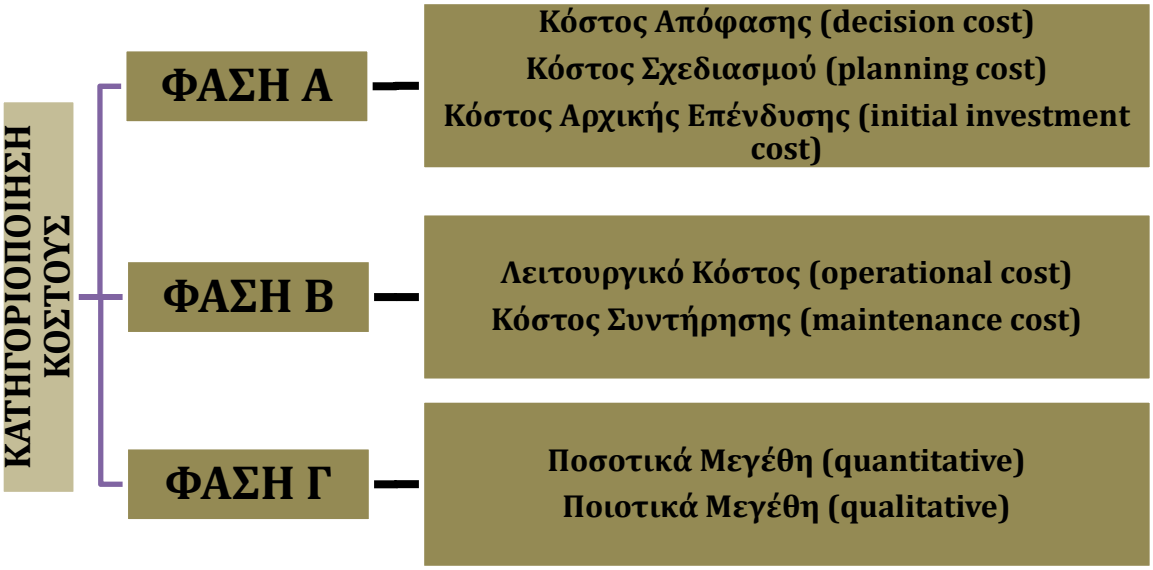
Στην περίπτωση που ο Οργανισμός πάρει κάποια μέτρα για την προστασία του, πρέπει αυτή η διαφορά να υπολογιστεί σε σύγκριση με το ίδιο το κόστος αυτών των μέτρων για να αποφανθούν οι ειδικοί αν τα μέτρα συμφέρουν ή όχι. Βέβαια το κόστος αυτών των μέτρων πρέπει να υπολογιστεί για το ίδιο διάστημα που υπολογίζεται και το ALE, για έναν χρόνο.

5.1.2 Κατηγοριοποίηση του Κόστους

Σε αυτήν την φάση, σκοπός είναι η κατηγοριοποίηση για τα κόστη που αναφέρθηκαν στο προηγούμενο Κεφάλαιο. Έχουν προταθεί διάφοροι τρόποι για την

κατηγοριοποίηση τους, είτε σε έξι (6) κατηγορίες (Sklavos & Souras 2005:15), είτε διαιρώντας τα σε διάφορες κατηγορίες π.χ. άμεσα και έμμεσα κόστη.

Σε αυτήν την Διατριβή, υπολογίζουμε τρεις (3) διαφορετικές φάσεις για την κατηγοριοποίηση του κόστους της επένδυσης στα συστήματα Τ.Π.Ε, ενώ θα διαιρέσουμε τις οικονομικές επιπτώσεις μετά από μία επίθεση στα συστήματα στην Φάση Γ, σε δύο μεγάλες κατηγορίες που θα βοηθήσουν και στην ανάλυση της πρότασης που θα αναλυθεί παρακάτω, δηλαδή σε ποιοτικά και ποσοτικά μεγέθη και οι οποίες με την σειρά τους θα διαιρεθούν σε επιπλέον υπό-κατηγορίες.



Πίνακας 2. Κατηγοριοποίηση του Κόστους

Στην πρώτη Φάση ένας Οργανισμός πρέπει να υπολογίσει ή να συνυπολογίσει στην απόφαση για την επένδυση του στα συστήματα Τ.Π.Ε και Ασφαλείας όλα τα κόστη που αναλύθηκαν στο προηγούμενο Κεφάλαιο, όπως είναι το κόστος απόφασης, το κόστος σχεδιασμού και το κόστος της αρχικής επένδυσης.

Κατόπιν σε δεύτερη Φάση να υπολογίσει το κόστος για την χρήση αυτών των συστημάτων, όπως είναι το κόστος συντήρησης και το λειτουργικό κόστος.

Τέλος να υπολογίσει τις συνέπειες που θα έχει μία Κυβερνοεπίθεση στα συστήματα του. Στην πρώτη κατηγορία θα μπουν όλα αυτά τα ποιοτικά μεγέθη που δεν είναι εύκολο να

ποσοτικοποιηθούν σε χρήμα, αυτό δηλαδή που θα καταλάβουν οι μέτοχοι ή η Διεύθυνση ενός Οργανισμού και τα οποία απαιτούν μία πιο ποιοτική προσέγγιση.

Η δεύτερη κατηγορία περιλαμβάνει όλα τα μεγέθη που μπορούν θεωρητικά εύκολα να ποσοτικοποιηθούν οπότε και να υπολογιστούν, εφαρμόζοντας αυστηρά ποσοτικά χρηματοοικονομικές τεχνικές όπως η ΚΠΑ. Ο παρακάτω Πίνακας περιλαμβάνει αναλυτικά την διαμόρφωση αυτών των δύο (2) κατηγοριών βασισμένος κυρίως στον αντίστοιχο Πίνακα της Deloitte για τις οικονομικές επιπτώσεις μετά από μία Κυβερνοεπίθεση.[11]

	ΚΑΤΗΓΟΡΙΑ	
ΠΟΙΟΤΙΚΑ ΜΕΓΕΘΗ	Αρνητική Φήμη	Loss of Reputation
	Απώλεια Εμπιστοσύνης	Loss of Trust
	Εξασθένηση της εμπορικής αξίας	Devaluation of Trade Name
	Απώλεια Πνευματικής Ιδιοκτησίας	Loss of Intellectual Property
	Αυξημένο Κόστος Ασφάλισης	Insurance Premium Increases
	Αργή υιοθέτηση νέας τεχνολογίας	Slow adaption of new technology
ΠΟΣΟΤΙΚΑ ΜΕΓΕΘΗ	Κόστος επιδιόρθωσης	Repair Cost
	Απώλεια παραγωγικότητας	Productivity loss
	Κόστος αντικατάστασης	Replacement Cost
	Τεχνική διερεύνηση	Technical Investigation
	Βελτιώσεις στα συστήματα ασφαλείας του Οργανισμού	Cyber security Improvements
	Δημόσιες Σχέσεις	Public Relations

Πίνακας 3. Ποιοτικά και Ποσοτικά Μεγέθη

[11] Deloitte, 2016. «Beneath the surface of a cyber-attack. A deeper look at business impacts».

Σύμφωνα πάντα με την επεξήγηση της Deloitte, τα επιπλέον μεγέθη που χρησιμοποιούνται σε σχέση με το Κεφάλαιο 4, είναι:

- Το αυξημένο κόστος ασφάλισης, που ουσιαστικά θα επιβάλλει μία ασφαλιστική εταιρεία σε έναν Οργανισμό μετά από μία κυβερνοεπίθεση στα συστήματα του. Η αύξηση αυτή μπορεί να φτάσει και στο 200% του αρχικού κόστους ασφάλισης
- Την απώλεια Πνευματικής Ιδιοκτησίας που σχετίζεται με την απώλεια ελέγχου επαγγελματικών μυστικών, μελλοντικών επενδύσεων, ευρεσιτεχνιών του Οργανισμού και που μπορεί να οδηγήσουν σε απώλεια ανταγωνιστικού εμπορικού πλεονεκτήματος και απώλεια εσόδων.

5.2 Υπολογισμός Ποσοτικών μεγεθών

Εκτός από τις ποιοτικές παραμέτρους, στο προηγούμενο Κεφάλαιο αναφέρθηκαν και οι ποσοτικές παράμετροι, αυτές δηλαδή που μπορούν να μετρηθούν σχετικά εύκολα από έναν Οργανισμό. Ειδικότερα όπως αναφέρθηκε και στο παραπάνω κεφάλαιο, κάποια από τα κόστη μιας κυβερνοεπίθεσης μπορεί να είναι το κόστος για την επισκευή του νέου συστήματος ασφαλείας, το κόστος από την απώλεια της παραγωγικότητας που μπορεί να αντιμετωπίσει το προσωπικό και γενικότερα ο Οργανισμός ή ακόμα το κόστος από την απώλεια εσόδων και από έλλειψη ικανότητας πώλησης εμπορευμάτων/υπηρεσιών, για παράδειγμα στον τομέα του ηλεκτρονικού εμπορίου.

5.3 Ποσοτικοποίηση των ποιοτικών παραμέτρων

Ο δείκτης πρόβλεψης χρεοκοπίας Z-score δημιουργήθηκε από τον καθηγητή Χρηματοοικονομικών του Πανεπιστημίου της Νέας Υόρκης, Edward I. Altman (1968). Η έρευνα του δημοσιεύτηκε το 1968 και βρίσκει εφαρμογή μέχρι και σήμερα δίνοντας πληροφορίες για την οικονομική ευμάρεια της, υπό εξέταση επιχείρησης. Ο καθηγητής δημιουργώντας το πλαίσιο του τύπου που θα χρησιμοποιούσε προέβη σε μια σειρά του προσδιορισμού της συνεισφοράς της εκάστοτε μεταβλητής, της αξιολόγησης, της παρατήρησης, της ακρίβειας στην πρόβλεψη και στην κριτική του ανάλυση. Επίσης, μεθοδολογίες τέτοιου τύπου εφαρμόζονται συνήθως για συγκεκριμένες ομοιογενείς ομάδες εταιριών.

Ωστόσο στην παρούσα έρευνα, αυτή η μέθοδος τροποποιείται στην εξής μορφή:

$$\boldsymbol{Z = \sum_{i=1}^{n} w_i X_i}$$

Το αρχικό βήμα στην εφαρμογή τους είναι η επιλογή ορισμένων βασικών ποιοτικών δεικτών κόστους, οι οποίοι χαρακτηρίζουν το μέγεθος της ζημιάς που μπορεί να πάθει μια εταιρεία από μια κυβερνοεπίθεση. Έπειτα επί των στοιχείων αυτών, εφαρμόζεται το πολυμεταβλητό υπόδειγμα Z με στόχο τον προσδιορισμό του μεγέθους των ζημιών που μπορεί να υποστεί η εταιρεία σε ποιοτικές μεταβλητές. Για παράδειγμα αν πάρουμε τρεις (3) διαφορετικές μεταβλητές που θα επηρεαστούν μετά από μία επίθεση στα συστήματα της εταιρείας τότε:

Χ1 = Κόστος από την αρνητική φήμη, Χ2 = Κόστος από την Οικονομική απάτη, Χ3 = Κόστος από την πιο αργή υιοθέτηση της τεχνολογίας και των συστημάτων Τ.Π.Ε

Οι συγκεκριμένες μεταβλητές στο υπόδειγμα λαμβάνουν ένα βαθμό βαρύτητας (w_i) που καθορίζει πόσο εξαρτημένη/ευαίσθητη είναι η εταιρεία σε αυτές. Για παράδειγμα, αν η εταιρεία υπό εξέταση έχει μεγάλη ευαισθησία στην αρνητική φήμη και λιγότερο στην οικονομική απάτη και στην υιοθέτηση της τεχνολογίας και των συστημάτων Τ.Π.Ε., ο τύπος θα διαμορφωθεί κάπως έτσι: $Z = 0{,}6X_1 + 0{,}2X_2 + 0{,}2X_3$. Δηλαδή θα δείχνει πόσο περισσότερο ευαίσθητο είναι το Z στην συγκεκριμένη μεταβλητή. Για παράδειγμα εάν μια εταιρεία που ασχολείται με δίκτυα υπολογιστών δεχτεί μια επίθεση στα συστήματα ασφαλείας θα έχει μεγαλύτερο αντίκτυπο στην βαθμολογία από ότι μια άλλη που δραστηριοποιείται εκτός του χώρου της πληροφορικής.

Στην συνέχεια, διαμορφώνεται ένα ερωτηματολόγιο που θα παραθέτει μια σειρά ερωτήσεων στην εταιρεία στο οποίο θα εξετάζεται το μέγεθος ζημιάς που μπορεί να πάθει μια επιχείρηση από την συγκεκριμένη μεταβλητή σύμφωνα με ιστορικά στοιχεία της συγκεκριμένης εταιρείας (μη ποσοτικά). Το ερωτηματολόγιο θα έχει ως αποτέλεσμα την βαθμολογία από 0 έως 10 στην συγκεκριμένη μεταβλητή, δηλαδή θα μπει η κάθε μεταβλητή σε συγκεκριμένη κλίμακα . Ειδικότερα, εάν η εταιρεία έχει ιστορικά αρκετές ζημιές από επιθέσεις στα συστήματα ασφαλείας στην φήμη της, τότε θα παρουσιάζει μια βαθμολογία για $X_1 = 7$ έως 10. Εάν όμως δεν παρουσιάζει μεγάλη ζημία ή απειλή στην συγκεκριμένη ποιοτική μεταβλητή τότε θα λαμβάνει τιμές για $X_1 = 1$ έως 4.

Το τελικό βήμα είναι η κλίμακα των μεταβλητών να μετατραπεί σε χρηματικές μονάδες ($). Αυτό γίνεται μέσω της επεξεργασίας ιστορικών δεδομένων της εταιρείας υπό εξέταση που θα δείχνει το εύρος ζημιάς που έχει πάθει από την συγκεκριμένη ποιοτική μεταβλητή. Για παράδειγμα για μια εταιρεία που έχει το εξής εύρος ζημιών, η κλίμακα διαμορφώνεται ως εξής:

1	10,000$
2	20,000$
.	.
.	.
8	670,000$
9	850,000$
10	1,000,000$

Ένα από τα σημαντικότερα πλεονεκτήματα της συγκεκριμένης μεθοδολογίας είναι ότι το Z της συγκεκριμένης επιχείρησης ποσοτικοποιεί τις μεταβλητές αυτές που έχουν ποιοτικά χαρακτηριστικά.

5.4 Αξία σε Κίνδυνο (Var)

Ο κίνδυνος (ή η αξία σε κίνδυνο) σε συστήματα ασφαλείας μπορεί να ορισθεί ως ο κίνδυνος που αναφέρεται στην αβεβαιότητα της αξίας των συστημάτων ασφαλείας, η οποία οφείλεται στις κυβερνοεπιθέσεις που δέχεται ο οργανισμός.

Ένα από τα δημοφιλέστερα εργαλεία διαχείρισης κινδύνου την τελευταία δεκαετία είναι η μέθοδος της μέτρησης των κινδύνων που βασίζεται στην πιθανότητα εμφάνισης κάποιων ζημιών στην αξία ενός οργανισμού και είναι γνωστή ως αξία σε κίνδυνο ή Value at Risk (VaR). Η έννοια της VaR αναπτύχθηκε κατά τη διάρκεια της δεκαετίας του 1970 και του 1980, όταν ορισμένα χρηματοπιστωτικά ιδρύματα ξεκίνησαν τη μελέτη εσωτερικών μοντέλων για τη μέτρηση του κινδύνου συνολικά. Κατόπιν τη δημοσίευση του συστήματος RiskMetricsTM για τη μέτρηση του κινδύνου της αγοράς από την JP Morgan το 1994, δόθηκε μεγάλη βαρύτητα στην VaR και τώρα θεωρείται πρότυπο εργαλείο για τη μέτρηση των κινδύνων της αγοράς (Ammann & Reich 2001:2). Στην

συνέχεια η μεθοδολογία VaR επεκτάθηκε και σε Οργανισμούς εκτός των χρηματοπιστωτικών, με διάφορες παραλλαγές της (CfaR-Cash flow at Risk και EaR-Earnings at Risk).

Η μεγάλη δημοτικότητα που έχει επιτύχει αυτό το μέσο οφείλεται κυρίως στην απλοϊκή μορφή που έχει, δηλαδή στην κατανόηση του σαν εργαλείου: η VaR ανάγει τον κίνδυνο (της αγοράς) που σχετίζεται με οποιοδήποτε χαρτοφυλάκιο σε έναν μόνο αριθμό. Στόχος της VaR είναι να προσδιορίσει μια ευέλικτη και αμερόληπτη αξιολόγηση των κινδύνων του χαρτοφυλακίου διαχρονικά, έτσι ώστε τα ανώτερα διευθυντικά στελέχη να έχουν τη δυνατότητα να αναλύσουν όλους τους κινδύνους και να πάρουν στρατηγικές αποφάσεις με βάση τον κίνδυνο (Tsai 2004:22). Σύμφωνα με τον Best (1998) (όπως παρατίθεται από τον Corkalo 2011:81), ένας ευρεία αποδεκτός ορισμός της VaR είναι ο ακόλουθος: "*Η αξία σε κίνδυνο (VaR) είναι το μέγιστο ποσό που μπορεί να χαθεί σε ένα χαρτοφυλάκιο σε ένα δεδομένο χρονικό ορίζοντα, με δεδομένο επίπεδο εμπιστοσύνης και κάτω από την υπόθεση των κανονικών συνθηκών της αγοράς".*

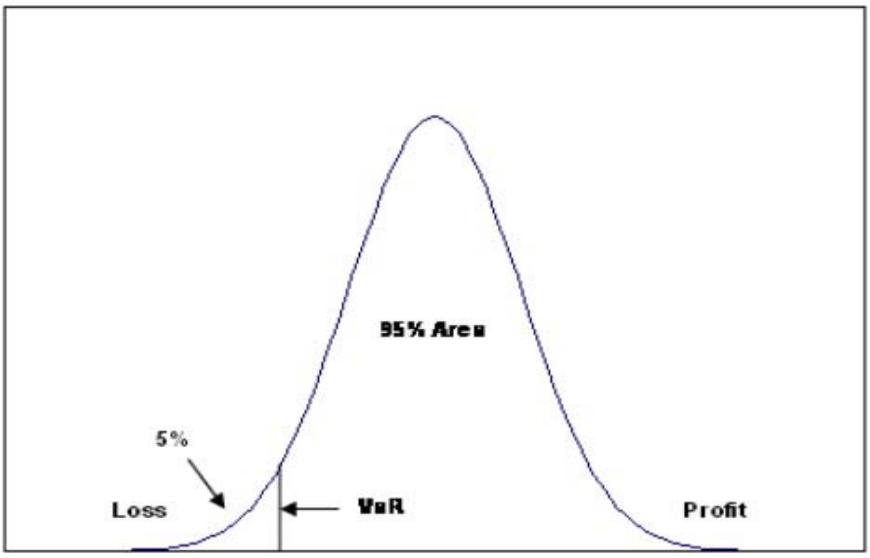
Ουσιαστικά μπορούμε να πούμε ότι η VaR υπολογίζει τη μέγιστη δυνατή ζημία που μπορεί να υποστεί ένα χαρτοφυλάκιο για μία δεδομένη χρονική περίοδο και για ένα δεδομένο επίπεδο εμπιστοσύνης. Η VaR δηλαδή αποτελεί μία συνοπτική απεικόνιση του κινδύνου της αγοράς και παράλληλα περιλαμβάνει δύο (2) πάρα πολύ σημαντικά χαρακτηριστικά:

- Την πιθανότητα, που εκφράζει το πόσο πιθανό είναι οι ζημίες να είναι μεγαλύτερες από το δεδομένο ποσό.

- Την μέτρηση του Κινδύνου σε νομισματικές μονάδες, δηλαδή μετράει το ποσό το οποίο θα χαθεί σε μία δεδομένη χρονική περίοδο, η οποία εξαρτάται από τη χρονική περίοδο για την οποία το χαρτοφυλάκιο παραμένει σταθερό. Αν δηλαδή το c είναι το επιλεγμένο διάστημα εμπιστοσύνης, η VaR αναφέρεται στο 1-c διάστημα εμπιστοσύνης, στην αριστερή ουρά της κατανομής.

Η VaR ενός χαρτοφυλακίου που υπάρχουν ενδεχόμενες πιθανότητες ύπαρξης ζημιογόνων γεγονότων είναι συνάρτηση δύο παραμέτρων: της περιόδου διακράτησης (holding period) και του επιπέδου εμπιστοσύνης (confidence level). Η επιλογή των συστατικών αυτών από τους διαχειριστές του κινδύνου επηρεάζει σε μεγάλο βαθμό τη φύση του μοντέλου της VaR. Τα μοντέλα VaR υποθέτουν ότι η σύνθεση του συνόλου

των ενδεχομένων δεν αλλάζει κατά τη διάρκεια της περιόδου διακράτησης. Αυτή η υπόθεση υποστηρίζει τη ύπαρξη βραχυπρόθεσμων περιόδων διακράτησης, επειδή η σύνθεση των χαρτοφυλακίων είναι ικανή να αλλάζει συχνά. Όσον αφορά το επίπεδο εμπιστοσύνης, υπάρχουν κάποια επίπεδα εμπιστοσύνης που χρησιμοποιούνται συχνά, τα οποία είναι το 95% και το 99%. Η επιλογή του επιπέδου εμπιστοσύνης αντικατοπτρίζει την αποστροφή στον κίνδυνο. Για παράδειγμα, με 95% διάστημα εμπιστοσύνης η VaR πρέπει να είναι τόση ώστε να μην ξεπερνά το 5% του συνολικού αριθμού των παρατηρήσεων στην κατανομή όπως φαίνεται και στο παρακάτω σχήμα.



Εικόνα 14. Διαγραμματική Απεικόνιση της VaR με 95% διάστημα εμπιστοσύνης

Συγκριτικά με τις παραδοσιακές μεθόδους μέτρησης κινδύνων, η VaR παρέχει μία ολοκληρωμένη εικόνα του κινδύνου ενός χαρτοφυλακίου, η οποία λαμβάνει υπόψη της τη μόχλευση (leverage), τις διάφορες συσχετίσεις (correlations) καθώς και την τρέχουσα θέση (current position) του χαρτοφυλακίου. Συνεπώς, η VaR είναι μία μέθοδος, η οποία προβλέπει τους πιθανούς μελλοντικούς κινδύνους με πολύ μεγάλη ακρίβεια.

Οι βασικές υποθέσεις για τον ακριβή υπολογισμό της είναι οι ακόλουθες:

- Η κατανομή των επιθέσεων στα συστήματα ασφαλείας (για παράδειγμα εάν ακολουθούν οι επιθέσεις την κανονική κατανομή)

- Η έκταση κατά την οποία η σημερινή μεταβολή των ποσοστών των απωλειών από επιθέσεις σε περιουσιακά στοιχεία της εταιρείας συσχετίζονται με τις μεταβολές του παρελθόντος.

- Η έκταση κατά την οποία τα χαρακτηριστικά του μέσου και της μέσης απόκλισης τετραγώνου είναι σταθερά στο χρόνο.

- Η αλληλοσυσχέτιση μεταξύ δύο ή περισσότερων διαφορετικών μετατοπίσεων των τιμών των ενδεχομένων από κυβερνοεπιθέσεις , σε όρους χρηματικών απωλειών.

- Η χρονολογική σειρά στοιχείων στα οποία εφαρμόζονται οι υποθέσεις (σε ποια δεδομένα αναφέρονται οι υποθέσεις).

Εφαρμογές της VaR

Διαχρονικά το VaR χρησιμοποιούνταν για χρονολογικές σειρές αποδόσεων χαρτοφυλακίων. Έτσι εκτιμάται το μέγεθος του κινδύνου που μπορεί να υποστεί ένα χαρτοφυλάκιο από τις «ακραίες καταστάσεις» της αγοράς. Οι εφαρμογές της Αξίας σε Κίνδυνο μπορούν να ταξινομηθούν στις ακόλουθες κατηγορίες:

- Πληροφόρηση (Reporting). Η αρχική εφαρμογή της μεθόδου VaR ήταν η μέτρηση του συνολικού κινδύνου.

- Έλεγχος των Κινδύνων (Controlling Risk).

- Διαχείριση των Κινδύνων (Managing Risk). Τα τελευταία χρόνια η μέθοδος VaR χρησιμοποιείται όλο και περισσότερο από τα πιστωτικά ιδρύματα και τις επιχειρήσεις για τον υπολογισμό του κεφαλαίου που απαιτείται για την αντιμετώπιση των χρηματοοικονομικών κινδύνων.

Επίσης το VAR μπορεί να χρησιμοποιηθεί για την μελέτη της αποδιδόμενης αξίας στους μετόχους (Shareholder Value Analysis - SVA) ώστε να βοηθήσει στην λήψη αποφάσεων για το ποιοι επιχειρηματικοί τομείς θα πρέπει να αναπτυχθούν , διατηρηθούν ή περιοριστούν αλλά και να βοηθήσει στην μεγιστοποίηση της συνολικής αποδιδόμενης αξίας στους μετόχους. Η μελέτη SVA χρησιμοποιεί την έννοια της Καθαρής Παρούσας Αξίας (Net Present Value - NPV), σύμφωνα με την οποία οι αναμενόμενες χρηματορροές θα πρέπει να μετατρέπονται ώστε να αντικατοπτρίζουν την σημερινή τους αξία.

Έτσι, μελετώντας την μορφή του, στο πλαίσιο αυτής της έρευνας **το προσαρμόσαμε στις ανάγκες ενός Οργανισμού για εκτίμηση και ποσοτικοποίηση του κινδύνου στα συστήματα ασφαλείας από μελλοντικές επιθέσεις και κατά επέκταση τις απώλειες και ζημιές στην καθαρή θέση της, σε ένα συγκεκριμένο χρονικό διάστημα.**

Στην πραγματικότητα η VaR μετράει ή εκτιμάει την αξία που θα μπορούσε να χαθεί στο χειρότερο σενάριο για έναν Οργανισμό, όταν δηλαδή οι ζημίες υπερβαίνουν αυτές που μπορεί να αναμένονται. Το γεγονός αυτό είναι πολύ σημαντικό , επειδή η VaR μπορεί να είναι πολύ υψηλότερη από την απώλεια αξίας που θα μπορούσε να είναι εύλογα αναμενόμενη και συνεπώς βοηθάει στον εντοπισμό του επιπέδου αβεβαιότητας.

Επίσης ένα τέτοιο μοντέλο θα βοηθήσει τους Οργανισμούς να υπολογίσουν μετά από μία επιτυχημένη Κυβερνοεπίθεση στα συστήματα της, π.χ. με επίπεδο εμπιστοσύνης 95%, ότι δεν θα χάσει παραπάνω από ένα συγκεκριμένο ποσό Χ σε συγκεκριμένο χρονικό διάστημα με 95% ακρίβεια.

Πλεονεκτήματα και Μειονεκτήματα

Παρά την σπουδαιότητα του VaR ως μέτρου εκτίμησης του κινδύνου, αποτελεί μόνο μια στατιστική εκτίμηση, η οποία βασίζεται συνήθως σε μια κατανομή ιστορικών χρονολογικών στοιχείων και δεδομένων. Τα πλεονεκτήματα αυτής της μεθόδου είναι πολλά, όπως πολλά είναι και τα μειονεκτήματα που το καθιστούν μη απόλυτα ακριβές στον πραγματικό κόσμο.

Αρχικά τα πλεονεκτήματα που αναδεικνύουν το VaR ως πολύ ισχυρό εργαλείο εκτίμησης του κινδύνου είναι τα εξής:

- Το μεγάλο πλεονέκτημα του VaR συνίσταται στο ότι ενσωματώνει σε έναν και μόνον αριθμό τη συνολική έκθεση στον κίνδυνο ενός Οργανισμού που μπορεί να βρεθεί εκτεθειμένος σε επιθέσεις κατά των συστημάτων του, οπότε δεν υπάρχει ανάγκη για ειδικές τεχνικές γνώσεις προκειμένου να υπάρξει γρήγορη κατανόηση από στελέχη που βρίσκονται εκτός του αντικειμένου.

- Καθορισμός ορίων διαπραγμάτευσης. Οι τράπεζες μπορούν να καθορίσουν συναλλαγές, με την εταιρεία για την εξασφάλιση και την προφύλαξη της από μελλοντικούς κινδύνους, χρησιμοποιώντας το μέγεθος του VaR. Για παράδειγμα, θα μπορεί να δημιουργήσει ένα

είδους ασφαλιστικό συμβόλαιο από μια τράπεζα που θα προστατεύει την εταιρεία από κακόβουλες εξωτερικές ενέργειες διαδικτύου.

- Επιπλέον, με την χρήση του VaR είναι δυνατή η σύγκριση θέσεων σε διαφορετικά περιβάλλοντα όπως διαφορετικές χώρες ή εταιρείες του ίδιου ομίλου.

- Δημιουργία σχέσης κινδύνου-απόδοσης ενός χαρτοφυλακίου με βάση ένα δείκτη αναφοράς (benchmark index).

- Αφού οι επενδυτές και η διοίκηση της εταιρείας κατανοεί ποιο εύκολα της εταιρείας υπόσταση του κινδύνου,. λαμβάνει καλύτερες αποφάσεις σχετικά με τη στρατηγική επένδυση ή διαχείριση των συστημάτων ασφαλείας, επιτυγχάνοντας τη βέλτιστη απόδοση.

- Τέλος είναι εύκολος ο υπολογισμός της, αφού χρησιμοποιεί τις κλασικές στατιστικές τεχνικές (Συριόπουλος 2008).

Ωστόσο τα προβλήματα του VaR το καθιστούν μη απολύτως ρεαλιστικό:

- Μια ουσιαστική κριτική για τον υπολογισμό του VaR είναι ότι η κατανομή των αποδόσεων δεν είναι η κανονική.

- Το VaR επίσης δεν λαμβάνει υπόψη του τον μη γραμμικό τρόπο με τον οποίο μεταβάλλονται οι επιθέσεις στα συστήματα ασφαλείας και το ποσοστό ζημιών που έχει επωμιστεί από αυτές.

- Ο αριθμός VaR εξαρτάται από την υπόθεση ότι το μέλλον θα μιμηθεί το παρόν, υποεκτιμώντας την πιθανότητα εμφάνισης ακραίων φαινομένων. Εκτιμάει δηλαδή την πιθανή μελλοντική ζημία στηριζόμενη σε ιστορικά παρελθοντικά στοιχεία που μπορεί να μην ισχύουν στο επόμενο διάστημα χρόνου.

- Αν η επιχείρηση έχει στην κατοχή της σε μεγάλο βαθμό μη ρευστοποιήσιμα στοιχεία, που σημαίνει οτι δεν μπορούν μεταπωληθούν γρήγορα, το VaR μπορεί να υποεκτιμά τις πραγματικές ζημιές αφού τα στοιχεία ίσως χρειάζεται να πωληθούν με έκπτωση.

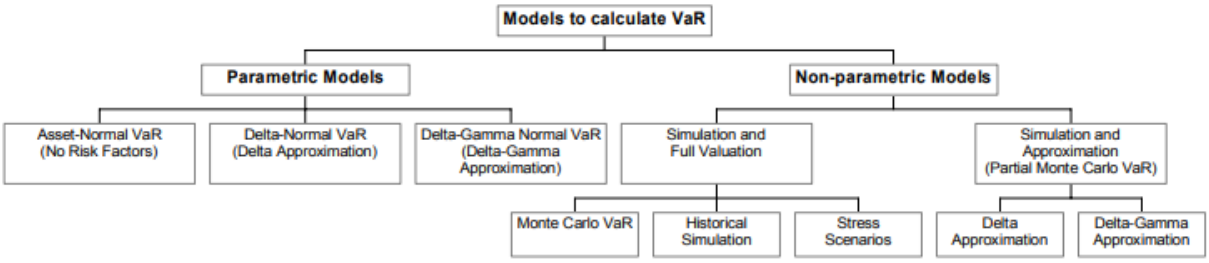
- Ένα επιπλέον πρόβλημα σχετίζεται με την ισχύ των υποθέσεων πάνω στις οποίες στηρίζεται ο υπολογισμός της VaR. Εάν οι υποθέσεις αυτές ελεγχθούν και δεν ισχύουν, τότε το μέγεθος της VaR δεν είναι σημαντικό και δεν θα πρέπει να ληφθεί υπόψη.

Συνεπώς, θα πρέπει να γνωρίζουμε καλά τα δεδομένα που χρησιμοποιούνται και τα χαρακτηριστικά τους.

- Τέλος η ύπαρξη ενός αριθμού που να υποδεικνύει όλους τους κινδύνους μια εταιρείας ελλοχεύει τον κίνδυνο να μην περιέχει όλη την πληροφορία. Αυτό μπορεί με τη σειρά του να δημιουργήσει παραπλανητικές ερμηνείες των αναλυτικών αποτελεσμάτων. Επιπλέον, οι επικριτές της VaR συχνά τονίζουν ότι οι διαφορετικές προσεγγίσεις οδηγούν σε διαφορετικές αξίες. Θα πρέπει επίσης να σημειωθεί ότι η VaR μετρά μόνο ποσοτικά μετρήσιμους κινδύνους, δεν μπορεί να μετρήσει κινδύνους όπως ο κίνδυνος ρευστότητας, ο πολιτικός κίνδυνος (political risk), ή ο κανονιστικός κίνδυνος (regulatory risk) (Bohdalova, 2007), δηλαδή δεν μπορεί να μετρήσει κινδύνους που είναι ποιοτικά μετρήσιμοι.

5.4.1 Μορφές της Μεθοδολογίας VaR

Σε αυτό το κομμάτι θα παρατεθούν δύο μορφές του VaR, η παραμετρική εκτίμηση και η υπό συνθήκη Αξία σε Κίνδυνο.



Εικόνα 15. Διαφορετικές Προσεγγίσεις της VaR (Πηγή: Ammann & Reich 2001, σελ.2)

Στη περίπτωση της παραμετρικής εκτίμησης συνήθως υποθέτουμε ότι το ποσοστό ζημιάς από την κυβερνοεπίθεση σε κάποιο περιουσιακό στοιχείο της εταιρείας ακολουθεί τη κανονική κατανομή. Σ' αυτή τη περίπτωση η Αξία σε Κίνδυνο δίνεται από τη παρακάτω σχέση:

$$\mathbf{VaR = W_0 \times \alpha \times \sigma(I),\ I(O_i)}$$

Στην παραπάνω σχέση η ζημιά μετριέται σαν απόκλιση από το αναμενόμενο ύψος της περιουσίας $W_0(1 + E(I))$ που βρίσκεται σε κίνδυνο στο τέλος της περιόδου που αναφέρεται το ενδεχόμενο επίθεσης. Το W_0 δείχνει την αξία της περιουσίας της

εταιρείας στην αρχή της περιόδου που εκτίθεται στον κίνδυνο. Το I(0) είναι η ποσοστιαία ζημιά που δέχεται μια επιχείρηση από μία επίθεση στα συστήματα ασφαλείας. Το σ(I) δείχνει την τυπική απόκλιση του αποτελέσματος των αρνητικών ενδεχομένων/επιθέσεων σε χρηματικό ποσό. Ο συντελεστής α προσδιορίζει τον αριθμό των τυπικών αποκλίσεων τετραγώνου που απέχει η τυχαία μεταβλητή της ποσοστιαίας ζημιάς, I, από την αναμενόμενη τιμή I(O), δηλαδή α = (I – E(I)/ σ(I)). Η τιμή του συντελεστή α προκύπτει από τους πίνακες της τυποποιημένης κανονικής κατανομής και ενδεικτικές τιμές που παρουσιάζονται στο παρακάτω πίνακα.

Επίπεδο εμπιστοσύνης (μονοκατάληκτο)	**99,87%**	**99,00%**	**97,5%**	**95%**
α = (I-E(I))/σ	3,00	2,32	1,96	1,65

Τέλος, αν και η ζημιά είναι αρνητικό μέγεθος την παρουσιάζουμε σε απόλυτες τιμές.

<u>Παράδειγμα 1: Υπολογισμός της Αξίας σε Κίνδυνο μεμονωμένης θέσης</u>

Έστω ότι η αξία των περιουσιακών στοιχείων που βρίσκονται σε κίνδυνο ενός οργανισμού είναι 100ευρώ, η ημερήσια τυπική απόκλιση τιμών I είναι 2% και ότι τα ποσοστά ζημιών από μια επίθεση στα συστήματα ασφαλείας ακολουθούν κανονική κατανομή. Ποια είναι η εκτίμηση της μέγιστης ζημιάς που μπορεί να υποστούμε για την αυριανή ημέρα σε επίπεδο σημαντικότητας 5%;

Απάντηση: VaR = 100*(1,65)*0,02 = 3,3 ευρώ

Ωστόσο το πρόβλημα της μελέτης της παραμετρικής εκτίμησης είναι πως οι τιμές των I δεν ακολουθούν κανονική κατανομή. Δηλαδή, είναι τυχαίες και σε πολλές περιπτώσεις οι μελλοντικές επιθέσεις δεν έχουν σχέση με τις παρελθούσες επιθέσεις και ζημιές. **Αυτό το πρόβλημα προσπαθεί να λύσει η παρούσα έρευνα με την μέθοδο της υπό συνθήκης Αξία σε Κίνδυνο (Conditional VaR, CVaR).**

<u>Υπό συνθήκη Αξία σε Κίνδυνο (Conditional VaR)</u>

Έτσι, τον ορισμό του μέτρου της Αξίας σε Κίνδυνο μπορούμε να τον γενικεύσουμε στην περίπτωση που η συνάρτηση πυκνότητας πιθανότητας της τυχαίας μεταβλητής του

κέρδους – ζημιάς της θέσης, X = W0 x I, δεν είναι η κανονική κατανομή αλλά δίνεται από την συνάρτηση f(x). Σε αυτή την περίπτωση η Αξία σε Κίνδυνο, VaR, σε επίπεδο εμπιστοσύνης c, δίνεται από την σχέση:

$$\boldsymbol{C = \int_{-VaR}^{\infty} f(x)dx}$$

Όπως είναι προφανές από τα παραπάνω η υιοθέτηση της κανονικής κατανομής για τις τιμές I έχει το πλεονέκτημα ότι προσφέρει έναν εύκολο υπολογισμό της Αξίας σε Κίνδυνο που απαιτεί τη χρήση μιας μόνο παραμέτρου, της τυπικής απόκλισης των ποσοστιαίων ζημιών, σ (I).

Το παραπάνω μέτρο του κινδύνου έχει δεχτεί κριτική όσον αφορά την καταλληλότητα του δεδομένου ότι δεν εκφράζει το μέγεθος της ζημιάς σε εκδηλώσεις «ακραίων» καταστάσεων. Δηλαδή υποστηρίζεται ότι ίσως περισσότερο χρήσιμη είναι η πληροφορία για την αναμενόμενη ζημιά, E(x/ x < -VaR), αν η τυχαία μεταβλητή του κέρδους – ζημιάς, x, πάρει τιμές μικρότερες από το –VaR. Σε αυτή την περίπτωση η σωρευτική πιθανότητα πραγματοποίησης αυτών των τιμών είναι ίση με

$$\boldsymbol{(1 - c) = \int_{-\infty}^{-VaR} f(x)dx .}$$

Το μέτρο του κινδύνου σε αυτή τη περίπτωση **ονομάζεται υπό συνθήκη Αξία σε Κίνδυνο (Conditional VaR, CVaR)** και ορίζεται από την σχέση:

$$\boldsymbol{E(x/x < VaR) = \{\int_{-\infty}^{-VaR} xf(x)dx\} / \int_{-\infty}^{-VaR} f(x)dx.}$$

Σχεδιασμένα για να μετρούν το κίνδυνο εμφάνισης ακραίων ζημιών, το CVaR είναι μια επέκταση του VaR που δίνει το συνολικό ποσό των ζημιών ενός ζημιογόνου γεγονότος, π.χ. μίας επίθεσης στα συστήματα ασφαλείας του Οργανισμού. Το CVaR υπολογίζεται ως VaR ενός χαρτοφυλακίου καθώς και η πιθανότητα σταθμισμένη μέση απώλεια εκτιμώμενη σε υπέρβαση της VaR. Μια εκτίμηση CVaR δεν μπορεί να είναι κατώτερη από ό, τι μια εκτίμηση VaR. Ωστόσο το CVaR συχνά απαιτεί ένα μεγάλο αριθμό παρατηρήσεων για να δημιουργήσει μια αξιόπιστη εκτίμηση, και είναι πιο ευαίσθητο στην εκτίμηση των σφαλμάτων από ότι είναι το VaR (Yamai & Yoshiba, 2002).

5.4.2 Εφαρμογή της CVaR στο προτεινόμενο πλαίσιο

Σκοπό της παρούσας Διατριβής δεν είναι φυσικά να προτείνει κάποια αλλαγή στον τρόπο υπολογισμού της μεθοδολογίας VaR, αλλά να προτείνει τον τρόπο που θα μπορούσε να χρησιμοποιηθεί από τους Οργανισμούς που θέλουν να υπολογίσουν την επένδυση τους και να ποσοτικοποιήσουν μέσω της μεθοδολογίας αυτής τους κίνδυνους στα συστήματα ασφαλείας της από μελλοντικές επιθέσεις. Για να γίνει αυτό πρέπει όλα τα δεδομένα να τροποποιηθούν ώστε να ανταποκρίνονται στις ανάγκες ενός τέτοιου Οργανισμού.

Αρχικά όταν μιλάμε για χαρτοφυλάκιο, σαφώς αναφερόμαστε στην ίδια την αξία του Οργανισμού που θα την χρησιμοποιήσει. Μία επιτυχημένη επίθεση και παραβίαση στα συστήματα του, θα προκαλέσει ζημίες στην καθαρή του Αξία, που ουσιαστικά θα αφορά ένα ποσό που θα συμπεριλαμβάνει όλα τα κόστη που αναφερθήκαμε στην Φάση Γ της κατηγοριοποίησης του Κόστους στην παράγραφο 5.1.2.

Κατόπιν υπολογίζουμε το χρονικό διάστημα που θα εφαρμοστεί η CVaR και το οποίο κάνοντας μία παραδοχή, το θέτουμε στο ένα (1) έτος, όπως ακριβώς και στον υπολογισμό του αριθμού των επιθέσεων.

Πολύ σημαντικός είναι και ο υπολογισμός των στατιστικών στοιχείων που διατηρεί ο Οργανισμός για τον υπολογισμό της συχνότητας επιτυχημένων επιθέσεων σε αυτόν και των επιπτώσεων που φέρνουν στην αξία του. Το πρόβλημα υφίσταται όταν ένας Οργανισμός δεν γνωρίζει ότι έχει υποστεί μία επίθεση που δεν ανίχνευσε ή που δεν επηρέασε τα συστήματα του γεγονός που μπορεί να αποφέρει μεγάλες αποκλίσεις στον υπολογισμό.

Τέλος, πρέπει ο κάθε Οργανισμός ανάλογα με την φύση του, την ευαισθησία του και την κρισιμότητα των συστημάτων που πρέπει να προστατεύσει, πρέπει να θέσει και το ανάλογο επίπεδο σημαντικότητας.

5.4.3 Εναλλακτικές προτεινόμενες μέθοδοι

Εναλλακτικές μέθοδοι για τον υπολογισμό του VaR παρουσιάζονται σε αυτήν την υπο-ενότητα, καθώς και την σύγκριση μεταξύ τους. Ο λόγος είναι για να λύσουμε τα προβλήματα που αντιμετωπίσαμε παραπάνω αλλά και για να υπολογίσουμε το VaR σε χρονικά διαστήματα μεγαλύτερα του ενός έτους. Συγκεκριμένα:

Η **προσομοίωση Monte Carlo** βασίζεται σε μεγάλο βαθμό στη θεωρία πιθανοτήτων για να προωθήσει τη διαδικασία της προσομοίωσης (Cheung & Powell, 2012:105). Η προσομοίωση Monte Carlo λειτουργεί πολύ καλά στην πιο γενική περίπτωση του υπολογισμού της VaR για μη γραμμικά σύνολα δεδομένων και για μεγάλες χρονικές περιόδους όπου τα ιστορικά δεδομένα είναι ασταθή και μη σταθερά και όταν η υπόθεση της κανονικότητας είναι αμφισβητήσιμη (Corkalo, 2011:84). Οι τεχνικές προσομοίωσης Monte Carlo, είναι μακράν οι πιο ευέλικτες και οι πιο ισχυρές, δεδομένου ότι είναι σε θέση να λαμβάνουν υπόψη όλες τις μη γραμμικότητες της αξίας των δεδομένων σε σχέση με τον υποκείμενο παράγοντα κινδύνου, καθώς και την ενσωμάτωση όλων των επιθυμητών ιδιοτήτων των κατανομών, όπως είναι οι χοντρές ουρές και οι χρονικά μεταβαλλόμενες διακυμάνσεις, ενώ είναι εύκολα κατανοητή και εξηγήσιμη (Bohdalova, 2007:4). Ένα άλλο πλεονεκτήματα της προσομοίωσης Monte Carlo είναι ότι η παραγωγή διαφορετικών συσχετισμένων σεναρίων είναι εύκολα δυνατή.

Στην προσομοίωση Monte Carlo χρησιμοποιούνται τυχαίες (random) τιμές I των βασικών εργαλείων για να κατασκευαστεί μια κατανομή των ποσοστιαίων ζημιών ενός οργανισμού, αντί των ιστορικών τιμών. Η συγκεκριμένη μεθοδολογία προσφέρει μία εκτίμηση του VaR για περίπλοκες περιπτώσεις ενδεχομένων. Το VaR ενός οργανισμού με συστήματα ασφαλείας εκτιμάται από την τυχαία κατασκευή ενός ιστογράμματος των πιθανών ποσοστιαίων ζημιών που θα σημειωθεί μέσα σε ένα προκαθορισμένο χρονικό ορίζοντα.

Ουσιαστικά με βάση την παρατηρούμενη στατιστική συμπεριφορά των μεταβλητών παράγεται ένας μεγάλος αριθμός μελλοντικών τιμών μέσω Η/Υ. Από το δείγμα υπολογίζεται η «χειρότερη» μείωση που μπορεί να συμβεί στην αξία της θέσης του οργανισμού που δέχεται επίθεση.

Επιπροσθέτως, οι προσομοιώσεις μπορούν να επεκταθούν σε μακροχρόνια περίοδο, το οποίο έχει ουσιώδης μορφή για τη μέτρηση πιστωτικού κινδύνου της εταιρείας αλλά και στα πιο σύνθετα πρότυπα των αναμενόμενων πιθανοτήτων ύπαρξης επιθέσεων μέσω διαδικτύου. Επίσης, μπορεί να χρησιμοποιηθεί για τη μέτρηση λειτουργικού κινδύνου, καθώς επίσης και την ολοκληρωμένη διαχείριση κινδύνου. Ως πιστωτικό κίνδυνο ορίζουμε τον κίνδυνο εμφάνισης ζημιών λόγω αθέτησης των υποχρεώσεων των πιστούχων της εταιρείας (Καλφάογλου, 2012:61) και ως λειτουργικό κίνδυνο ορίζουμε την οικονομική ζημία που προκύπτει από μια σειρά από πιθανές λειτουργικές βλάβες που μπορούμε να σκεφτούμε από την άποψη των κινδύνων των ανθρώπων (people

risks), των κινδύνων της διαδικασίας (process risks), και των κινδύνων της τεχνολογίας (technology risks) (Crouhy et al., 2014:501).

Η **ιστορική προσομοίωση** αυτό που κάνει είναι να παίρνει ένα σύνολο των στοιχείων που σχετίζεται με τους παράγοντες ή με τις κυβερνοεπιθέσεις (όπως αυτό αναφέρθηκε και ποιο πάνω στην έρευνα) σε κάποια δεδομένη χρονική στιγμή και έπειτα να αποτιμά αυτό σε ορισμένες φορές, χρησιμοποιώντας τις ιστορικές τιμές των στοιχείων που περιλαμβάνονται σε αυτό. Ο πιο απλός τρόπος υπολογισμού του VaR μέσω της μεθόδου αυτής, είναι να αποτιμήσει κανείς το σύνολο των μελλοντικών ενδεχομένων (επιθέσεων στα συστήματα ασφαλείας της εταιρείας) χρησιμοποιώντας ένα συγκεκριμένο αριθμό ιστορικών τιμών των στοιχείων. Έτσι έχουμε μια νέα τιμή του για κάθε μια από τις ημέρες έρευνας του παρελθόντος. Η αξία σε κίνδυνο τότε μας δίνεται από το κατάλληλο εκατοστημόριο για δεδομένο επίπεδο εμπιστοσύνης.

Το σημαντικότερο μειονέκτημα αυτής της μεθόδου είναι ότι καθώς η αξία των ενδεχομένων μεταβάλλεται με τον χρόνο, τα ποσοστά που χρησιμοποιούνται για τον υπολογισμό αυτής της αξίας μεταβάλλονται και αυτά, αυτό έχει ως αποτέλεσμα ότι δεν αντιπροσωπεύουν τη πραγματική διάρθρωση του χαρτοφυλακίου σήμερα. Αυτό σημαίνει ότι οι τιμές και οι παράγοντες αλλάζουν με αποτέλεσμα να αλλάζει ο υπολογισμός για όλο το χρονικό διάστημα για το οποίο χρησιμοποιήθηκαν ιστορικές τιμές. Η εκτίμηση ενός συνόλου ενδεχομένων με πραγματικές ιστορικές τιμές δε θα μας δώσει ένα έγκυρο αποτέλεσμα. Στη πραγματικότητα αυτό που μας χρειάζεται είναι οι ιστορικές τιμές των μεταβολών του, σύμφωνα με το σημερινό χαρτοφυλάκιο και τη σημερινή διάρθρωση και αξία του.

Στα **Stress Tests**, αντί της χρήσης ιστορικών αγοραίων τιμών ή τυχαίων επιλεγμένων δεδομένων τιμών, δημιουργούνται μια σειρά από σενάρια τιμών I για την εξέταση της απόδοσης χαρτοφυλακίου. Στην ουσία υποτίθενται διάφορα ακραία σενάρια (ακραία επεισόδια - outliers) και εξετάζεται η επίδραση τους στην αξία του οργανισμού που βρίσκεται σε κίνδυνο από μια ενδεχόμενη επίθεση στα συστήματα ασφαλείας. Η μέθοδος εξετάζει μόνο τις μεγάλες μεταβολές ορισμένων μεταβλητών, που ελάχιστα απασχολούν την καθημερινή παρακολούθηση των κινδύνων αλλά μπορούν δυνητικά να συμβούν.

Θέλοντας να δώσουμε μια ποιο σφαιρική εικόνα για τις εναλλακτικές μεθόδους σε σύγκριση με τις μεθόδους του VaR που χρησιμοποιούν παραμετρικά στοιχεία, παρουσιάζουμε τον παρακάτω πίνακα (Terpezan-Tabara, 2008:598).

	Παραμετρική Μέθοδος	**Μέθοδος Ιστορικής Προσομοίωσης**	**Μέθοδος Προσομοίωσης Monte Carlo**
Είναι σε θέση να καταγράψει τους κινδύνους των χαρτοφυλακίων;[12]	Όχι, εκτός αν υπολογίζεται χρησιμοποιώντας ένα σύντομο χρονικό διάστημα διακράτησης για χαρτοφυλάκια με περιορισμένο ή μέτριο περιεχόμενο σε δικαιώματα.	Ναι, είναι ανεξάρτητη από τα δικαιώματα που περιέχονται στο χαρτοφυλακίου.	Ναι, είναι ανεξάρτητη από τα δικαιώματα που περιέχονται στο χαρτοφυλακίου.
Είναι εύκολο να εφαρμοστεί;	Ναι, για χαρτοφυλάκια που περιορίζονται σε μέσα και νομίσματα και καλύπτονται από πρόχειρα λογισμικά. Διαφορετικά είναι εύκολο έως μετρίως δύσκολο να εφαρμοστεί, ανάλογα με την πολυπλοκότητα των μέσων και την διαθεσιμότητα των δεδομένων.	Ναι, για χαρτοφυλάκια που υπάρχουν διαθέσιμα στοιχεία σχετικά με τις προηγούμενες αξίες των παραγόντων της αγοράς.	Ναι, για χαρτοφυλάκια που περιορίζονται σε μέσα και νομίσματα και καλύπτονται από πρόχειρα λογισμικά. Διαφορετικά, είναι μέτρια έως εξαιρετικά δύσκολο να εφαρμοστεί.

Πίνακας 4. Σύγκριση μεθόδων VaR (Terpezan-Tabara 2008:598)

Ο διαχειριστής κινδύνου πρέπει να εξετάσει τη σύνθεση του χαρτοφυλακίου του και στη συνέχεια να επιλέξει την κατάλληλη μέθοδο που είναι ωφέλιμη στον Οργανισμό του. Είναι χρήσιμο να αναλυθούν τα ιστορικά δεδομένα και να αναλυθεί η κατανομή των αποδόσεων για να διαφανεί ποια προσέγγιση μπορεί ή δεν μπορεί να εφαρμοστεί. Ωστόσο μια μη παραμετρική μέθοδος υπολογισμού του VaR θα έδινε μια καλύτερη

[12] *Στον όρο χαρτοφυλάκιο του παραπάνω πίνακα, χρησιμοποιούμε σε αυτήν την έρευνα το σύνολο των μελλοντικών ενδεχομένων/πιθανοτήτων για μελλοντικές κυβερνοεπιθέσεις στα συστήματα ασφαλείας της εταιρείας.

εικόνα στον υπολογισμό του ρίσκου που διατρέχει η εταιρεία από τους πιθανούς παράγοντες.

5.5 Αξιολόγηση της Επένδυσης

Σύμφωνα λοιπόν με την έρευνα που ανάπτυξαν ο Sklavos και Souras το 2005, το μοντέλο για την αξιολόγησης μια επένδυσης στην ασφάλεια είναι ο γνωστός δείκτης ROI. Η μεθοδολογία του αποτελεί το μέσο για να διαπιστωθεί εάν μια επένδυση συνεισφέρει ή όχι στον οργανισμό, καθώς αυτό που κάνει είναι να εξετάζει εάν τα οφέλη από το πρόγραμμα, εκφρασμένα σε αξία, ξεπερνούν τα κόστη. Ο Οργανισμός μπορεί να συγκρίνει τη συνεισφορά διαφόρων επενδύσεων μεταξύ τους, καθώς η χρονική περίοδος εξέτασης είναι ετήσιος, και να εκτελεί μόνο τις επικερδείς. Το μοντέλο της συγκεκριμένης έρευνας και με κάποιες επιπλέον τροποποιήσεις που πραγματοποιούνται σε αυτήν την μεταπτυχιακή Διατριβή, διαμορφώνεται ως εξής:

Σύμφωνα με την ανάλυση στα προηγούμενα κεφάλαια της μεθοδολογίας της Διατριβής, το κόστος αποταμίευσης είναι το παρακάτω:

$$\mathbf{S = \underbrace{ALE_{BASELINE} - ALE_{WITH\ SAFEGUARDS}}_{1.} + \underbrace{Z_{BASELINE} - Z_{WITH\ SAFEGUARDS}}_{(2)}}$$

Η μεθοδολογία ξεχωρίζει δύο διαφορές (1 και 2) που υποδηλώνουν τα το κέρδος που έχει η εταιρεία από την αποταμίευσης χρηματικού ποσού λόγω αποτροπής κάποιας επίθεσης στα συστήματα ασφαλείας της. Συγκεκριμένα:

- Η (1) αφορά τα ποσοτικά μεγέθη και υποδηλώνει την διαφορά μεταξύ του κόστους που μπορεί να υποστεί ένας Οργανισμός από διάφορες κυβερνοεπιθέσεις χωρίς να υπάρχουν κάποιου είδους μηχανισμοί αποφυγής ή μετρίασης του κινδύνου όπως antivirus, με το κόστος όταν ο Οργανισμός έχει εφαρμόσει διάφορα συστήματα ασφαλείας.

- Η (2) αφορά τα ποιοτικά μεγέθη και υποδηλώνει την διαφορά μεταξύ του κόστους που μπορεί να υποστεί ένας Οργανισμός από διάφορες κυβερνοεπιθέσεις χωρίς να υπάρχουν κάποια συστήματα ασφαλείας, όπως καμπάνιες brand marketing που εδραιώνουν στο κοινό πως το όνομα της εταιρείας είναι ισχυρό και μπορεί να αντιμετωπίσει οποιοδήποτε

σφάλμα, με το κόστος που μπορεί να υποστεί από διάφορες κυβερνοεπιθέσεις όταν έχει εφαρμόσει κάποιους μηχανισμούς αντιμετώπισης.

Η διαφορά τους μας δίνει το κέρδος που έχει μια εταιρεία από την επένδυση σε συστήματα ασφαλείας. Ο τελικός τύπος διαμορφώνεται προσθέτοντας και τα κέρδη από τις καινούργιες ανακαλύψεις μηχανισμών ή μεθόδων αποτροπής τέτοιων επιθέσεων.

B = S + (profit from new ventures)

Με αυτό τον τρόπο φτάνουμε στο σημείο που οι ερευνητές Sklavos και Souras προσαρμόζουν το υπόδειγμα του ROI στα πλαίσια των συστημάτων ασφαλείας:

$$\boldsymbol{ROI = \frac{Benefit\ of\ safeguards}{Cost\ of\ safeguards}}$$

$$\boldsymbol{= \frac{Savings\ from\ safeguards}{cost\ of\ safeguards} + \frac{profit\ from\ new\ ventures}{Cost\ of\ safeguards}}$$

$$\boldsymbol{= \frac{ALE_{BASELINE} - ALE_{WITH\ SAFEGUARDS}}{Cost\ of\ safeguards} + \frac{(Z_{BASELINE} - Z_{WITH\ SAFEGUARDS})}{Cost\ of\ safeguards} + \frac{profit\ from\ new\ ventures}{Cost\ of\ safeguards}}$$

Έτσι το ROI (Return on security Investment) μας δείχνει αν η εταιρεία έχει παραπάνω κέρδος από την επένδυση στην ασφάλεια σε σχέση με το κόστος που χρειάστηκε για την υλοποίηση της, εάν ο δείκτης είναι πάνω από την μονάδα (<1) . Όμως εάν ο δείκτης είναι κάτω από την μονάδα τότε τα κόστη για την επένδυση είναι μεγαλύτερα από τα κέρδη που δίνει. Σε αυτό το σημείο πρέπει να τονίσουμε πως ο συγκεκριμένος δείκτης μας δίνει τιμές που εξετάζουν ένα ετήσιο διάστημα. Για να εξετάσουμε μια επένδυση στην ασφάλεια σε πάνω από ένα χρόνο πρέπει να χρησιμοποιήσουμε το IRR (Internal Rate of Return) επειδή προεξοφλεί τις ταμειακές ροές για διαφορετικά κόστη (C) και για διαφορετικά κέρδη (B). Ο τύπος διαμορφώνεται ως εξής:

$$\boldsymbol{C_0 = \sum_{i=1}^{n} (B_t - C_t)/(1 + IRR)^t}$$

Όπου το C_0 είναι το πραγματικό κόστος στην επένδυση των πληροφοριακών συστημάτων, το C_t είναι το κόστος της χρονιάς t, και το B_t είναι το κέρδος της χρονιάς t.

Επίσης η εταιρεία σύμφωνα με αυτά τα ισχυρά εργαλεία για την αξιολόγηση της συγκεκριμένης επένδυσης μπορεί να διαχωρίσει σε διάφορες περιόδους το μοντέλο ανάλογα με τον τρόπο που θέλει να αξιολογήσει τα στοιχεία του κόστους της και των κερδών της στον χρόνο. Δύο προτεινόμενες χρονολογικοί διαχωρισμοί για αυτό το πλαίσιο είναι η εξής:

- **Short term: t = 1, για χρονικό διάστημα 1 έτους**

Η εφαρμογή αυτής της περιόδου προκύπτει από την υπόθεση πως τα συστήματα ασφαλείας, όπως antivirus ανανεώνονται με γρήγορους ρυθμούς λόγω της μεγάλης ανάπτυξης της τεχνολογίας. Επίσης δεν μπορούμε να θεωρήσουμε ή να αξιολογήσουμε την αρχική μας επένδυση για μεγάλο χρονικό διάστημα, γιατί οι απειλές αλλάζουν συνεχώς, τα συστήματα που χρησιμοποιούν οι hackers αποκτούν όλο και μεγαλύτερες δυνατότητες, οπότε είναι πολύ δύσκολο να υπολογίσουμε αν τα συστήματα μας θα παραμείνουν ικανά σε βάθος χρόνου. Συνολικά ο δείκτης θα μας δείξει την **βραχυχρόνια** αξιολόγηση της εταιρείας με στόχο να ανακαλύψει άμεσα προβλήματα χρηματοδότησης και επενδυτικής απόφασης που έχουν επίπτωση στα συστήματα ασφαλείας.

- **Long term: t = n, για χρονικό διάστημα 1 έως 5 ετών**

Η εφαρμογή αυτής της περιόδου προκύπτει από την υπόθεση πως τα διάφορα συστατικά μέρη του πληροφοριακού συστήματος του Οργανισμού ανανεώνονται **μακροχρόνια** όπως το hardware. Συνολικά ο δείκτης θα μας δείξει την μακροχρόνια αξιολόγηση της εταιρείας με στόχο να ανασκάψει προβλήματα και παθογένειες της εταιρείας που έχουν επίπτωση στα συστήματα ασφαλείας.

Κεφάλαιο 6

Συμπεράσματα

Αυτή την στιγμή παγκοσμίως συμβαίνει μία θεμελιώδης αλλαγή: η ιδέα ότι οι κυβερνοεπιθέσεις είναι εξαιρετικά πιθανές – και πιθανώς αναπόφευκτες – έχει αρχίσει να επικρατεί μεταξύ στελεχών των Οργανισμών.[13] Σε μία κοινωνία που κυριαρχεί η μετάδοση Πληροφοριών και ειδήσεων, η προστασία της Πληροφορίας και των πελατών ενός Οργανισμού είναι θεμελιώδης.

Η αξία του ποσοτικού προσδιορισμού του κινδύνου του κυβερνοχώρου είναι η κατανόηση της ισορροπίας μεταξύ του κινδύνου και της ανταμοιβής σε έναν Οργανισμό, η οποία αποκτά όλο και μεγαλύτερη σημασία καθώς η πολυπλοκότητα των απειλών συνεχίζει να αυξάνεται. Με σκοπό τον ορθότερο καθορισμό προτεραιοτήτων, οι Οργανισμοί θα πρέπει να καταλαβαίνουν τα είδη των ρίσκων που αντιμετωπίζουν αλλά και της σχετικής πιθανότητας εμφάνισης που έχουν οι επιθέσεις στα συστήματα Τ.Π.Ε που χρησιμοποιούν. Επιπρόσθετα το ίδιο σημαντικό είναι να καταλάβουν τις επιχειρηματικές επιπτώσεις που μπορεί να έχουν αυτά τα ρίσκα.

Μια σημαντική πρόκληση, παρόλα αυτά, είναι ότι κοινές αντιλήψεις για την επίδραση των κυβερνοεπιθέσεων δημιουργούνται κυρίως από το είδος των επιθέσεων που απαιτείται να αναφέρουν οι επιχειρήσεις δημόσια – κυρίως υποκλοπή προσωπικών πληροφοριών, δεδομένων πληρωμών, και πληροφορίες σχετικές με την προσωπική υγεία. Οι συζητήσεις τείνουν να επικεντρώνονται γύρω από κόστη που σχετίζονται με την ενημέρωση πελατών, επίβλεψη πιστώσεων, και την πιθανότητα νομικών κρίσεων ή ρυθμιστικών προστίμων.

Τα κόστη που συνήθως συνδέονται με παραβιάσεις δεδομένων αφορούν μόνο τις επιπτώσεις που συνήθως γίνονται ευρέως γνωστές – η ζημιά που φαίνεται πάνω από την επιφάνεια. Αλλά η υποκλοπή προσωπικών πληροφοριών δεν είναι πάντα στους στόχους του επιτιθέμενου. Σπάνια εμφανίζονται περιπτώσεις υποκλοπής πνευματικής περιουσίας, κατασκοπείας, καταστροφής δεδομένων, επιθέσεων σε βασικές λειτουργίες ή προσπάθειες απενεργοποίησης υποδομών υψίστης σημασίας. Κάτω από την επιφάνεια, αυτές οι επιθέσεις μπορούν να έχουν πολύ πιο σημαντικές επιπτώσεις στους οργανισμούς. Παρόλα αυτά, οι απώλειες που έχουν δεν γίνονται

[13] Deloitte, 2016. Beneath the Surface Beneath the surface of a cyberattack. A deeper look at business impacts.

ευρέως γνωστές και είναι πολύ πιο δύσκολο να ποσοτικοποιηθούν. Για να υπολογιστούν αυτές οι λιγότερο φανερές επιπτώσεις, πρέπει να εφαρμοστούν διάφορες συνδυαστικές προσεγγίσεις οι οποίες θα συνδυάζουν εκτεταμένη γνώση από περιστατικά στον κυβερνοχώρο, τεχνικές αποτίμησης αλλά και οικονομική ποσοτικοποίηση.

Επειδή είναι δύσκολο να υπολογιστούν σε ακριβή μεγέθη για πολλούς και διάφορους λόγους (ανεπαρκή στοιχεία, αδυναμία υπολογισμού διάφορων μεγεθών, μη δημοσιοποίηση στοιχείων από τους Οργανισμούς), τουλάχιστον μπορούμε να τοποθετήσουμε αυτές τις επιπτώσεις σε ένα γενικότερο πλαίσιο.

Απαιτούνται μεθοδολογικά πλαίσια εκτίμησης τα οποία θα αποφέρουν άμεσα ποσοτικά αποτελέσματα στους Οργανισμούς με έναν πολύ αντικειμενικό τρόπο. Η διοίκηση ενός Οργανισμού πρέπει να έχει στην διάθεση της αξιόπιστα και κατανοητά μεγέθη και το κυριότερο σε γλώσσα που μπορεί να καταλάβει, σε νομισματικούς όρους. Έτσι μόνο θα μπορέσει να λάβει σημαντικές αποφάσεις για την ίδια την επιχείρηση, για το μέγεθος της επένδυσης που θα κάνει σε συστήματα ασφαλείας και σε συστήματα Τ.Π.Ε, για την βέλτιστη και συμφέρουσα λύση που θα την βοηθήσει να λειτουργήσει και να επιβιώσει στο δύσκολο ανταγωνιστικό περιβάλλον.

Η εκτεταμένη βιβλιογραφική ανασκόπηση αλλά και η μελέτη όλων των υφιστάμενων μεθόδων αξιολόγησης και υπολογισμού της Επένδυσης, ανέδειξε την ανυπαρξία προς το παρόν ενός πλαισίου που θα μπορεί να αξιοποιήσει ο οποιοσδήποτε Οργανισμός (μικρή ή μεγάλη επιχείρηση) και θα αναδείξει την βέλτιστη λύση. Σκοπός λοιπόν της δημιουργίας αυτού του πλαισίου σε αυτήν την Διατριβή, ήταν να χρησιμοποιηθούν διάφοροι μέθοδοι, που εφαρμόζονται και αξιοποιούνται στις Οικονομικές επιστήμες για να υπολογιστεί η Επένδυση, η απόδοση που μπορεί να έχει και οι πιθανές απώλειες ή επιπτώσεις που θα αντιμετωπίσει ένας Οργανισμός από μία Κυβερνοεπίθεση, λαμβάνοντας υπόψη όλα τα μεγέθη που τον επηρεάζουν.

Το μεθοδολογικό αυτό πλαίσιο θα συνδύαζε τα πλεονεκτήματα όλων των υφιστάμενων μεθόδων και θα έκανε μία προσπάθεια να ποσοτικοποιήσει και να υπολογίσει όλα αυτά τα μεγέθη που όχι μόνο αποτελούν και το σημαντικότερο ποσοστό του συνολικού κόστους μετά από μία παραβίαση αλλά και είναι και δύσκολο να προσεγγιστούν λόγω της φύσης τους (π.χ. κίνδυνος από την απώλεια της καλής φήμης ενός Οργανισμού).

Η ανάλυση και το προτεινόμενο πλαίσιο επικεντρώθηκε στους κινδύνους παραβιάσεων ασφαλείας τόσο στην πιθανότητα να συμβεί μία παραβίαση όσο και στην ίδια την επίπτωση. Με βάση τα συμπεράσματα από αυτήν, το γνωστό μοντέλο ALE τροποποιήθηκε έτσι ώστε να συμπεριλάβει και την πιθανότητα των απωλειών μέσα σε ένα έτος αντί της συχνότητας

εμφάνισης, εξαλείφοντας έτσι το πρόβλημα/μειονέκτημα που έχει αναφερθεί και από άλλους ερευνητές.

Κατόπιν έγινε μία προσπάθεια να συμπεριληφθούν όλα τα κόστη που επηρεάζουν μία επένδυση σε συστήματα Τ.Π.Ε και συστήματα ασφαλείας και να κατηγοριοποιηθούν με βάση το ήδη γνωστό ερευνητικό πεδίο, χωρισμένο όμως σε τρεις διαφορετικές Φάσεις.

Από το σύνολο των υφιστάμενων μεθόδων της Αξιολόγησης της επένδυσης, προκρίθηκε η μέθοδος της επιστροφής της επένδυσης (ROI) η οποία προσαρμοσμένη με τον δείκτη πρόβλεψης χρεωκοπίας Z-score, μας δίνει μία σαφή εκτίμηση για το κόστος που αντιμετωπίζει μία εταιρεία. Κατόπιν για να εξετάσουμε μια επένδυση στην ασφάλεια σε πάνω από ένα χρόνο, πρέπει να χρησιμοποιήσουμε το IRR (Internal Rate of Return) επειδή προεξοφλεί τις ταμειακές ροές για διαφορετικά κόστη και για διαφορετικά κέρδη και το κυριότερο λαμβάνει υπόψη την χρονική αξία του χρήματος.

Πολύ σημαντική είναι και η πρόταση της Διατριβής για την χρήση της μεθοδολογίας VaR, για τον τρόπο που θα μπορούσε να χρησιμοποιηθεί από τους Οργανισμούς που θέλουν να υπολογίσουν την επένδυση τους και να ποσοτικοποιήσουν μέσω της μεθοδολογίας αυτής τους κίνδυνους στα συστήματα ασφαλείας της από μελλοντικές επιθέσεις. Η μεθοδολογία αυτή βρίσκει όλο και πιο πολλούς υποστηριχτές παγκοσμίως και αν συνδυαστεί με την μέθοδο Monte Carlo ή με την μέθοδο της ιστορικής προσομοίωσης και εφόσον εφαρμοστεί καταλλήλως, μπορεί να δώσει σημαντικά αποτελέσματα προς ενίσχυση της κατανόησης των Οργανισμών ως προς τους κινδύνους που αντιμετωπίζουν.

<u>Συνεισφορά της Διατριβής</u>

Η παρούσα Διατριβή αποτελεί μία μελέτη σε θέματα επένδυσης σε συστήματα ασφαλείας, καθώς επίσης και μία πρόταση χρήσης ενός συγκεκριμένου μεθοδολογικού πλαισίου για τον υπολογισμό της επένδυσης που θα συνδύαζε διάφορες υπάρχουσες οικονομικές μεθόδους, αξιοποιώντας κάθε φορά τα πλεονεκτήματα τους. Συμπληρωματικά της εν λόγω Διατριβής, μία επιπρόσθετη συνεισφορά της είναι οι μέθοδοι προτεινόμενης ιεράρχησης του συνολικού κόστους από την χρήση συστημάτων Τ.Π.Ε και συστημάτων Ασφαλείας σε έναν Οργανισμό.

Η αναφορά και χρήση της Μεθόδου VaR σαφώς και δεν αποτελεί μία καινοτομία, καθώς ήδη χρησιμοποιείται από μεγάλους Οργανισμούς για την εκτίμηση του Κινδύνου. Προσφέρει όμως μία επιπλέον μελέτη στα υπάρχουσα οικονομικά μοντέλα, προτείνοντας σαφώς αυτήν κατεύθυνση. Οι κατευθύνσεις της μελλοντικής έρευνας θα πρέπει να έχουν ως στόχο την δημιουργία μοντέλων για την ανάπτυξη υψηλότερης ακρίβειας στις τεχνικές εκτίμησης της VaR,

ενώ η κατάλληλη χρήση της έχοντας πάντα επίγνωση των περιορισμών αυτής μπορεί να συνεχισθεί για βελτίωση της διαδικασίας λήψης αποφάσεων από όλους τους Οργανισμούς.

Επίλογος

Παρόλο που ο τίτλος της Διατριβής αναφέρεται μόνο στην επένδυση σε τεχνολογίες Πληροφορίας και Επικοινωνιών και στην εύρεση μίας βέλτιστης λύσης, οι σύγχρονες ανάγκες των Οργανισμών και οι διαρκώς αυξανόμενες απειλές που αντιμετωπίζουν δεν ήταν δυνατό να παραλειφθούν. Είναι απαραίτητο σε έναν σύγχρονο Οργανισμό να συμπεριλάβει στην επένδυση του το συνολικό κόστος από τα συστήματα και τα αντίμετρα που θα χρησιμοποιήσει. Μόνο τότε θα έχει μία ακριβή εικόνα από τα οφέλη που θα αποκομίσει από την χρήση αυτής της τεχνολογίας, τόσο στην απόδοση όσο και στην λειτουργία του Οργανισμού.

Σαφώς όπως αναδείχτηκε και στην Διατριβή, ο ακριβής υπολογισμός του κόστους και της επένδυσης σε συστήματα Τ.Π.Ε είναι δύσκολος, με πολλές προσεγγίσεις και διαφορετικές ερμηνείες. Όμως η σύγχρονη τεχνολογία, τα συστήματα και οι κίνδυνοι που σχετίζονται με αυτά, συνεχώς εξελίσσονται, επιβάλλοντας την διαρκή έρευνα για την εύρεση μεθοδολογιών και μοντέλων που θα προσφέρουν τις κατάλληλες λύσεις και τις βέλτιστες προσεγγίσεις στην Επένδυση και κατά συνέπεια στην ανάπτυξη και στην απόδοση ενός Οργανισμού.

Βιβλιογραφία

[01] Ammann M. and Reich C. (2001). VaR for Nonlinear Financial Instruments-Linear Approximation or full Monte Carlo? Financial Markets and Portfolio Management, 15 (3). 363-378.

[02] Adar E., Wuchner A., (2005). Risk management for critical infrastructure protection challenges, Best practices and tools. In: Proc. of the 1st IEEE International Workshop on Critical Infrastructure Protection (IWCIP '05), pp 90-100.

[03] Adler R., (2000). Strategic Investment Decision Appraisal Techniques- The Old and The New, Business Horizons, Vol. 43, No 6, pp 15-22.

[04] Andersen J, Baldwin A., Betts M., Carter C., Hamilton A., Stokes E. and Thorpe T. «A Framework for Measuring IT Innovation Benefits». Electronic Journal of Information Technology in Construction, 2000, Vol 5: 57-72.

[05] Basel Committee on Banking Supervision (2006). «International Convergence of Capital Measurement and Capital Standards-A Revised Framework». [Online] Available at https://www.bis.org/publ/bcbs128.htm (Accessed on 20-02-18)

[06] Beissel S. (2016). Cybersecurity Investments. Decision Support Under Economic Aspects. Springer

[07] Berle, A. A. and Means, G. C. (1933). The Modern Corporation and Private Property. Indiana Law Journal: Vol. 8: Iss. 8, Article 11. [Online]Available at: https://www.repository.law.indiana.edu/ilj/vol8/iss8/11 (Accessed on 20-12-17)

[08] Bessant J., Lamming R., Noke H. and Philips W. (2005). Managing Innovation Beyond the Steady State. Technovation, Vol. 25: 366-376.

[09] Bohdalova, M. (2007). A comparison of Value-at-Risk methods for measurement of the financial risk. E-Leader Conference, Prague, Czech Republic, 11-13 June 2007

[10] Botchkarev A. and Andru P. (2011). A Return on Investment as a Metric for Evaluating Information Systems: Taxonomy and Application. Interdisciplinary Journal of Information, Knowledge and Management Vol. 6, pp 245-269.

[11] Brecht M. and Nowey T. (2013). A Closer Look at Information Security Costs. The Economics of Information Security and Privacy, Springer, pp 3-24

[12] Brunner E., Sutter M. «International CIIP Handbook, 2008-2009»

[13] Brynjolfsson, E. (1993): The Productivity Paradox of Information Technology. Communications of the ACM, Vol. 36, pp 67–77.

[14] Brynjolfsson E. and Hitt L. (2000). Beyond Computation: Information Technology, Organizational Transformation and Business Performance. Journal of Economic Perspectives Vol. 14, No 4, pp 23-48.

[15] Business Encyclopedia, Return on Investment (ROI) defined and calculated, with examples, usage, and comparison to other financial metrics. [Online] Available at https://www.business-case-analysis.com/return-on-investment.html (Accessed on12-12-18)

[16] Cheung, Y. H., and Powell, R. J. (2012). Anybody can do Value at Risk: A Teaching Study using Parametric Computation and Monte Carlo Simulation. *Australasian Accounting Business and Finance Journal,* 6(5), pp 101-118

[17] Chronopoulos M, Panaousis E., Grossklags J., (2017). An Options Approach to Cybersecurity Investment, IEEE Access, Vol.6 Issue 99, pp 12175-12186

[18] Corkalo, S. (2011). Comparison of Value at Risk Approaches on a Stock Portfolio. *Croatian Operational Research Review (CRORR),* 2, 81-90.

[19] Crouhy, M., Galai, D., and Mark, R. (2014). The Essentials of Risk Management.2nd Edition. New York: McGraw-Hill

[20] Dunn, M and Wigert, I (2004). «Critical Information Infrastructure Protection», The International CIIP Handbook. Zurich, Switzerland. Centre for Security Studies. Available at http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224

[21] Freeman C. and Louca F. (2001). As Time Goes by. From the Industrial Revolutions to the Information Revolution.

[22] Friendman A. (2011) Economic and Policy Frameworks for Cybersecurity Risks. Center for Technology Innovation at Brookings.

[23] Gartner. Distributed Computing - Chart of Accounts. http://www.arsyseurope. net/Propalms/Datasheets/Propalms WhitePaper Gartner TCO Analyze for Distributed Computer.pdf, 2003.

[24] Gonzalez G., Ponchel C., Blanc G., Debal H. (2014). «Combining Technical and Financial Impacts for Countermeasure Selection». International Advanced Intrusion Detection and Prevention (AIDP'14) Workshop.2014. EPTCS 165, pp 1-14

[25] Gordon, L.A. and Loeb, M.P. (2002). «The Economics of Information Security Investment». ACM Transactions on Information and System Security, 5, 438-457

[26] Gordon L. , Loeb M. and Lucyshyn W. (2003). Information security expenditures and real options: A wait-and-see approach. Computer Security Journal., Vol. 19, No. 2, 16

[27] Gordon, T. J. (2009). The Delphi Method, Futures Research Methodology – V3.0, The Millennium Project. American Council for the UNU, Washington DC, σελ. 1-29.

[28] Grossklags J., Christin N. and Chuang J. (2008), Secure or Insure? A Game-Theoretic Analysis of information Security Games. Proceeding of the 17th international conference on World Wide Web, 2008.

[29] Grossman G., Helpman E. (1991). Innovation and Growth in the Global Economy.

[30] Ho J., Wu A. and Xu S. Corporate Governance and Returns on Information Technology Investment: Evidence from an Emerging Market. Strategic Management Journal, Vol. 32, 595-623, 2011

[31] Holton G. A. (2004). Defining Risks. Financial Analysts Journal Vol. 60, 6, 17-25.

[32] Hyslop M., (2004). Critical Information Infrastructures, Resilience and Protection.

[33] Jorgenson D. and Stiroch K., (1993). Computers and Growth. Econometrics - Economic Growth in the Information Age, Vol. 3: 43-71

[34] Jovanovic B. and Rousseau P., (2005). General Purpose Technologies. Handbook of Economic Growth, Volume 1B. Ch 18. Pp1181-1224. Edited by Philippe Aghion and Steven N. Durlauf

[35] Kosutic D. (2011). Is it possible to Calculate The ROSI?. [Online] Available at https://advisera.com/27001academy/blog/2011/06/13/is-it-possible-to-calculate-the-return-on-security-investment-rosi/ (Accessed on 05-02-18)

[36] Kroenke D., (2008). Experiencing MIS. 2nd Revised Edition

[37] Laudon K. and Laudon J., (2011). Management Information Systems. Managing the Digital Firm. 12th Edition.

[38] Lockstep (2004). A Guide for Government Agencies Calculating Return on Security Investment.

[39] Macdonald S., Anderson P., Kimbel D. (2000). Measurement or Management. Revisiting the Productivity Paradox of Information Technology. The Economics of Information Technology, Vol.69: 601-617.

[40] Milis K. and Mercken R., (2003). The use of the balanced scorecard for the evaluation of information and communication technology projects. International Journal of Project Management, Vol. 21: pp 87-97

[41] Noor, M.M. and Apadore, K. (2014). The association between IT related trainings and IT investments in Malaysia. International Journal of Business and Management, 9(1), 63-76.

[42] Oliner S. and Sichel D., (1994). Computers and Output Growth Revisited: How Big Is the Puzzle. Brookings Papers on Economic Activity, Vol. 25, issue 2: 273-334

[43] Perez C. (2010). Technological revolutions and techno-economic paradigms. Cambridge Journal of Economics, Vol. 34, Issue 1, pp185–202

[44] Sklavos N. and Souras P. (2005). Economic Models and Approaches in Information Security for Computer Networks. International Journal of Network Security, Vol.2, No.1, pp.14–20, Jan. 2006

[45] Stoneburner G., Goguen A. and Feringa A. (2002). Risk Management Guide for Information Technology Systems- Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30.

[46] Tarafdar M and Gordon S. (2007). Understanding the influence of information systems competencies on process innovation: A resource-based view. Journal of Strategic Information Systems, Vol. 4: 353-392.

[47] Terpezan-Tabara O. A. (2008). The Importance of Value at Risk Method in the Management of Banking Risk, 4th International Conference of ASECU: "Development Cooperation and Competitiveness", Bucharest, Romania.

[48] Tsai, K. T. (2004). Risk Management via Value at Risk. ICSA Bulletin, 20-29

[49] Turban E. and Volonino L. (2011). Information Technology for Management: Improving Strategic and Operational Performance. 8h Edition.

[50] Wieczorek M., Vos D., Bons H. (2014). Systems and Software Quality: The next step for industrialization. Springer

[51] World Bank Group, (2014). The little data book on information and communication technology.

[52] Yamai, Yosuhiro, and Toshinao Yoshiba (2002). Comparative Analyses of Expected Shortfall and Value at Risk. Institute for Monetary and Economic Studies, Bank of Japan (January, October).

ΕΛΛΗΝΟΓΛΩΣΣΗ

[53] Καλφάογλου, Φ. (2012). Το Πλαίσιο της Κεφαλαιακής Επάρκειας των Τραπεζών. Οικονομικό Δελτίο Τράπεζας της Ελλάδος, 36, 47-93

[54] Λούγκας Δ. (2009). Εφαρμογή της μεθόδου των πραγματικών χρηματοοικονομικών δικαιωμάτων-Real Options, στη λήψη επενδυτικών αποφάσεων με αβεβαιότητα. Μεταπτυχιακή Διατριβή

[55] Μαυρίδης Ι. (2015). Ασφάλεια Πληροφοριών στο Διαδίκτυο. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/1024 (Προσπελάστηκε στις 21-12-17)

[56] Επιτροπή των Ευρωπαϊκών Κοινοτήτων (2003). Πράσινη Βίβλος για την Επιχειρηματικότητα στην Ευρώπη. Ευρωπαϊκή Επιτροπή, COM (2003) 27, σ. 4-30

[57] Παπαδάμου Σ. και Συριόπουλος Κ. (2015). Βασικές Αρχές Αξιολόγησης Επενδύσεων: Χρηματοοικονομική και κοινωνικοοικονομική προσέγγιση. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/4365 (Προσπελάστηκε στις 21-12-17)

[58] Πηρούνιας Σ. (2012). Ποσοτικοποίηση των Κινδύνων Παραβιάσεων Ασφαλείας Πληροφοριακών Συστημάτων. Διδακτορική Διατριβή

[59] Συριόπουλος, Κ. (2008). Διαχείριση Τραπεζικού Κινδύνου (Τόμος Α). Πάτρα: Ε.Α.Π.

[60] Φυτσιλής Π. (2014). Σύγχρονα πληροφοριακά συστήματα επιχειρήσεων-ERP-CRM-BPR. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/2256 (Προσπελάστηκε στις 10-01-18)

OFFICIAL REPORTS

[61] Deloitte US (2016). Beneath the surface of a cyberattack. A deeper look at business impacts. [Online] Available at

https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html (Accessed on 17-02-18)

[62] Frost and Sullivan (2013). The 2013 (ISC) 2 Global Information Security Workforce Study. [Online] Available at https://www.isc2.org/-/media/CC5799BB1DA848E6B59A8374F7371EEE.ashx

[63] Kaspersky (2017). Damage Control: The Cost of Security Breaches. IT Security Risks Special Report Series. [Online] Available at https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf (Accessed at 20-01-18)

[64] Nucleus Research (2007). SPAM, the Repeat Offender. [Online] Available at https://www.businesswire.com/news/home/20070402005669/en/Nucleus-Research-Spam-Costing-Businesses-712-Employee (Accessed at 14-02-18)

[65] Ponemon Institute (2017). Cost of Cybercrime Study. [Online] Available at https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017 (Accessed at 04-01-18)

[66] World Economic Forum (2015). Partnering for Cyber Resilience. Towards the Quantification of Cyber Threat. [Online] Available at http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf (Accessed on 15-04-18)