Πανεπιστήμιο Πειραιώς

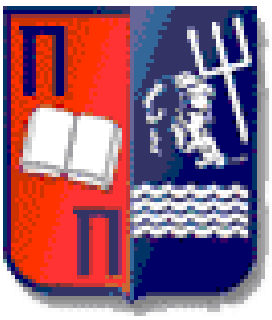
Τμήμα Πληροφορικής

Διδακτορική Διατριβή

Σωτήριος Γ. Πηρούνιας

«Ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας Πληροφοριακών Συστημάτων»

Πειραιάς, Αύγουστος 2012



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Συμβουλευτική επιτροπή

Επιβλέπων:

Ευάγγελος Φούντας
Καθηγητής Πανεπιστημίου
Πειραιώς

Μέλη:

Παναγιώτης-Γεώργιος Τσικούρας
Καθηγητής Πανεπιστημίου
Πειραιώς

Γρηγόριος Χονδροκούκης
Καθηγητής Πανεπιστημίου
Πειραιώς

Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

Διατριβή

Για την απόκτηση Διδακτορικού Διπλώματος
του τμήματος Πληροφορικής

Σωτήριου Γ. Πηρούνια

«*Ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας Πληροφοριακών Συστημάτων*»

Εξεταστική επιτροπή:

Ευάγγελος Φούντας
Καθηγητής Πανεπιστημίου
Πειραιώς

Παναγιώτης-Γεώργιος Τσικούρας
Καθηγητής Πανεπιστημίου
Πειραιώς

Γρηγόριος Χονδροκούκης
Καθηγητής Πανεπιστημίου
Πειραιώς

Γεώργιος Τσιχριντζής
Καθηγητής Πανεπιστημίου
Πειραιώς

Θεόδωρος Παπαηλίας
Καθηγητής Τ.Ε.Ι.
Πειραιώς

Ευάγγελος Σαμπράκος
Καθηγητής Πανεπιστημίου
Πειραιώς

Νικόλαος Μιχελακάκης
Επίκουρος Καθηγητής
Πανεπιστημίου Πειραιώς

«Τα κέρδη όλων των ανθρώπων αποτελούν καρπό του κινδύνου.»

Ηρόδοτος

Σωτήριος Γ. Πηρούνιας

Οικονομολόγος Πανεπιστημίου Πειραιώς, MBA University of Birmingham

Αφιέρωση

Αφιερώνω την παρούσα διατριβή στους γονείς μου που με βοήθησαν να γίνω πρωτίστως ένας καλός άνθρωπος και με καθοδήγησαν στις επιλογές που έκανα στην ζωή μου. Του ευχαριστώ που με παρότρυναν να ασχοληθώ με πράγματα που με ευχαριστούσαν και με βοήθησαν να σπουδάσω. Επίσης, αφιερώνω στην γυναίκα μου που έδειξε υπομονή και κατανόηση τα τελευταία χρόνια καθώς ήμουν αφοσιωμένος στην ερευνητική προσπάθεια. Στην διάρκεια αυτής της προσπάθειας ήρθε στον κόσμο η κόρη μου στην οποία αφιερώνω επίσης την παρούσα διατριβή. Υπόσχομαι σε όλους ότι θα χρησιμοποιήσω τις γνώσεις που απόκτησα ώστε να πετύχω πράγματα για τα οποία να είναι περήφανοι.

Ευχαριστίες

Θέλω να ευχαριστήσω αρχικώς το Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς που μου έδωσε την δυνατότητα να εκπονήσω την παρούσα διατριβή. Ευχαριστώ τον επιβλέποντα καθηγητή μου κ. Ευάγγελο Φούντα για την ερευνητική και ηθική καθοδήγηση που μου παρείχε όλα αυτά τα χρόνια καθώς χωρίς την βοήθεια του δεν θα ήταν δυνατόν να ολοκληρωθεί η παρούσα ερευνητική προσπάθεια. Θέλω επίσης να ευχαριστήσω τον καθηγητή κ. Παναγιώτη-Γεώργιο Τσικούρα για τις συμβουλές και τις γνώσεις που μου μετέδωσε καθώς και τον καθηγητή κ. Γρηγόριο Χονδροκούκη για την επιστημονική καθοδήγηση του και την συμπαράσταση που μου παρείχε.

Ευχαριστώ επίσης τους κ.κ. Γεώργιο Τσιχριντζή, Θεόδωρο Παπαηλία, Ευάγγελο Σαμπράκο και Νικόλαο Μιχελακάκη για την τιμή που μου έκαναν να είναι μέλη της Εξεταστικής Επιτροπής και για τις σημαντικές παρατηρήσεις και προεκτάσεις που έδωσαν στο σύνολο της διατριβής μου.

Θα ήθελα να ευχαριστήσω όλους τους συναδέλφους μου στο Πανεπιστήμιο που μου παρείχαν πολύτιμες συμβουλές όλα αυτά τα χρόνια. Ιδιαιτέρως ευχαριστώ θερμά τον Δρ Κωνσταντίνο Πατσάκη και τον υποψήφιο διδάκτορα Δημήτριο Μέρμηγκα για την ανεκτίμητη συνεργασία που είχαμε όλα αυτά τα χρόνια από την οποία προέκυψαν σημαντικά ερευνητικά αποκτήματα τα οποία ήταν απόρροια κυρίως άψογης ομαδικής προσπάθειας. Τους αισθάνομαι πρωτίστως ως δύο πολύ καλούς μου φίλους και δευτερευόντως ως συνεργάτες μου.

Δημοσιεύσεις

Σε αυτές τις δημοσιεύσεις, που παρουσιάζονται παρακάτω, περιλαμβάνονται εργασίες που έχουν δημοσιευτεί ή βρίσκονται υπό δημοσίευση σε διεθνή περιοδικά και διεθνή συνέδρια. Οι εργασίες αυτές σχετίζονται με την έρευνα που διεξήχθη στα πλαίσια της παρούσης διατριβής.

Σε διεθνή Περιοδικά:

- Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Gregory Chondrokoukis, «The role of weighted entropy in security quantification», International Journal of Information and Electronics Engineering (IJIEE, ISSN: 2010-3719), accepted for publication.

- Evangelos Fountas, Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, «Using time patterns to verify the utilization of stochastic calculus in security quantification», International Journal of Information and Electronics Engineering (IJIEE, ISSN: 2010-3719), accepted for publication.

- Sotirios Pirounias, Dimitrios Mermigas, Constantinos Patsakis, «The relation between information security events and firm market value, empirical evidence on recent disclosures», Information Systems Research Journal, under review.

- Dimitrios Mermigas, Constantinos Patsakis, Sotirios Pirounias, «Quantification of information systems security with stochastic calculus», ACM Transactions on Information and System Security, under review.

Σε Διεθνή Συνέδρια:

- Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, Evangelos Fountas, Constantinos Patsakis, «Towards a formalistic measuring of security using stochastic calculus», 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010), Chengdu, China, July 9-11 2010.

- Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Gregory Chondrokoukis, «The role of weighted entropy in security quantification», 2010 IEEE International Conference on Information Security and Artificial Intelligence (ISAI 2010), Chengdu, China, Dec. 17-19 2010.

- Evangelos Fountas, Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, «Using time patterns to verify the utilization of stochastic calculus in security quantification», 2010 IEEE International Conference on Information Security and Artificial Intelligence (ISAI 2010), Chengdu, China, Dec. 17-19 2010.

- Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Gregory Chondrokoukis, «The role of weighted entropy in security quantification», 2011 Global Congress on Science and Engineering (GCSE 2011), Dubai, Dec. 28-30 2011.

- Evangelos Fountas, Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, «Using time patterns to verify the utilization of stochastic calculus in security quantification», 2011 Global Congress on Science and Engineering (GCSE 2011), Dubai, Dec. 28-30 2011.

- D. Mermigas, S. Pirounias, N. Alexandris, "A probabilistic method for quantification of corporate losses due to security breaches", 2012 International Congress on Mathematics (MICOM), Sarajevo, Bosnia, Sep. 19-23 2012.

Περιεχόμενα

1 Εισαγωγή 1

1.1 Εισαγωγικές παρατηρήσεις 1

1.2 Περιγραφή του ερευνητικού πεδίου 7

1.3 Κίνητρα 8

1.4 Διατύπωση στόχων και συνεισφορά 9

1.5 Γενική επισκόπηση διατριβής 10

1.6 Διάρθρωση διατριβής 11

2 Βασικές έννοιες – Περιγραφή Ορολογίας 14

2.1 Εισαγωγή 14

2.2 Η έννοια του κινδύνου 15

2.2.1 Εννοιολογικές προσεγγίσεις και βασικά στοιχεία κινδύνου 15

2.2.2 Επιχειρησιακή θεώρηση κινδύνου 16

2.2.3 Περιστατικό κινδύνου 17

2.2.4 Εκτίμηση κινδύνων 18

2.3 Κατηγορίες κινδύνων 18

2.3.1 Λειτουργικοί κίνδυνοι 20

2.3.2 Νομικοί κίνδυνοι 24

2.3.3 Κίνδυνος φήμης 25

2.3.4 Κίνδυνος κανονιστικών πλαισίων 26

2.4 Κίνδυνοι Πληροφοριακών Συστημάτων 26

2.4.1 Βασικές έννοιες 26

2.4.2 Στοιχεία κινδύνων Πληροφοριακών Συστημάτων και προσδιορισμός 30

2.4.3 Τεχνικοί παράγοντες κινδύνου 34

2.4.4 Ταξινόμηση των οργανισμών υπό έκθεση σε κινδύνους Πληροφοριακών Συστημάτων 36

3 Διαχείριση κινδύνων Πληροφοριακών Συστημάτων 38

3.1 Εισαγωγή 38

3.2 Τα στάδια της διαδικασίας Διαχείρισης Κινδύνων Πληροφοριακών Συστημάτων . 40

3.2.1 Προσδιορισμός κινδύνων ΠΣ ... 42

3.2.2 Εκτίμηση κινδύνων ΠΣ ... 47

3.2.3 Αντιμετώπιση κινδύνων ΠΣ ... 52

3.2.4 Αξιολόγηση και αποτίμηση κινδύνων ΠΣ ... 56

3.3 Οι κίνδυνοι Πληροφοριακών Συστημάτων στα πλαίσια του συνόλου εταιρικών κινδύνων ... 57

4 Παραβίαση ασφαλείας και πηγές δεδομένων περιστατικών παραβίασης ασφαλείας ... 63

4.1 Εισαγωγή ... 63

4.2 Περιστατικά παραβίασης ασφάλειας ... 64

4.2.1 Εννοιολογική προσέγγιση ... 64

4.2.2 Κίνδυνοι Πληροφοριακών Συστημάτων και κίνδυνοι παραβιάσεων ασφαλείας ... 65

4.2.3 Κατηγορίες του κόστους παραβίασης ασφαλείας ... 66

4.2.4 Κατηγορίες περιστατικών παραβίασης ασφαλείας ... 69

4.2.5 Διαδικασία αντιμετώπισης περιστατικών παραβίασης ασφαλείας ... 73

4.3 Πηγές δεδομένων παραβιάσεων ασφαλείας ... 78

4.3.1 Γενικά περί των ερευνών μελετητικών οργανισμών για την ασφάλεια ... 80

4.3.2 Γενική περιγραφή των κυριότερων οργανισμών εκπόνησης ερευνών ... 84

4.3.3 Ανάλυση των μελετών ανά κατηγορία δεδομένων ... 86

4.3.4 Οργανισμοί καταγραφής και ανάλυσης περιστατικών ασφαλείας ... 99

5 Μέτρηση της οικονομικής επίπτωσης παραβιάσεων ασφάλειας μέσω της μεθοδολογίας ανάλυσης γεγονότων ... 102

5.1 Εισαγωγή ... 102

5.2 Μελέτες ανάλυσης γεγονότων σχετικών με Πληροφοριακά Συστήματα ... 103

5.3 Εμπειρική συνεισφορά της παρούσας έρευνας ... 113

5.4 Ανάλυση της μεθοδολογίας σε χρήση στην παρούσα μελέτη ... 115

5.4.1 Περιγραφή της μεθοδολογίας ανάλυσης γεγονότων ... 115

5.4.2 Προσδιορισμός παραθύρων περιόδου ανάλυση γεγονότων ... 117

5.4.3 Ανάλυση των μοντέλων αποτίμησης επενδυτικών κεφαλαίων 119
5.4.4 Μεθοδολογία στατιστικής ανάλυσης δεδομένων 126
5.5 Μεθοδολογία επιλογής δείγματος 128
5.6 Ανάπτυξη υποθέσεων προς ανάλυση 135
5.6.1 Υπόθεση στο συνολικό δείγμα 137
5.6.2 Υπόθεση σε επιμέρους δείγματα με βάση το είδος οργανισμού 138
5.6.3 Υπόθεση σε επιμέρους δείγματα με βάση το μέγεθος του περιστατικού 139
5.7 Ανάλυση αποτελεσμάτων 140
5.7.1 Ανάλυση συνολικού δείγματος 141
5.7.2 Ανάλυση με κριτήριο το είδος οργανισμού 146
5.7.3 Ανάλυση με κριτήριο το μέγεθος της παραβίασης ασφάλειας 149
5.8 Συμπεράσματα 153
6 Μέτρηση του επιπέδου ασφαλείας με την χρήση στοχαστικών μεθόδων 158
6.1 Εισαγωγή 158
6.2 Βάσεις καταχώρησης ευπαθειών και η χρήση τους στην μεθοδολογία 159
6.2.1 Βάσεις καταχώρησης ευπαθειών ανοικτού κώδικα 160
6.2.2 Η βάση ανοικτού κώδικα OSVDB 161
6.2.3 Η βάση ανοικτού κώδικα NVD 162
6.2.4 Χρήση βάσεων καταχώρησης ευπαθειών ανοικτού κώδικα 163
6.3 Τεχνικοί παράγοντες κινδύνου 164
6.3.1 Κατηγορίες μεθοδολογιών ποσοτικοποίησης της ασφάλειας 165
6.3.2 Τεχνικοί παράγοντες κινδύνου σε σχέση με το σύνολο κινδύνων ενός ΠΣ 166
6.4 Βασικό μοντέλο ποσοτικοποίησης της ασφάλειας με την χρήση στοχαστικών μεθόδων 168
6.4.1 Η χρήση στοχαστικών μεθόδων στην ασφάλεια ΠΣ 168
6.4.2 Βασικό μοντέλο ποσοτικοποίησης της ασφάλειας 170
6.5 Χρήση της σταθμισμένης εντοπίας στο υπολογισμό του συντελεστή βαρύτητας των παραγόντων κινδύνου 173
6.5.1 Εντροπία πληροφόρησης 173

6.5.2 Υπολογισμός πιθανότητας εμφάνισης ευπαθειών συγκεκριμένου επίπεδου επίπτωσης..... 174
6.5.3 Αρχικός υπολογισμός του συντελεστή βαρύτητας των παραγόντων κινδύνου..... 175
6.5.4 Εισαγωγή της παραμέτρου του χρόνου στους συντελεστές βαρύτητας..... 177
6.5.5 Υπολογισμός των συντελεστών βαρύτητας..... 180

6.6 Ανάπτυξη του μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας..... 183

6.6.1 Ενσωμάτωση του συντελεστή βαρύτητας στο μοντέλο..... 183
6.6.2 Ανάλυση των χρονικών μοτίβων των ευπαθειών..... 184
6.6.3 Τελικό μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας ενός συστήματος..... 196

6.7 Συμπεράσματα..... 198

7 Ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας..... 200

7.1 Εισαγωγή..... 200

7.2 Τα στοιχεία που συνθέτουν τους κινδύνους παραβιάσεων ασφαλείας..... 201

7.2.1 Ανάλυση της πιθανότητας επίπτωσης..... 203
7.2.2 Ανάλυση της επίπτωσης..... 204

7.3 Υπολογισμός της πιθανότητας πραγμάτωσης παραβιάσεων ασφάλειας..... 206

7.4 Υπολογισμός της επίπτωσης παραβιάσεων ασφάλειας..... 209

7.4.1 Ανάλυση αριθμού εγγραφών σε έκθεση..... 209
7.4.2 Ανάλυση κόστους ανά περιστατικό παραβίασης ασφαλείας..... 210

7.5 Μοντέλο ποσοτικοποίησης των κινδύνων παραβιάσεων ασφάλειας..... 215

7.6 Η μεθοδολογία Value at Risk και η εφαρμογή της στους κινδύνους παραβιάσεων ασφάλειας..... 219

7.6.1 Εισαγωγικά..... 219
7.6.2 Η μεθοδολογία Value at Risk..... 220
7.6.3 Εφαρμογή της μεθοδολογίας Value at Risk στους κινδύνους παραβιάσεων ασφαλείας..... 222

7.7 Συμπεράσματα..... 226

8 Σύνοψη διατριβής..... 228

8.1 Συμπεράσματα..... 228

8.1.1 Προσδιορισμός των επιπτώσεων παραβιάσεων ασφαλείας..... 229
8.1.2 Προσδιορισμός του επιπέδου ασφαλείας Πληροφοριακών Συστημάτων..... 233

8.1.3 Προσδιορισμός των κινδύνων παραβιάσεων ασφαλείας 234

8.2 Προτεινόμενα πεδία περεταίρω έρευνας 236

8.3 Επίλογος 238

I Λεξιλόγιο όρων 240

II Δείγμα γεγονότων παραβίασης ασφαλείας 245

III Παραδείγματα δημοσίευσης γεγονότων παραβίασης ασφαλείας 253

IV Πρόγραμμα υπολογισμών διαδικασιών ανάλυσης γεγονότων 256

V Αποτελέσματα ανάλυσης του μεγέθους γεγονότος με την χρήση του CAPM 274

VI Βιβλιογραφία 275

ΔΙΑΓΡΑΜΜΑΤΑ

Διάγραμμα 1: Ανάλυση κόστους ανά περιστατικό σε άμεσο και έμμεσο από Ponemon 90

Διάγραμμα 2: Προσέγγιση συνολικού κόστους ανά περιστατικό από Ponemon & FBI/CSI 91

Διάγραμμα 3: Επιμερισμός περιστατικών παραβίασης ασφαλείας ανά κατηγορία από Ponemon 94

Διάγραμμα 4: Κατανομή ευπαθειών των Windows XP ανά ημέρα της εβδομάδας με την χρήση της OSVDB 185

Διάγραμμα 5: Κατανομή ευπαθειών των Windows XP ανά ημέρα της εβδομάδας με την χρήση της OSVDB 186

Διάγραμμα 6: Κατανομή ευπαθειών των Windows 2000 ανά ημέρα της εβδομάδας με την χρήση της OSVDB 186

Διάγραμμα 7: Κατανομή ευπαθειών των Windows 2000 ανά ημέρα της εβδομάδας με την χρήση της NVD 187

Διάγραμμα 8: Κατανομή ευπαθειών των Windows Vista ανά ημέρα της εβδομάδας με την χρήση της OSVDB 188

Διάγραμμα 9: Κατανομή ευπαθειών των Windows Vista ανά ημέρα της εβδομάδας με την χρήση της NVD 189

Διάγραμμα 10: Κατανομή ευπαθειών ανά ημέρα της εβδομάδας στο σύνολο των προϊόντων της Microsoft με την χρήση της OSVDB 190

Διάγραμμα 11: Κατανομή ευπαθειών ανά ημέρα της εβδομάδας στο σύνολο των προϊόντων της Microsoft με την χρήση της NVD 190

Διάγραμμα 12: Κατανομή ευπαθειών της Oracle Database 10g ανά ημέρα της εβδομάδας με την χρήση της OSVDB 192

Διάγραμμα 13: Κατανομή ευπαθειών των Windows XP ανά ημέρα του μήνα με την χρήση της OSVDB 193

Διάγραμμα 14: Κατανομή ευπαθειών των Windows XP ανά ημέρα του μήνα με την χρήση της NVD 193

Διάγραμμα 15: Κατανομή ευπαθειών των Windows 2000 ανά ημέρα του μήνα με την χρήση της OSVDB 194

Διάγραμμα 16: Κατανομή ευπαθειών του Office XP ανά ημέρα του μήνα με την χρήση της OSVDB 195

Διάγραμμα 17: Κατανομή ευπαθειών ανά ημέρα του μήνα στο σύνολο των προϊόντων της Microsoft με την χρήση της OSVDB 195

Διάγραμμα 18: Κατανομή ευπαθειών ανά ημέρα του μήνα στο σύνολο των προϊόντων της Microsoft με την χρήση της NVD 196

ΕΙΚΟΝΕΣ

Εικόνα 1: Το σύνολο των εταιρικών κινδύνων 20

Εικόνα 2: Ανάλυση λειτουργικών κινδύνων 23

Εικόνα 3: Κίνδυνοι Πληροφοριακών Συστημάτων 30

Εικόνα 4: Στοιχεία ενεργητικού Πληροφοριακών Συστημάτων 34

Εικόνα 5: Στάδιο προσδιορισμού κινδύνων Πληροφοριακών Συστημάτων 43

Εικόνα 6: Πλαίσια ορισμού περιβάλλοντος Πληροφοριακών Συστημάτων 46

Εικόνα 7: Στάδιο εκτίμησης κινδύνων Πληροφοριακών Συστημάτων 48

Εικόνα 8: Μέθοδοι εκτίμησης κινδύνων 50

Εικόνα 9: Στάδιο αντιμετώπισης κινδύνων Πληροφοριακών Συστημάτων 54

Εικόνα 10: Κόστος κινδύνων παραβιάσεων ασφαλείας 67

Εικόνα 11: Κατηγορίες παραβιάσεων ασφαλείας με βάση τον τύπο παραβίασης 70

Εικόνα 12: Κατηγορίες παραβιάσεων ασφαλείας με βάση την αιτία πρόκλησης 73

Εικόνα 13: Διαδικασία αντιμετώπισης παραβιάσεων ασφαλείας 76

Εικόνα 14: Διαχωρισμός των πηγών δεδομένων παραβιάσεων ασφαλείας 79

Εικόνα 15: Στοιχεία κινδύνων πληροφοριακών συστημάτων 202

Εικόνα 16: Κίνδυνοι παραβιάσεων ασφαλείας 203

ΠΙΝΑΚΕΣ

Πίνακας 1: Συντομογραφίες xv

Πίνακας 2: Κόστος παραβιάσεων ασφαλείας από την Ponemon Institute 89

Πίνακας 3: Κόστος παραβιάσεων ασφαλείας από το CSI/FBI 89

Πίνακας 4: Επιμερισμός περιστατικών παραβίασης ασφαλείας ανά κατηγορία από Ponemon 94

Πίνακας 5: Τρόπος επίθεσης σε σχέση με τον αριθμό των επιθέσεων σύμφωνα με την Verizon 95

Πίνακας 6: Τρόπος επίθεσης σε σχέση με τον αριθμό των προσβεβλημένων εγγραφών σύμφωνα με την Verizon 96

Πίνακας 7: Κατανομή του αριθμού περιστατικών σύμφωνα με την πηγή απειλής με στοιχεία της Verizon 97

Πίνακας 8: Κατανομή του αριθμού των προσβεβλημένων εγγραφών ανά πηγή απειλής με στοιχεία της Verizon 98

Πίνακας 9: Βασικά χαρακτηριστικά μελετών της επίδρασης στην μετοχή από ανακοινώσεις παραβιάσεων ασφαλείας 105

Πίνακας 10: Εφαρμογή κριτηρίων επιλογής δείγματος 133

Πίνακας 11: Βασικά χαρακτηριστικά εταιριών δείγματος 135

Πίνακας 12: Γεγονότα ανά κατηγορία παραβίασης ασφαλείας 135

Πίνακας 13: Στατιστική μεθοδολογία μελετών ανάλυσης γεγονότων 136

Πίνακας 14: Ανάλυση αριθμού επιρρεασμένων εγγραφών - περιστατικών 140

Πίνακας 15: CAPM - Ανάλυση συνολικού δείγματος 141

Πίνακας 16: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος 143

Πίνακας 17: CAPM - Ανάλυση τομέα εταιριών τεχνολογίας 147

Πίνακας 18: CAPM - Ανάλυση εταιριών εκτός τομέα τεχνολογίας 147

Πίνακας 19: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση τομέα εταιριών τεχνολογίας 147

Πίνακας 20: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση εταιριών εκτός τομέα τεχνολογίας 148

Πίνακας 21: Εκτιμήσεις οικονομικής απώλειας για παράθυρα ανάλυσης με στατιστική σημαντικότητα 149

Πίνακας 22: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος περιστατικών προσβολής μέχρι 100.000 εγγραφών 151

Πίνακας 23: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος περιστατικών προσβολής 100.000 - 1.000.000 εγγραφών 151

Πίνακας 24: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος περιστατικών προσβολής άνω των 1.000.000 εγγραφών 151

Πίνακας 25: Υπολογισμός των συντελεστών βαρύτητας προϊόντων της Microsoft με δεδομένα ευπαθειών από την OSVDB 182

Πίνακας 26: Υπολογισμός των συντελεστών βαρύτητας προϊόντων της Microsoft με δεδομένα ευπαθειών από την NVD 182

Πίνακας 27: Βασικά χαρακτηριστικά γεγονότων παραβιάσεων ασφαλείας 245

Πίνακας 28: CAPM - Ανάλυση συνολικού δείγματος περιστατικών προσβολής μέχρι 100.000 εγγραφών 274

Πίνακας 29: CAPM - Ανάλυση συνολικού δείγματος περιστατικών προσβολής 100.000 - 1.000.000 εγγραφών 274

Πίνακας 30: CAPM - Ανάλυση συνολικού δείγματος περιστατικών προσβολής άνω των 1.000.000 εγγραφών 274

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Στον παρακάτω Πίνακα παραθέτονται οι συντομογραφίες που χρησιμοποιήθηκαν στην παρούσα διατριβή. Μέρος των συντομογραφιών είναι στην Ελληνική και μέρος στην Αγγλική γλώσσα.

ΣΥΝΤΟΜΟΓΡΑΦΙΑ	ΕΠΕΞΗΓΗΣΗ
APT	Advanced Persistent Threat
CAPM	Capital Asset Pricing Model
Cobit	Control objectives for information and related technology
CRSP	Center for Research in Security Prices
CSI	Computer Security Institute
CVE	Common Vulnerabilities Exposures
dDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSF	Open Security Foundation
OSVDB	Open Source Vulnerability Database
RAT	Remote Administration Tools
SDLC	System Development Life Cycle
ΑΠ	Ασφάλεια Πληροφόρησης
ΔΚΠΣ	Διαχείριση Κινδύνων Πληροφοριακών Συστημάτων
ΕΔΚ	Εταιρική Διαχείριση Κινδύνων
ΠΣ	Πληροφοριακό Σύστημα
ΣΤΠ	Σύστημα Τεχνολογίας Πληροφόρησης
ΤΠ	Τεχνολογία Πληροφόρησης

Πίνακας 1: Συντομογραφίες

ΠΕΡΙΛΗΨΗ

Η παρούσα διδακτορική διατριβή αφορά την ανάλυση των κινδύνων που προέρχονται από παραβιάσεις ασφαλείας Πληροφοριακών Συστημάτων. Δημιουργήθηκε ένα μεθοδολογικό πλαίσιο απόδοσης ποσοτικών και αντικειμενικών αποτελεσμάτων με κύριο στόχο την δυνατότητα χρήσης του από το σύνολο της διοικητικής δομής ενός οργανισμού για την λήψη αποφάσεων. Προτάθηκε ένα θεωρητικό πλαίσιο για τις παραβιάσεις ασφαλείας με βάση την συσχέτιση τους με το σύνολο των εταιρικών κινδύνων. Το επίπεδο των επιπτώσεων που επιφέρουν οι παραβιάσεις ασφαλείας προσεγγίστηκε αναλύοντας συνδυαστικά μελέτες επαγγελματικών οργανισμών, της ακαδημαϊκής κοινότητας και τα αποτελέσματα εμπειρική μελέτης, που πραγματοποιήθηκε στα πλαίσια της παρούσας. Οι επιπτώσεις εκτιμήθηκαν σε επίπεδο περιστατικού και σε επίπεδο εκτιθέμενης εγγραφής πληροφόρησης αναφορικά με το άμεσο και έμμεσο κόστος. Η μοντελοποίηση της πιθανότητας παραβιάσεων ασφαλείας βασίστηκε σε δύο ερευνητικές περιοχές: Την ποσοτικοποίηση του επιπέδου ασφαλείας το οποίο επιτεύχθηκε με αντικειμενικότητα κάνοντας χρήση στοχαστικών μεθόδων και την κατάλληλη εφαρμογή του μεθοδολογικού πλαισίου που προέρχεται από το μοντέλο των Gordon-Loeb. Ο συνδυασμός των παραπάνω ερευνητικών αποτελεσμάτων οδήγησε στην σύνθεση ενός μοντέλου μέσω του οποίου μπορεί να εκτιμηθεί το επίπεδο των κινδύνων παραβιάσεων ασφαλείας για έναν οργανισμό εκφρασμένο σε νομισματικούς όρους. Τέλος, ερευνήθηκε ο τρόπος εφαρμογής της μεθοδολογίας VaR στους κινδύνους παραβιάσεων ασφαλείας με βάση το προτεινόμενο μοντέλο.

ABSTRACT

This thesis deals with the analysis of risks emanating from security breaches of Information Systems. It proposes a new quantitative methodology that, returns objective security level measurement of an IS, which can be implemented by all management members of an organization. A new theoretical frame for handling security breaches was suggested, based on their correlation to the total amount of enterprise risks. The impact level, caused by security breaches, was studied by the combined analysis of studies stemming from professional organizations, the academic community and by the empirical study that was accomplished during this thesis. The impact was assessed at incident level as well as the affected records of data, with respect to direct and indirect costs. The modeling of security breaches probability was based on two research areas: The quantification of security level that was accomplished with objectivity utilizing stochastic methods and the proper application of the methodological frame that accrues from the Gordon-Loeb model. The combination of the aforementioned research results, led to the synthesis of a model from which the level of security breaches risks of an organization can by assessed in monetary terms. At the end, the application of the VaR methodology to the security breaches risks was researched based on the proposed model.

1 Εισαγωγή

1.1 Εισαγωγικές παρατηρήσεις

Η εξάρτηση της σημερινής εποχής στην Τεχνολογία Πληροφόρησης (ΤΠ) απεικονίζεται από την προοδευτικά αυξανόμενη χρήσης της σε κάθε πτυχή δραστηριότητας που χαρακτηρίζει την καθημερινότητα της σύγχρονης κοινωνίας. Κάθε στιγμή, εκατομμύρια Πληροφοριακά Συστήματα (ΠΣ) λειτουργούν συνδεδεμένα σε δημόσιους και ιδιωτικούς τομείς (domains) και παράγουν την καθημερινή ψηφιακή πραγματικότητα στην οποία είναι συνηθισμένες οι σύγχρονες κοινωνίες. Ο αριθμός των διαδικτυακών διακομιστών αυξήθηκε από τα 26 εκατομ. περίπου το 2001 σε παραπάνω από 512 εκατομ. μία δεκαετία αργότερα. Την στιγμή συγγραφής του παρόντος, ο αριθμός των διαδικτυακών διακομιστών ανέρχεται σε περίπου 640 εκατομ. καταγράφοντας μία συνολική αύξηση, σε σχέση με το 2001, κατά 2300% [**1**]. Στο τέλος του 2010 ο αριθμός των χρηστών του διαδικτύου παγκοσμίως ανερχόταν σε περίπου 2 δις, με τον αριθμό των λογαριασμών ηλεκτρονικού ταχυδρομείου να προσεγγίζει τα 3 δις και το αριθμό των ηλεκτρονικών μηνυμάτων ημερησίως να αγγίζει τα 294 εκατομ [**2**]. Ο εξαιρετικά μεγάλος ρυθμός αύξησης των διακομιστών και της χρήσης του διαδικτύου σε παγκόσμιο επίπεδο αποτυπώνει ξεκάθαρα την εκθετικά αυξανόμενη εξάρτηση της σύγχρονου τρόπου ζωής στην συνεχή και ικανοποιητική λειτουργία των ΠΣ.

Ωστόσο, η ένταξη των ΠΣ, στο σύνολο σχεδόν των βασικών διαστάσεων που απαρτίζουν την εύρυθμη λειτουργία των σύγχρονων κοινωνιών, δεν έχει πραγματοποιηθεί χωρίς κόστος. Τα πλεονεκτήματα της χρήσης εξελιγμένων ΠΣ είναι αλληλένδετα με τον κίνδυνο που απορρέει από την εξάρτηση της σύγχρονης πραγματικότητας στην μοντέρνα τεχνολογία η οποία είναι υπεύθυνη για την διαχείριση της ευαίσθητης πληροφόρησης από την οποία εξαρτώνται οι οικονομίες παγκοσμίως.

Συνεπώς, το κόστος που πηγάζει από την εξάρτηση στην μοντέρνα τεχνολογία προέρχεται από τους κινδύνους που δημιουργούνται. Οι κίνδυνοι αυτοί, καθώς η χρήση των ΠΣ εξαπλώνεται σε κάθε πτυχή δραστηριότητας των σύγχρονων οργανισμών, γίνονται σταδιακά περισσότερο πολύπλοκοι στον ακριβή προσδιορισμό τους και στην εκτίμηση της πλήρης διάστασης των επιπτώσεων που δύναται να επιφέρουν σε έναν οργανισμό. Πλέον, οι κίνδυνοι ΠΣ δεν αποτελούν

μία απομονωμένη διάσταση στον συνολικό γαλαξία κινδύνων ενός οργανισμού. Αντιθέτως, η πολύπλευρη και σχεδόν καθολική χρήση των ΠΣ, έχει δημιουργήσει μεγάλες αλληλοσυσχετίσεις μεταξύ των κινδύνων ΠΣ και άλλων κινδύνων που αντιμετωπίζουν το σύνολο των σύγχρονων οργανισμών.

Επομένως, η εξέταση των κινδύνων ΠΣ στην πλήρη τους διάσταση απαιτεί την ένταξη τους στο σύνολο του οργανισμού και την ανάλυση των συσχετίσεων που έχουν με τους υπόλοιπους κινδύνους που αντιμετωπίζει. Μόνο κατά αυτό τον τρόπο μπορεί να υπολογιστεί με ακρίβεια η δυναμική των κινδύνων αυτών και συνεπώς το επίπεδο των επιπτώσεων που μπορούν να επιφέρουν σε έναν οργανισμό. Η αντικειμενική θεώρηση του μεγέθους των κινδύνων ΠΣ είναι απαραίτητη για έναν οργανισμό προκειμένου να είναι σε θέση να αποφασίσει με ακρίβεια το ύψος των επενδύσεων που θα διαθέσει για την ασφάλεια.

Σήμερα, οργανισμοί και κυβερνήσεις παγκοσμίως δαπανούν ετησίως περισσότερα από $1 τρις σε επενδύσεις ΤΠ. Καθίσταται φανερό, πως ακόμα και ένα σχετικά μικρό ποσοστό αποτυχίας των ΤΠ σε θέματα λειτουργικότητας και ασφάλειας, ισοδυναμεί με τεράστιες απώλειες για τους μετόχους και τους φορολογούμενους. Δυστυχώς, το προαναφερόμενο επίπεδο αποτυχίας δεν έχει περιοριστεί κατά την διάρκεια της τελευταίας δεκαετίας. Ερευνητές, βασιζόμενοι σε πρόσφατα στοιχεία, εκτιμούν ότι μόνο στις ΗΠΑ η μέση ετήσια απώλεια από την αποτυχία της ΤΠ ανέρχεται σε $15 δις. Αν προστεθούν οι επιπλέον απώλειες που προέρχονται από νομικές διενέξεις, την μείωση χρηματοροών και τις προϋπολογιστικές και χρονικές υπερβάσεις, που είναι δύσκολο να υπολογιστούν με ακρίβεια στο σύνολο τους, το προαναφερόμενο μέγεθος εκτιμάται ότι ανέρχεται μεταξύ $60 δις – $70 δις [**3**]. Στο Ηνωμένο Βασίλειο το ετήσιο συνολικό κόστος, προερχόμενο από το ηλεκτρονικό έγκλημα, υπολογίζεται σε $43 δις. Το μεγαλύτερο ποσοστό του κόστους προέρχεται από την προσβολή ευαίσθητων δεδομένων [**4**].

Η αυξανόμενη εξάρτηση των οργανισμών στην σύγχρονη τεχνολογία και στους κινδύνους ΠΣ αποτυπώνεται στην έρευνα των Gerencser και Aguirre πάνω στην ασφάλεια [**5**]. Σύμφωνα με αυτήν την έρευνα ήδη το 2002 περισσότεροι από τους μισούς οργανισμούς, της μεγάλης κεφαλαιοποίησης, είχαν ήδη προσλάβει γενικό διευθυντή ασφαλείας (chief security officer – CSO) για ένα διάστημα δύο ετών. Στην ίδια μελέτη η πλειοψηφία των οργανισμών θεωρούσε την ασφάλεια ως «προτεραιότητα υψίστης σημασίας για την ανώτερη διοίκηση». Πρόσφατες μελέτες επιβεβαιώνουν αυτή την τάση με τους οργανισμούς πλέον, ανεξαρτήτου μεγέθους και

δραστηριότητας, να θεωρούν την ασφάλεια ένα από τα σοβαρότερα θέματα και πηγή προέλευσης σοβαρών κινδύνων [**6**], [**7**].

Στις δύο πρόσφατες έρευνες που υλοποίησε η PriceWaterHouseCoopers με την InfoSecurity Europe πάνω στην ασφάλεια ΠΣ, προκύπτει ότι περίπου το 70% των μεγάλων και περίπου το 80% των μικρών οργανισμών, θεωρεί την ασφάλεια προτεραιότητα υψηλής ή πολύ υψηλής σημασίας [**7**], [**8**]. Είναι χαρακτηριστικό ότι η ασφάλεια δεν αποτελεί πλέον σημαντική παράμετρο για την εύρυθμη λειτουργία μόνο των μεγάλων οργανισμών. Η μικροί οργανισμοί τα τελευταία χρόνια, προκειμένου να παραμείνουν ανταγωνιστικοί, έχουν επενδύσει στην ΤΠ μεγάλα κεφάλαια σε σχέση με το μέγεθος τους. Το γεγονός αυτό έχει οδηγήσει την εξάρτηση των οργανισμών στην σύγχρονη τεχνολογία να μην είναι πλέον αναλογική με το μέγεθος τους. Επιπλέον, οι πηγές κινδύνων, με κυριότερη τους επίδοξους εισβολείς από το εξωτερικό περιβάλλον ενός οργανισμού, δεν κάνουν πλέον στον ίδιο βαθμό διακρίσεις σύμφωνα με το μέγεθος ή το εύρος δημοσιότητας ενός οργανισμού. Κάθε επιχείρηση είναι, στην σύγχρονη εποχή που διαμορφώνεται, εν δυνάμει θύμα των επιπτώσεων από την πραγμάτωση κινδύνων ΠΣ.

Τις δύο τελευταίες δεκαετίες οι προτεραιότητες σχετικά με την ασφάλεια, για τις διοικήσεις των οργανισμών παγκοσμίως, ουσιαστικά αντιστράφηκαν. Στην μελέτη που διεξήχθη από τους Loch et. al. το 1992 [**9**], η πλειοψηφία των διαχειριστών ΠΣ δήλωνε πως οι κίνδυνοι ΠΣ που θεωρούν ότι χρειάζεται μεγαλύτερη προσοχή και προτεραιότητα είναι οι κίνδυνοι που προέρχονται από φυσικές καταστροφές. Στη σημερινή εποχή οι κίνδυνοι φυσικών καταστροφών σαφώς παραμένουν ανάμεσα στους κινδύνους που αντιμετωπίζει ένας οργανισμός αλλά βαθμιαία, ειδικά μέσα στην τελευταία δεκαετία, υποσκελίστηκαν από άλλους κινδύνους όπως είναι οι παραβιάσεις ασφαλείας. Σύμφωνα με την τελευταία μελέτη από το Computer Security Institute (CSI) ο προϋπολογισμός που διαθέτουν οι οργανισμοί στις υποδομές ασφαλείας υπολογιστικών συστημάτων σε πολλές περιπτώσεις ξεπερνάει το 10% επί του συνολικού προϋπολογισμού επενδύσεων σε ΠΣ [**10**]. Τα ποσά που επενδύουν πλέον οι οργανισμοί στην ασφάλεια έχουν έντονα αυξητική τάση το οποίο υποδηλώνει την προτεραιότητα που έχει λάβει το θέμα της ασφάλειας σε οργανισμούς από κάθε τομέα δραστηριότητας.

Η συχνότητα των περιστατικών ασφαλείας βαθμιαία αυξάνεται σύμφωνα με πρόσφατες έρευνες. Παρατηρείται μία τάση αύξησης ταυτόχρονα των οργανισμών που γίνονται στόχος καθώς και του αριθμού των περιστατικών ανά οργανισμό. Μέσα στα τελευταία τρία χρόνια, ο

μέσος αριθμός περιστατικών τριπλασιάστηκε. Η συντριπτική πλειοψηφία των εταιριών παγκοσμίως, ανεξαρτήτου μεγέθους, διέγνωσε ότι εκτέθηκε τουλάχιστον μία φορά από κάποιο περιστατικό ασφαλείας [**7**], [**11**].

Η πρώτη σημαντική καταγραφή περιστατικού ηλεκτρονικού εγκλήματος πραγματοποιήθηκε το έτος 2000 όταν ένας μοναδικός ιός μόλυνε περίπου 45 εκατομ. χρήστες παγκοσμίως. Κατά την διάρκεια της προηγούμενης δεκαετίας το έγκλημα στον κυβερνοχώρο εξελίχθηκε και ωρίμασε με γοργούς ρυθμούς. Τα τελευταία χρόνια τα σοβαρά περιστατικά παραβιάσεων ασφαλείας δεν προέρχονται πλέον από ιούς υπολογιστών μαζικής αποστολής αλλά από οργανωμένες επιθέσεις μεθοδευμένες προς συγκεκριμένους στόχους με τη χρήση εξαιρετικά εξελιγμένων εργαλείων. Η πρώτη στοχευόμενη, μαζικής κλίμακας επίθεση, διαδραματίστηκε το 2007 όταν η Εσθονία έγινε στόχος κυβερνοεπίθεσης τύπου DoS. Στην διάρκεια της επίθεσης αυτής προσβλήθηκαν στόχοι κυβερνητικών υπηρεσιών, οργανισμοί του χρηματοπιστωτικού τομέα καθώς και μέσα μαζικής επικοινωνίας [**12**]. Είναι χαρακτηριστικό ότι η επίθεση αυτή αποκαλέστηκε «Πρώτος Διαδικτυακός Πόλεμος» (Web War I) το οποίο αποτυπώνει απόλυτα την βαρύτητα του γεγονότος και υποδεικνύει την βαθμιαία αλλαγή των σύγχρονων κοινωνιών και των προβλημάτων που έχουν να αντιμετωπίσουν όπου ένα από τα πλέον σημαντικά είναι το ηλεκτρονικό έγκλημα.

Από τον Νοέμβριο του 2009 μέχρι σήμερα, έχουν διαδραματιστεί παγκοσμίως πληθώρα σοβαρών περιστατικών ασφαλείας εναντίων μεγάλων ενεργειακών, πετρελαϊκών, πετροχημικών, κατασκευής αμυντικών συστημάτων, ηλεκτρονικών και χρηματοπιστωτικών οργανισμών. Οι επιθέσεις αυτές χαρακτηρίζονται από την χρήση εξελιγμένων και πολύπλοκων εργαλείων, τον ακριβή συντονισμό τους και την μαζική προσβολή μεγάλων οργανισμών σε παγκόσμια κλίμακα και γενικά ονομάστηκαν ως «εξελιγμένες επίμονες απειλές» (Advanced Persistent Threats - APT). Οι παρατηρήσεις αυτές μας οδηγούν στην διαπίστωση ότι, κατά την διάρκεια των τριών τελευταίων ετών, το θέμα της ασφάλειας και οι κίνδυνοι ΠΣ έχουν εισέλθει σε μία νέα εποχή. Στην νέα εποχή, οι κύριοι στόχοι δεν περιορίζονται πλέον σε κυβερνητικούς, στρατιωτικούς και κατασκευής οπλικών συστημάτων οργανισμούς αλλά σε στόχους κάθε κατηγορίας. Ενδεικτικό της βαρύτητας που έχουν πλέον οι στοχευόμενες επιθέσεις είναι το πρόσφατο αποτέλεσμα της έρευνας από την Verizon από την οποία προέκυψε πως, παρόλο που οι επιθέσεις αυτού του τύπου καταλαμβάνουν μόνο το 16% επί του συνόλου των περιστατικών ασφαλείας, προκαλούν το 63% των απωλειών σε ευαίσθητα δεδομένα [**13**].

Οι αντίπαλοι των υπεύθυνων ασφαλείας έχουν αναπτύξει πολύπλοκα συστήματα κατασκευής κακόβουλου λογισμικού που τους δίνουν την δυνατότητα κατασκευής, σε μαζική κλίμακα, αποτελεσματικών κακόβουλων εργαλείων. Επίσης, κατά την διάρκεια την περασμένης δεκαετίας η κοινότητα των hackers ωρίμασε σε μεγάλο βαθμό και απόδειξη σε αυτό είναι τα άνευ προηγουμένου, σε κλίμακα και σοβαρότητα, μαζικά περιστατικά παραβίασης ασφαλείας που καταγράφτηκαν. Πλέον γίνεται ολοένα και περισσότερο κατανοητό ότι τα προϊόντα λογισμικού μπορούν να είναι ευπαθή όχι αποκλειστικά λόγω αστοχιών στον σχεδιασμό και την εφαρμογή τους αλλά και λόγω της αύξησης των ικανοτήτων καθώς και της πολυπλοκότητας και αποτελεσματικότητας των εργαλείων που χρησιμοποιούν οι επιτιθέμενοι προς τα ΠΣ.

Χαρακτηριστική ένδειξη της νέα εποχής, στην οποία έχουν εισέλθει οι σύγχρονες κοινωνίες, είναι ο αριθμός των περιστατικών παραβίασης ασφαλείας, από hackers με έδρα την Κίνα, ο οποίος κατά την τελευταία δεκαετία έχει αγγίξει τις 760. Το νούμερο αυτό οδηγεί στο συμπέρασμα ότι αυτή η νέα εποχή χαρακτηρίζεται από έναν νέο τύπο Ψυχρού Πολέμου [**14**].

Τα εργαλεία και οι τεχνικές που χρησιμοποιήθηκαν σε αυτά τα περιστατικά, όπως εξελίχθηκαν τα τελευταία τρία χρόνια, επονομάστηκαν από την McAfee ως "Night Dragon" [**15**]. Οι βασικοί στόχοι αυτών των επιθέσεων είναι η πρόσβαση και εκμετάλλευση ευαίσθητων πληροφοριών προκειμένου για κατασκοπεία στον κυβερνοχώρο (cyber-espionage), οικονομικά οφέλη, πολιτικά οφέλη και λιγότερο πλέον για την προσωπική προβολή των εισβολέων.

Διάφοροι οργανισμοί όπως η McAfee και η Information Warfare Monitor ερεύνησαν, διαχώρισαν και επονόμασαν τις ακόλουθες σειρές συντονισμένων περιστατικών ασφαλείας:

(α) "Επιχείρηση Ghostnet" η οποία ανακαλύφθηκε τον Μάρτιο του 2009 και αφορούσε μεγάλης κλίμακας επιθέσεις τύπου APT σε πολιτικούς κυρίως στόχους παγκοσμίως. Οι επιθέσεις κατά κύριο λόγο προέρχονταν από την Κίνα και υπολογίζεται ότι προσβλήθηκαν 1.295 υπολογιστές σε 103 χώρες [**16**]. Μετά από εκτενείς έρευνες που διεξήχθησαν τα συμπεράσματα ήταν ανάμεικτα σχετικά με τον ενορχηστρωτή των συγκεκριμένων επιθέσεων. Ερευνητές από το University of Cambridge ανέφεραν πως είχαν βάσιμες υποψίες ότι η Κινεζική Κυβέρνηση υποκίνησε τουλάχιστον το μέρος που αφορούσε τους πολιτικούς στόχους στο Θιβέτ [**17**].

(β) "Επιχείρηση Night Dragon" η οποία ξεκίνησε τον Νοέμβριο του 2009 και κατά κύριο λόγο είχε ως στόχο πετρελαϊκούς, πετροχημικούς και ενεργειακούς οργανισμούς [**15**]. Οι επιθέσεις

κατά κύριο λόγο προέρχονταν από την Κίνα και χρησιμοποιήθηκε πλήθος εξελιγμένων εργαλείων εισβολής όπως είναι τα εργαλεία απομακρυσμένης διαχείρισης (Remote Administration Tools – RAT). Θεωρείται η πρώτη περίπτωση ομαδικών διαδικτυακών επιθέσεων όπου οι στόχοι δεν περιορίστηκαν σε κυβερνητικούς και αμυντικούς οργανισμούς αλλά επεκτάθηκαν σε διεθνής επιχειρηματικούς και εμπορικούς στόχους και κατά κύριο λόγο στον ενεργειακό τομέα.

(γ) "Επιχείρηση Aurora" η οποία ήρθε στην δημοσιότητα τον Ιανουάριο του 2010 και υπολογίζεται ότι περισσότερες από 200 μεγάλες εταιρίες προσβλήθηκαν. Η πρώτη εταιρία που ανακάλυψε αυτές τις επιθέσεις ήταν η Google [**18**]. Οι επιθέσεις χαρακτηρίστηκαν ως κατασκοπευτικές και η προέλευση τους θεωρήθηκε πως ήταν η Κίνα με την κυβέρνηση της τελευταίας όμως να δηλώνει πως όλη η επιχείρηση ήταν συνομωσία προερχόμενη από τις ΗΠΑ [**19**]. Οι επιθέσεις ήταν τύπου APT και στόχος ήταν πρόσβαση και αλλοίωση πηγαίου κώδικα σε οργανισμούς υψηλής τεχνολογίας, ασφαλείας και κατασκευής αμυντικών εξοπλισμών.

(δ) "Επιχείρηση Shady Rat" η οποία ήρθε στην δημοσιότητα τον Αύγουστο του 2011 και περιελάμβανε περιστατικά ασφαλείας που προκλήθηκαν σε περισσότερους από 70 οργανισμούς σε 14 κράτη παγκοσμίως [**20**].

Τα παραπάνω πρωτόγνωρα περιστατικά αποτυπώνουν την νέα τάξη πραγμάτων που δημιουργείται πλέον τα τελευταία χρόνια. Οι επιθέσεις τύπου Night Dragon και Aurora άλλαξαν τον τύπο των επιθέσεων στους οποίους ήταν συνηθισμένη η παγκόσμια κοινότητα και επιπλέον προστέθηκαν και άλλα σημαντικά κίνητρα για τις πηγές απειλών εκτός του βασικού κινήτρου που είναι το χρηματικό όφελος. Τα περιστατικά ασφαλείας αποτελούν πλέον καίριο πρόβλημα για τους οργανισμούς κάθε είδους, μεγέθους και γεωγραφικής προέλευσης. Είναι επίσης χαρακτηριστικό ότι τα περιστατικά ασφαλείας φτάνουν πλέον σε διάρκεια ακόμα και 28 μήνες.

Είναι επαρκώς τεκμηριωμένο από την υφιστάμενη βιβλιογραφία ότι η χρήση ΤΠ, χωρίς παράλληλα μελετημένη ασφάλεια των συστημάτων και πληροφοριών, μπορεί να οδηγήσει αντί στην πρόσθετη αξία που αναμένει ένας οργανισμός, στην δημιουργία υψηλών - που μπορεί να ανέλθουν σε καταστρεπτικά επίπεδα – απωλειών. Τα προαναφερόμενα επίπεδα αποτυχίας των ΠΣ είναι κυρίως απόρροια της εφαρμογής αναποτελεσματικών μεθοδολογιών εκτίμησης του επιπέδου ασφάλειας των ΠΣ και γενικότερα της εκτίμησης των κινδύνων που προέρχονται από την χρήση ΠΣ. Αυτό οδηγεί στο συμπέρασμα ότι παράλληλα με την εξάρτηση των οργανισμών στην ΤΠ,

αυξάνεται η αναγκαιότητα δημιουργίας αποδοτικότερων μεθόδων εκτίμησης των κινδύνων (risk assessment methodologies). Η εκτίμηση των κινδύνων αποτελεί το σημαντικότερο στοιχείο της ασφάλειας ΠΣ και αποτελεί το γενικότερο αντικείμενο της παρούσας διατριβής.

1.2 Περιγραφή του ερευνητικού πεδίου

Όπως αναφέρθηκε στην προηγούμενη ενότητα, το γενικότερο πλαίσιο της παρούσας διατριβής αποτελείται από την διερεύνηση μεθοδολογιών εκτίμησης κινδύνων που αφορούν τα ΠΣ που χρησιμοποιεί ένας οργανισμός οποιασδήποτε νομικής υπόστασης, κλάδου και μεγέθους. Ειδικότερα, η έρευνα επικεντρώνεται στους κινδύνους που προκαλούνται από περιστατικά παραβιάσεων ασφαλείας (security breach incidents), όπως ορίζονται στην ενότητα 4.2. Τα περιστατικά αυτά αποτελούν, σύμφωνα με αυτά που αναφέρθηκαν στην εισαγωγική ενότητα, την σοβαρότερη κατηγορία κινδύνων ΠΣ που έχει να αντιμετωπίσει σήμερα ένας οργανισμός. Το κόστος των κινδύνων παραβιάσεων ασφαλείας είναι πολύ μεγαλύτερο σε σχέση με άλλες κατηγορίες κινδύνων ΠΣ όπως η καθυστέρηση εφαρμογής ενός νέου συστήματος και η δυσλειτουργία και αλλαγή υλικού, γεγονός που του προσδίδει την μεγαλύτερη προτεραιότητα αντιμετώπισης.

Ο βασικότερος στόχος της διατριβής είναι η ανάπτυξη νέων και βελτίωση υφιστάμενων μοντέλων και μεθοδολογιών προς την αντικειμενικότερη και ακριβέστερη μέτρηση του επιπέδου ασφαλείας και γενικότερα των κινδύνων παραβιάσεων ασφαλείας που αντιμετωπίζει ένας οργανισμός. Ειδικότερα, έγινε μελέτη των αποτελεσμάτων ερευνών σχετικά με το κόστος και την συχνότητα παραβιάσεων ασφαλείας, τα οποία στην συνέχεια συγκρίθηκαν με αντίστοιχα εμπειρικά αποτελέσματα προκειμένου για την εκροή ολοκληρωμένων συμπερασμάτων. Επιπρόσθετα, έγινε ανάπτυξη μεθοδολογίας μέτρησης του επιπέδου ασφαλείας προκειμένου να χρησιμοποιηθεί μεταξύ άλλων και για την μέτρηση της πιθανότητας εμφάνισης ενός περιστατικού ασφαλείας.

Τελικός στόχος είναι η σύνθεση των παραπάνω προκειμένου για την περισσότερο ολοκληρωμένη και αντικειμενική μέτρηση των κινδύνων πληροφοριακών συστημάτων από παραβιάσεις ασφαλείας.

1.3 Κίνητρα

Τα κίνητρα που οδήγησαν στην συγκεκριμένη διατριβή ήταν πολλά και στην συγκεκριμένη ενότητα επιχειρείται η ανάλυση των ουσιαστικότερων.

Βασικότερο κίνητρο για την έρευνα είναι η ραγδαία αυξανόμενη εξάρτηση της ζωής των σύγχρονων κοινωνιών από τις τεχνολογίες πληροφόρησης. Κάθε δραστηριότητα που χαρακτηρίζει τις ουσιαστικές πτυχές της καθημερινότητας φυσικών και νομικών προσώπων εξαρτάται, σε ολοένα και μεγαλύτερο βαθμό, από τις σύγχρονες τεχνολογίες πληροφόρησης. Το γεγονός αυτό, σε συνάρτηση με την τεράστια ανάπτυξη του Διαδικτύου στις δύο τελευταίες δεκαετίες, έχει οδηγήσει το θέμα της ασφάλειας και απρόσκοπτης λειτουργίας των ΠΣ, βασισμένων σε τεχνολογικές υποδομές, να είναι πλέον ένα πολύ σημαντικό ερευνητικό θέμα που απασχολεί παγκοσμίως κάθε σύγχρονη κοινωνία.

Οι κίνδυνοι παραβιάσεων ασφαλείας και οι επιπτώσεις τους αποτελούν μία από τις κυριότερες προτεραιότητες ενός σύγχρονου οργανισμού ανεξαρτήτως του μεγέθους του, του κλάδου δραστηριότητας και της νομικής του υπόστασης. Υπάρχουν πλέον περιπτώσεις όπου μεγάλοι οργανισμοί οδηγήθηκαν σε πολύ άσχημη οικονομική κατάσταση ή ακόμα και στα όρια της χρεοκοπίας από ένα περιστατικό παραβίασης ασφαλείας. Το γεγονός αυτό επιβάλει την αναγκαιότητα ακριβέστερης μέτρησης των κινδύνων που ενέχουν αυτά τα περιστατικά για τους οργανισμούς.

Το μέγεθος των κινδύνων παραβιάσεων ασφαλείας αυξάνεται διαρκώς τα τελευταία χρόνια και σήμερα είναι το μεγαλύτερο πρόβλημα που έχει να αντιμετωπίσει ένας οργανισμός στην διαχείριση της ασφάλειας ΠΣ. Επίσης, η συγκεκριμένη κατηγορία κινδύνων είναι για ορισμένους τομείς της οικονομίας, όπως αυτού της τεχνολογίας, μία από τις σημαντικότερες που καλούνται να αντιμετωπίσουν οι οργανισμοί στο πλαίσιο του συνόλου των εταιρικών κινδύνων.

Η πολυπλοκότητα της δομής των σύγχρονων ΠΣ έχει αυξηθεί σε πολύ μεγάλο βαθμό προκειμένου να εξυπηρετήσει τις επιχειρησιακές ανάγκες των οργανισμών. Η πολυπλοκότητα αυτή, σε συνδυασμό με το γεγονός ότι το σύνολο σχεδόν των δραστηριοτήτων ενός σύγχρονου οργανισμού και των ευαίσθητων πληροφοριών που διαχειρίζεται, πραγματοποιείται μέσω της σύγχρονης τεχνολογίας, οδηγεί στην αύξηση της αλληλοσυσχέτισης των κινδύνων παραβιάσεων ασφαλείας με άλλους σοβαρούς εταιρικούς κινδύνους. Το μεγαλύτερο μέρος του κόστους από ένα

περιστατικό ασφαλείας αποτελείται από έμμεσες και μακροπρόθεσμες οικονομικές επιπτώσεις οι οποίες, κατά κύριο λόγο, προέρχονται από άλλες κατηγορίες κινδύνων που ενεργοποιούνται. Η συγκεκριμένη ερευνητική προσπάθεια διερεύνησε σε μεγάλο βαθμό την αλληλοσυσχέτιση των εταιρικών κινδύνων με τους κινδύνους παραβιάσεων ασφαλείας.

Συνολικά, η έλλειψη αντικειμενικών ποσοτικών μεθόδων μέτρησης του επιπέδου ασφαλείας και των κινδύνων παραβιάσεων ασφαλείας, και η ευρεία πλέον αναγνώριση από τον επιχειρηματικό και ακαδημαϊκό κόσμο της αναγκαιότητας τους, είναι το σημαντικότερο κίνητρο για την έρευνα που διεξήχθη στα πλαίσια της παρούσας διατριβής.

1.4 Διατύπωση στόχων και συνεισφορά

Η ερευνητική προσπάθεια, που επιχειρείται στην παρούσα διατριβή, έχει ως κύριο στόχο την δημιουργία καθώς και τη βελτίωση υφιστάμενων μεθοδολογιών μέτρησης του επιπέδου ασφαλείας ενός ΠΣ και των κινδύνων που προέρχονται από παραβιάσεις ασφαλείας. Προς αυτήν την κατεύθυνση στόχος είναι η όσο το δυνατόν μεγαλύτερη χρήση ποσοτικών μεθοδολογιών μέτρησης και η αντιστοίχως μικρότερη εξάρτηση από ποιοτικές μεθοδολογίες. Η μεθοδολογία που δημιουργήθηκε έχει ως στόχο την παραγωγή αποτελεσμάτων με την μεγαλύτερη δυνατή αντικειμενικότητα.

Γίνεται εξέταση της μέτρησης του επιπέδου ασφαλείας σε δυναμικό επίπεδο με την χρήση στοχαστικών μεθόδων προκειμένου για την μείωση, στον μεγαλύτερο δυνατό βαθμό, των ποιοτικών μεγεθών που χρησιμοποιούνται και την επίτευξη περισσότερο αντικειμενικών αποτελεσμάτων. Επιπρόσθετος στόχος του προτεινόμενου μοντέλου είναι τα αποτελέσματα να έχουν κατανοητή υπόσταση για την ανώτερη διοίκηση ενός οργανισμού προκειμένου για την διευκόλυνση των αποφάσεων σε θέματα επενδύσεων στην ασφάλεια ΠΣ.

Έγινε εμπειρική μελέτη του κόστους παραβιάσεων ασφαλείας με χρήση περιστατικών των τελευταίων ετών καλύπτοντας το κενό που υφίσταται από την υφιστάμενη βιβλιογραφία. Αναφέρθηκαν τρόποι βελτίωσης της υφιστάμενης μεθοδολογίας και επιχειρήθηκε επεξήγηση των παραγόντων που έχουν οδηγήσει μέχρι σήμερα σε ανάμικτα συμπεράσματα προγενέστερες παρόμοιες μελέτες.

Έγινε συνδυασμός των ερευνητικών πορισμάτων προκειμένου για την αντικειμενικότερη ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας. Προτάθηκε η χρήση μέτρων κινδύνου που παραδοσιακά έχουν χρησιμοποιηθεί στην ποσοτικοποίηση οικονομικών κινδύνων προκειμένου για την δημιουργία τελικών μετρήσεων κατανοητών από τα κλιμάκια διοίκησης ενός οργανισμού που λαμβάνουν αποφάσεις σχετικές με τις μελλοντικές επενδύσεις σε ΠΣ και την ασφάλεια τους.

Αποτυπωμένο διαφορετικά, βασικός στόχος είναι η δημιουργία ενός πλαισίου εκτίμησης των κινδύνων παραβιάσεων ασφαλείας το οποίο δεν απευθύνεται αποκλειστικά σε μηχανικούς υπολογιστών και ειδικούς για την ασφάλεια αλλά στο σύνολο της διοίκησης ενός οργανισμού που λαμβάνει τις τελικές αποφάσεις και χαράζει την στρατηγική.

1.5 Γενική επισκόπηση διατριβής

Στα πλαίσια της παρούσας διατριβής επιχειρήθηκε η ανάπτυξη μεθοδολογιών αντικειμενικής μέτρησης των κινδύνων παραβιάσεων ασφαλείας.

Μελετήθηκε διεξοδικά η έννοια της παραβίασης ασφαλείας και επιχειρήθηκε συστηματοποίηση του θεωρητικού της υπόβαθρου. Αναλύθηκαν οι κυριότερες μελέτες σχετικά με την ασφάλεια ΠΣ και των περιστατικών παραβίασης ασφαλείας με στόχο την αξιολόγηση των αποτελεσμάτων που επιφέρουν και την αποκόμιση συμπερασμάτων.

Μελετήθηκε η εφαρμογή της μεθοδολογίας ανάλυσης γεγονότων στα περιστατικά παραβίασης ασφαλείας. Προτάθηκαν βελτιώσεις των πρακτικών προηγούμενων μελετών και επεξηγήσεις των αιτιών που έχουν οδηγήσει σε διφορούμενα αποτελέσματα. Έγινε έρευνα στα περιστατικά που καταγράφηκαν τα τελευταία χρόνια και δημιουργήθηκε ένα από τα μεγαλύτερα δείγματα σε σύγκριση με υφιστάμενες μελέτες. Τα αποτελέσματα παρουσίασαν στατιστική σημαντικότητα σχετικά με την αρνητική επίπτωση που δύναται να επωμιστεί ένας οργανισμός από ένα περιστατικό ασφαλείας. Αναλύθηκε επίσης η ύπαρξη διαφοροποίησης στις οικονομικές επιπτώσεις με κριτήριο τον τύπο του οργανισμού που εκτίθεται και το μέγεθος του περιστατικού. Το σύνολο των αποτελεσμάτων αξιολογήθηκε σε συνάρτηση με τα αποτελέσματα μελετών σχετικά με την ασφάλεια από επαγγελματικούς οργανισμούς.

Έγινε χρήση στοχαστικών μεθόδων προκειμένου για την αντικειμενική ποσοτικοποίηση του επιπέδου ασφαλείας ΠΣ. Τα δεδομένα που χρησιμοποιήθηκαν στόχος ήταν να αποτελούνται από ανοικτές βάσεις και η μεθοδολογία να είναι σχετικά εύκολα εφαρμόσιμο από κάθε οργανισμό. Επιχειρήθηκε η δημιουργία ενός μοντέλου που να αποφέρει αντικειμενικά και κατανοητά αποτελέσματα και η εφαρμογή του να διευκολύνει την επικοινωνία μεταξύ των υπευθύνων για την ασφάλεια και της ανώτερης διοίκησης και την λήψη αποφάσεων σε αποδοτικότερη και αμεσότερη βάση.

Εφαρμόστηκε η σύνδεση του στοχαστικού μοντέλου μέτρησης του επιπέδου ασφαλείας με την μεθοδολογία των Gordon-Loeb σχετικά με την επένδυση στην ασφάλεια σε συνδυασμό με τα αποτελέσματα για την επίπτωση των παραβιάσεων ασφαλείας που προήλθαν από το σύνολο της ερευνητικής προσπάθειας. Σκοπός ήταν η δημιουργία ενός μοντέλου ποσοτικοποίησης των κινδύνων παραβιάσεων ασφαλείας το οποίο να περιλαμβάνει όλες τις επιμέρους παραμέτρους που ερευνήθηκαν. Τέλος, μελετήθηκε η δυνατότητα σύνδεσης αυτού του μοντέλου με την μεθοδολογία “value at risk” που έχει αναπτυχθεί για την εκτίμηση των οικονομικών κινδύνων.

1.6 Διάρθρωση διατριβής

Η δομή της παρούσας διατριβής περιγράφεται στην συγκεκριμένη ενότητα ως ακολούθως.

Στο επόμενο κεφάλαιο αρχικώς γίνεται περιγραφή των όρων και εννοιών στους οποίους βασίζεται η συγκεκριμένη ερευνητική προσπάθεια. Στην συνέχεια η ανάλυση επικεντρώνεται στις έννοιες που σχετίζονται με τους κινδύνους Πληροφοριακών Συστημάτων.

Το τρίτο κεφάλαιο χωρίζεται σε δύο βασικές ενότητες. Στην πρώτη ενότητα αναλύονται τα στάδια της διαδικασίας διαχείρισης κινδύνων πληροφοριακών συστημάτων Στην δεύτερη ενότητα εντάσσονται οι κίνδυνοι πληροφοριακών συστημάτων, όπως ορίστηκαν στο δεύτερο κεφάλαιο, στα πλαίσια του συνόλου των εταιρικών κινδύνων που αντιμετωπίζει ένας οργανισμός.

Το τέταρτο κεφάλαιο χωρίζεται σε δύο βασικές ενότητες. Στην πρώτη ενότητα πραγματοποιείται εννοιολογική προσέγγιση και αναλυτική περιγραφή των γεγονότων παραβίασης ασφαλείας. Στην δεύτερη ενότητα διαχωρίζονται σε κατηγορίες οι κυριότερες πηγές δεδομένων για τις παραβιάσεις ασφαλείας με συνθετική ανάλυση των δεδομένων που αντλήθηκαν από αυτές και χρησιμοποιήθηκαν κατά την πορεία της ερευνητικής προσπάθειας. Στο συγκεκριμένο

κεφάλαιο αναλύονται τα δεδομένα που προέρχονται από μελέτες συμβουλευτικών οργανισμών καθώς και από διαδικτυακούς τόπους καταγραφής περιστατικών με έμφαση στα πρώτα.

Στο πέμπτο κεφάλαιο γίνεται ανάλυση της εμπειρικής ερευνητικής προσπάθειας που πραγματοποιήθηκε αναφορικά με την σχέση των χρηματιστηριακών αποδόσεων οργανισμών που δέχθηκαν μία παραβίαση ασφαλείας προκειμένου για την ποσοτικοποίηση της οικονομικής επίπτωσης των γεγονότων αυτών. Γίνεται ανάλυση των υφιστάμενων μελετών καθώς το συγκεκριμένο ερευνητικό ρεύμα αποτελεί μία από τις κυριότερες πηγές δεδομένων για τις παραβιάσεις ασφαλείας. Στην συνέχεια περιγράφεται η μεθοδολογία που χρησιμοποιήθηκε στην έρευνα και ακολούθως παραθέτονται τα αποτελέσματα για κάθε στατιστική υπόθεση που τέθηκε με τα τελικά συμπεράσματα.

Στο έκτο κεφάλαιο αναλύεται η μεθοδολογία ποσοτικοποίησης του επιπέδου ασφάλειας ενός συστήματος με την χρήση στοχαστικών μεθόδων. Περιγράφονται οι βάσεις δεδομένων που χρησιμοποιήθηκαν για την άντληση των δεδομένων ευπαθειών που αναλύθηκαν. Ακολούθως, περιγράφονται οι κατηγορίες μεθοδολογιών ποσοτικοποίησης του επιπέδου ασφαλείας. Αναφέρεται η χρήση από το προτεινόμενο μοντέλο των τεχνικών παραγόντων κινδύνου και των πλεονεκτημάτων που δύναται να επιφέρει σε σχέση με τις λοιπές προαναφερόμενες μεθοδολογίες. Περιγράφεται η μεθοδολογική ένταξη των τεχνικών παραγόντων κινδύνου, σε σχέση με το σύνολο των κινδύνων ΠΣ, που ακολουθήθηκε στην διατριβή. Στην συνέχεια αναλύεται η μεθοδολογία που αναπτύχθηκε για τον υπολογισμό του συντελεστή βαρύτητας των παραγόντων κινδύνου σε ένα σύστημα. Ακολούθως, αναλύεται η δημιουργία του μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας σε μία δεδομένη χρονική περίοδο.

Στο έβδομο κεφάλαιο πραγματοποιείται η σύνδεση των ερευνητικών ευρημάτων, εκ του συνόλου της διατριβής, προκειμένου για την δημιουργία ενός μοντέλου ποσοτικοποίησης των κινδύνων παραβιάσεων ασφαλείας. Γίνεται συγκριτική αξιολόγηση των αποτελεσμάτων, σχετικά με τις επιπτώσεις από παραβιάσεις ασφαλείας, που προέρχονται από έρευνες συμβουλευτικών οργανισμών και εμπειρικές μελέτες ανάλυσης γεγονότων. Η περιγραφή και αρχική αξιολόγηση των αποτελεσμάτων ερευνών συμβουλευτικών οργανισμών πραγματοποιείται στο τέταρτο κεφάλαιο ενώ αντίστοιχη περιγραφή και αξιολόγηση των εμπειρικών μελετών στο πέμπτο. Ακολούθως, περιγράφεται η μοντελοποίηση της εκτίμησης πιθανότητας περιστατικών ασφαλείας με βάση την μεθοδολογία ποσοτικοποίησης του επιπέδου ασφαλείας που αναλύθηκε στο έκτο

κεφάλαιο και την μεθοδολογία των Gordon-Loeb για την επένδυση στην ασφάλεια ΠΣ. Στην συνέχεια περιγράφεται το τελικό προτεινόμενο μοντέλο το οποίο αποτελεί απόρροια του συνόλου της ερευνητικής προσπάθειας. Τέλος, περιγράφεται η μεθοδολογία "value at risk" και προτείνεται ο τρόπος εφαρμογής της στην ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας.

Το τελευταίο κεφάλαιο χωρίζεται σε δύο ενότητες. Στην πρώτη συγκεντρώνονται τα συμπεράσματα εκ του συνόλου της ερευνητικής προσπάθειας. Στην δεύτερη ενότητα περιγράφονται τα προτεινόμενα πεδία περεταίρω έρευνας προκειμένου για την ενίσχυση και επέκταση των μεθοδολογικών πλαισίων που θέτει η παρούσα.

2 Βασικές έννοιες – Περιγραφή Ορολογίας

2.1 Εισαγωγή

Το κεφάλαιο αυτό είναι αφιερωμένο στην περιγραφή των αναγκαίων εννοιών και ορολογιών που θέτουν το θεωρητικό υπόβαθρο για την ανάπτυξη της ερευνητικής προσπάθειας και των αποτελεσμάτων που προέκυψαν. Πολλές έννοιες και ορολογίες λαμβάνουν διάφορες ερμηνείες και όρια εφαρμογής ανάλογα με το ερευνητικό πεδίο στο οποίο εφαρμόζονται. Προς αυτή την κατεύθυνση, οι εννοιολογικές προσεγγίσεις πραγματοποιήθηκαν με γνώμονα την εφαρμογή τους στην διαχείριση κινδύνων ΠΣ και ειδικότερα στην μέτρηση της ασφάλειας και την εκτίμηση των κινδύνων που προκαλούνται από παραβιάσεις ασφαλείας.

Τα θέματα της παρούσας διατριβής κινούνται μεταξύ της επιστήμης της διαχείρισης κινδύνων και της επιστήμης των υπολογιστών. Η έρευνα δεν επικεντρώνεται σε συγκεκριμένους τύπους και μεγέθη οργανισμών. Απεναντίας, γίνεται προσέγγιση της διαφοροποίησης στις επιπτώσεις και την συχνότητα των κινδύνων περιστατικών ασφαλείας με κριτήριο τον κλάδο δραστηριότητας ενός οργανισμού.

Αναφορικά με την επιστήμη της διαχείρισης κινδύνων, η έρευνα εστιάζεται στον τομέα εκτίμησης κινδύνων (risk assessment) και στις μεθόδους ποσοτικοποίησης. Στην επιστήμη των υπολογιστών η έρευνα εστιάζεται στο θέμα της ασφάλειας Πληροφοριακών Συστημάτων και ειδικότερα στην ποσοτικοποίηση του επιπέδου ασφάλειας και των κινδύνων που προκαλούνται από τα περιστατικά παραβίασης ασφαλείας (security breach incidents).

Πρέπει να σημειωθεί πως όπου κρίνεται αναγκαίο, ανάλογα με την σημαντικότητα και φύση κάθε έννοιας, παραθέτονται μαζί με τους ελληνικούς όρους και οι αντίστοιχοι αγγλικοί. Ο κύριος λόγος έγκειται στο ότι το θεωρητικό υπόβαθρο της επιστήμης διαχείρισης κινδύνων καθώς και της επιστήμης των υπολογιστών έχει θεσπιστεί παγκοσμίως στην αγγλική και συνεπώς οι πρωτότυπες ορολογίες έχουν καθιερωθεί στην συγκεκριμένη γλώσσα.

Το υπόλοιπο του παρόντος κεφαλαίου χωρίζεται σε τρείς θεματικές ενότητες. Στην πρώτη ενότητα προσεγγίζεται αρχικώς η έννοια του κινδύνου καθώς αποτελεί την βασικότερη έννοια της διατριβής. Ακολουθεί εν συνεχεία ανάλυση των υπολοίπων βασικών εννοιών σχετιζόμενων με τον κίνδυνο.

Στην δεύτερη ενότητα αναλύονται οι γενικοί κίνδυνοι που αντιμετωπίζει κάθε οργανισμός ανά κατηγορία, ανεξάρτητα από τον κλάδο στον οποίο ανήκει και το μέγεθος του. Η προσέγγιση γίνεται με γνώμονα την σχέση που έχει η κάθε κατηγορία κινδύνων με τους κινδύνους ΠΣ γενικότερα και με τους κινδύνους από παραβιάσεις ασφαλείας ειδικότερα.

Στην τρίτη ενότητα ορίζεται το θεωρητικό υπόβαθρο των κινδύνων ΠΣ. Θέτονται οι βασικές έννοιες αυτής της θεματικής ενότητας με την βασικότερη να αποτελεί την ασφάλεια συστημάτων τεχνολογίας πληροφόρησης η οποία αναλύεται διεξοδικά. Ακολούθως παραθέτεται ανάλυση για τα ποιοτικά χαρακτηριστικά των κινδύνων ΠΣ.

2.2 Η έννοια του κινδύνου

2.2.1 Εννοιολογικές προσεγγίσεις και βασικά στοιχεία κινδύνου

Η βασικότερη έννοια της παρούσας διατριβής είναι αυτή του κινδύνου. Γενικώς, μπορούμε να διακρίνουμε δύο διαφορετικές θεωρήσεις του κινδύνου: (α) Κίνδυνος που αφορά φυσικά υποκείμενα και (β) κίνδυνος που αφορά νομικά υποκείμενα. Ο τελευταίος μπορεί να ονομαστεί και επιχειρησιακός κίνδυνος. Τα δύο βασικά στοιχεία του κινδύνου, κοινά σε οποιαδήποτε θεώρηση ληφθεί υπόψη, είναι αυτά της αβεβαιότητας και του μεγέθους της επίπτωσης. Το στοιχείο της αβεβαιότητας χαρακτηρίζει μία κατάσταση για την οποία είτε δεν είμαστε βέβαιοι για την πραγματική της υπόσταση, είτε δεν γνωρίζουμε με βεβαιότητα ποια θα είναι η μελλοντική της υπόσταση. Το στοιχείο της επίπτωσης αναφέρεται στην έκταση των οικονομικών απωλειών που δύναται να έχει σε ένα υποκείμενο η υλοποίηση ενός ανεπιθύμητου αποτελέσματος σε μία συγκεκριμένη κατάσταση.

Στην εννοιολογική προσέγγιση του κινδύνου είναι πολύ βασικό να διευκρινιστεί πως τα δύο βασικά συστατικά του στοιχεία - αβεβαιότητα και επίπτωση - είναι εντελώς ανεξάρτητα μεταξύ τους. Ο βαθμός αβεβαιότητας για ένα ζήτημα δεν επιρρεάζει τον βαθμό έκθεσης ενός υποκειμένου σε αυτό. Προκειμένου να υφίσταται η έννοια του κινδύνου, για μία συγκεκριμένη κατάσταση, πρέπει και τα δύο συστατικά του στοιχεία να έχουν οντότητα. Αν σε μία κατάσταση, όπου ένα υποκείμενο έχει έκθεση, είναι βέβαιο ότι ανεπιθύμητα αποτελέσματα θα πραγματωθούν οδηγώντας σε απώλειες τότε ουσιαστικά δεν υφίσταται κίνδυνος. Συγκεκριμένα, αν ένας υπεύθυνος ασφαλείας ΠΣ είναι βέβαιος ότι μία συγκεκριμένη ευπάθεια των συστημάτων θα

προκαλέσει απώλειες, λόγω της έκθεσης στην οποία υποβάλλονται συγκεκριμένα στοιχεία ενεργητικού, τότε ουσιαστικά δεν υφίσταται κίνδυνος. Η λέξη *βέβαιος* είναι κρίσιμη για την παραπάνω πρόταση και καταργεί κάθε έννοια του κινδύνου χωρίς να λαμβάνεται υπόψη ο βαθμός απωλειών που θα προκαλέσει η έκθεση.

2.2.2 Επιχειρησιακή θεώρηση κινδύνου

Στο [**21**] αναλύεται η επιχειρησιακή θεώρηση του κινδύνου (operational perspective on risk) σε αντιπαράθεση με την προαναφερόμενη γενικότερη θεώρηση. Η επιχειρησιακή θεώρηση του κινδύνου δεν μπορεί να οριστεί με την γενική προσέγγιση των εννοιών της αβεβαιότητας και της έκθεσης καθώς η προσέγγιση αυτή είναι εφαρμόσιμη μόνο σε φυσικά υποκείμενα όπου δεν είναι απαραίτητη η πλήρη επίγνωση των καταστάσεων κινδύνου. Σε νομικά πρόσωπα η γενική θεώρηση του κινδύνου δεν είναι εφαρμόσιμη καθώς, σε αυτά είναι πρακτικά αδύνατο να υφίσταται πλήρης αντίληψη της αβεβαιότητας και της έκθεσης.

Συνεπώς, η ύπαρξη επιχειρησιακού κινδύνου, σε μία συγκεκριμένη κατάσταση, ορίζεται όταν υφίσταται αντιληπτή αβεβαιότητα και αντιληπτή έκθεση σχετικά με την μελλοντική υπόσταση της κατάστασης όπου υλοποίηση ανεπιθύμητων υποστάσεων δύναται να οδηγήσουν σε απώλειες για το εκτεθειμένο υποκείμενο. Ως αποτέλεσμα, προκειμένου να υφίσταται ένας επιχειρησιακός κίνδυνος, πρέπει να έχει αναγνωριστεί ως υπαρκτός από έναν οργανισμό. Αυτό οδηγεί στην έννοια του προσδιορισμού κινδύνων (risk identification) η οποία αποτελεί βασικό στάδιο της διαδικασίας διαχείρισης κινδύνων όπως αναλύεται στην ενότητα 3.2.1.

Με βάση τα παραπάνω, επιχειρησιακός κίνδυνος ορίζεται ο συνδυασμός της πιθανότητας πραγμάτωσης ενός ανεπιθύμητου συμβάντος με την επίπτωση που δύναται να επιφέρει πάνω σε υλικές και άυλες αξίες.

Το πρώτο στοιχείο του συγκεκριμένου ορισμού – η πιθανότητα πραγμάτωσης – προέρχεται από μέτρηση της αβεβαιότητας πραγμάτωσης ενός ανεπιθύμητου συμβάντος. Το δεύτερο στοιχείο – η επίπτωση – προέρχεται από μέτρηση της αντιληπτής έκθεσης ενός υποκειμένου σε ένα ανεπιθύμητο συμβάν σε συνδυασμό με την αξία του υποκειμένου.

2.2.3 Περιστατικό κινδύνου

Ένα περιστατικό κινδύνου (risk event) μπορεί να οριστεί ως το συμβάν το οποίο, στην περίπτωση υλοποίησης του, μπορεί να προκαλέσει αρνητικές επιπτώσεις σε έναν οργανισμό. Η πιθανότητα υλοποίησης του συμβάντος και το επίπεδο των επιπτώσεων αποτελούν τις δύο βασικές παραμέτρους ενός περιστατικού κινδύνου. Όπως θα αναλυθεί στην συνέχεια, ο υπολογισμός των δύο αυτών παραμέτρων αποτελεί το κυριότερο μέρος της διαδικασίας εκτίμησης κινδύνων. Ο παραπάνω ορισμός είναι επίσης βασικός προκειμένου να καταστεί διακριτή η έννοια του περιστατικού κινδύνου από την επίπτωση κινδύνου οι οποίες συχνά είναι δύσκολο να διακριθούν μεταξύ τους.

Οι πηγές απειλών που προκαλούν περιστατικά κινδύνου διαχωρίζονται σε εσωτερικές και εξωτερικές σε σχέση με το στενό περιβάλλον ενός οργανισμού. Εσωτερικές πηγές απειλών είναι π.χ. οι εργαζόμενοι με πρόσβαση σε ευαίσθητα δεδομένα ενώ εξωτερικές πηγές απειλών είναι π.χ. διαδικτυακοί εγκληματίες και κατασκευαστές κακόβουλου λογισμικού. Οι πηγές απειλών, προκειμένου να προκαλέσουν ένα περιστατικό κινδύνου, εκμεταλλεύονται ευπάθειες και ο επερχόμενος συνδυασμός απειλής – ευπάθειας οδηγεί στην έκθεση. Λεπτομερής ανάλυση των στοιχείων που απαρτίζουν τους κινδύνους ΠΣ γίνεται στην ενότητα 2.4.2.

Ένα περιστατικό κινδύνου κατατάσσεται στο ευρύτερο πλαίσιο της εταιρικής διαχείρισης κινδύνων με βάση τον προσδιορισμό που λαμβάνει ως προς την ευρύτερη και ειδικότερη κατηγορία κινδύνων στην οποία ανήκει. Ο προσδιορισμός και η κατάταξη των περιστατικών κινδύνων αποτελεί το πρωταρχικό στάδιο της διαδικασίας διαχείρισης κινδύνων όπως αναλύεται στην ενότητα 3.2.1. Επίσης, ένα περιστατικό κινδύνου συχνά προκαλεί και άλλα περιστατικά κινδύνου τα οποία ουσιαστικά αποτελούν μέρος των επιπτώσεων του στον οργανισμό. Αυτή είναι η βασική αιτία ύπαρξης της λεγόμενης αλληλοσυσχέτισης των εταιρικών κινδύνων η οποία οδηγεί στην αναγκαιότητα διαχείρισης των κινδύνων σε ολιστικό επίπεδο.

Οι οικονομικές επιπτώσεις ενός περιστατικού κινδύνου χωρίζονται σε άμεσες και έμμεσες με την δεύτερη να είναι η πλέον σημαντική. Το μεγαλύτερο μέρος των έμμεσων επιπτώσεων προκαλείται από την αλληλοσυσχέτιση, που υφίσταται μεταξύ των διαφορετικών κατηγοριών κινδύνων, η οποία οδηγεί στην ενεργοποίηση δευτερευόντων περιστατικών κινδύνου από την πραγμάτωση ενός πρωταρχικού περιστατικού.

Τέλος, τα περιστατικά κινδύνου αποτελούν ένα από τα βασικότερα δομικά στοιχεία της παρούσας διατριβής καθώς τα δεδομένα εκτίμησης βασίζονται στην άντληση στοιχείων που αφορούν περιστατικά. Όπως αναλύεται στην ενότητα 4.2 τα περιστατικά κινδύνου, που πραγματεύεται η παρούσα μελέτη, είναι αυτά που αφορούν παραβιάσεις ασφαλείας και αποτελούν το βασικότερο συστατικό των κινδύνων ΠΣ.

2.2.4 Εκτίμηση κινδύνων

Προκειμένου να μετρήσουμε αυτό που είναι αντιληπτό και να καταλήξουμε στην οριοθέτηση του κινδύνου, που προκαλείται από μία κατάσταση, χρησιμοποιούνται εργαλεία τα οποία γενικά ονομάζονται μέτρα κινδύνου (risk metrics). Ένα μεγάλο μέρος της διατριβής είναι αφιερωμένο στην αξιολόγηση και εξεύρεση εργαλείων μέτρησης των κινδύνων ΠΣ. Τα εργαλεία αυτά αποσκοπούν στην εκτίμηση των κινδύνων. Η λέξη εκτίμηση είναι ουσιαστικής σημασίας καθώς είναι αδύνατο να μετρηθεί ο οποιοσδήποτε επιχειρησιακός κίνδυνος με απόλυτη αντικειμενικότητα και ακρίβεια και συνεπώς να τοποθετηθεί η έννοια της μέτρησης. Σκοπός ενός μέτρου κινδύνου είναι να επιτύχει την μέγιστη δυνατή αντικειμενικότητα και ακρίβεια στην προσέγγιση των κινδύνων. Θέτοντας το διαφορετικά, σκοπός είναι να επιτευχθεί μέσω ενός μέτρου κινδύνου κατά το μέγιστο βαθμό μέτρηση και κατά το ελάχιστο εκτίμηση.

Οι οικονομικές συνέπειες που μπορεί να επιφέρει μία παραβίαση ασφαλείας σε έναν οργανισμό θεωρούνται ένα από τα δυσκολότερα μεγέθη προς μέτρηση. Η δημιουργία ενός μέτρου των κινδύνων παραβιάσεων ασφάλειας περιλαμβάνει δυσκολίες διαφόρων ειδών μέρος των οποίων επιχειρεί να επιλύσει η παρούσα διατριβή.

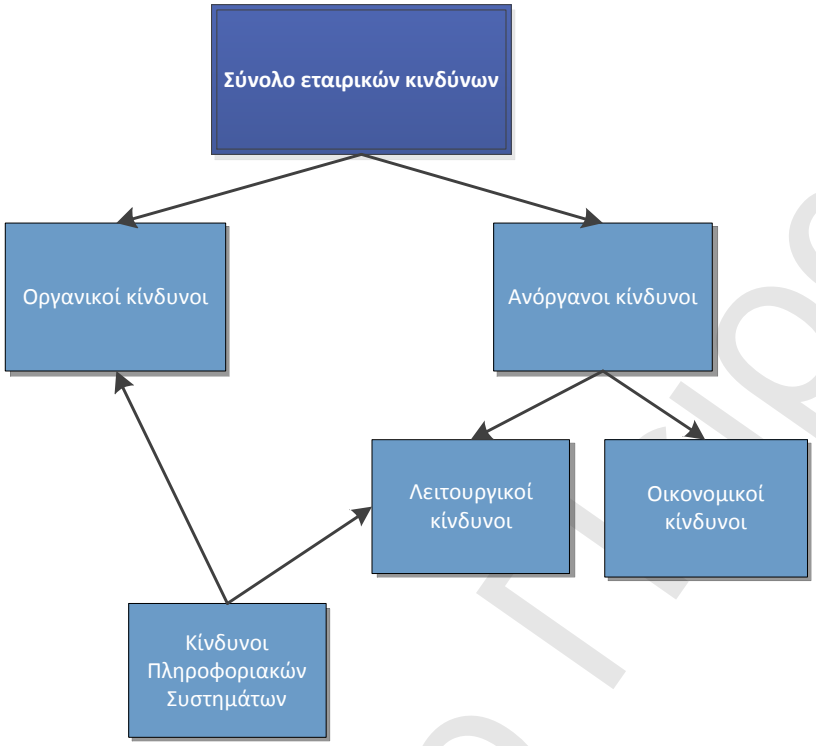
2.3 Κατηγορίες κινδύνων

Από την μελέτη της βιβλιογραφίας διαπιστώνεται ότι δεν υφίσταται μία ευρέως αποδεκτή ταξινόμηση του γαλαξία κινδύνων που αντιμετωπίζει ένας οργανισμός ανεξάρτητα από τον οικονομικό κλάδο στον οποίο δραστηριοποιείται. Διαφορετική ταξινόμηση των κινδύνων μπορεί να διακρίνει κανείς ανάλογα τον κλάδο ή ακόμα και σε επιχειρήσεις που ανήκουν στον ίδιο κλάδο δραστηριότητας. Στο ανώτερο επίπεδο θεώρησης, μπορούμε να διακρίνουμε δύο γενικές κατηγοριοποιήσεις κινδύνων: (α) χρηματοοικονομικών επιχειρήσεων, (β) μη χρηματοοικονομικών επιχειρήσεων. Μία ταξινόμηση των κινδύνων που μπορεί να εφαρμοστεί στους οργανισμούς,

ανεξαρτήτως του κλάδου στον οποίο δραστηριοποιούνται και του μεγέθους τους, παρουσιάζεται στην Εικόνα 1.

Ο βασικός διαχωρισμός του συνόλου των εταιρικών κινδύνων ή, όπως αποκαλείται συνήθως από την βιβλιογραφία, του «γαλαξία των κινδύνων» (galaxy of risks), είναι μεταξύ των οργανικών και ανόργανων κινδύνων [**22**]. Οι οργανικοί κίνδυνοι (business risks) προέρχονται από την κύρια λειτουργία ενός οργανισμού και αναλαμβάνονται προκειμένου για την δημιουργία προστιθέμενης αξίας προς τους μετόχους. Το είδος των λειτουργικών κινδύνων κυρίως εξαρτάται από τον κλάδο στον οποίο δραστηριοποιείται ένας οργανισμός και συνεπώς από το είδος της παραγωγικής λειτουργίας που επιτελεί. Αυτό οδηγεί στο επίπεδο της έκθεσης που έχει ένας οργανισμός σε κίνδυνο προϊόντος, κίνδυνο τεχνολογίας καθώς και το είδος των μακροοικονομικών κινδύνων που αντιμετωπίζει. Μέρος των κινδύνων ΠΣ μπορούν να θεωρηθούν ως οργανικοί κίνδυνοι. Αυτοί αφορούν κυρίως την δημιουργία και υιοθέτηση νέων επενδυτικών προγραμμάτων σε τεχνολογίες πληροφόρησης προκειμένου για την διατήρηση ανταγωνιστικών πλεονεκτημάτων, διατήρηση και αύξηση του μεριδίου αγοράς και μείωση του κόστους. Το σύνολο αυτών των κινδύνων αναφέρονται ως συμμετρικοί με την έννοια ότι η επίπτωση τους μπορεί να είναι είτε θετική, είτε αρνητική για έναν οργανισμό. Το χαρακτηριζόμενο ως οργανικό μέρος των κινδύνων ΠΣ είναι εκτός των ερευνητικών θεμάτων της παρούσας διατριβής.

Η δεύτερη γενική κατηγορία κινδύνων αποτελείται από τους ανόργανους κινδύνους (nonbusiness risks). Οι κίνδυνοι που υπάγονται σε αυτήν την κατηγορία χαρακτηρίζονται έτσι καθώς δεν πηγάζουν από τις βασικές παραγωγικές λειτουργίες ενός οργανισμού. Είναι κίνδυνοι από τους οποίους ένας οργανισμός δεν αναμένει αποδώσεις από την υιοθέτηση τους αλλά αντιθέτως πληρώνει για την αντιμετώπιση τους. Προκειμένου για τις ανάγκες τις παρούσας μελέτης, όπως απεικονίζεται στην Εικόνα 1, θα τους διαχωρίσουμε περεταίρω σε λειτουργικούς κινδύνους (operational risks) και οικονομικούς κινδύνους (financial risks). Οι λειτουργικοί κίνδυνοι προκαλούνται από απρόβλεπτα περιστατικά τα οποία είναι εκτός του άμεσου ελέγχου ενός οργανισμού και αναλύονται διεξοδικότερα στην επόμενη ενότητα. Οι οικονομικοί κίνδυνοι προκαλούνται από τις απρόβλεπτες μεταβολές των βασικών οικονομικών μεταβλητών όπως είναι τα επιτόκια, οι συναλλαγματικές ισοτιμίες, οι μεταβολές στα επίπεδα ρευστότητα της αγοράς και από την πιστοληπτική ικανότητα του πελατολογίου ενός οργανισμού.



Εικόνα 1: Το σύνολο των εταιρικών κινδύνων

Οι ανόργανοι κίνδυνοι χαρακτηρίζονται στο σύνολο τους ως μη συμμετρικοί κίνδυνοι καθώς η αναμενόμενη επίπτωση τους αποφέρει μόνο αρνητικά οικονομικά αποτελέσματα σε έναν οργανισμό.

Το μέρος των κινδύνων ΠΣ, που δεν υπάγεται στους οργανικούς κινδύνους, υπάγεται στους λειτουργικούς κινδύνους. Η ερευνητική θεματολογία της παρούσας διατριβής επικεντρώνεται στους κινδύνους παραβιάσεων ασφαλείας οι οποίοι ανήκουν στους κινδύνους ΠΣ που υπάγονται στους ανόργανους κινδύνους συμβάντων.

2.3.1 Λειτουργικοί κίνδυνοι

Η κατηγορία που περιλαμβάνει του λειτουργικούς κινδύνους είναι από τις πιο δύσκολες προς τον προσδιορισμό και την αποτίμηση. Η λέξη αποτίμηση δεν χρησιμοποιείται τυχαία καθώς το μεγαλύτερο πλήθος των μεθοδολογιών απασχολείται με υποκειμενική αποτίμηση του επιπέδου έκθεσης και λιγότερο με αντικειμενικές μεθοδολογίες μέτρησης. Οι αντικειμενικές μεθοδολογίες μέτρησης είναι αναγκαίες καθώς οδηγούν τελικά σε αποτελεσματικότερη διαχείριση των κινδύνων. Ο εννοιολογικός προσδιορισμός τους είναι απόλυτα απαραίτητος καθώς χωρίς μία

επαρκή και κατάλληλα τεκμηριωμένη εννοιολογική προσέγγιση των λειτουργικών κινδύνων, δεν δύναται να εφαρμοστεί επαρκώς η διαδικασία διαχείρισης κινδύνων. Μπορούμε να διακρίνουμε στην βιβλιογραφία τρεις βασικές προσεγγίσεις για την έννοια των λειτουργικών κινδύνων:

Σύμφωνα με την πρώτη προσέγγιση, χαρακτηρίζονται ως λειτουργικοί οι κίνδυνοι αυτοί που δεν ανήκουν στην κατηγορία των οικονομικών κινδύνων [**23**]. Ο συγκεκριμένος εννοιολογικός προσδιορισμός είναι αρκετά ευρύς καθώς περιλαμβάνει κατηγορίες κινδύνων, όπως τους οργανικούς, που λόγω της φύσης τους δεν μπορούν να ελεγχθούν άμεσα από το επιτελείο διαχείρισης κινδύνων ενός οργανισμού, το επίπεδο λήψης τους οριοθετείται από την ανώτατη διοίκηση και η λήψη τους θεωρείται απαραίτητη για την επιχειρηματική λειτουργία και την επίτευξη των σκοπών του οργανισμού.

Η δεύτερη προσέγγιση χαρακτηρίζει ως λειτουργικούς κινδύνους μόνο αυτούς που σχετίζονται με τις λειτουργίες ή διαδικασίες ενός οργανισμού. Περιλαμβάνονται δηλαδή μόνο οι ανόργανοι ενδογενείς κίνδυνοι διαδικασιών όπως π.χ. ο κίνδυνος συμβολαίων (contract risk) ή ο κίνδυνος λογιστικών αστοχιών (accounting error). Σε αντίθεση με την πρώτη προσέγγιση, η συγκεκριμένη είναι υπερβολικά περιορισμένη [**24**], [**25**].

Η τρίτη προσέγγιση χαρακτηρίζει ως λειτουργικούς κινδύνους αυτούς που προκαλούνται από ανεπαρκής ή αποτυχημένες εσωτερικές διαδικασίες, από το ανθρώπινο δυναμικό, από συστήματα λειτουργίας και εξωγενείς παράγοντες [**26**]. Ο παραπάνω ορισμός διαχωρίζει ουσιαστικά του λειτουργικούς κινδύνους σε τέσσερις γενικές κατηγορίες :

- Κίνδυνοι προερχόμενοι από τους ανθρώπους (People)
- Κίνδυνοι από τις εταιρικές διαδικασίες (Processes)
- Κίνδυνοι από τα συστήματα λειτουργίας (Systems)
- Εξωγενείς κίνδυνοι (External Risks)

Ο συγκεκριμένος ορισμός των λειτουργικών κινδύνων, και η συνεπαγόμενη οριοθέτηση των εταιρικών κινδύνων, υιοθετείται από την παρούσα διατριβή. Το κριτήριο επιλογής είναι η αποδοτικότερη απεικόνιση των κινδύνων ΠΣ. Στην Εικόνα 2 απεικονίζεται η ανάλυση των λειτουργικών κινδύνων βασιζόμενη στον παραπάνω ορισμό. Οι κίνδυνοι προερχόμενοι από ανθρώπους, διαδικασίες και συστήματα μπορούν να αποτελέσουν μία ευρύτερη κατηγορία

χαρακτηριζόμενοι ως «ενδογενείς λειτουργικοί κίνδυνοι». Η τέταρτη κατηγορία αποτελείται από τους εξωγενείς κινδύνους οι οποίοι διακρίνονται περεταίρω σε φυσικούς κινδύνους και κινδύνους προερχομένους από τεχνικά αίτια. Οι φυσικοί κίνδυνοι περιλαμβάνουν φυσικές καταστροφές, ατυχήματα, κλοπές και τρομοκρατικές ενέργειες. Οι τεχνικοί κίνδυνοι, των οποίων εκτενέστερη περιγραφή γίνεται στις επόμενες παραγράφους, διακρίνονται περεταίρω σε:

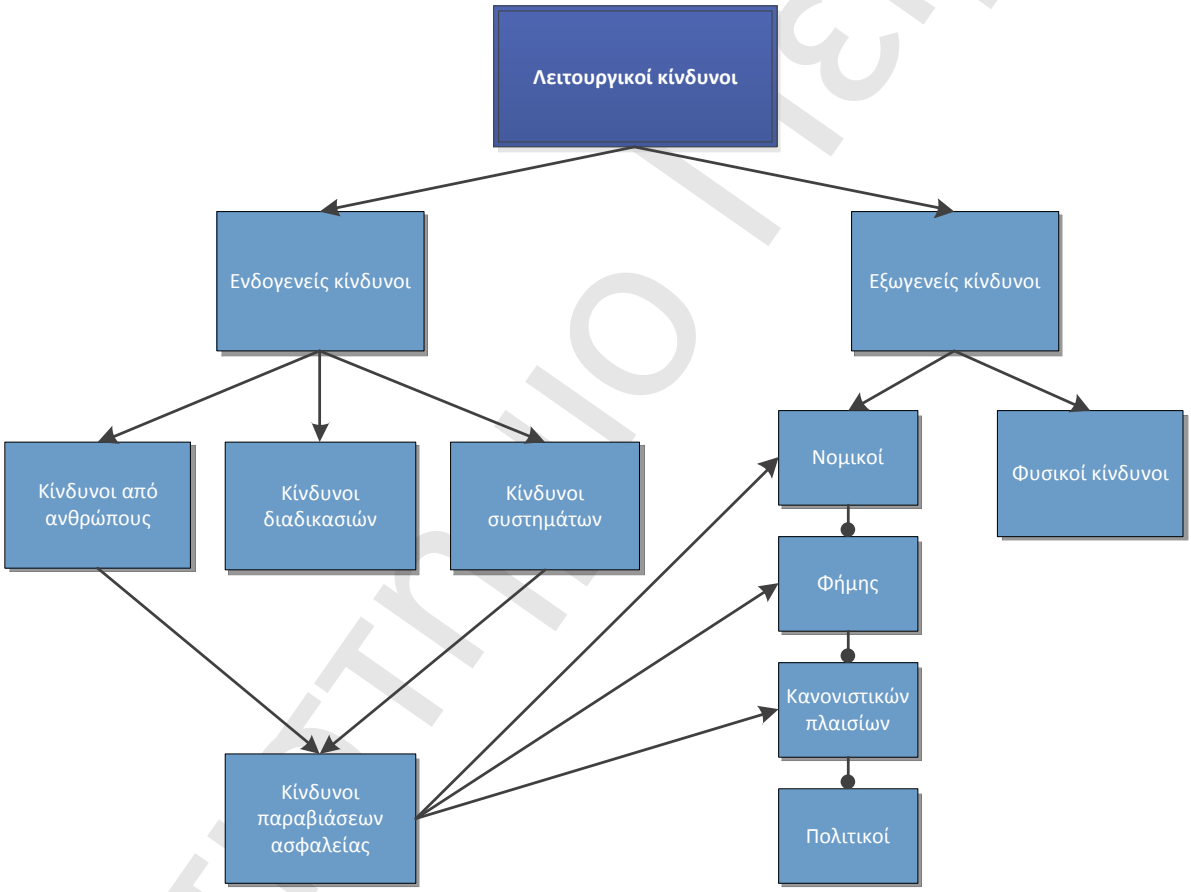
- Νομικούς κινδύνους
- Κινδύνους φήμης
- Κινδύνους προερχόμενους από κανονιστικά πλαίσια
- Πολιτικούς κινδύνους

Ακολουθώντας τις πρακτικές και τα κανονιστικά πλαίσια του χρηματοοικονομικού τομέα [**23**], μπορούμε να εντάξουμε τους κινδύνους παραβιάσεων ασφαλείας στους ενδογενείς κινδύνους συστημάτων όπως φαίνεται στην Εικόνα 2. Από την έρευνα που διεξήχθη, οι κίνδυνοι παραβιάσεων ασφαλείας εντάχθηκαν παράλληλα και στους κίνδυνους προερχόμενους από ανθρώπους. Όπως αναφέρεται στην ενότητα 4.2, μία από τις βασικές αιτίες που οδηγούν σε περιστατικά παραβίασης ασφαλείας είναι η αμέλεια από το ανθρώπινο δυναμικό. Σύμφωνα με έρευνες η αιτία αυτή, μαζί με τις κακόβουλες επιθέσεις, είναι πλέον μία από τις βασικότερες προτεραιότητες αντιμετώπισης για τις διοικήσεις των οργανισμών. Υπολογίζεται ότι σχεδόν το 40% των παραβιάσεων ασφαλείας προκαλείται από ανθρώπινη αμέλεια [**27**].

Ο χρηματοοικονομικός τομέας οδηγεί τις εξελίξεις και στην περίπτωση της κατηγορίας των λειτουργικών κινδύνων όπου έχουν θεσμοθετηθεί κανόνες ελέγχου από τα Ιδρύματα Ρύθμισης των Τραπεζών (Bank Regulators). Τα τελευταία χρόνια εισήχθη για πρώτη φορά υποχρέωση των χρηματοοικονομικών επιχειρήσεων να λαμβάνουν υπόψη τους λειτουργικούς κινδύνους στους προσδιορισμούς των κεφαλαιακών απαιτήσεων που τους επιβάλλονται από τις ρυθμιστικές αρχές. Ουσιαστικά οι επιχειρήσεις αυτής της κατηγορίας ξεκινάνε να λαμβάνουν σοβαρά υπόψη τους, κατά την διαδικασία λήψης αποφάσεων, άλλους κινδύνους πέραν των αμιγώς οργανικών που παραδοσιακά αναλύουν.

Για τις επιχειρήσεις του χρηματοοικονομικού κλάδου ένα μέρος των οικονομικών κινδύνων αποτελούν στην ουσία μέρος του συνολικού επιχειρηματικού κινδύνου που αναλαμβάνουν. Για τις

μη χρηματοοικονομικές επιχειρήσεις ισχύει το αντίθετο καθώς δεν αναλαμβάνουν χρηματοοικονομικούς κινδύνους στα πλαίσια της οργανικής λειτουργίας τους. Η σημαντικότητα όμως των λειτουργικών κινδύνων είναι το ίδιο σοβαρή και στις δύο γενικές κατηγορίες οργανισμών. Συνεπώς το ρυθμιστικό πλαίσιο των λειτουργικών κινδύνων που επέβαλαν οι τραπεζικές αρχές πρέπει να ληφθεί ως σαφής ένδειξη για τον τρόπο λειτουργίας της μη χρηματοοικονομικής αγοράς έστω και χωρίς κανονιστικά πλαίσια επιβολής.



Εικόνα 2: Ανάλυση λειτουργικών κινδύνων

Οι χρηματοοικονομικοί οργανισμοί οδηγήθηκαν σε αυτήν την κίνηση μετά την συνειδητοποίηση των εξαιρετικά μεγάλων ζημιών που προκάλεσαν γεγονότα που μπορούν να ενταχθούν στους λειτουργικούς κινδύνους και οφείλονται κυρίως σε εσωτερικές απάτες και έλλειψη επαρκούς ελέγχου. Κατά αναλογία σε μη χρηματοοικονομικούς οργανισμούς οι ζημιές ως

απόρροια υλοποίησης λειτουργικών κινδύνων βρίσκονται σε εξαιρετικά υψηλά επίπεδα. Κύριος σκοπός της παρούσας είναι η ποσοτικοποίηση του λειτουργικών κινδύνων που προέρχονται από τις παραβιάσεις ασφαλείας.

Στις επόμενες ενότητες περιγράφονται οι κατηγορίες εξωγενών λειτουργικών κινδύνων οι οποίοι, όπως απεικονίζεται στην Εικόνα 2, έχουν αλληλοσυσχέτιση με τους κινδύνους παραβιάσεων ασφαλείας και κατά συνέπεια η ακριβής περιγραφή τους είναι απαραίτητη προκειμένου για την θέσπιση του θεωρητικού υπόβαθρου της παρούσας διατριβής.

2.3.2 Νομικοί κίνδυνοι

Γενικότερα ως νομικός μπορεί να θεωρηθεί ο κίνδυνος μία συναλλαγή να μην δύναται η ολοκλήρωση της λόγω νομικών δυσκολιών. Οι κίνδυνοι που ανήκουν στην συγκεκριμένη κατηγορία προκαλούνται από περιστατικά τα οποία μπορούν να οδηγήσουν σε νομικές διαδικασίες έναν οργανισμό οι οποίες μπορούν να έχουν ως αποτέλεσμα την απορρόφηση εταιρικών πόρων και χρηματοροών και σε τελική ανάλυση την απόσπαση του οργανισμού από τους κύριους εταιρικούς σκοπούς.

Τα περιστατικά που προκαλούν νομικούς κινδύνους, προκειμένου για τις ανάγκες τις παρούσας διατριβής, διακρίνονται σε δύο γενικές κατηγορίες. Η πρώτη κατηγορία περιλαμβάνει την αθέτηση εκπλήρωσης των όρων ενός συμβολαίου από τα συμβαλλόμενα μέρη λόγω νομικών δυσχερειών που προκαλούνται από ατελή τεκμηρίωση, κανονιστικές απαγορεύσεις και την αδυναμία επιβολής.

Η δεύτερη κατηγορία περιλαμβάνει γεγονότα που μπορούν να προκαλέσουν νομικό παθητικό σε έναν οργανισμό. Αυτός είναι ο λόγος που συναντάμε συχνά την υπαγωγή των νομικών κινδύνων στην γενικότερη κατηγορία των κινδύνων γεγονότων (event risks). Παραδείγματα γεγονότων που μπορούν να προκαλέσουν νομικό παθητικό σε έναν οργανισμό είναι προβληματικά προϊόντα, παραβιάσεις κανονιστικών πλαισίων καθώς και διαρροή ευαίσθητων πληροφοριών μέσω παραβιάσεων ασφαλείας. Πηγές απειλών σε αυτήν την κατηγορία κινδύνων είναι πελάτες, προμηθευτές, εργαζόμενοι, η πολιτεία κλπ.

Οι κίνδυνοι παραβιάσεων ασφαλείας συνδέονται έμμεσα με τους νομικούς κινδύνους καθώς ένα μέρος της συνολικής επίπτωσης ενός περιστατικού μπορεί να οφείλεται από περιστατικά

νομικών κινδύνων τα οποία δύναται να προκληθούν ως δευτερογενή συμβάντα. Τα σχετικά νομικά πλαίσια που μπορούν να παραβιαστούν αφορούν την προστασία δεδομένων και πνευματικής ιδιοκτησίας καθώς και των κανονισμών περί ανακοίνωσης ενός περιστατικού. Το έμμεσο κόστος, που προκαλείται από ένα περιστατικό παραβίασης ασφαλείας, πολλές φορές προέρχεται από το νομικό παθητικό που δημιουργείται. Το παθητικό αυτό, λόγω της φύσης του, είναι μακροπρόθεσμο προκειμένου να λάβει πλήρη διάσταση. Αυτός είναι ο κύριος λόγος που θεωρείται από τα δυσκολότερα στοιχεία των κινδύνων παραβιάσεων ασφαλείας προς ποσοτικοποίηση.

2.3.3 Κίνδυνος φήμης

Ο κίνδυνος φήμης θεωρείται η απώλεια που μπορεί να δεχθεί έναν οργανισμός από ένα δυσμενές γεγονός το οποίο δημοσιεύτηκε και προκάλεσε μείωση της εμπιστοσύνης της αγοράς. Η κατηγορία αυτή κινδύνων δεν αφορά άμεσες χρηματικές απώλειες και οι επιπτώσεις του είναι κατά κύριο λόγο μακροπρόθεσμες προκειμένου να αποκρυσταλλωθεί η πλήρης διάσταση τους μετά τον χρόνο έλευσης ενός γεγονότος. Σοβαρός παράγοντας, στο επίπεδο του αντίκτυπου που έχει ο κίνδυνος φήμης σε έναν οργανισμό, είναι ο κλάδος στον οποίο δραστηριοποιείται. Συγκεκριμένοι κλάδοι οργανισμών έχουν ιδιαίτερη ευαισθησία σε συγκεκριμένες κατηγορίες δυσμενών γεγονότων ενώ έχουν ανοχή σε άλλες.

Τα περιστατικά παραβίασης ασφαλείας προκαλούν μία κατηγορία κινδύνων η οποία μπορεί να οδηγήσει σε σημαντικές απώλειες την φήμη ενός οργανισμού. Στις περιπτώσεις που ο τομέας δραστηριοποίησης του οργανισμού είναι ιδιαίτερα ευαίσθητος σε ένα περιστατικό παραβίασης ασφαλείας, το έμμεσο κόστος που θα επωμιστεί από την απώλεια φήμης δύναται να είναι εξαιρετικά μεγάλο. Παραδείγματα αποτελούν οι εταιρίες τεχνολογίας και οι εταιρίες ηλεκτρονικού εμπορίου των οποίων η φήμη παρουσιάζει εξαιρετικά μεγάλη ευαισθησία στην αξιοπιστία των συστημάτων τεχνολογίας πληροφόρησης που διαθέτουν.

Ένα περιστατικό παραβίασης ασφαλείας, σε οργανισμούς αυτού του είδους, αναμένεται να προκαλέσει μεγαλύτερες έμμεσες οικονομικές επιπτώσεις, από ότι σε άλλους τύπους οργανισμών, λόγω απωλειών σε φήμη και κατά συνέπεια σε μείωση της υπάρχουσας και εν δυνάμει πελατείας. Η υπόθεση αυτή έχει εξεταστεί εμπειρικά τα τελευταία χρόνια από την ακαδημαϊκή κοινότητα. Στα πλαίσια της παρούσας διατριβής γίνεται επίσης εμπειρική εξέταση αυτής της υπόθεσης

χρησιμοποιώντας δεδομένα των τελευταίων ετών. Η μελέτη αυτή αναλύεται στο κεφάλαιο 5 της παρούσας.

2.3.4 Κίνδυνος κανονιστικών πλαισίων

Ο κίνδυνος κανονιστικών πλαισίων προέρχεται από αλλαγές σε κανονισμούς καθώς και από ερμηνείες υφιστάμενων κανονισμών οι οποίες μπορούν να προκαλέσουν οικονομικές επιπτώσεις σε έναν οργανισμό. Χαρακτηριστικό παράδειγμα αποτελεί το υφιστάμενο κανονιστικό πλαίσιο παγκοσμίως σχετικά με τις παραβιάσεις ασφαλείας. Ουσιαστικά δεν υφίσταται ενιαίο πλαίσιο σχετικά με την οριοθέτηση της ίδιας της έννοιας των παραβιάσεων ασφαλείας καθώς και των υποχρεώσεων που έχει ένας οργανισμός σχετικά με την γνωστοποίηση ενός περιστατικού [**28**].

Συγκεκριμένα, στις ΗΠΑ η θεώρηση ενός περιστατικού ως παραβίαση ασφαλείας είναι πολύ γενική με αποτέλεσμα ένα μεγάλο ποσοστό καταγραμμένων περιστατικών να μην αφορά πραγματικές παραβιάσεις ασφαλείας με αποτέλεσμα κατανάλωση πόρων από έναν οργανισμό στην αντιμετώπιση ενός γεγονότος για το οποίο έχει ληφθεί λανθασμένη ερμηνεία. Το παραπάνω φαινόμενο μπορεί να θεωρηθεί ως απόρροια του γεγονότος ότι οι παραβιάσεις ασφαλείας αποτελούν ένα πρόσφατο σχετικά φαινόμενο με την εξέλιξη τους ως ένα από τα σοβαρότερα προβλήματα ενός οργανισμού να διαδραματίζεται μόλις την τελευταία πενταετία. Αυτό οδηγεί τα νομοθετικά και κανονιστικά πλαίσια των ανεπτυγμένων κρατών ακόμα να μην έχουν εξελιχθεί σε επαρκές επίπεδο με αποτέλεσμα σήμερα ο κίνδυνος προερχόμενος από κανονιστικά πλαίσια σε σχέση με γεγονότα παραβιάσεων ασφαλείας να είναι αρκετά σημαντικός.

2.4 Κίνδυνοι Πληροφοριακών Συστημάτων

2.4.1 Βασικές έννοιες

Οι δύο βασικότεροι όροι που χρησιμοποιούνται στην παρούσα διατριβή είναι αυτοί που αφορούν ένα Πληροφοριακό Σύστημα (Information System) και την Τεχνολογία Πληροφόρησης (Information Technology). Ως Πληροφοριακά Συστήματα (ΠΣ) νοούνται τα συστήματα στα οποία οι ροές πληροφόρησης είναι κατά τέτοιο τρόπο σχεδιασμένες ώστε να ικανοποιούν τις προσδιορισμένες απαιτήσεις πληροφόρησης ενός οργανισμού [**29**]. Τα βασικά στοιχεία ενός ΠΣ

είναι (α) το ανθρώπινο στοιχείο που συλλέγει, επεξεργάζεται και αξιοποιεί την πληροφόρηση, (β) ο σχεδιασμός, η οργάνωση και η λειτουργία των ροών πληροφόρησης και (γ) τα δεδομένα.

Η Τεχνολογία Πληροφόρησης (ΤΠ) ως έννοια περιλαμβάνει λογισμικό, υποδομή και τεχνολογίες επικοινωνιών εστιάζοντας περισσότερο στον υλικό εξοπλισμό. Ο όρος Σύστημα Τεχνολογίας Πληροφόρησης (IT system) αναφέρεται σε ένα υποστηρικτικό σύστημα που περιλαμβάνει κεντρικούς υπολογιστές (mainframe computers), υπολογιστές-πελάτες, υποδομές δικτύωσης και εφαρμογές ευρείας χρήσης των οποίων η χρήση ικανοποιεί συγκεκριμένες απαιτήσεις και καλύπτει συγκεκριμένες ανάγκες ενός οργανισμού [**30**]. Καθώς σήμερα σχεδόν το σύνολο των σύγχρονων ΠΣ είναι βασισμένα σε Συστήματα Τεχνολογίας Πληροφόρησης (ΣΤΠ), οι όροι ΠΣ και ΣΤΠ χρησιμοποιούνται ευρέως κατ' εναλλαγή. Από τον ορισμό των Πληροφοριακών Συστημάτων και των Συστημάτων Τεχνολογίας Πληροφόρησης διαφαίνεται ότι η δεύτερη έννοια αποτελεί μέρος ουσιαστικά της πρώτης. Στην παρούσα διατριβή, επιλέγεται η χρήση της ευρύτερης έννοιας των Πληροφοριακών Συστημάτων (ΠΣ) και συνεπώς οι αντίστοιχοι κίνδυνοι θα αναφέρονται ως κίνδυνοι ΠΣ.

Η βασικότερη ίσως έννοια που αναλύεται στην διατριβή είναι αυτή της ασφάλειας πληροφόρησης (information security). Ασφάλεια πληροφόρησης είναι η διαφύλαξη σε ένα ΠΣ της εμπιστευτικότητας (confidentiality), ακεραιότητας (integrity) και διαθεσιμότητας (availability) των πληροφοριών που διαχειρίζεται καθώς και της λειτουργικότητας του ιδίου του ΠΣ. Σύμφωνα με πολλαπλές πηγές, όπως οι [**31**], [**32**], η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών θεωρούνται ως οι θεμελιώδεις αρχές της ασφάλειας πληροφόρησης.

Ως αρχή της εμπιστευτικότητας των πληροφοριών, που διαχειρίζεται ένα ΠΣ, ορίζεται η διαβάθμιση της ευαισθησίας των πληροφοριών και τα φυσικά ή νομικά πρόσωπα που έχουν εξουσιοδότηση πρόσβασης σε κάθε επίπεδο πληροφόρησης. Η συγκεκριμένη αρχή διακρίνεται σε δύο κατηγορίες ανάλογα με την φύση των δεδομένων: (α) Αρχή της μυστικότητας στην περίπτωση δεδομένων νομικών προσώπων. (β) Αρχή της ιδιωτικότητας στην περίπτωση δεδομένων φυσικών προσώπων. Η αρχή της ακεραιότητας αφορά την προστασία των δεδομένων από αλλαγές για τις οποίες δεν έχει δοθεί εξουσιοδότηση από τον ιδιοκτήτη τους. Οι αλλαγές αυτές περιλαμβάνουν δημιουργία, αλλαγή και διαγραφή δεδομένων και όταν επέρχονται από μη εξουσιοδοτημένους χρήστες χαρακτηρίζονται ως ανεπιθύμητες. Τέλος, η αρχή της διαθεσιμότητας

αφορά την έγκαιρη και πλήρη ανταπόκριση ενός ΠΣ προκειμένου για την κάλυψη των αναγκών των εξουσιοδοτημένων χρηστών.

Η έννοια που χρήζει ιδιαίτερης προσοχής είναι αυτή που αναφέρεται στους κινδύνους ΠΣ. Μπορούμε να ορίσουμε ως κίνδυνους ΠΣ το φάσμα κινδύνων κάθε μορφής που μπορούν να επηρεάσουν αρνητικά κάθε στοιχείο ενεργητικού που άμεσα ή έμμεσα συσχετίζεται με ένα ΠΣ. Ο κίνδυνος ΠΣ ορίζεται ως η καθαρή αρνητική επίπτωση από την εκμετάλλευση μίας ευπάθειας λαμβάνοντας υπόψη την πιθανότητα καθώς και τη διάσταση του συμβάντος [**30**]. Μπορεί επίσης να οριστεί ως συνάρτηση της πιθανότητας που έχει μία συγκεκριμένη απειλή (threat) να επιτύχει την εκμετάλλευση μίας συγκεκριμένης ευπάθειας (vulnerability), με το μέγεθος έκθεσης (exposure) ενός στοιχείου ενεργητικού ΠΣ, της ποιότητας των ελέγχων ασφαλείας (counter-measures) και της αξίας του στοιχείου ενεργητικού που προσβάλλεται. Το μέγεθος έκθεσης αναφέρεται συχνά και ως παράγοντας έκθεσης (exposure factor).

Οι φορείς TrueSecure – ICSA Labs έχουν προτείνει μία απλή προσέγγιση περιγραφής των κινδύνων ΠΣ η οποία αποτυπώνει τον ορισμό που μόλις αναφέρθηκε [**33**]. Προτείνουν την παρακάτω εξίσωση:

$$\text{Κίνδυνος} = \text{Απειλή X Ευπάθεια X Κόστος}$$

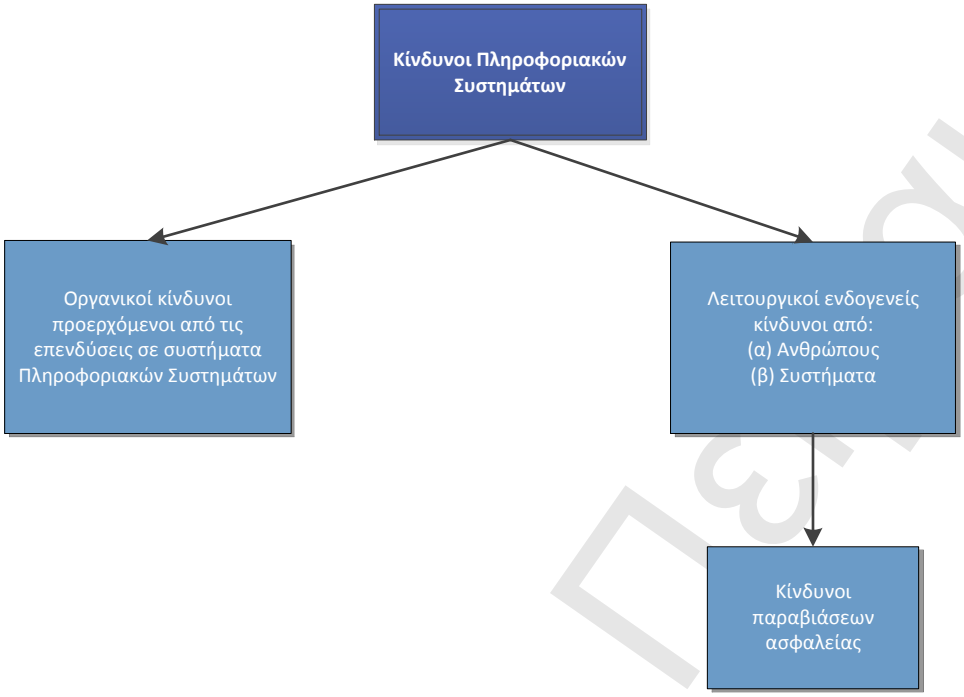
Ο τελεστής απειλή αναφέρεται στην πιθανότητα να εμφανιστεί μία απειλή, ο τελεστής ευπάθεια αναφέρεται στην πιθανότητα επιτυχούς εκμετάλλευσης μίας ευπάθειας από μία απειλή που έχει εμφανιστεί και ο τελεστής κόστος αναφέρεται στο μέγεθος της επίπτωσης που αναμένεται να επιφέρει. Συνεπώς, η παραπάνω προσέγγιση υποδεικνύει ότι η πιθανότητα εμφάνισης των κινδύνων εξαρτάται από δύο παραμέτρους, το επίπεδο απειλής και ευπάθειας οι οποίες, σε συνδυασμό με το μέγεθος της επίπτωσης, ορίζουν το επίπεδο των κινδύνων ΠΣ. Εκτενέστερη ανάλυση των συστατικών των κινδύνων ΠΣ πραγματοποιείται στην παράγραφο 2.4.2, ενώ στο κεφάλαιο 7 αναπτύσσεται μοντέλο προσέγγισης των κινδύνων παραβιάσεων ασφαλείας του οποίου οι βασικές δομές στηρίζονται στην ανάλυση της συγκεκριμένης ενότητας.

Όπως αναφέρθηκε στην ενότητα 2.3, οι κίνδυνοι ΠΣ περιλαμβάνονται ταυτόχρονα στις κατηγορίες των οργανικών και ανόργανων κινδύνων όπως αυτό αποτυπώνεται στην Εικόνα 3. Μέρος των κινδύνων ΠΣ συνδέεται άμεσα με τις οργανικές δραστηριότητες ενός οργανισμού. Η ανάληψη μεγάλων επενδυτικών προγραμμάτων ενίσχυσης των ΠΣ ενός οργανισμού και του

επιπέδου σύγχρονων τεχνολογιών που χρησιμοποιεί, οδηγούν σε συμμετρικούς επιχειρηματικούς κινδύνους οι οποίοι δύναται να παράγουν θετικά και αρνητικά αποτελέσματα. Υπέρβαση προϋπολογισμών, καθυστέρηση υλοποίησης, μειωμένη ανταποδοτικότητα, άρνηση υιοθέτησης από τους εργαζομένους είναι ορισμένες καταστάσεις οργανικών κινδύνων ΠΣ. Το μέρος των κινδύνων ΠΣ που εντάσσεται στην οργανική κατηγορία των εταιρικών κινδύνων, όπως αναφέρθηκε και προγενέστερα, δεν αποτελεί άμεσο αντικείμενο μελέτης της παρούσας διατριβής.

Οι κίνδυνοι ΠΣ, που δεν χαρακτηρίζονται ως οργανικοί, τοποθετούνται στην κατηγορία των ανόργανων λειτουργικών κινδύνων. Αναλυτικότερα, εντάσσονται στους ενδογενείς κινδύνους που προέρχονται είτε από το ανθρώπινο στοιχείο ή από τα συστήματα που χρησιμοποιεί ένας οργανισμός. Διάφοροι ερευνητές όπως οι Dhillon et. al. [**34**] και Willcocks et. al. [**35**] έχουν επισημάνει την διαφοροποίηση των κινδύνων που προέρχονται από την ανάληψη ενός επενδυτικού προγράμματος σε ΠΣ και τους κινδύνους από την χρήση τους. Το μέγεθος του κινδύνου απώλειας κεφαλαίων για έναν οργανισμό από μία άστοχη ανάληψη ενός επενδυτικού προγράμματος σε ΠΣ είναι σε ευθεία αναλογία με το μέγεθος, την πολυπλοκότητα και το εύρος εφαρμογής του στον οργανισμό.

Αντιθέτως, οι κίνδυνοι που αναδύονται, αφού γίνει υλοποίηση ενός νέου ΠΣ, δεν εξαρτώνται από τους προαναφερόμενους παράγοντες αλλά είναι σε μεγάλο βαθμό κοινοί για όλα τα ΠΣ. Για αυτό τον λόγο οι κίνδυνοι αυτοί ονομάζονται συστημικοί κίνδυνοι (systemic risks) και εντάσσονται στους ενδογενείς λειτουργικούς κινδύνους που περιλαμβάνουν τους κινδύνους που ενσωματώνονται στην χρήση των συστημάτων ενός οργανισμού. Οι κίνδυνοι αυτοί είναι ασύμμετροι με την έννοια ότι προκαλούν μόνο παθητικό και βασικός στόχος για έναν οργανισμό είναι ο προσδιορισμός, η ποσοτικοποίηση και η αντιμετώπιση τους παρά η υιοθέτηση τους. Όπως αποτυπώνεται συνδυαστικά στην Εικόνα 2 και στην Εικόνα 3, οι κίνδυνοι παραβιάσεων ασφαλείας μπορούν να θεωρηθούν ως μέρος των λειτουργικών ενδογενών κινδύνων προκαλούμενων είτε από το ανθρώπινο στοιχείο είτε από τα συστήματα που λειτουργούν μέσα σε έναν οργανισμό. Μεγάλο μέρος της ερευνητικής προσπάθειας της παρούσας διατριβής αφιερώνεται στην ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας. Στο κεφάλαιο 4 γίνεται εκτενής προσέγγιση της έννοιας παραβίασης ασφαλείας σε συνάρτηση με την ένταξη της στο ευρύτερο πλαίσιο των εταιρικών κινδύνων.



Εικόνα 3: Κίνδυνοι Πληροφοριακών Συστημάτων

2.4.2 Στοιχεία κινδύνων Πληροφοριακών Συστημάτων και προσδιορισμός

2.4.2.1 Ευπάθειες ΠΣ

Η έννοια της ευπάθειας (vulnerability) είναι το βασικότερο στοιχείο που καθορίζει τους κινδύνους που αντιμετωπίζει ένα ΠΣ και ορίζεται ως ένα ελάττωμα ή αδυναμία το οποίο δύναται να έγκειται στον σχεδιασμού του ΠΣ, στην εφαρμογή και στις διαδικασίες ασφαλείας και στα αντίμετρα που αποσκοπούν στην διαφύλαξη ενός ενεργητικού στοιχείου ΠΣ από εν δυνάμει απειλές. Οι ευπάθειες προκαλούν έκθεση ενός οργανισμού σε πιθανές απώλειες που δύναται να προκληθούν από μία απειλή όταν εκμεταλλευόμενη μία αδυναμία είτε εσκεμμένα, είτε ακούσια καταφέρει να επιτύχει μία παραβίαση ασφαλείας. Οι ευπάθειες γενικότερα μπορούν να χαρακτηριστούν και ως μία ιδιότητα του σχεδιασμού, της φυσικής εφαρμογής και των εσωτερικών ελέγχων ενός ΠΣ και είναι ανεξάρτητες από τις απώλειες που μπορούν να επιφέρουν. Μία ευπάθεια εξατομικευμένα δεν μπορεί να προκαλέσει απώλειες σε ένα σύστημα καθώς είναι απαραίτητη η ανεξάρτητη ύπαρξη μίας απειλής ικανής να εκμεταλλευτεί την συγκεκριμένη ευπάθεια.

Μία ερμηνεία του συγκεκριμένου όρου τύπου «ελέγχου πρόσβασης» (access control) αναφέρεται στις ευπάθειες ως ελαττώματα τα οποία επιτρέπουν σε έναν εισβολέα να παρακάμψει τους ελέγχους ασφαλείας ενός συστήματος [**36**]. Βασικός διαχωρισμός των ευπαθειών είναι σε κρίσιμες και μη κρίσιμες με βάση τον βαθμό ευαισθησίας των δεδομένων που μπορεί να οδηγήσουν σε έκθεση και το επίπεδο ελέγχου που δίνουν στον επιτιθέμενο. Μία κρίσιμη ευπάθεια μπορεί να οδηγήσει εξαιρετικά ευαίσθητα δεδομένα σε διαρροή με σοβαρά συνεπακόλουθα για τον οργανισμό που προσβλήθηκε από την επίθεση.

Είναι σημαντικό να διευκρινιστεί πως όταν η ίδια ευπάθεια συνδυάζεται με διαφορετικά είδη απειλών συνίσταται διαφορετικοί τύποι κινδύνων. Κάθε δυνατός συνδυασμός ευπάθειας και απειλής έχει ξεχωριστή οντότητα και χρήζει ιδιαίτερης μεταχείρισης. Επίσης πρέπει να αναφερθεί πως κάθε ξεχωριστή ευπάθεια είναι εξ ορισμού απόλυτα ανεξάρτητη από το οποιοδήποτε είδος απειλής και η ύπαρξη της και μόνο δεν μπορεί να προκαλέσει ζημιά σε ένα σύστημα. Οι κύριες μέθοδοι για τον προσδιορισμό των ευπαθειών ενός συστήματος είναι οι εξής:

(α) Πηγές που περιέχουν καταχωρημένες ευπάθειες ταξινομημένες με βάση κάποια μεθοδολογία. Οι μεγαλύτερες πηγές αυτού του είδους είναι ανοικτού κώδικα βάσεις δεδομένων ευπαθειών όπως είναι η Open Source Vulnerability Database (OSVDB) για την οποία υπάρχει ανάλυση στο κεφάλαιο 6.

(β) Χρήση μεθόδων ελέγχου του επιπέδου ασφαλείας που παρουσιάζει ένα σύστημα σε μία δεδομένη χρονική στιγμή. Παραδείγματα μεθόδων αποτελούν οι επονομαζόμενες ως Penetration Testing και Automated Vulnerability Scanning.

(γ) Χρήση μεθόδων δημιουργίας καταλόγου των απαιτήσεων ενός συστήματος σε θέματα ασφαλείας.

Οι μέθοδοι (β) και (γ) αποκαλούνται και προνοητικές μέθοδοι (proactive methods) καθώς στοχεύουν στην εύρεση εν δυνάμει ευπαθειών σε ένα σύστημα πριν την ανακάλυψη και κακόβουλη εκμετάλλευση τους από μία πηγή απειλής.

Βασικό θέμα σχετικά με τις ευπάθειες αφορά τον τρόπο ταξινόμηση τους. Το συγκεκριμένο θέμα είναι ακόμα αντικείμενο αντιπαράθεσης ανάμεσα σε διάφορους μελετητές είτε από τον επιχειρησιακό, είτε από τον ακαδημαϊκό κλάδο. Η περισσότερο αποδεκτή ταξινόμηση έχει γίνει από το National Institute of Standards and Technology (NIST) μέσω του National Vulnerability

Database (NVD) [**37**]. Η NVD είναι μία ανοικτή βάση δεδομένων καταγραμμένων ευπαθειών την οποία διαχειρίζεται ο NIST όπου η ταξινόμηση των ευπαθειών πραγματοποιείται με κριτήριο την αιτία. Η δεύτερη επίσης διαδεδομένη προσέγγιση ταξινόμησης προέρχεται από το Common Vulnerability Scoring System (CVSS) το οποίο είναι μία ανοικτή βάση, μέσω της οποίας καταγράφονται τα χαρακτηριστικά των ευπαθειών, τα οποία ταξινομούνται με βάση την σοβαρότητα (severity) που εμφανίζουν [**38**]. Η βάση αυτή είναι υπό τον διαχειριστικό έλεγχο του Forum of Incident Reports and Security Teams (FIRST) [**39**].

Η βάση CVSS ανήκει στην γενικότερη ομάδα «συστημάτων βαθμολόγησης ευπαθειών» (vulnerability scoring systems). Τα συστήματα αυτά κατά κύριο λόγο υπολογίζουν την σπουδαιότητα και τον συνολικό κίνδυνο μίας ευπάθειας και με βάση τα αποτελέσματα προσδίδουν σε κάθε ευπάθεια μία συγκεκριμένη βαθμολογία. Στην συνέχεια, με κριτήριο την βαθμολογία αυτή, πραγματοποιείται η ταξινόμηση τους. Εκτός του CVSS, άλλα σημαντικά μοντέλα βαθμολόγησης ευπαθειών είναι το Vulnerability Scoring από τον CERT, το Threat Scoring System από την Microsoft και το Threat Scoring System από την Symantec.

Η βάσεις NVD και OSVDB, που αναφέρθηκαν παραπάνω, είναι οι δύο ανοικτές βάσεις που επιλέχτηκαν από την παρούσα ερευνητική προσπάθεια προκειμένου για την άντληση δεδομένων ευπαθειών. Τα δεδομένα αυτά χρησιμοποιήθηκαν για την ανάλυση και ποσοτικοποίηση του επιπέδου ασφαλείας ενός ΠΣ όπως αναλύεται στο κεφάλαιο 6.

2.4.2.2 Πηγές απειλών ΠΣ

Το επόμενο σημαντικό συστατικό των κινδύνων ΠΣ είναι αυτό των πηγών απειλών (threat-sources) το οποίο ορίζεται ως κάθε γεγονός ή μέθοδος που έχει την δυνατότητα να επιφέρει αρνητικές επιπτώσεις σε ένα στοιχείο ενεργητικού ΠΣ είτε ακούσια, είτε εκούσια. Οι πηγές απειλών διαχωρίζονται σε τρεις κατηγορίες με κριτήριο την προέλευση τους: (α) Απειλές προερχόμενες από το φυσικό στοιχείο, (β) απειλές προερχόμενες από την λειτουργική δομή του οργανισμού και (γ) απειλές προερχόμενες από το ανθρώπινο στοιχείο προερχόμενο είτε από το εσωτερικό, είτε από το εξωτερικό περιβάλλον του οργανισμού.

Μία οποιαδήποτε απειλή χωρίς την ύπαρξη μίας ευπάθειας, την οποία δύναται να εκμεταλλευτεί, δεν μπορεί να προκαλέσει ζημιά σε ένα σύστημα το οποίο ισχύει και αντιστρόφως για τις ευπάθειες όπως αναφέρθηκε στην προηγούμενη ενότητα. Συνεπώς, μία πολύ σημαντική

ιδιότητα των απειλών είναι η ανεξαρτησία τους από την φυσική ύπαρξη των ΠΣ. Επίσης, η ίδια απειλή όταν εκμεταλλευθεί μία διαφορετική ευπάθεια δημιουργείται ένας διαφορετικός κίνδυνος ΠΣ.

2.4.2.3 Έλεγχοι ασφαλείας ΠΣ

Οι έλεγχοι ασφαλείας (security controls) αποτελούν το τρίτο συστατικό των κινδύνων ΠΣ. Αποκαλούνται επίσης και ως αντίμετρα (countermeasures), διασφαλίσεις (safeguards) ή απλά έλεγχοι και περιλαμβάνουν διαδικασίες, πολιτικές, υλικό, εξοπλισμό ασφαλείας και συστήματα προστασίας τα οποία στο σύνολο τους έχουν ως πρωταρχικό στόχο την μείωση ή εξάλειψη των ευπαθειών και απειλών ώστε να μετριαστούν οι κίνδυνοι ΠΣ.

Σε γενικό επίπεδο, ο βασικός στόχος των αντίμετρων ασφαλείας είναι η διαφύλαξη του επιπέδου εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, που αναλύθηκαν στην ενότητα 2.4.1, και τα οποία στο σύνολο τους διασφαλίζουν την δυνατότητα ενός οργανισμού στην εκπλήρωση των στρατηγικών του στόχων. Καθώς η πρωταρχική λειτουργία τους είναι η μετρίαση κινδύνων που προσβάλουν την αποστολή ενός οργανισμού, καλούνται επίσης δεξιότητες ασφαλείας ουσιώδεις για την εταιρική αποστολή.

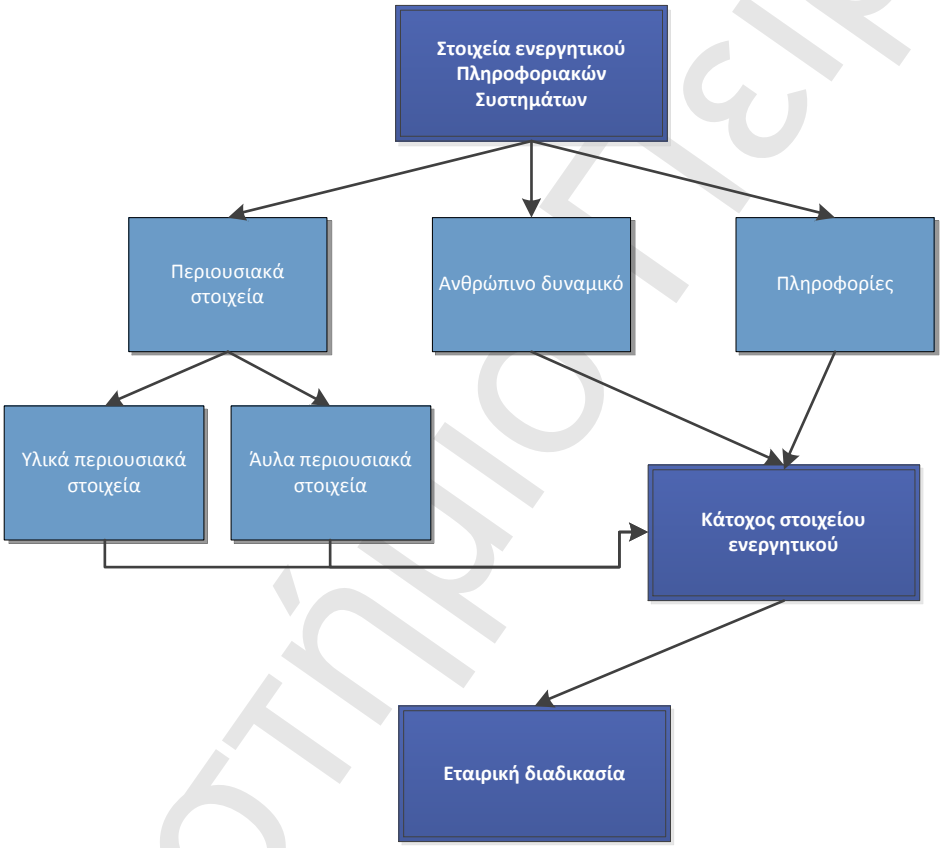
Μπορούμε να διακρίνουμε τρεις βασικούς σκοπούς για τους ελέγχους ασφαλείας: (α) Μείωση έκθεσης μέσω περιορισμού απωλειών, (β) μείωση των κινδύνων μέσω περιορισμού της πιθανότητας επίθεσης και (γ) μείωση των κινδύνων μέσω περιορισμού της επίπτωσης μιας επίθεσης. Οι έλεγχοι μπορούν να διαχωριστούν σε δύο κατηγορίες: Τεχνικοί έλεγχοι και μη τεχνικοί έλεγχοι με τους τελευταίους να κατηγοριοποιούνται περαιτέρω σε διαχειριστικούς ελέγχους και σε λειτουργικούς ελέγχους.

2.4.2.4 Στοιχεία ενεργητικού ΠΣ

Τα στοιχεία ενεργητικού ενός οργανισμού, που αποτελούνται από δεδομένα, υλικό, λογισμικό και προσωπικό και συνθέτουν ένα σύστημα πληροφόρησης ονομάζονται στοιχεία ενεργητικού ΠΣ. Γενικά μπορούν να κατηγοριοποιηθούν ως εξής: Ανθρώπινο δυναμικό, περιουσιακά και πληροφοριακά στοιχεία. Τα περιουσιακά στοιχεία διαχωρίζονται περαιτέρω σε υλικά όπως λογισμικό και εγκαταστάσεις και άυλα όπως είναι η τεχνογνωσία. Η κατηγορία των

πληροφοριακών στοιχείων περιλαμβάνει βάσεις δεδομένων, κώδικα λογισμικού, εγγραφές δεδομένων και εμπορικά μυστικά.

Όπως αποτυπώνεται στην Εικόνα 4 για κάθε στοιχείο ενεργητικού σε ένα ΠΣ, ορίζεται ένας κάτοχος. Πρέπει να διευκρινιστεί ότι δεν υφίσταται στοιχείο ενεργητικού που να μην έχει έναν άμεσο ή έμμεσο κάτοχο ο οποίος είναι υπεύθυνος για την λειτουργία του στοιχείου, την ασφάλεια του και την επιτέλεση της εταιρικής διαδικασίας με την οποία συνδέεται.



Εικόνα 4: Στοιχεία ενεργητικού Πληροφοριακών Συστημάτων

2.4.3 Τεχνικοί παράγοντες κινδύνου

Η έννοια του τεχνικού παράγοντα κινδύνου χρήζει ιδιαίτερης σημασίας για την παρούσα διατριβή. Προκειμένου για τις ανάγκες της έρευνας ορίζουμε ως τεχνικό παράγοντα κινδύνου για ένα ΠΣ ως κάθε διακριτό στοιχείο ενός συστήματος η χρήση του οποίου μπορεί να επηρεάσει το επίπεδο ασφάλειας [**40**]. Αποτυπώνοντας το διαφορετικά, κάθε στοιχείο ενός συστήματος με τεχνική υπόσταση, το οποίο μπορεί να εκθέσει σε κίνδυνο τα επίπεδα εμπιστοσύνης, ακεραιότητας

και διαθεσιμότητας των ευαίσθητων πληροφοριών που χειρίζεται ένα σύστημα, ορίζεται ως τεχνικός παράγοντας κινδύνου. Η τεχνική υπόσταση που αναφέρεται παραπάνω περιλαμβάνει μόνο τα στοιχεία λογισμικού όπως π.χ. λειτουργικά συστήματα, βάσεις δεδομένων, εμπορικά πακέτα διαχωρίζοντας με αυτόν τον τρόπο την συγκεκριμένη έννοια από τα στοιχεία υλικού που περιλαμβάνονται σε ένα ΠΣ. Συνεπώς, τεχνικοί παράγοντες κινδύνου που σχετίζονται με το υλικό όπως π.χ. η αστοχία υλικού είναι εκτός του πεδίου ενδιαφέροντος της παρούσας διατριβής.

Ο παραπάνω ορισμός επικέντρωσε το σύνολο της ερευνητικής προσπάθειας κατά κύριο λόγο σε επίπεδο παράγοντα κινδύνου (risk factor-specific) σε αντίθεση με τον κύριο όγκο προηγούμενων, συναφών μελετών που είναι επικεντρωμένες σε επίπεδο ευπάθειας (vulnerability-specific). Επιπρόσθετα, η υιοθέτηση της παραπάνω μεθοδολογίας, οδήγησε στα παρακάτω πλεονεκτήματα:

- Αποφυγή του διαχωρισμού των τεχνικών παραγόντων κινδύνου με βάση την ταξινόμηση των ευπαθειών που διαπιστώνεται ότι εμφανίζονται σε ένα ΠΣ. Ο κυριότερος λόγος προέρχεται από την έλλειψη ευρέως αποδεκτής μεθοδολογίας ταξινόμησης μεταξύ των ερευνητών όπως αναφέρεται στο [**41**]. Όπως αναφέρθηκε στο 2.4.2.1, οι μεθοδολογίες ταξινόμησης που έχουν μέχρι σήμερα υιοθετηθεί βασίζονται είτε στην αιτία (cause) της ευπάθειας, είτε στην σοβαρότητα (severity) της ευπάθειας και δεν υπάρχει ακόμα γενική συμφωνία ανάμεσα στην κοινότητα των μελετητών για μία κοινή μεθοδολογία ταξινόμησης.

- Ο τεράστιος όγκος των ευπαθειών, που μπορεί να έχει ένα ΠΣ, οδηγεί αναπόφευκτα μία ανάλυση κινδύνων επικεντρωμένη σε επίπεδο ευπάθειας να είναι εξαιρετικά χρονοβόρα και πολυδάπανη.

- Η στάθμιση των παραγόντων κινδύνου, όταν η ανάλυση είναι επικεντρωμένη σε επίπεδο παράγοντα κινδύνου, είναι εφικτή με μεγαλύτερη ακρίβεια και αντικειμενικότητα όπως προκύπτει από την ανάλυση που γίνεται στο κεφάλαιο 6.

- Η μέτρηση του επιπέδου ασφαλείας ανά το χρόνο είναι περισσότερο εφικτή και μπορεί να αποτυπωθεί με μεγαλύτερη ακρίβεια από ένα μοντέλο μέτρησης όπως επίσης αναλύεται στο κεφάλαιο 6.

2.4.4 Ταξινόμηση των οργανισμών υπό έκθεση σε κινδύνους Πληροφοριακών Συστημάτων

Προκειμένου για τις ανάγκες της παρούσας διατριβής υιοθετήθηκαν ορισμένες κατηγοριοποιήσεις των οργανισμών που είναι αντικείμενο έκθεσης σε κινδύνους ΠΣ. Μία γενική ταξινόμηση των οργανισμών είναι μεταξύ παραδοσιακών οργανισμών και οργανισμών που ασχολούνται με το ηλεκτρονικό εμπόριο. Οι οργανισμοί που ανήκουν στην πρώτη κατηγορία αποκαλούνται επίσης οργανισμοί τύπου "τούβλα και λάσπη" (bricks and mortar firms) και θεωρητικά έχουν μικρότερη ευαισθησία σε κινδύνους ΠΣ σε σύγκριση με τις εταιρίες της δεύτερης κατηγορίας.

Οι οργανισμοί που ανήκουν στην δεύτερη κατηγορία μπορούν να διαχωριστούν περαιτέρω σε τύπου "κλικς και λάσπη" (clicks and mortar firms) και στους οργανισμούς που εξαρτώνται αποκλειστικά από το διαδίκτυο. Η πρώτη κατηγορία περιλαμβάνει οργανισμούς οι οποίοι χρησιμοποιούν το διαδίκτυο για την επιχειρηματική λειτουργία τους σε συμπληρωματικό επίπεδο στην παραδοσιακή λειτουργία τους. Η δεύτερη κατηγορία περιλαμβάνει τις λεγόμενες εταιρίες διαδικτύου (internet firms or net firms or pure play firms) οι οποίες επιτελούν το σύνολο της επιχειρηματικής τους λειτουργίας ηλεκτρονικά.

Οι οργανισμοί οι οποίοι έχουν ως οργανικό αντικείμενο το ηλεκτρονικό εμπόριο, και ιδιαίτερα αυτοί που ασχολούνται αποκλειστικά με αυτό, αναμένεται οι απώλειες που δύναται να επωμισθούν από κινδύνους ΠΣ να είναι σοβαρότερες κυρίως στο μέρος των έμμεσων επιπτώσεων που προέρχονται από νομικούς κινδύνους και κινδύνους φήμης και πελατείας. Επίσης, η αναγκαιότητα πλήρους και αντικειμενικής ποσοτικοποίησης των αναμενόμενων οικονομικών επιπτώσεων των κινδύνων ΠΣ είναι πολύ μεγαλύτερη για τις εταιρίες αυτού του τύπου.

Μία άλλη ταξινόμηση που υιοθετήθηκε είναι μεταξύ των οργανισμών που ανήκουν στο τομέα τεχνολογίας και των οργανισμών που ανήκουν σε όλους τους υπόλοιπους τομείς. Η ταξινόμηση αυτή είναι ευρύτερη από την προηγούμενη αλλά η θεωρητική παραδοχή, κατά την οποία οι οργανισμοί τεχνολογίας αναμένονται να δεχθούν σοβαρότερες επιπτώσεις από κινδύνους ΠΣ σε σχέση με έναν οργανισμό άλλου τύπου, παραμένει ίδια.

Στην έρευνα που διεξήχθη αναλύθηκαν προγενέστερες εμπειρικές μελέτες οι οποίες σύγκριναν το επίπεδο των επιπτώσεων ανά κατηγορία οργανισμών. Τα αποτελέσματα που προήλθαν από τις

μελέτες αυτές συγκρίθηκαν με αντίστοιχη εμπειρική μελέτη που υλοποιήθηκε στα πλαίσια της παρούσας. Το επίπεδο της επίπτωσης των κινδύνων παραβιάσεων ασφαλείας, όπως αναλύεται στο κεφάλαιο 5, λαμβάνει ως μία από τις κύριες παραμέτρους του, τον τύπο του οργανισμού που εκτίθεται. Επιπρόσθετα, ο τύπος του οργανισμού υιοθετείται ως μία από τις σημαντικότερες παραμέτρους στην μοντελοποίηση των κινδύνων παραβιάσεων ασφαλείας όπως αναλύεται στο κεφάλαιο 7.

3 Διαχείριση κινδύνων Πληροφοριακών Συστημάτων

3.1 Εισαγωγή

Η βασική έννοια της διαχείρισης κινδύνων πληροφοριακών συστημάτων (ΔΚΠΣ) ορίζεται ως η διαδικασία η οποία έχει ως βασικό στόχο την προστασία των στοιχείων ενεργητικού ΠΣ από όλες τις απειλές, που πηγάζουν από το εσωτερικό και το εξωτερικό περιβάλλον ενός οργανισμού, ούτως ώστε το κόστος των απωλειών από την πιθανή υλοποίηση των απειλών να ελαχιστοποιείται [**42**]. Προστατεύοντας τα στοιχεία ενεργητικού ΠΣ ενός οργανισμού, την ίδια στιγμή προστατεύεται η αποστολή του οργανισμού από του κινδύνους σχετιζόμενους με τα ΠΣ. Ουσιαστικά ο πρωτεύον στόχος ενός συστήματος ΔΚΠΣ είναι η προστασία της ίδιας της αποστολής του οργανισμού και δευτερευόντως τα σχετικά στοιχεία ενεργητικού. Η αποστολή του οργανισμού προστατεύεται με την παράλληλη διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητων των δεδομένων που διαχειρίζονται τα ΠΣ που επιτελούν τους σκοπούς της αποστολής του. Συνεπώς, οι βασικοί στόχοι της ΔΚΠΣ ενός οργανισμού είναι παράλληλα οι θεμελιώδεις αρχές της ασφάλειας πληροφόρησης όπως περιγράφτηκαν στο 2.4.1.

Σύμφωνα με το [**43**] ο προαναφερόμενος στόχος υλοποιείται μέσω της επιλογής και υλοποίησης του αποδοτικότερου συνδυασμού από ελέγχους ασφαλείας. Στον οδηγό της NIST [**30**] για την διαχείριση κινδύνων ΠΣ αναφέρεται ότι η σημασία ενός ΠΣ για έναν οργανισμό μπορεί να αξιολογηθεί από τον βαθμό που εξαρτάται η επίτευξη των στρατηγικών σκοπών από αυτό. Συνεπώς, η δαπάνες για την ασφάλεια ενός ΠΣ είναι σε άμεση συνάρτηση με την σημαντικότητα που έχει το συγκεκριμένο ΠΣ για τον ίδιο τον οργανισμό. Η αντικειμενική αξιολόγηση της σημαντικότητας ενός ΠΣ μπορεί να οδηγήσει στην εξισορρόπηση μεταξύ των λειτουργικών και οικονομικών δαπανών από την υλοποίηση των ελέγχων ασφαλείας και της ενίσχυσης της δυνατότητας επίτευξης της αποστολής του οργανισμού.

Επομένως, ένα από τα ζητούμενα ενός συστήματος ΔΚΠΣ είναι η οργάνωση και ταξινόμηση με βάση την σημαντικότητα που ενέχουν για έναν οργανισμό τα στοιχεία ενεργητικού ΠΣ. Παρεμφερής στόχος είναι ο ορισμός των εταιρικών διαδικασιών κρίσιμης σημασίας και ταξινόμηση τους. Επίσης, βασικό ζητούμενο είναι η οργάνωση των περιορισμένων πόρων που έχει στην διάθεση του ένας οργανισμός προκειμένου για την επίτευξη του βέλτιστου επιπέδου

ασφαλείας. Τέλος, η κατάλληλη οργάνωση ενός συστήματος ΔΚΠΣ πρέπει να οδηγεί στην συμμόρφωση με τα κανονιστικά πλαίσια. Η επίτευξη του συνόλου των επιμέρους προαναφερόμενων στόχων οδηγεί στον βασικό σκοπό της ΔΚΠΣ που είναι η διαφύλαξη της δυνατότητας ενός οργανισμού προς την επίτευξη της εταιρικής αποστολής.

Η διοίκηση ενός οργανισμού πρέπει να έχει την κατάλληλη πληροφόρηση, μέσα από το σύστημα διαχείρισης κινδύνων, ώστε να είναι σε θέση να απαντήσει σε δύο καίρια ερωτήματα: (α) Πόσα κεφάλαια πρέπει να αφιερώσει στα ΠΣ και την ασφάλεια τους. (β) Σε ποια συγκεκριμένα σημεία πρέπει τα κεφάλαια να τοποθετηθούν. Η αντικειμενική αντιμετώπιση αυτών των ερωτημάτων αποσκοπεί τελικώς στην επίτευξη της βέλτιστης αναλογίας μεταξύ του κόστους και της ωφέλειας από ένα σύστημα ΔΚΠΣ.

Από τα παραπάνω προκύπτει πως η οργάνωση ενός αποδοτικού συστήματος ΔΚΠΣ δεν είναι ένα θέμα που αφορά αποκλειστικά τους ειδικούς πληροφορικής ενός οργανισμού. Οι Birch et. al. [**44**] από πολύ νωρίς ανέφεραν πως ο βασικός στόχος της ανάλυσης των κινδύνων που αντιμετωπίζει ένα ΠΣ είναι η παροχή της απαραίτητης πληροφόρησης, στην διοίκηση ενός οργανισμού, ώστε να λάβει τις κατάλληλες αποφάσεις σχετικά με επενδύσεις σε ΠΣ και στην διαχείριση της ασφάλειας τους.

Επιπλέον, η ανώτερη διοίκηση χρησιμοποιεί την προαναφερόμενη πληροφόρηση προκειμένου να προσδιορίσει το συνολικό εταιρικό κίνδυνο ενός οργανισμού, στοιχείο το οποίο αποτελεί πλέον πολύ σημαντικό μέγεθος για την στρατηγική διαχείριση του οργανισμού. Η συσχέτιση του συνολικού εταιρικού κινδύνου με τους κινδύνους ΠΣ αυξάνεται διαρκώς τα τελευταία χρόνια και το γεγονός αυτό καθιστά τους κινδύνους ΠΣ μία από σημαντικότερες ή - για συγκεκριμένες κατηγορίες οργανισμών – την σημαντικότερη κατηγορία κινδύνων που καλούνται να αντιμετωπίσουν.

Ένα σύστημα ΔΚΠΣ μπορεί να χαρακτηριστεί ως ένας συνεχής και αδιάκοπος κύκλος διαδικασιών εφαρμογής πολιτικών. Κατά την εφαρμογή του συστήματος, εναλλακτικές στρατηγικές προς την αντιμετώπιση των κινδύνων εξετάζονται προκειμένου να ληφθούν αποφάσεις σχετικά με τα ανεκτά επίπεδα κινδύνων. Τα βασικά συστατικά αυτού του κύκλου διαδικασιών είναι σταθερά αλλά οι διαδικασίες, που επιτελούνται στα πλαίσια του, δεν πρέπει να είναι μηχανικές και στατικές αλλά να χαρακτηρίζονται από ευελιξία και να προσαρμόζονται

γρήγορα και αποδοτικά στις αλλαγές που πραγματοποιούνται αδιάκοπα στο εσωτερικό και εξωτερικό περιβάλλον ενός οργανισμού [**45**]. Οι δυναμικές του σύγχρονου παγκοσμιοποιημένου περιβάλλοντος, στο οποίο οι οργανισμοί καλούνται να δραστηριοποιηθούν, μπορούν να προκαλέσουν αναπάντεχες και σοβαρές αλλαγές οι οποίες δύναται, ένα απόλυτα δομημένο, σταθερό και αυστηρά οριοθετημένο σύστημα ΔΚΠΣ, να το οδηγήσουν σε μερική ή ακόμα και πλήρη απαξίωση. Επομένως, είναι σημαντικό ένα σύστημα ΔΚΠΣ να εξελίσσεται διαρκώς, παράλληλα με την εξέλιξη του εσωτερικού και εξωτερικού περιβάλλοντος του οργανισμού τον οποίο εξυπηρετεί, ώστε να έχει την δυνατότητα να ανταπεξέλθει αποδοτικά σε κάθε κατάσταση.

Τέλος, πρέπει επίσης να αναφερθεί πως οι διαδικασίες ΔΚΠΣ είναι ένα σχετικά πρόσφατο τμήμα της ευρύτερης διαχείρισης εταιρικών κινδύνων και ακόμα δεν παρουσιάζει ευρεία υιοθέτηση. Συγκεκριμένα, στην πρόσφατη ετήσια μελέτη από την Ernst & Young για την ασφάλεια ΠΣ [**6**], προκύπτει πως το 44% των οργανισμών διεθνώς δεν έχει ακόμα εγκαταστήσει σύστημα ΔΚΠΣ. Επίσης, μόνο το 25% των οργανισμών δηλώνει πως έχει εγκατεστημένο σύστημα ΔΚΠΣ για διάστημα άνω των τριών ετών. Τα μεγέθη αυτά καταδεικνύουν ότι η διαχείριση κινδύνων ΠΣ βρίσκεται ακόμα σε πρώιμο στάδιο ανάπτυξης και σίγουρα πολλά πρέπει να γίνουν προκειμένου οι οργανισμοί να διακρίνουν τα οφέλη από την χρήση της. Όπως αποτυπώνεται στην επόμενη ενότητα, το στάδιο της εκτίμησης κινδύνων είναι το βασικότερο στάδιο του συνόλου της διαδικασίας και σίγουρα η έλλειψη ποσοτικών μεθόδων με ικανοποιητική ακρίβεια αποτελούν έναν από τους σημαντικότερους παράγοντες που οδηγούν στην ανασταλτικότατα των οργανισμών στην υιοθέτηση επίσημων μεθόδων διαχείρισης των κινδύνων ΠΣ.

3.2 Τα στάδια της διαδικασίας Διαχείρισης Κινδύνων Πληροφοριακών Συστημάτων

Η ενότητα αυτή είναι αφιερωμένη στην ανάλυση των σταδίων που απαρτίζουν ένα σύστημα ΔΚΠΣ. Ένας από τους πρώτους που πρότεινε την διάρθρωση ενός τέτοιου συστήματος ήταν ο Boehm [**46**]. Η μεθοδολογία του περιελάμβανε αρχικώς δύο βασικά στάδια: (α) Εκτίμηση κινδύνων (risk assessment) και (β) αντιμετώπιση κινδύνων (risk control). Το πρώτο στάδιο απαρτιζόταν από τρία υπό-στάδια: (α) Προσδιορισμός των κινδύνων (risk identification), (β) ανάλυση των κινδύνων (risk analysis) και (γ) ιεράρχηση των κινδύνων (risk prioritization). Η

συγκεκριμένη διαδικασία ΔΚΠΣ, βασίστηκε στις υπάρχουσες διαδικασίες αντιμετώπισης κινδύνων που είχαν εφαρμοστεί κυρίως για τους οικονομικούς κινδύνους από τους χρηματοπιστωτικούς οργανισμούς.

Σε μελέτες που ακολούθησαν, από ακαδημαϊκούς και κυβερνητικούς φορείς, ορισμένες διαδικασίες, που περιλαμβάνονταν στα βασικά προτεινόμενα στάδια, μετατράπηκαν σε βασικά στοιχεία του συστήματος προκειμένου να αποτυπωθεί η αυξανόμενη σπουδαιότητα τους και να προσαρμοστεί η μεθοδολογία στις εξελισσόμενες απαιτήσεις της διαχείρισης των κινδύνων ΠΣ. Προς αυτή την κατεύθυνση οι διαδικασίες προσδιορισμού των κινδύνων ΠΣ καθώς και της αξιολόγησης – αποτίμησης μετατράπηκαν σε βασικά στάδια της διαδικασίας.

Η διαδικασία που προτείνει ο NIST στην ειδική έκδοση 800-39 [**47**] για την διαχείριση κινδύνων ΠΣ περιλαμβάνει τέσσερα πλέον στάδια. Στην προγενέστερη ειδική έκδοση 800-30 του ίδιου φορέα [**30**], το πλαίσιο διαχείρισης κινδύνων περιείχε τρία στάδια με το στάδιο της εκτίμησης κινδύνων να ενσωματώνει τις διαδικασίες προσδιορισμού. Στην ειδική έκδοση 800-39 το πρώτο στάδιο αναφέρεται ως «πλαισίωση των κινδύνων» (framing risk) και αφορά κυρίως τον προσδιορισμό των συγκεκριμένων κινδύνων που αντιμετωπίζει ένας οργανισμός, την αποτύπωση της συμπεριφοράς του οργανισμού απέναντι στους κινδύνους και την θέσπιση στρατηγικών και στόχων για το πρόγραμμα αντιμετώπισης που προτίθεται να υλοποιήσει. Το δεύτερο στάδιο ονομάζεται «εκτίμηση κινδύνων» (risk assessment) και αφορά την διαδικασία αξιολόγησης και ταξινόμησης των κινδύνων. Στην συγκεκριμένη έκδοση το στάδιο αυτό προτείνεται πλέον να είναι διακριτό από την αρχική διαδικασία του προσδιορισμού κινδύνων. Το τρίτο στάδιο αναφέρεται ως «ανταπόκριση στους κινδύνους» (risk response) και περιλαμβάνει την ανάλυση, ταξινόμηση, επιλογή και εφαρμογή των προτεινόμενων μέτρων ελέγχου ασφαλείας. Το τελευταίο στάδιο αναφέρεται ως «παρακολούθηση κινδύνων» (risk monitoring) και περιλαμβάνει την δημιουργία ελεγκτικού μηχανισμού για την παρακολούθηση της εφαρμογής των επιλεγμένων μέτρων ελέγχου ασφαλείας, της αποδοτικότητας τους και την αξιολόγηση των αλλαγών στο εσωτερικό και εξωτερικό περιβάλλον του οργανισμού.

Το διεθνές ινστιτούτο IT Governance και ο διεθνής οργανισμός ISACA έχουν δημιουργήσει ένα πλαίσιο διαδικασιών και πρακτικών προκειμένου για την διαχείριση των κινδύνων ΠΣ με μία ολοκληρωμένη μεθοδολογία εφαρμόσιμη καθολικά στους οργανισμούς ανεξάρτητα της χώρας προέλευσης και του κλάδου δραστηριότητας [**48**], [**49**]. Το πλαίσιο αυτό περιλαμβάνει τις

μεθοδολογίες COBIT και Risk IT και πλέον έχει παγκόσμια ανταπόκριση σε περισσότερες από 160 χώρες. Το πλαίσιο διαχείρισης κινδύνων, που προτείνεται από τις συγκεκριμένες μεθοδολογίες, βασίζεται στις ίδιες βασικές αρχές στις οποίες θεμελιώνεται το αντίστοιχο πλαίσιο του NIST.

Η μεγάλη αναγνώριση, των παραπάνω πλαισίων διαχείρισης κινδύνων, από την ακαδημαϊκή και επιχειρηματική κοινότητα παγκοσμίως οδήγησαν την παρούσα μελέτη στην επιλογή της διαδικασίας ΔΚΠΣ που περιγράφεται στις επόμενες ενότητες. Το σύνολο της διαδικασίας βασίζεται στα προαναφερόμενα πλαίσια και στα πορίσματα από το σύνολο της παρούσας ερευνητικής προσπάθειας.

Στο [**50**] αναφέρεται η σημασία της διασύνδεσης, συσχέτισης των τεσσάρων βασικών προαναφερόμενων σταδίων της διαδικασίας ΔΚΠΣ προκειμένου το σύνολο του μηχανισμού αντιμετώπισης των κινδύνων ΠΣ να είναι ενιαίο. Πρωταρχική σημασία για έναν οργανισμό δεν πρέπει να είναι η διάκριση του σταδίου που θεωρεί περισσότερο σημαντικό για την φύση των δραστηριοτήτων του. Έμφαση πρέπει αντιθέτως να δίνεται στα στοιχεία της διαδικασίας που έχουν ιδιαιτερότητες κυρίως σε θέματα υπολογισμών. Συνεπώς, η έμφαση που δίνεται από την παρούσα μελέτη στο στάδιο της εκτίμησης κινδύνων δεν εξυπακούεται θεώρηση ιδιαίτερης σημαντικότητας σε σχέση με τα άλλα στάδια της διαδικασίας. Η έμφαση προέρχεται από το ερευνητικό ενδιαφέρον που παρουσιάζει η εκτίμηση κινδύνων προκειμένου για την εξεύρεση ποσοτικών μεθοδολογιών οι οποίες έχουν την δυνατότητα να αποδώσουν αντικειμενικά αποτελέσματα.

3.2.1 Προσδιορισμός κινδύνων ΠΣ

Το πρώτο στάδιο, με το οποίο ξεκινούν οι διαδικασίες ενός συστήματος ΔΚΠΣ, είναι ο προσδιορισμός των κινδύνων ΠΣ που αντιμετωπίζει ένας οργανισμός (IS risk identification).

Όπως αναλύθηκε στην ενότητα 2.4.2, τα βασικά δομικά στοιχεία των κινδύνων ΠΣ είναι τα εξής: (α) Στοιχεία ενεργητικού ΠΣ , (β) ευπάθειες, (γ) απειλές, και (δ) έλεγχοι ασφαλείας. Στην Εικόνα 5 απεικονίζονται τα προαναφερόμενα στοιχεία σε συνδυασμό με την μεταξύ τους σχέση. Οι ευπάθειες συνδυάζονται με συγκεκριμένες απειλές οι οποίες έχουν ως κύριο στόχο την ανακάλυψη ευπαθειών και την εν συνεχεία εκμετάλλευση τους προκειμένου να επιτεθούν σε στοιχεία ενεργητικού ΠΣ. Οι έλεγχοι ασφαλείας επιδιώκουν την προφύλαξη των στοιχείων

ενεργητικού αποτρέποντας τις απειλές να εκμεταλλευθούν επιτυχώς τις ευπάθειες που έχουν τα ΠΣ.

Σύμφωνα με τα παραπάνω, και όπως αποτυπώνεται στην Εικόνα 5, το στάδιο προσδιορισμού των κινδύνων ενός ΠΣ αποτελείται από τα εξής βήματα:

(α) Προσδιορισμός και ταξινόμηση των στοιχείων ενεργητικού

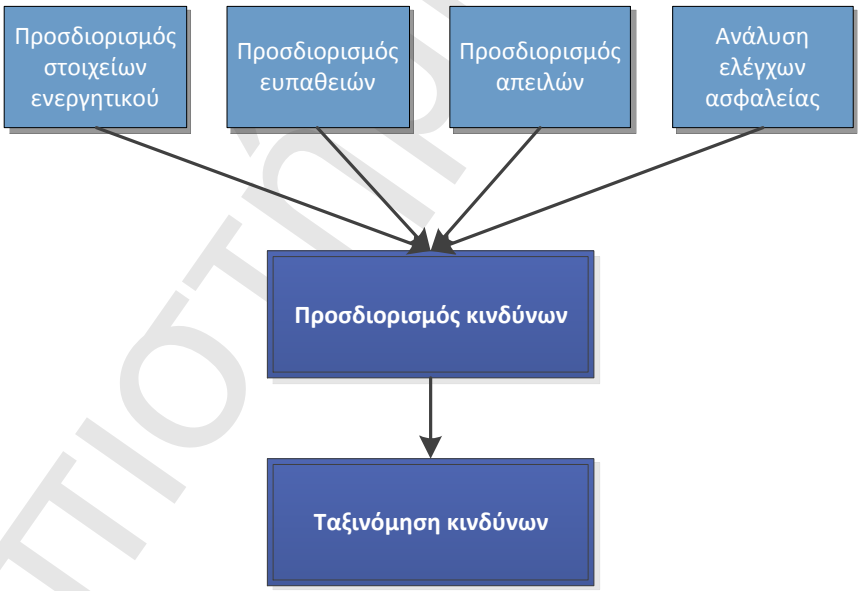
(β) Προσδιορισμός των ευπαθειών

(γ) Προσδιορισμός των απειλών

(δ) Ανάλυση των υφιστάμενων ελέγχων ασφαλείας

(ε) Προσδιορισμός των κινδύνων ενός ΠΣ

(στ) Ταξινόμηση των κινδύνων ενός ΠΣ



Εικόνα 5: Στάδιο προσδιορισμού κινδύνων Πληροφοριακών Συστημάτων

Η πρώτη διαδικασία, που επιτελείται σε αυτό το στάδιο, είναι ο προσδιορισμός και η ταξινόμηση των στοιχείων ενεργητικού που απαρτίζουν τα ΠΣ ενός οργανισμού. Αυτό επιτυγχάνεται σε τρία βήματα:

(1) Προσδιορισμός των στοιχείων ενεργητικού.

(2) Προσδιορισμός του άμεσου ή έμμεσου κατόχου για κάθε στοιχείο ενεργητικού.

(3) Προσδιορισμός της ακριβής εταιρικής διαδικασίας που επιτελεί κάθε στοιχείο ενεργητικού.

Οι παραπάνω πληροφορίες αποτελούν τα κριτήρια, προκειμένου για την ταξινόμηση των στοιχείων ενεργητικού, και τον προσδιορισμό των πλέον κρίσιμων για την επίτευξη της εταιρικής αποστολής. Παραδείγματα κρίσιμων στοιχείων για ένα ΠΣ είναι ευαίσθητες πληροφορίες πελατών, εταιρικά μυστικά και ανθρώπινο δυναμικό με σημαντική τεχνογνωσία.

Η δεύτερη διαδικασία αφορά τον προσδιορισμό των ευπαθειών των ΠΣ ενός οργανισμού και την καταγραφή τους με τις μεθόδους που αναφέρθηκαν στην ενότητα 2.4.2.1. Η καταγραφή των ευπαθειών γίνεται με βάση την ταξινόμηση σπουδαιότητας που έχουν λάβει κατά τον προσδιορισμό τους. Βασικό κριτήριο επιλογής της μεθοδολογίας προσδιορισμού των ευπαθειών κάθε ΠΣ είναι το στάδιο, στον κύκλο ανάπτυξης (System Development Life Cycle – SDLC), στο οποίο βρίσκεται το υπό εξέταση σύστημα. Συγκεκριμένα, ο τύπος ευπαθειών που παρουσιάζει ένα σύστημα, κατά τις τρεις γενικές φάσεις του SDLC (σχεδιασμού, εφαρμογής και λειτουργίας), είναι διαφορετικός με αποτέλεσμα την αναγκαιότητα εφαρμογής διαφορετικών εργαλείων προσδιορισμού των ευπαθειών.

Η τρίτη διαδικασία αφορά τον προσδιορισμό των πηγών απειλών προς τα ΠΣ ενός οργανισμού. Όπως αναλύθηκε στην ενότητα 2.4.2.2, οι πηγές απειλών χωρίζονται σε τρεις γενικές κατηγορίες. Η πρώτη κατηγορία περιλαμβάνει το ανθρώπινο στοιχείο το οποίο διακρίνεται σε αυτό που επιχειρεί εσωτερικά και σε αυτό που επιχειρεί εξωτερικά σε έναν οργανισμό. Το εξωτερικό ανθρώπινο στοιχείο χωρίζεται περαιτέρω ως εξής: (α) Hackers, (β) διαδικτυακοί εγκληματίες, (γ) τρομοκράτες, (δ) βιομηχανικοί κατάσκοποι. Ο προσδιορισμός του συνόλου των πηγών απειλής για ένα σύστημα πραγματοποιείται σε συνδυασμό με τις ευπάθειες που προσδιορίσθηκαν στην προηγούμενη διαδικασία. Η λίστα των πηγών απειλής περιλαμβάνει όλους τους συνδυασμούς ευπαθειών και απειλών οι οποίοι μπορούν να προκαλέσουν κάποιο ανεπιθύμητο γεγονός.

Το σύνολο των πηγών απειλής ταξινομείται με βάση τον βαθμό επικινδυνότητας κάθε απειλής ο οποίος προσδιορίζεται από δύο παραμέτρους: (α) Την πιθανότητα επίτευξης εκμετάλλευσης κάθε δυνατής ευπάθειας του ΠΣ με τις οποίες συνδυάζεται κάθε πηγή απειλής. (β) Την επίπτωση

που μπορεί να επιφέρει μία πηγή απειλής σε συνδυασμό με κάθε ευπάθεια που ανήκει σε συγκεκριμένο στοιχείο ενεργητικού. Από τα προαναφερόμενα προκύπτει πως η ταξινόμηση των πηγών απειλής πραγματοποιείται με συνδυασμό των ξεχωριστών ταξινομήσεων που αφορούν τα στοιχεία ενεργητικού, τις ευπάθειες και τις ίδιες τις πηγές απειλής.

Η τέταρτη διαδικασία, του προσδιορισμού των κινδύνων ΠΣ, αφορά την ανάλυση των υφιστάμενων και σχεδιαζόμενων ελέγχων και αντίμετρων ασφαλείας. Σκοπός της συγκεκριμένης ανάλυσης είναι η αξιολόγηση των ελέγχων ασφαλείας με κριτήριο τις απαιτήσεις που έχουν τεθεί από το εσωτερικό και εξωτερικό περιβάλλον ενός οργανισμού. Τα αποτελέσματα της αξιολόγησης μπορούν να αποτυπωθούν υπό την μορφή ταξινόμησης σύμφωνα με την αποδοτικότητα και αξιοπιστία που κρίνεται ότι έχει κάθε έλεγχος και κάθε αντίμετρο ασφαλείας.

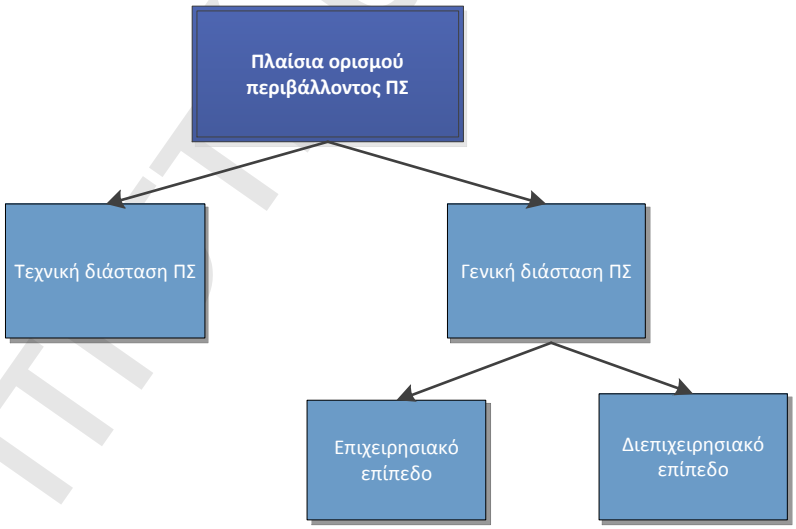
Τα αποτελέσματα των τεσσάρων προηγούμενων διαδικασιών συνδυάζονται, κατά την πέμπτη διαδικασία, προκειμένου να αποτυπωθούν όλοι οι δυνατοί συνδυασμοί στοιχείων ενεργητικού, ευπαθειών και πηγών απειλής. Κάθε συνδυασμός αποτελεί ένα διακριτό ανεπιθύμητο περιστατικό για έναν οργανισμό. Αναφέροντας «δυνατός συνδυασμός» δεν εννοούμε όλους τους μαθηματικά εφικτούς συνδυασμούς, καθώς περιστατικά τα οποία δεν έχουν πιθανότητα πραγμάτωσης, λόγω επαρκών αντίμετρων ασφαλείας, δεν λαμβάνονται υπόψη προς περαιτέρω ανάλυση. Επίσης, περιπτώσεις όπου είναι ανέφικτος τεχνικά ο συνδυασμός συγκεκριμένης ευπάθειας και συγκεκριμένης απειλής, δεν λαμβάνονται υπόψη.

Τα περιστατικά που προκαλούν κινδύνους ΠΣ ομαδοποιούνται προκειμένου να αποτυπωθεί, σε αρχικό επίπεδο ανάλυσης. η οντότητα κάθε κινδύνου ΠΣ στα πλαίσια ενός οργανισμού. Ο στόχος της ανάλυσης είναι η ολοκλήρωση της έκτης διαδικασίας που αφορά την ταξινόμηση των προσδιορισμένων κινδύνων.

Ο Corder [**51**] πρότεινε την ταξινόμηση των κινδύνων με χρήση ποιοτικών μεθοδολογιών καθώς, σε αυτό το στάδιο ανάλυσης, μεγαλύτερη ακρίβεια δεν είναι αναγκαία. Προς αυτήν την κατεύθυνση ταξινομεί τους κινδύνους σε τρία επίπεδα σημαντικότητας: (α) Υψηλού κινδύνου, (β) μεσαίου κινδύνου και (γ) χαμηλού κινδύνου. Η ταξινόμηση των κινδύνων ουσιαστικά ολοκληρώνεται στο στάδιο εκτίμησης των κινδύνων όπου – όπως περιγράφεται στην επόμενη ενότητα – είναι επιθυμητή η χρήση κατά κύριο λόγο ποσοτικών μεθοδολογιών.

Ένα σύνολο ερευνητών όπως οι Dhillon et. al. [**34**] έχουν επισημάνει την σπουδαιότητα της επιλογής της φύσης του πλαισίου ΠΣ που λαμβάνεται ως βάση στο στάδιο του προσδιορισμού των κινδύνων. Διακρίνουμε δύο προτεινόμενα πλαίσια ΠΣ στην βιβλιογραφία [**9**], [**34**], [**35**], με το δεύτερο να αναλύεται σε δύο ακόμα όπως αποτυπώνεται στην Εικόνα 6. Το πρώτο πλαίσιο επικεντρώνεται στους παράγοντες κινδύνων που δημιουργούνται από την τεχνική διάσταση των ΠΣ, όπως οι παραβιάσεις ασφαλείας και τα σφάλματα λειτουργίας. Το πλαίσιο αυτό ορίζει το περιβάλλον των ΠΣ σε επίπεδο λογισμικού (application level). Το δεύτερο πλαίσιο λαμβάνει μία γενικότερη αντίληψη των ΠΣ και κατά συνέπεια οδηγεί σε έναν διευρυμένο καθορισμό των παραγόντων κινδύνου.

Το δεύτερο πλαίσιο διακρίνεται σε επιχειρησιακό και σε διεπιχειρησιακό επίπεδο θεώρησης του περιβάλλοντος ΠΣ. Κατά την επιχειρησιακή θεώρηση, λαμβάνονται προς ανάλυση το σύνολο των λειτουργικών πτυχών ενός οργανισμού χωρίς να πραγματοποιείται επικέντρωση σε συγκεκριμένα στοιχεία λογισμικού. Κατά την διεπιχειρησιακή θεώρηση, αναλύεται η θέση ενός οργανισμού μέσα σε ένα ευρύτερο δικτυακό περιβάλλον. Κύριο σημείο αναφοράς έχουν οι νέες τεχνολογίες επικοινωνίας που διευρύνουν τα νοητά όρια του περιβάλλοντος λειτουργίας ενός οργανισμού και καλούνται διεπιχειρησιακά συστήματα (interorganizational systems).



Εικόνα 6: Πλαίσια ορισμού περιβάλλοντος Πληροφοριακών Συστημάτων

Μία ευρύτερη θεώρηση του επιχειρησιακού περιβάλλοντος μπορεί να δημιουργήσει το υπόβαθρο για ένα αποδοτικότερο σύστημα διαχείρισης κινδύνων στον προσδιορισμό των

παραγόντων κινδύνου που επηρεάζουν το επίπεδο ασφαλείας των ΠΣ. Πέρα από το στενό τεχνικό περιβάλλον ενός οργανισμού, εκπορεύονται σημαντικοί παράγοντες κινδύνου οι οποίοι προκύπτουν μέσα από την ευρύτερη θεώρηση του επιχειρησιακού περιβάλλοντος. Στηρίζοντας τον προσδιορισμό των κινδύνων σε αυτή την θεώρηση, προκύπτει ένας αρτιότερος προσδιορισμός των κινδύνων ΠΣ από τον οποίο μπορεί να προέλθει μία αποδοτικότερη εκτίμηση των κινδύνων.

Τέλος, πρέπει να αναφερθεί ότι στην περίπτωση της διαχείρισης οργανικών κινδύνων ΠΣ, προερχομένων από την ανάληψη καινούριων επενδυτικών προγραμμάτων σε ΠΣ, τα στάδια του προσδιορισμού και της εκτίμησης των κινδύνων θα πρέπει να διενεργούνται πριν την υλοποίηση των εν λόγο προγραμμάτων.

3.2.2 Εκτίμηση κινδύνων ΠΣ

Το στάδιο της εκτίμησης των κινδύνων ενός ΠΣ (risk assessment) θεωρείται το κυριότερο της διαδικασίας διαχείρισης κινδύνων καθώς θέτει τα θεμέλια για την επίτευξη των στόχων της συνολικής διαδικασίας. Η αποτίμηση ενός κινδύνου ΠΣ, του οποίου η ύπαρξη έχει προσδιορισθεί στο προηγούμενο στάδιο της διαδικασίας, έχει δύο βασικά στοιχεία:

(α) Η πιθανότητα πραγμάτωσης του κινδύνου.

(β) Το μέγεθος της επίπτωσης (impact) που δύναται να επιφέρει η πραγμάτωση του κινδύνου.

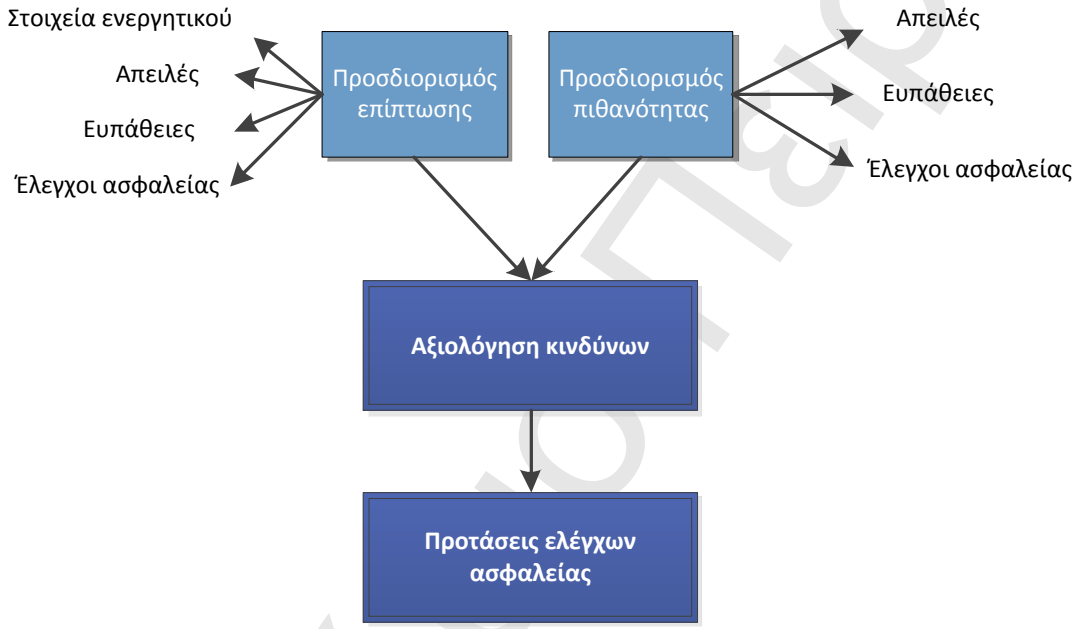
Κάθε ένα, εκ των προαναφερόμενων στοιχείων, πρέπει να εκτιμηθεί προκειμένου να ολοκληρωθεί η αξιολόγηση κάθε κινδύνου που έχει προσδιορισθεί και ταξινομηθεί. Όπως αποτυπώνεται στην Εικόνα 7, ο προσδιορισμός των βασικών στοιχείων των κινδύνων ΠΣ αποτελεί τις δύο πρώτες διαδικασίες του συγκεκριμένου σταδίου ΔΚΠΣ.

Κατά την πρώτη διαδικασία, γίνεται εκτίμηση της πιθανότητας πραγμάτωσης ενός κινδύνου ΠΣ. Η πιθανότητα εμφάνισης προσδιορίζεται από τα εξής στοιχεία:

(α) Οι υφιστάμενοι έλεγχοι ασφαλείας που προστατεύουν ένα συγκεκριμένο στοιχείο ενεργητικού ή μία διαδικασία ενός ΠΣ από την απειλή που συντελεί στην δημιουργία του κινδύνου που αποτιμάται. Η εκτίμηση της παρούσας κατάστασης των ελέγχων μπορεί να δώσει μία εκτίμηση της πιθανότητας μία συγκεκριμένη απειλή να εκμεταλλευτεί μία συγκεκριμένη ευπάθεια.

(β) Τα στοιχεία που χαρακτηρίζουν την απειλή που δημιουργεί τον υπό εξέταση κίνδυνο. Μπορούμε να διακρίνουμε δύο βασικά χαρακτηριστικά για μία απειλή: Κίνητρο και ικανότητα.

(γ) Τα στοιχεία που χαρακτηρίζουν την ευπάθεια που δύναται να εκμεταλλευτεί η συγκεκριμένη απειλή.



Εικόνα 7: Στάδιο εκτίμησης κινδύνων Πληροφοριακών Συστημάτων

Κατά την δεύτερη διαδικασία, γίνεται εκτίμηση της επίπτωσης ενός συγκεκριμένου κινδύνου ΠΣ. Ο Boehm [**46**] επεσήμανε την ιδιαιτερότητα που έχει το υπό-στάδιο ανάλυσης των κινδύνων λόγω της σημασίας που έχει στο σύνολο της διαδικασίας καθώς και της δυσκολίας προσέγγισης αντικειμενικών μετρήσεων για την έκθεση ενός υποκειμένου σε κινδύνους ΠΣ. Η επίπτωση προσδιορίζεται από τα εξής βασικά στοιχεία:

(α) Τα ιδιαίτερα χαρακτηριστικά του στοιχείου ενεργητικού ΠΣ που δύναται να προσβληθεί από τον κίνδυνο. Τα χαρακτηριστικά αυτά αποτελούνται από την κρισιμότητα της εταιρικής διαδικασίας, που επιτελεί το συγκεκριμένο στοιχείο, καθώς την ιδιαιτερότητα και ευαισθησία των δεδομένων που χειρίζεται, προκειμένου για τον

προσδιορισμό του επιπέδου προσβολής στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφόρησης.

(β) Ο παράγοντας έκθεσης. Το επίπεδο έκθεσης ενός συγκεκριμένου στοιχείου ΠΣ, σε μία συγκεκριμένη επίθεση, αποτελεί τον παράγοντα έκθεσης (exposure factor) και είναι ένα από τα βασικά προσδιοριστικά στοιχεία των κινδύνων ΠΣ. Το μέγεθος του παράγοντα έκθεσης εξαρτάται από την ευπάθεια που προκαλεί την έκθεση, το επίπεδο ασφαλείας που παρέχουν οι υφιστάμενοι έλεγχοι καθώς και την συγκεκριμένη απειλή που δύναται να αξιοποιήσει την συγκεκριμένη ευπάθεια.

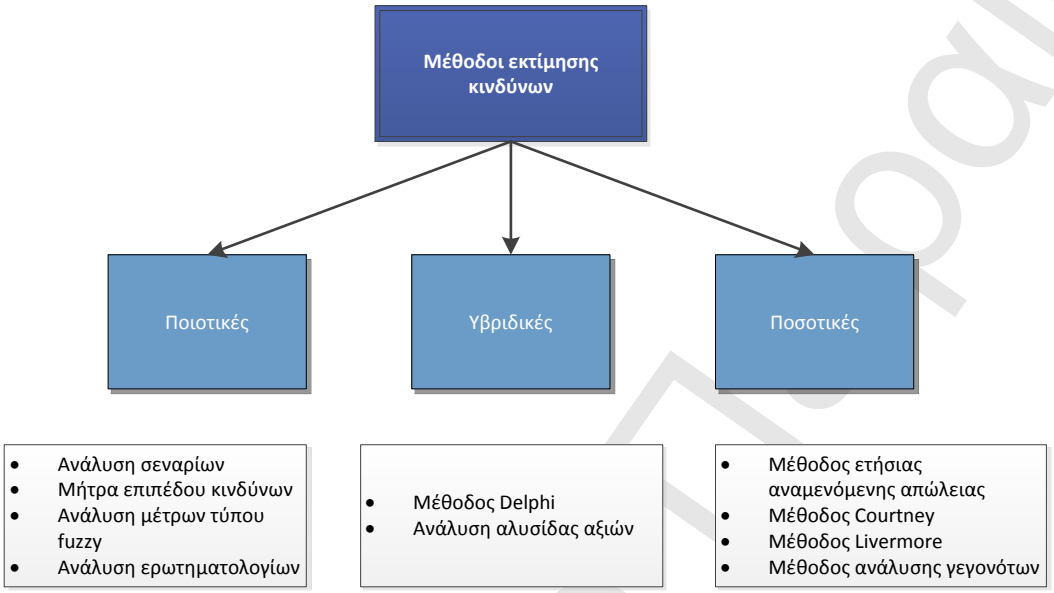
Ο αντικειμενικός προσδιορισμός των δύο παραπάνω στοιχείων προϋποθέτει την χρήση δεδομένων. Όπως θα αναφερθεί αναλυτικά παρακάτω, η ποσοτική εκτίμηση των κινδύνων και ο βαθμός αντικειμενικότητας των αποτελεσμάτων εκτίμησης εξαρτώνται από το επίπεδο χρήσης πραγματικών δεδομένων.

Ο τρόπος αποτύπωσης της εκτίμησης της πιθανότητας εμφάνισης των κινδύνων ΠΣ καθώς και του παράγοντα έκθεσης εξαρτώνται από την μεθοδολογία αποτίμησης που ακολουθείται. Στην περίπτωση που η αποτίμηση είναι ποιοτικού χαρακτήρα (qualitative analysis), η εκτιμήσεις αποτυπώνονται με όρους ταξινόμησης π.χ. χαμηλή, μεσαία, υψηλή. Στην περίπτωση που η αποτίμηση είναι ποσοτικού χαρακτήρα (quantitative analysis) οι εκτιμήσεις εκφράζονται σε ποσοστά και νομισματικούς όρους.

Οι ποιοτικές μέθοδοι χρησιμοποιούν περιγραφικές μεταβλητές για την ανάλυση των κινδύνων ΠΣ οι οποίες μετράνε κατά κύριο λόγο τα χαρακτηριστικά των συστατικών στοιχείων ενός συστήματος. Στο στάδιο αυτό μπορεί να χρησιμοποιηθεί η ποιοτική ανάλυση των απειλών, ευπαθειών, στοιχείων ενεργητικού καθώς και των ελέγχων ασφαλείας που διεξήχθη, κατά το στάδιο προσδιορισμού των κινδύνων, ως βάση προς περεταίρω ανάλυση. Όπως αποτυπώνεται στην Εικόνα 8, διαδεδομένες μέθοδοι αυτής της κατηγορίας είναι: (α) Ανάλυση σεναρίων, (β) κατασκευή μήτρας επιπέδου κινδύνων, (γ) ανάλυση μέτρων τύπου fuzzy και (δ) ανάλυση ερωτηματολογίων.

Η ποιοτική μέθοδος ανάλυσης ερωτηματολογίων είναι από τις πλέον διαδεδομένες και εφαρμόζεται από ιδιωτικούς μελετητικούς οργανισμούς όπως η Ponemon Institute και η Ernst &

Young. Ανάλυση της συγκεκριμένης μεθόδου και επισκόπηση των αποτελεσμάτων που έχουν επιφέρει πραγματοποιείται στο κεφάλαιο 4.



Εικόνα 8: Μέθοδοι εκτίμησης κινδύνων

Το μέγεθος της επίπτωσης εκφράζεται σε όρους απώλειας σε σχέση με την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφόρησης που προσβάλλεται. Οι όροι αποτύπωσης είναι είτε ποιοτικοί, είτε ποσοτικοί ανάλογα με τον τύπο μεθοδολογίας που εφαρμόζεται. Συνήθως, είναι πιο εφικτός ο ποσοτικός υπολογισμός της επίπτωσης για υλικά περιουσιακά στοιχεία ΠΣ. Αντιθέτως, η επίπτωση σε άυλα περιουσιακά στοιχεία, δεδομένα και σε ανθρώπινο δυναμικό είναι περισσότερο εφικτή με την χρήση ποιοτικών μεθόδων.

Οι ποσοτικές μέθοδοι επιχειρούν την απόδοση σε αντικειμενικούς, αριθμητικούς όρους των παραμέτρων που επηρεάζουν την πιθανότητα και την επίπτωση των κινδύνων ΠΣ. Όπως αποτυπώνεται στην Εικόνα 8, διαδεδομένες μέθοδοι αυτής της κατηγορίας είναι: (α) Μέθοδος της ετήσιας αναμενόμενης απώλειας (annual loss expectancy), (β) μέθοδος Courtney, (γ) μέθοδος Livermore και (δ) μέθοδος ανάλυσης γεγονότων. Μέσω των ποσοτικών μεθόδων, ο παράγοντας έκθεσης υπολογίζεται ως ποσοστό απώλειας για ένα συγκεκριμένο στοιχείο ενεργητικού προκαλούμενο από έναν συγκεκριμένο, προσδιορισμένο κίνδυνο.

Μελετητές έχουν προτείνει μία τρίτη κατηγορία μεθοδολογιών αποτίμησης η οποία προέρχεται από την ανάμιξη μεθοδολογιών ποιοτικού και ποσοτικού χαρακτήρα. Οι Rainer et. al. [**43**]

πρότειναν μία υβριδική μεθοδολογία (hybrid methodology) η οποία μέσω αλυσίδας αξιών (value chain) προσδιορίζουν τους κινδύνους ΠΣ που θα προκύψουν από εναλλακτικές μορφές χρήσης της τεχνολογίας. Μία πολύ διαδεδομένη υβριδική μεθοδολογία είναι η τεχνική Delphi η οποία έχει ευρεία αποδοχή μεταξύ της ακαδημαϊκής και επαγγελματικής κοινότητας.

Κατά την τελευταία δεκαετία, έχει αναπτυχθεί μία εναλλακτική ποσοτική μέθοδος κατά την οποία ο παράγοντας έκθεσης υπολογίζεται μέσω της μεθόδου ανάλυσης γεγονότων (event analysis). Τα δεδομένα που χρησιμοποιούνται σε αυτή την μέθοδο είναι πραγματικά περιστατικά ασφαλείας και η επίδραση τους σε έναν οργανισμό υπολογίζεται μέσω των χρηματιστηριακών αποδόσεων σε συγκεκριμένα διαστήματα ανάλυσης. Στο κεφάλαιο 5 αναλύονται προηγούμενες σημαντικές μελέτες αυτού του τύπου και τα αποτελέσματα τους συγκρίνονται με αντίστοιχη εμπειρική μελέτη που πραγματοποιήθηκε στα πλαίσια της παρούσας διατριβής.

Το βασικό πλεονέκτημα των ποιοτικών και υβριδικών μεθοδολογικών εκτίμησης είναι η άμεση ταξινόμηση των κινδύνων ΠΣ και ο εν συνεχεία προσδιορισμός των σημείων μέσα σε ένα σύστημα τα οποία χρήζουν αναγκαιότητας βελτίωσης. Το βασικό μειονέκτημα των ποιοτικών μεθόδων είναι η υποκειμενικότητα που διακατέχει τον προσδιορισμό όλων των παραμέτρων με συνέπεια την άμεση εξάρτηση της ποιότητας των αποτελεσμάτων τους από τις ιδιαίτερες ικανότητες του εκτιμητή. Επίσης, η έλλειψη ποσοτικών αποτελεσμάτων, ειδικά στον προσδιορισμό των επιπτώσεων, δημιουργεί σοβαρές δυσκολίες στην ανάλυση κόστους – ωφέλειας των προτεινόμενων ελέγχων και αντίμετρων ασφαλείας. Το μειονέκτημα αυτό γίνεται σοβαρότερο τα τελευταία χρόνια καθώς οι κίνδυνοι ΠΣ σταδιακά λαμβάνουν μεγάλη προτεραιότητα για τις διοικήσεις των οργανισμών με τις τελευταίες να χρειάζονται πλέον αντικειμενικές, μετρήσιμες εκτιμήσεις των κινδύνων που, λόγω την αυξανόμενης χρήσης σύγχρονων τεχνολογιών, γίνονται ολοένα και πιο σοβαροί.

Το βασικό πλεονέκτημα των ποσοτικών μεθόδων είναι η δυνατότητα που δίνουν τα αποτελέσματα τους προκειμένου για την ανάλυση κόστους – ωφέλειας στην επιλογή των κατάλληλων μεθόδων ελέγχου ασφαλείας κατά το στάδιο της αντιμετώπισης των κινδύνων ΠΣ. Επίσης, τα ποσοτικά αποτελέσματα έχουν μικρότερη εξάρτηση από τις ιδιαίτερες ικανότητες του εκτιμητή προσδίδοντας τους, κατά αυτόν τον τρόπο, μεγαλύτερη αντικειμενικότητα. Το μειονέκτημα αυτών των μεθόδων έγκειται κυρίως στην δυσκολία ανεύρεσης ποσοτικών στοιχείων για το σύνολο των αναγκαίων παραμέτρων και πολλές φορές απαιτείται μεγάλη κατανάλωση

εταιρικών πόρων για την εφαρμογή τους. Επιπλέον, τα αποτελέσματα δύναται να εκφράζονται σε διαστήματα ποσοτικών εκτιμήσεων απαιτώντας την συνδρομή ποιοτικών μεθόδων για την ολοκληρωμένη επεξήγηση τους καταργώντας κατά αυτόν τον τρόπο τον αμιγώς ποσοτικό χαρακτήρα τους.

Στην παρούσα ερευνητική προσπάθεια έγινε έρευνα στην ποσοτικοποίηση του επιπέδου ασφαλείας μέσω της εφαρμογής στοχαστικών ολοκληρωμάτων η οποία αναλύεται διεξοδικά στο κεφάλαιο 6. Επίσης, έγινε έρευνα στην ποσοτικοποίηση των επιπτώσεων των κινδύνων μέσω της εφαρμογής της μεθοδολογίας ανάλυσης γεγονότων με την εμπειρική μελέτη πραγματικών περιστατικών ασφαλείας. Η συγκεκριμένη έρευνα αναλύεται διεξοδικά στο κεφάλαιο 5. Επιπρόσθετα, στο κεφάλαιο 7 επιχειρήθηκε η χρήση των αποτελεσμάτων του συνόλου της προαναφερόμενης έρευνας προκειμένου για την ολοκληρωμένη πρόταση μίας ποσοτικής μεθοδολογίας εκτίμησης των κινδύνων ΠΣ.

Όταν ολοκληρωθεί η αξιολόγηση των κινδύνων ΠΣ, που προσδιορίσθηκαν στο προηγούμενο στάδιο, θεμιτό είναι να επαναληφθεί η διαδικασία ταξινόμησης κινδύνων, η οποία πραγματοποιήθηκε αρχικώς στο στάδιο του προσδιορισμού κινδύνων. Το πλεονέκτημα από την επανάληψη της διαδικασίας είναι η ταξινόμηση των κινδύνων με μεγαλύτερη ακρίβεια και αντικειμενικότητα προκειμένου να δοθεί μεγαλύτερη βαρύτητα αντιμετώπισης, με χρήση ισχυρότερων αντίμετρων, στους κινδύνους που πραγματικά μπορούν να επιφέρουν ισχυρές επιπτώσεις σε έναν οργανισμό.

Κατά το τελικό υπό-στάδιο της διαδικασίας εκτίμησης κινδύνων, με βάση τα αποτελέσματα αξιολόγησης των κινδύνων και την επανάληψη της διαδικασίας καθορισμού προτεραιοτήτων, δημιουργείται ένας κατάλογος προτεινόμενων εναλλακτικών αντίμετρων ασφαλείας προκειμένου να γίνει η επιλογή του βέλτιστου συνδυασμού στο επόμενο στάδιο. Συνολικά, τα στάδια του προσδιορισμού και εκτίμησης κινδύνων οδηγούν σε αυτό που αποκαλείται επίγνωση κινδύνου. Γενικά είναι αποδεκτό, από την υπάρχουσα βιβλιογραφία, ότι η επαρκής επίγνωση κινδύνου είναι το πιο σημαντικό μέρος ενός συστήματος ΔΚΠΣ.

3.2.3 Αντιμετώπιση κινδύνων ΠΣ

Στο στάδιο αντιμετώπισης κινδύνων ΠΣ (risk mitigation) πραγματοποιείται επαναξιολόγηση, αναθεώρηση και βελτίωση των υφιστάμενων ελέγχων ασφαλείας και εισαγωγή νέων όπως αυτοί

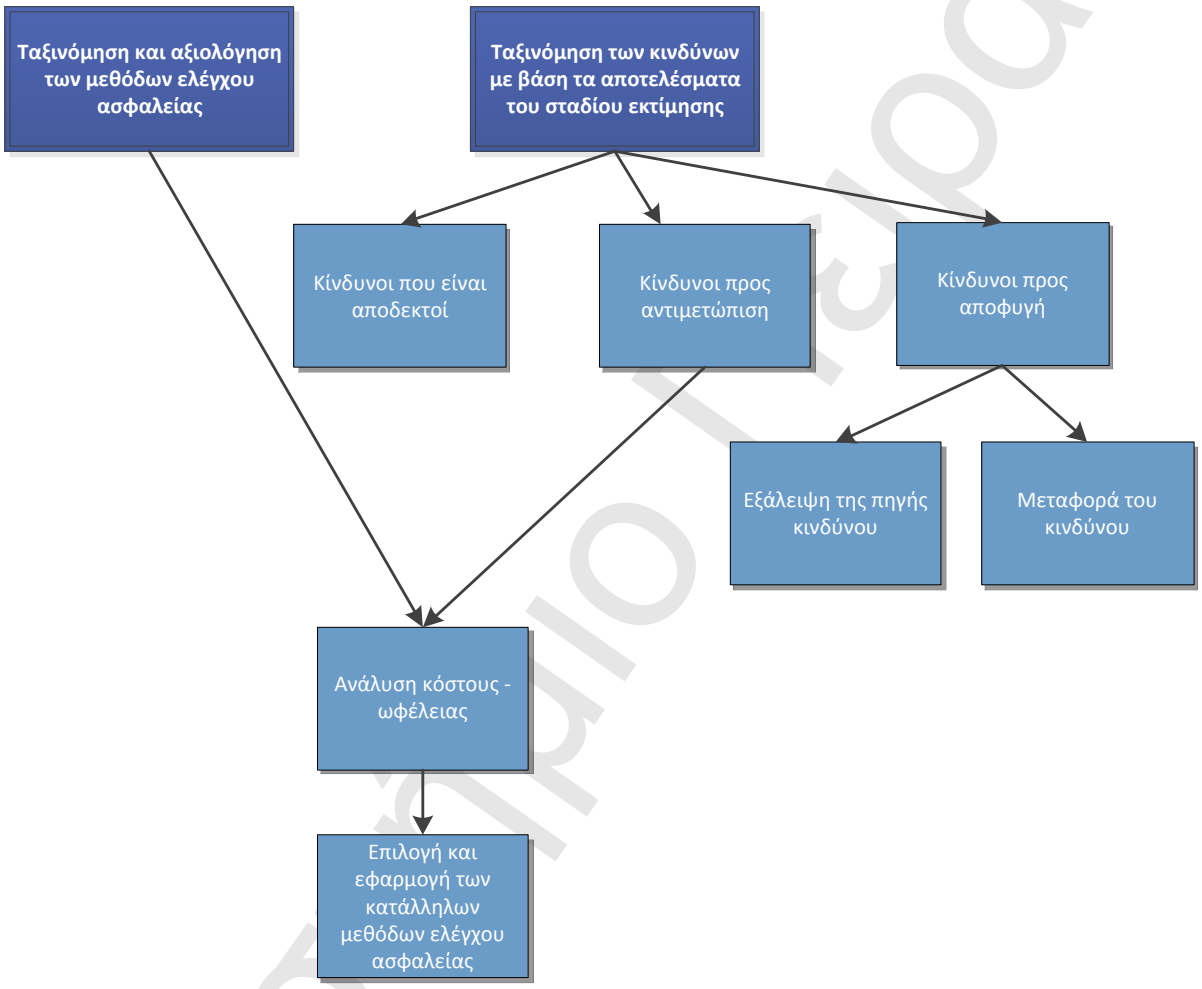
αναλύθηκαν στην ενότητα 2.4.2.3. Οι δύο βασικές πηγές δεδομένων προέρχονται από το στάδιο της εκτίμησης κινδύνων. Η πρώτη είναι η ταξινόμηση των προσδιοριζόμενων κινδύνων με βάση την εκτιμώμενη επίπτωση που δύναται να επιφέρουν στην ικανότητα του οργανισμού προκειμένου να επιτελέσει την εταιρική αποστολή του. Η δεύτερη πηγή δεδομένων αποτελείται από το σύνολο των εναλλακτικών μέτρων ελέγχων και αντίμετρων ασφαλείας που προτάθηκαν.

Όπως αποτυπώνεται στην Εικόνα 9, η πρώτη διαδικασία αυτού του σταδίου αποτελείται από δύο βήματα τα οποία μπορούν να γίνουν παράλληλα. Το ένα βήμα αφορά την ταξινόμηση των κινδύνων με βάση τα αποτελέσματα του σταδίου εκτίμησης. Το άλλο βήμα αφορά την ταξινόμηση και αξιολόγηση των μεθόδων ελέγχου ασφαλείας. Το πρώτο περιλαμβάνει τον διαχωρισμό των κινδύνων ΠΣ σε τρεις κατηγορίες, με βάση την ταξινόμηση που έχει προηγηθεί στο προηγούμενο στάδιο, σε συνάρτηση με το επίπεδο επιθυμίας ανάληψης κινδύνων (risk appetite) που έχει ο οργανισμός. Οι κατηγορίες διαχωρισμού των κινδύνων ΠΣ είναι ως εξής:

(1) Κίνδυνοι που κρίνονται ως αποδεκτοί στο επίπεδο που βρίσκονται την στιγμή της αξιολόγησης. Αυτό συνήθως συμβαίνει με κινδύνους που ταξινομήθηκαν σε σχετικά χαμηλό επίπεδο επίπτωσης το οποίο είναι αποδεκτό σύμφωνα με το επίπεδο επιθυμίας αποδοχής κινδύνων του οργανισμού. Εναλλακτικά, το επίπεδο του κινδύνου δύναται να μην είναι χαμηλό αλλά η φύση του οργανισμού να επιτάσσει την αποδοχή του ως οργανικό κίνδυνο συνυφασμένο με την επιχειρηματική λειτουργία του οργανισμού. Οι κίνδυνοι που χαρακτηρίζονται ως αποδεκτοί, στην περίπτωση που υφίστανται μέθοδοι ελέγχων ασφαλείας, παραμένουν με το ίδιο επίπεδο ελέγχων. Στην εναλλακτική, όπου δεν υφίστανται έλεγχοι ασφαλείας, μέχρι να τροποποιηθεί κάποια παράμετρος στην αξιολόγηση και ταξινόμηση τους καθώς και στην λειτουργία του ίδιου του οργανισμού, παραμένουν ως έχουν.

(2) Κίνδυνοι που κρίνονται προς αποφυγή σύμφωνα με την ταξινόμηση που λάβανε και με το επίπεδο επιθυμίας αποδοχής κινδύνων του οργανισμού. Στην περίπτωση αυτή διακρίνονται δύο εναλλακτικές μέθοδοι αντιμετώπισης αυτής της κατηγορίας κινδύνων. Η πρώτη μέθοδος αφορά την εξάλειψη της πρωτογενής πηγής του κινδύνου. Προκειμένου να επιτευχθεί αυτό καταργείται η χρήση των στοιχείων ενεργητικού στα οποία υφίσταται οι ευπάθειες που δημιουργούν τον συγκεκριμένο κίνδυνο. Η δεύτερη

μέθοδος αφορά την μεταφορά του κινδύνου σε τρίτο αντισυμβαλλόμενο μέσο της υπογραφής κάποιου συμβολαίου ασφάλισης.



Εικόνα 9: Στάδιο αντιμετώπισης κινδύνων Πληροφοριακών Συστημάτων

(3) Στην τρίτη κατηγορία ανήκουν οι κίνδυνοι προς αντιμετώπιση. Οι κίνδυνοι αυτοί δεν θεωρούνται τόσο υψηλοί ώστε να κριθεί σκόπιμη η αποφυγή τους αλλά παράλληλα, δεν θεωρούνται τόσο χαμηλοί ώστε να κριθούν ως αποδεκτοί χωρίς την λήψη μέτρων αντιμετώπισης. Κρίνεται αποδεκτή συνεπώς η ύπαρξη υπολειμματικών κινδύνων (residual risks) οι οποίοι θα παραμείνουν αφού εφαρμοστούν τα επιλεγμένα μέτρα αντιμετώπισης τους. Το αποδεκτό επίπεδο των υπολειμματικών κινδύνων εξαρτάται από το επίπεδο επιθυμίας ανάληψης κινδύνων του οργανισμού. Ουσιαστικά, το κύριο

μέρος του συγκεκριμένου σταδίου της διαδικασίας ΔΚΠΣ αφορά την αντιμετώπιση των κινδύνων που υπάγονται σε αυτή την κατηγορία.

Το δεύτερο βήμα του συγκεκριμένου σταδίου αφορά την ταξινόμηση και αξιολόγηση των μεθόδων ελέγχου ασφαλείας που προτάθηκαν κατά το στάδιο της εκτίμησης κινδύνων. Τα κριτήρια που χρησιμοποιούνται σε αυτήν την διαδικασία είναι η δυνατότητα εφαρμογής μία μεθόδου ελέγχου και η εκτιμώμενη αποδοτικότητα στην μείωση του υφιστάμενου επιπέδου κινδύνου που αντιμετωπίζει. Τα ιδιαίτερα χαρακτηριστικά ενός οργανισμού δύναται να καταστήσουν μία θεωρητικά αξιόλογη μέθοδο ελέγχου ως μη εφικτή προς εφαρμογή ή ως μη επαρκή προς κάλυψη ενός συγκεκριμένου κινδύνου σε έναν συγκεκριμένο οργανισμό.

Στο τρίτο βήμα πραγματοποιείται ανάλυση κόστους ωφέλειας, μεταξύ των κινδύνων προς αντιμετώπιση και των ελέγχων ασφαλείας που κρίθηκαν ως αποδεκτοί, χρησιμοποιώντας τα δεδομένα από τα δύο προαναφερόμενα βήματα. Προκειμένου να επιτελεστεί ολοκληρωμένα η συγκεκριμένη διαδικασία είναι αναγκαία τα εξής:

(α) Το επίπεδο του υπό εξέταση κινδύνου χωρίς την χρήση νέων μέτρων ελέγχου ή την τροποποίηση των υπαρχόντων. Τα δεδομένα αυτά προέρχονται από το στάδιο της εκτίμησης κινδύνων ΠΣ.

(β) Το επίπεδο του υπό εξέταση κινδύνου αφού εφαρμοστούν νέα μέτρα ελέγχου ή αφού τροποποιηθούν τα ήδη υπάρχοντα. Η συγκεκριμένη ανάλυση επιτελείται με συνδυασμό των δεδομένων που αναφέρθηκαν στο (α) και των δεδομένων που προέκυψαν κατά το δεύτερο βήμα του συγκεκριμένου σταδίου.

(γ) Εκτίμηση του κόστους εφαρμογής νέων μέτρων ελέγχου ή τροποποίησης των υπαρχόντων. Το κόστος μπορεί να καταμεριστεί σε άμεσο και έμμεσο με κριτήριο την ευκολία ποσοτικοποίησης των επιμέρους στοιχείων που το συνθέτουν. Στο άμεσο κόστος επιμερίζονται κατά κύριο λόγο οι δαπάνες που αφιερώνονται σε αγορά υλικού και λογισμικού, στην μισθοδότηση επιπλέον εργατοημερών προσωπικού και στην εκπαίδευση των εργαζομένων που σχετίζονται με την χρήση του στοιχείου ενεργητικού το οποίο εκτίθεται στον υπό εξέταση κίνδυνο. Στο έμμεσο κόστος συμπεριλαμβάνονται κυρίως οι οικονομικές επιπτώσεις από την ενδεχόμενη μειωμένη παραγωγικότητα των ΠΣ λόγω της εφαρμογής των υπό εξέταση μέτρων ελέγχου.

Όπως αναφέρθηκε στην ανάλυση του σταδίου εκτίμησης κινδύνων ΠΣ, ένα από τα βασικά πλεονεκτήματα των ποσοτικών μεθόδων είναι η δημιουργία αποτελεσμάτων τα οποία μπορούν να εφαρμοστούν με μεγαλύτερη αποτελεσματικότητα, σε σχέση με τα αντίστοιχα ποιοτικά, στην ανάλυση κόστους – ωφέλειας. Η ωφέλεια εφαρμογής ενός μέτρου ελέγχου ασφαλείας προκύπτει από την διαφορά του στοιχείου (α) με το (β). Είναι συνεπώς εύκολα αντιληπτό ότι, με τη χρήση ποιοτικών προσεγγίσεων για τα (α) και (β), το αποτέλεσμα που θα προκύψει δεν θα έχει την απαιτούμενη ακρίβεια και πολύ πιθανό να μην είναι επαρκώς κατανοητό από την διοίκηση ενός οργανισμού που καλείται να λάβει αποφάσεις σε θέματα επενδύσεων ασφαλείας.

Η παροχή ποσοτικών δεδομένων για τους κινδύνους ΠΣ με επαρκή αντικειμενικότητα και ακρίβεια προκειμένου – μεταξύ άλλων - για την αποτελεσματική εφαρμογή τους στην ανάλυση κόστους – ωφέλειας αποτέλεσε ένα από τα βασικά ερευνητικά θέματα της παρούσας διατριβής.

Η τελική διαδικασία του συγκεκριμένου σταδίου αφορά την επιλογή των κατάλληλων ελέγχων ασφαλείας και την εφαρμογή τους. Η επιλογή γίνεται με βάση την αξιολόγηση των αποτελεσμάτων της ανάλυσης κόστους – ωφέλειας. Η εφαρμογή αφορά την απόδοση αρμοδιοτήτων σε κατάλληλο προσωπικό, την εκπαίδευση τους και την εν συνεχεία παρακολούθηση εφαρμογής του προγράμματος υλοποίησης του πλάνου αντιμετώπισης κινδύνων το οποίο απαρτίζεται από το σύνολο των επιλεγμένων ελέγχων.

3.2.4 Αξιολόγηση και αποτίμηση κινδύνων ΠΣ

Στο τελευταίο στάδιο της διαδικασίας ΔΚΠΣ πραγματοποιείται συνεχής έλεγχος και αξιολόγηση της εφαρμογής των μέτρων ελέγχου καθώς και την αποδοτικότητας τους στην αντιμετώπιση των κινδύνων (evaluation). Επίσης, πραγματοποιείται διαρκής αξιολόγηση (assessment) των προσδιορισμένων κινδύνων προκειμένου για την διαπίστωση τυχών σημαντικών αποκλίσεων σε σχέση με τις αξιολογήσεις που έχουν προηγηθεί κατά το στάδιο εκτίμησης. Συνεπώς, η συγκεκριμένη διαδικασία έχει διττό χαρακτήρα καθώς είναι ταυτόχρονα αξιολογική και ελεγκτική. Τα πορίσματα που προκύπτουν συνθέτουν προτάσεις βελτίωσης των μέτρων ελέγχου καθώς και των διαδικασιών εφαρμογής τους.

Το συγκεκριμένο στάδιο διαρκεί για συγκεκριμένο χρονικό ορίζοντα το μέγεθος του οποίου θα πρέπει να ορίζεται από την διοίκηση ενός οργανισμού. Μόλις λήξει θα πρέπει το σύνολο της διαδικασίας ΔΚΠΣ να ξεκινήσει πάλι από το πρώτο στάδιο. Τα κριτήρια επιλογής του χρόνου

διάρκειας του σταδίου αξιολόγησης και αποτίμησης κινδύνων είναι κυρίως ο τύπος του οργανισμού και η αποστολή του.

Οργανισμοί που ανήκουν στον τεχνολογικό τομέα της οικονομίας και ιδιαίτερα εταιρίες του διαδικτύου, εξαρτώνται σε πολύ μεγάλο βαθμό από την χρήση της τεχνολογίας και από τις ραγδαίες αλλαγές που πραγματοποιούνται στο εξωτερικό κυρίως περιβάλλον λειτουργίας τους. Επομένως, ένας οργανισμός αυτού του είδους πρέπει να θέσει μικρότερο χρονικό ορίζοντα εφαρμογής για αυτό το στάδιο, σε σχέση με τους παραδοσιακούς οργανισμούς, προκειμένου ο κύκλος της ΔΚΠΣ να έχει συνολικά μικρότερη διάρκεια. Αυτό θα έχει ως αποτέλεσμα οι αλλαγές στις παραμέτρους που προσδιορίζουν τους κινδύνους (ευπάθειες, πηγές απειλών) να προσδιορίζονται με επαρκή αμεσότητα προκειμένου για την έγκαιρη αντιμετώπιση τους. Η σημασία παρακολούθησης του επιπέδου ασφαλείας των ΠΣ ενός οργανισμού, λαμβάνοντας την διάσταση του χρόνου δυναμικά, αναλύεται στο κεφάλαιο 6. Το μοντέλο ποσοτικοποίησης που περιγράφεται δημιουργήθηκε χρησιμοποιώντας τον χρόνο ως μια από τις βασικές παραμέτρους του.

3.3 Οι κίνδυνοι Πληροφοριακών Συστημάτων στα πλαίσια του συνόλου εταιρικών κινδύνων

Η διαδικασία ΔΚΠΣ μπορεί να θεωρηθεί ως ένα μέρος του συνόλου διαδικασιών που απαρτίζουν την Εταιρική Διαχείριση Κινδύνων (Enterprise Risk Management). Η εννοιολογική προσέγγιση της Εταιρικής Διαχείρισης Κινδύνων (ΕΔΚ) έχει αποδοθεί με διάφορους τρόπους. Η πλέον αποδεκτή προσέγγιση προέρχεται από την Committee of Sponsoring Organizations of the Treadway Commission (COSO) [**52**] όπου η ΕΔΚ αναφέρεται ως η διαδικασία που επηρεάζεται από όλα τα κλιμάκια διοίκησης ενός οργανισμού, εφαρμόζεται στον καθορισμό στρατηγικών, σχεδιάζεται προκειμένου να προσδιορίζει πιθανά αρνητικά γεγονότα, ώστε να διαχειρίζεται τους κινδύνους σύμφωνα με τα ιδιαίτερα χαρακτηριστικά ενός οργανισμού και να παρέχει επαρκή ασφάλεια κατά την διαδικασία επίτευξης των εταιρικών του στόχων. Η λειτουργία της ΕΔΚ ασχολείται με την έκθεση σε κινδύνους σε μία γενική βάση με την έννοια ότι εξετάζει όλες τις πτυχές της εταιρείας και αναλύει τους κινδύνους σε βραχυπρόθεσμο και σε μακροπρόθεσμο χρονικό ορίζοντα.

Το προτεινόμενο πλαίσιο ΕΔΚ της COSO περιλαμβάνει οκτώ αλληλεξαρτώμενα στάδια τα οποία έχουν μεγάλη συσχέτιση με τα στάδια της διαδικασίας ΔΚΠΣ που περιγράφτηκαν στις προηγούμενες ενότητες. Το στάδιο του προσδιορισμού των κινδύνων χωρίζεται ουσιαστικά σε τρία διακριτά στάδια: (α) Ανάλυση εσωτερικού περιβάλλοντος, (β) θέσπιση των στόχων του συστήματος διαχείρισης κινδύνων και (γ) προσδιορισμός αρνητικών γεγονότων. Το στάδιο της εκτίμησης κινδύνων είναι διακριτό και σε αυτή την μεθοδολογία επιβεβαιώνοντας την σημασία που έχει η συγκεκριμένη διαδικασία για το σύνολο του συστήματος. Το στάδιο της αντιμετώπισης κινδύνων διακρίνεται επίσης σε τρία στάδια τα οποία είναι ως εξής: (α) Επιλογή μέτρων αντιμετώπισης κινδύνων, (β) θέσπιση κανόνων και διαδικασιών για την αποτελεσματική εφαρμογή των επιλεγμένων μέτρων αντιμετώπισης κινδύνων και (γ) επικοινώνηση της πορείας εφαρμογής και των αποτελεσμάτων του συστήματος διαχείρισης. Το τελευταίο στάδιο της αξιολόγησης και αποτίμησης κινδύνων είναι κοινό στο προτεινόμενο πλαίσιο από την COSO και το πλαίσιο που περιγράφεται στην ενότητα 3.2.

Η παραπάνω αναφερόμενη συσχέτιση των πλαισίων διαχείρισης κινδύνων, σε ολιστικό επίπεδο και σε επίπεδο ΠΣ, επιβεβαιώνεται από το γεγονός ότι το πλαίσιο Risk IT του ISACA [**49**] βασίζεται στο πλαίσιο της COSO για την ΕΔΚ. Η σχέση της φύσης των κινδύνων ΠΣ και της διαχείρισης τους υπό το πρίσμα της ολιστικής θεώρησης των κινδύνων αναλύεται στις επόμενες παραγράφους.

Η εξασφάλιση της ακεραιότητας του ΠΣ ενός οργανισμού εξασφαλίζει παράλληλα την απρόσκοπτη συνέχιση της λειτουργίας του και προστατεύει την φήμη και το όνομα του. Μπορούμε να πούμε πως, καθώς η ευαισθησία των αγορών αυξάνεται σε θέματα ασφαλείας ΠΣ, αυξάνεται αναλογικά και η συσχέτιση των κινδύνων ΠΣ με τις λοιπές κατηγορίες κινδύνων που αντιμετωπίζει ένας οργανισμός. Η συσχέτιση μεταξύ εταιρικών κινδύνων είναι μία ιδιότητα που υφίσταται λόγω της φύσης των ίδιων των κινδύνων. Το θέμα όμως της συσχέτισης των κινδύνων ΠΣ με άλλους εταιρικούς κινδύνους όπως είναι ο νομικός κίνδυνος ή ο κίνδυνος φήμης θεωρούταν μέχρι πρότινος πολύ μικρής ή άνευ σημασίας. Η ανάπτυξη όμως της ΕΔΚ και η δημιουργία μίας περισσότερο διευρυμένης και ολοκληρωμένης άποψης για τους κινδύνους, σε συνδυασμό με την αυξανόμενη βαρύτητα των κινδύνων ΠΣ και στις επιπλοκές που δύναται να έχουν με άλλα είδη κινδύνων, οδηγεί πλέον στην αναγκαιότητα ανάλυσης των κινδύνων ΠΣ υπό διαφορετική σκοπιά. Διάφοροι παράγοντες, που πρότινος είτε δεν υφίσταντο είτε είχαν σχετικά

μικρή σημασία, έχουν οδηγήσει την κατηγορία των κινδύνων ΠΣ να είναι πλέον μία από τις πολυπλοκότερες που έχει να αντιμετωπίσει ένας οργανισμός. Οι παράγοντες αυτοί μπορούν να συνοψισθούν ως εξής:

(α) Η σημαντικότητα και η διάδοση των ΠΣ βασισμένων σε τεχνολογίες πληροφορικής σχεδόν σε κάθε σημαντική δραστηριότητα των οργανισμών κάθε κατηγορίας είναι ο βασικότερος παράγοντας της ολοένα και πιο έντονης συσχέτισης των κινδύνων ΠΣ με αρκετούς από τους λοιπούς βασικότερους εταιρικούς κινδύνους. Συνεπώς η διάδοση της τεχνολογίας πληροφορικής οδηγεί τους κινδύνους ΠΣ να λαμβάνουν ολοένα και μεγαλύτερη βαρύτητα στο σύνολο των κινδύνων που αντιμετωπίζει ένας οργανισμός. Επίσης, η αυξανόμενη πολυπλοκότητα των κινδύνων ΠΣ κάνει την μέτρηση και τον απολογισμό των επιπτώσεων ένα εγχείρημα ολοένα και πιο δύσκολο.

(β) Μία άλλη παράμετρος, που οδηγεί στην πολυπλοκότητα των κινδύνων ΠΣ, είναι η ραγδαία πρόοδος της τεχνολογίας πληροφόρησης. Η ταχύτητα ανακάλυψης νέων δεδομένων για την επιστήμη της Πληροφορικής συχνά δεν ακολουθείται από την ταυτόχρονη προσαρμογή των κανόνων, των τεχνολογιών και των μεθοδολογιών για την διαχείριση των κινδύνων ΠΣ. Συνεπώς η ακατάπαυστη πρόοδος της τεχνολογίας οδηγεί στον χαρακτηρισμό των κινδύνων ΠΣ ως μία έννοια εντελώς μεταβλητή στο χρόνο ανεξάρτητα από το είδος του οργανισμού που τον αντιμετωπίζει.

(γ) Επίσης σημαντική παράμετρος είναι ο αυξανόμενος αριθμός επιχειρήσεων που πραγματοποιούν το σύνολο των οργανικών δραστηριοτήτων τους μέσω του διαδικτύου. Οι κίνδυνοι ΠΣ για αυτές τις επιχειρήσεις είναι πολύ μεγαλύτεροι και πολυπλοκότεροι στην ανάλυση και διαχείριση. Αυτός είναι ο βασικότερος λόγος που υιοθετήθηκε στην παρούσα διατριβή ο διαχωρισμός των οργανισμών μεταξύ τεχνολογικών και μη τεχνολογικών.

Γενικώς, η αλληλοσυσχέτιση μεταξύ των διαφορετικών κατηγοριών κινδύνου πρέπει να λαμβάνεται υπόψη κατά την διαδικασία ποσοτικοποίησης του συνολικού επιπέδου έκθεσης καθώς το τελευταίο δεν προέρχεται από την απλή πρόσθεση των εκτιμήσεων που έχει λάβει ο κάθε κίνδυνος. Η απλοϊκή αυτή ενοποίηση των διαφορετικών εκτιμήσεων υπερεκτιμά το συνολικό επίπεδο έκθεσης καθώς δεν λαμβάνεται υπόψη η επίδραση διασποράς (diversification) η οποία

αποτελεί ένα από τα σημαντικότερα οφέλη από την εφαρμογή των μεθοδολογιών ΕΔΚ. Επίσης, ένα δεύτερο μειονέκτημα της εξατομικευμένης διαχείρισης κινδύνων, χωρίς να λαμβάνονται υπόψη οι αλληλοσυσχετίσεις που υφίσταται, είναι η αγνόηση της περίπτωσης μεταβίβασης μίας έκθεσης από ένα σημείο ενός οργανισμού σε ένα άλλο. Για παράδειγμα, η υιοθέτηση μίας καινούριας τεχνολογίας μπορεί να μειώσει οργανικούς κινδύνους που σχετίζονται με την διατήρηση ανταγωνιστικών πλεονεκτημάτων αλλά παράλληλα να δημιουργήσει ανόργανους κινδύνους σχετικούς με θέματα ασφαλείας οι οποίοι με την σειρά τους να αυξήσουν έμμεσα τους νομικούς κινδύνους.

Επανερχόμενοι στους κινδύνους ΠΣ, ορισμένοι εξ αυτών δύναται να αποτελούν μέρος ενός μεγαλύτερου εταιρικού κινδύνου και συνεπώς η εξατομικευμένη αντιμετώπιση τους μπορεί να μην αποδώσει επιθυμητά αποτελέσματα. Οι οργανικοί κίνδυνοι ΠΣ, που προέρχονται από την υιοθέτηση νέων επενδυτικών σχεδίων πληροφορικής, αποτελούν μία τέτοια περίπτωση. Ορισμένοι κίνδυνοι αυτής της κατηγορίας, όπως είναι η υπέρβαση προϋπολογισμού και η καθυστέρηση αποπεράτωσης, μπορούν να υπαχθούν στην ευρύτερη κατηγορία των κινδύνων επενδυτικών σχεδίων (project risks). Εφαρμόζοντας συνολική αντιμετώπιση των κινδύνων επενδυτικών σχεδίων μπορεί να οδηγήσει σε διασπορά και αντιστάθμιση σημαντικού μέρους του συνολικού κινδύνου. Γενικά, το μέρος των κινδύνων ΠΣ που υπάγεται στους οργανικούς κινδύνους μπορεί να ενταχθεί σε ευρύτερες κατηγορίες κινδύνων που αντιμετωπίζει ένας οργανισμός και μέσω εφαρμογής μεθοδολογιών ΕΔΚ, να επιτευχθούν σημαντικές ωφέλειες διασποράς και αντιστάθμισης μέρους των κινδύνων. Η δυνατότητα αντιστάθμισης προέρχεται από το γεγονός ότι οι συγκεκριμένοι κίνδυνοι είναι συμμετρικοί.

Επομένως, εφαρμόζοντας ένας οργανισμός επαρκώς διαδικασίες ΕΔΚ μπορεί να επιτύχει εξοικονόμηση πόρων καθώς σε περιπτώσεις αντιμετώπισης κινδύνων, όπως είναι οι οργανικοί κίνδυνοι ΠΣ, θα χρειαστεί η επιλογή αντίμετρων μόνο για τον εναπομείναν κίνδυνο (residual risk). Ο εναπομείναν κίνδυνος προκύπτει ως το υπόλοιπο έκθεσης που έχει ένα στοιχείο ενεργητικό σε κινδύνους αφού εφαρμοστούν πρώτα μέθοδοι αντιμετώπισης του. Αντιθέτως, οι μη συμμετρικοί κίνδυνοι ΠΣ είναι δύσκολο να αντισταθμιστούν και συνεπώς τα οφέλη, από την εφαρμογή μεθοδολογιών ΕΔΚ, για αυτήν την κατηγορία κινδύνων είναι περιορισμένα. Οι κίνδυνοι παραβιάσεων ασφαλείας είναι ανόργανοι λειτουργικοί κίνδυνοι μη συμμετρικού χαρακτήρα

καθώς οι συνέπειες τους είναι πάντα αρνητικές για έναν οργανισμό. Οι κίνδυνοι αυτοί είναι δύσκολο να αντιμετωπισθούν σε συνολική βάση με άλλους τύπους κινδύνων.

Τα προαναφερόμενα οδηγούν σε μία ακόμα κατηγοριοποίηση των κινδύνων ΠΣ με κριτήριο την δυνατότητα επίτευξης αντιστάθμισης μέσω της αντιμετώπισης τους υπό το πλαίσιο της ΕΔΚ. Η πρώτη κατηγορία περιλαμβάνει τους κινδύνους που μπορούν να αντισταθμιστούν σε μεγάλο βαθμό μέσω της αντιμετώπισης τους σε συνδυασμό με κινδύνους άλλων κατηγοριών. Σε αυτήν την κατηγορία ανήκουν κυρίως οι οργανικοί κίνδυνοι ΠΣ. Η δεύτερη κατηγορία περιλαμβάνει τους κινδύνους στους οποίους τα οφέλη αντιστάθμισης, μέσω της χρήσης μεθόδων ΕΔΚ, είναι είτε πολύ μικρά είτε ανύπαρκτα. Η ασφάλεια ΠΣ και οι κίνδυνοι που οδηγούν στην παραβίαση της, όπως είναι φυσικές καταστροφές, η κλοπή στοιχείων ΠΣ και η διαδικτυακή εισβολή ανήκουν σε αυτήν την κατηγορία.

Συνεπώς, η εφαρμογή ΕΔΚ μπορεί να προσδώσει μεγάλη προστιθέμενη αξία σε έναν οργανισμό και να αντιμετωπισθεί αποτελεσματικότερα ένα σημαντικό μέρος των κινδύνων ΠΣ. Η έννοια αποτελεσματικότερα αναφέρεται κυρίως στην επίτευξη του ίδιου επιπέδου εναπομείναντος κινδύνου με την κατανάλωση λιγότερων εταιρικών πόρων. Η εφαρμογή ΕΔΚ δεν επιρρεάζει τις άμεσα ποσοτικοποιήσιμες οικονομικές επιπτώσεις των κινδύνων παραβιάσεων ασφαλείας. Οι έμμεσες επιπτώσεις, καθώς έχουν συσχέτιση και προκαλούνται σε συνδυασμό με άλλες κατηγορίες κινδύνων, μπορούν να μελετηθούν πληρέστερα μέσω της μεθοδολογίας ΕΔΚ. Κατά κύριο λόγο, η ωφέλεια της ΕΔΚ έγκειται στην εκτενέστερη εμβάθυνση των αλληλοσυσχετίσεων που έχουν οι κίνδυνοι παραβιάσεων ασφαλείας με άλλους κινδύνους όπως είναι οι νομικοί κίνδυνοι, οι κίνδυνοι φήμης και οι κίνδυνοι κανονιστικών πλαισίων.

Επομένως, η εφαρμογή διαδικασιών ΕΔΚ μπορεί να αποδώσει σημαντική προστιθέμενη αξία στην διαχείριση του έμμεσου μέρους των λειτουργικών ενδογενών κινδύνων ΠΣ. Η εμβάθυνση στις αλληλοσυσχετίσεις των κινδύνων ΠΣ αυτής της κατηγορίας με άλλων ειδών εταιρικούς κινδύνους μπορεί να ενισχύσει την διαδικασία ΔΚΠΣ σε όλα τα στάδια και κυρίως τα δύο πρώτα. Συγκεκριμένα, στο στάδιο προσδιορισμού των κινδύνων μπορεί να επιτευχθεί αποτελεσματικότερη οριοθέτηση των στόχων για το σύνολο της διαδικασίας και στην συνέχεια πληρέστερη καταγραφή των πιθανών γεγονότων με εν δυνάμει αρνητικό αντίκτυπο. Επίσης, στο στάδιο της εκτίμησης κινδύνων μπορεί να γίνει ακριβέστερη ποσοτικοποίηση του έμμεσου κόστους το οποίο είναι πολύ δυσκολότερο να αποτιμηθεί σε σχέση με το άμεσο κόστος. Η

ποσοτικοποίηση του έμμεσου κόστους των παραβιάσεων ασφαλείας και η διερεύνηση της συσχέτισης των κινδύνων ΠΣ με άλλους εταιρικούς κινδύνους αποτέλεσαν σημαντικές ερευνητικές θεματολογίες στα πλαίσια της παρούσας.

4 Παραβίαση ασφαλείας και πηγές δεδομένων περιστατικών παραβίασης ασφαλείας

4.1 Εισαγωγή

Το κεφάλαιο αυτό είναι χωρισμένο σε δύο βασικές ενότητες. Η πρώτη ενότητα είναι αφιερωμένη στην εννοιολογική προσέγγιση της παραβίασης ασφαλείας και στην ανάλυση των ιδιαίτερων χαρακτηριστικών που την διέπουν. Θεωρήθηκε θεμιτό να αναπτυχθεί σε ξεχωριστή ενότητα η συγκεκριμένη έννοια καθώς αποτελεί ένα από τα κύρια θεματικά κέντρα της συγκεκριμένης διατριβής και πρέπει να αποδοθεί αναλυτικά η προσέγγιση που έλαβε στο πλαίσιο της ερευνητικής προσπάθειας. Προς αυτή την κατεύθυνση γίνεται ανάλυση των κατηγοριών στις οποίες μπορούν να διαχωριστούν τα συγκεκριμένα περιστατικά καθώς και των κατηγοριών στις οποίες μπορούν να ενταχθούν οι οικονομικές επιπτώσεις τους. Επίσης, αναλύεται η διαδικασία αντιμετώπισης ενός περιστατικού παραβίασης ασφαλείας από έναν οργανισμό.

Στην επόμενη ενότητα αναλύονται οι βασικές πηγές καταγραφής και ανάλυσης δεδομένων περιστατικών παραβίασης ασφαλείας. Οι πηγές αυτές διαχωρίστηκαν σε κατηγορίες με κριτήριο τις ανάγκες τις παρούσας έρευνας. Η κυριότερη κατηγορία αποτελείται από έρευνες σχετικά με την ασφάλεια ΠΣ και την προσέγγιση των οικονομικών επιπτώσεων που επιφέρουν τα περιστατικά παραβίασης ασφαλείας. Αρχικά, παραθέτονται κάποιες εισαγωγικές παρατηρήσεις σχετικά με τις έρευνες αυτού του είδους, τα πλεονεκτήματα αλλά και τους περιορισμούς που έχουν. Στην συνέχεια αναλύονται τα αποτελέσματα των πρόσφατων ερευνών καταμερισμένα σε βασικές κατηγορίες με συγκριτική ανάλυση των αποτελεσμάτων τους, προκειμένου για την εκροή συγκεντρωτικών και περιεκτικών συμπερασμάτων. Η δεύτερη κατηγορία πηγών δεδομένων, που μπορούμε να διακρίνουμε, αποτελείται από τις εμπειρικές μελέτες που βασίζονται στην μεθοδολογία ανάλυσης γεγονότων. Οι μελέτες αυτές αναλύονται διεξοδικά στο Κεφάλαιο 5. Τα συγκεντρωτικά αποτελέσματα και συμπεράσματα χρησιμοποιήθηκαν, σε συνάρτηση με τα αντίστοιχα συμπεράσματα των εμπειρικών προσεγγίσεων, στο Κεφάλαιο 7 στην εκτίμηση των κινδύνων παραβιάσεων ασφαλείας. Τέλος, περιγράφεται η τρίτη κατηγορία πηγών δεδομένων περιστατικών ασφαλείας που περιλαμβάνει διαδικτυακούς τόπους καταγραφής και ανάλυσης περιστατικών.

4.2 Περιστατικά παραβίασης ασφάλειας

4.2.1 Εννοιολογική προσέγγιση

Στην Ενότητα 2.2.3 ορίστηκε η έννοια του περιστατικού κινδύνου. Η παρούσα διατριβή πραγματεύεται περιστατικά κινδύνου που σχετίζονται με παραβιάσεις ασφάλειας. Ακριβής ορισμός της παραβίασης ασφαλείας με ευρεία αποδοχή από τις ρυθμιστικές αρχές και την ερευνητική κοινότητα δεν υφίσταται. Τα σημεία τα οποία υπάρχει σύγχυση μεταξύ των διαφόρων ορισμών είναι τα εξής:

(α) Οριοθέτηση με αντικειμενικότητα και ακρίβεια των ευαίσθητων προσωπικών δεδομένων.

(β) Ο προσδιορισμός ύπαρξης κινήτρου, από την πλευρά του μη εξουσιοδοτημένου φορέα, προκειμένου να χρησιμοποιήσει για εγκληματικούς σκοπούς προσωπικά δεδομένα που περιέρχονται στην κατοχή του.

(γ) Η απόδειξη προσπέλασης προσωπικών δεδομένων από μη εξουσιοδοτημένο φορέα, στην κατοχή του οποίου περιήλθαν συγκεκριμένα δεδομένα.

Οι περιπτώσεις κλοπής αποθηκευτικών μέσων είναι από τα περισσότερο συχνά περιστατικά κινδύνου που, λόγω των προαναφερομένων (β) και (γ) σημείων, έχουν προβληματίσει υπό ποιες συνθήκες μπορούν να θεωρηθούν παραβιάσεις ασφαλείας. Ένα μεγάλο μέρος των κλοπών υλικού τεχνολογίας γίνεται με κίνητρο την αξία του ίδιου του υλικού χωρίς να ενδιαφέρει την πηγή απειλής η πιθανή αξία που μπορεί να αποφέρει η εκμετάλλευση των ευαίσθητων δεδομένων που περιέχονται. Συνεπώς σε αυτές τις περιπτώσεις, που έχουμε έλλειψη κινήτρου για τον φορέα της απειλής, δεν υλοποιείται ουσιαστικά περιστατικό παραβίασης ασφαλείας. Αυτό που μπορούμε να συμπεράνουμε είναι πως η χρήση κινητών μέσων αποθήκευσης αυξάνει σημαντικά την πιθανότητα παραβίασης ασφαλείας αλλά η πραγμάτωση της πρέπει, εκτός της απώλειας του υλικού, να προϋποθέτει ταυτόχρονα κίνητρο και απόδειξη προσπέλασης των δεδομένων.

Λαμβάνοντας υπόψη τα παραπάνω, προκειμένου για της ανάγκες της παρούσας διατριβής, μία παραβίαση ασφάλειας ορίζεται ως ένα περιστατικό το οποίο οδηγεί στην αποδεδειγμένη παραβίαση είτε της εμπιστευτικότητας, είτε της διαθεσιμότητας, είτε της ακεραιότητας ενός ΠΣ και των δεδομένων που διαχειρίζεται. Ο ορισμός δεν περιορίζει τα περιστατικά μόνο σε αυτά που

αφορούν την εμπιστευτικότητα και την ακεραιότητα δεδομένων που είναι πλέον η συνήθης πρακτική σε κανονιστικά πλαίσια, νομολογίες αλλά και ακαδημαϊκές μελέτες. Προϋποθέτει δε την αποδεδειγμένη παραβίαση ενός εκ των τριών προαναφερομένων βασικών ιδιοτήτων της ασφάλειας δεδομένων.

Είναι βασικό σε αυτό το σημείο να οριοθετηθεί η έννοια της εγγραφής πληροφοριών (record of data). Στα πλαίσια της παρούσας διατριβής μία εγγραφή πληροφοριών ορίζεται ως μία αυτόνομη, εμπιστευτικού χαρακτήρα ευαίσθητη πληροφόρηση για ένα πρόσωπο είτε φυσικό, είτε νομικό. Μία εγγραφή[1] μπορεί να αφορά είτε προσωπικά δεδομένα όπως αριθμούς κοινωνικής ασφάλισης, κινήσεις Τραπεζικών λογαριασμών και αριθμούς πιστωτικών καρτών. Εξίσου, και περισσότερο κατά περιπτώσεις, σημαντικό είναι μία εγγραφή να αποτελείται από εταιρικά μυστικά όπως πιστοποιητικά ασφαλείας, κώδικα προγραμμάτων, κωδικούς ασφαλείας, απόρρητα έγγραφα με εμπορικά μυστικά και λίστες πελατών. Ο αριθμός των εγγραφών, που εκτίθενται μέσω μίας παραβίασης ασφαλείας, μπορεί να αποτελέσει κριτήριο για το μέγεθος ενός περιστατικού, όπως αναλύεται στην Παράγραφο 5.6.3, και να χρησιμοποιηθεί ως κριτήριο για τον διαχωρισμό των περιστατικών σε κατηγορίες.

4.2.2 Κίνδυνοι Πληροφοριακών Συστημάτων και κίνδυνοι παραβιάσεων ασφαλείας

Στο Κεφάλαιο 2 περιγράφτηκε το σύνολο των εταιρικών κινδύνων και αναλύθηκε η ένταξη των κινδύνων Πληροφοριακών Συστημάτων (ΠΣ) μέσα στον «γαλαξία κινδύνων» ενός οργανισμού. Όπως ήδη αναλύθηκε οι κίνδυνοι ΠΣ μπορούν να διακριθούν σε δύο γενικές κατηγορίες με κριτήριο την οργανική ή ανόργανη υπόσταση που έχουν μέσα σε έναν οργανισμό.

Οι οργανικοί κίνδυνοι ΠΣ, που απαρτίζουν την πρώτη κατηγορία, προέρχονται από τους κινδύνους ανάληψης, υλοποίησης και ένταξης στην παραγωγική δομή ενός οργανισμού επενδυτικών σχεδίων ΠΣ (Information System projects). Χαρακτηριστικά παραδείγματα κινδύνων, που ανήκουν σε αυτή την κατηγορία, είναι υπερβάσεις προϋπολογισμού, αποκλίσεις από τον χρόνο υλοποίησης, άρνηση αποδοχής ενός συστήματος από την υφιστάμενη εταιρική

[1] Στο υπόλοιπο της συγκεκριμένης διατριβής, χάριν συντομίας, η εγγραφή πληροφοριών θα αναφέρεται απλά ως εγγραφή.

κουλτούρα και μείωση της αποδοτικότητας και παραγωγικότητας από την εγκατάσταση ενός συστήματος.

Οι ανόργανοι κίνδυνοι ΠΣ, που αποτελούν την δεύτερη κατηγορία, εντάσσονται στην γενικότερη κατηγορία των λειτουργικών ενδογενών κινδύνων ενός οργανισμού που προέρχονται από το ανθρώπινο στοιχείο και τα συστήματα. Αποτελούνται από τους κινδύνους ΠΣ που δεν αναλαμβάνονται από έναν οργανισμό προκειμένου για την εκπλήρωση των εταιρικών σκοπών. Αντιθέτως, οι κίνδυνοι αυτοί εμποδίζουν τους εταιρικούς σκοπούς και βασικός μέλημα ενός οργανισμού είναι η διαχείριση τους.

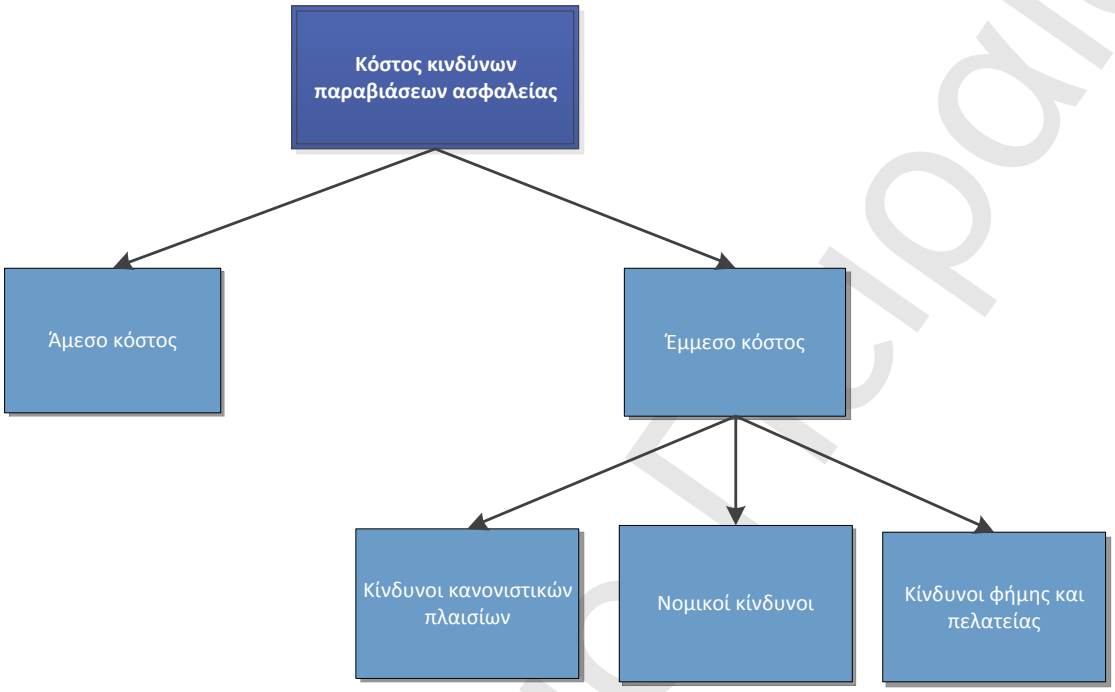
Η βασικότερη κατηγορία των κινδύνων ΠΣ είναι οι κίνδυνοι που προέρχονται από περιστατικά παραβιάσεων ασφαλείας των οποίων η ποσοτικοποίηση και η κατάλληλη αντιμετώπιση αποτελεί πλέον μία από τις βασικές προτεραιότητες ενός οργανισμού. Οι επιπτώσεις που μπορούν να επιφέρουν οι συγκεκριμένοι κίνδυνοι αυξάνονται διαρκώς σε πολυπλοκότητα καθώς μπορούν να επηρεάσουν υλικές και άυλες αξίες, να υλοποιηθούν είτε σε βραχυπρόθεσμο είτε σε μακροπρόθεσμο ορίζοντα και εμφανίζουν σημαντική συσχέτιση με άλλες κατηγορίες σημαντικών κινδύνων. Στις παραγράφους που ακολουθούν αναλύονται τα σημαντικότερα χαρακτηριστικά που οδηγούν στην προαναφερόμενη πολυπλοκότητα τους κινδύνους παραβιάσεων ασφαλείας. Η περιγραφή αυτή είναι χρήσιμη προκειμένου για την οριοθέτηση διαφόρων παραμέτρων που χρησιμοποιήθηκαν από την ερευνητική προσπάθεια.

4.2.3 Κατηγορίες του κόστους παραβίασης ασφαλείας

Τα περιστατικά ασφαλείας στα οποία παραβιάζεται η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα ευαίσθητης πληροφόρησης δημιουργούν οικονομικές επιπτώσεις οι οποίες είναι αδύνατο να υπολογιστούν στο σύνολο τους εκ των προτέρων. Το συνολικό κόστος, που προέρχεται από ένα περιστατικό παραβίασης ασφαλείας είναι πολύπλευρο και επιμερίζεται σε άμεσο κόστος και έμμεσο κόστος όπως αποτυπώνεται στην Εικόνα 10. Το γεγονός της πολύπλευρης υπόστασης, που έχει το σύνολο των επιπτώσεων ενός περιστατικού ασφαλείας, δημιουργεί το βασικότερο πρόβλημα για την πλήρη και αντικειμενική κοστολόγηση τους.

Το άμεσο κόστος αποτελείται από τις οικονομικές επιπτώσεις που επωμίζεται ένας οργανισμός σε βραχυπρόθεσμο ορίζοντα. Καλείται επίσης και ενυπόστατο κόστος (tangible cost) καθώς τα

στοιχεία που το συνθέτουν είναι απτά και προσδιορίσιμα. Προέρχεται από διάφορες κατηγορίες αιτιών από τις οποίες οι πιο σημαντικές είναι οι εξής:



Εικόνα 10: Κόστος κινδύνων παραβιάσεων ασφαλείας

(α) Το κόστος παρακολούθησης των λογαριασμών φυσικών και νομικών προσώπων των οποίων προσωπικά, ευαίσθητα δεδομένα εκτέθηκαν. Η παρακολούθηση γίνεται προς την αποφυγή οικονομικής απάτης προερχόμενη από την χρήση ευαίσθητων πληροφοριών από κακόβουλους χειριστές.

(β) Το κόστος ενίσχυσης του λογισμικού συστημάτων ασφαλείας προκειμένου να αυξηθεί επαρκώς η αποδοτικότητα των αντίμετρων αντιμετώπισης των ευπαθειών που εκμεταλλεύτηκε κάποια πηγή απειλής και προκάλεσε ένα περιστατικό ασφαλείας.

(γ) Ενίσχυση των αντίμετρων αντιμετώπισης ευπαθειών μέσω ενίσχυσης των διατάξεων και της εφαρμογής των κανονιστικών πλαισίων ασφαλείας ΠΣ ενός οργανισμού.

(δ) Πληρωμή προστίμων προς τις εκάστοτε εποπτικές αρχές που είναι υπεύθυνες για την ασφάλεια των προσωπικών δεδομένων και στις οποίες υπάγεται ο οργανισμός που προσβλήθηκε.

Το σύνολο σχεδόν των άμεσων επιπτώσεων είναι μετρήσιμο και η ακριβής ποσοτικοποίηση του με επαρκή αντικειμενικότητα δεν αποτελεί ιδιαίτερο πρόβλημα για έναν οργανισμό. Όπως αναλύεται στην επόμενη ενότητα, σχετικά με τις έρευνες ασφαλείας από διεθνείς μελετητικούς οργανισμούς, το άμεσο κόστος από παραβιάσεις ασφαλείας μπορεί να προσεγγιστεί με σχετικά επαρκή αντικειμενικότητα και ακρίβεια.

Το έμμεσο κόστος αποτελείται από τις οικονομικές επιπτώσεις μίας παραβίασης ασφαλείας σε μεσοπρόθεσμο και μακροπρόθεσμο ορίζοντα. Καλείται επίσης και άυλο κόστος (intangible cost) προκειμένου να αποδοθεί η ασαφής υπόσταση του. Αποτελείται κυρίως από τις εξής κατηγορίες αιτιών:

(α) Νομικό κόστος από δικαστικές διενέξεις με τις εποπτικές αρχές, από φυσικά και νομικά πρόσωπα που θεωρούν ότι υπέστησαν βλάβη από την έκθεση ευαίσθητων προσωπικών τους δεδομένων. Το τελικό κόστος που μπορεί να επωμιστεί ένας οργανισμός, ως απόρροια μίας παραβίασης ασφαλείας, μπορεί να χρειαστούν χρόνια ώστε να λάβει πλήρη υπόσταση και δύναται να φτάσει σε τεράστια μεγέθη. Από το σύνολο της έρευνας που έγινε, προέκυψε το συμπέρασμα, πως ο νομικός κίνδυνος είναι ο περισσότερο άμεσα συσχετιζόμενος κίνδυνος με τους κινδύνους παραβιάσεων ασφαλείας.

(β) Κόστος προερχόμενο από την αρνητική επίπτωση ενός περιστατικού στην φήμη ενός οργανισμού. Ο παράγοντας αυτός είναι άμεσα συσχετιζόμενος με τον κλάδο δραστηριοποίησης στον οποίο υπάγεται ένας οργανισμός. Όπως αναλύεται στο Κεφάλαιο 5, εταιρίες τεχνολογίας, παροχείς συστημάτων ασφαλείας και εταιρίες ηλεκτρονικού εμπορίου επηρεάζονται σε σημαντικά μεγαλύτερη κλίμακα από μία παραβίαση ασφαλείας σε σχέση με το σύνολο των υπολοίπων οργανισμών. Η διαφοροποίηση αυτή προέρχεται κυρίως από το έμμεσο κόστος, το οποίο στους οργανισμούς αυτού του είδους, είναι περισσότερο ευαίσθητο σε περιστατικά ασφαλείας. Ο κίνδυνος φήμης ενός οργανισμού συνεπώς έχει μεγαλύτερη συσχέτιση με τους κινδύνους παραβιάσεων ασφαλείας για συγκεκριμένους τύπους οργανισμών.

(γ) Κόστος προερχόμενο από απώλεια πελατείας το οποίο οδηγεί στην απώλεια μελλοντικών χρηματοροών. Η αποτύπωση της συγκεκριμένης επίπτωσης

πραγματοποιείται επίσης σε μακροπρόθεσμο ορίζοντα. Το μέγεθος της επίπτωσης εξαρτάται κυρίως από το είδος του οργανισμού που προσβάλλεται και ισχύουν αυτά που διατυπώθηκαν στην προηγούμενη παράγραφο.

(δ) Κόστος προερχόμενο από τα υφιστάμενα κανονιστικά πλαίσια και τις πιθανές εναλλακτικές ερμηνείες που δύναται να επιδέχονται. Τα κανονιστικά πλαίσια διαφέρουν σε μεγάλο βαθμό ανάλογα με την χώρα εγκατάστασης ενός οργανισμού και συνεπώς η οικονομική επίπτωση τους εξαρτάται από την γεωγραφική προέλευση ενός περιστατικού παραβίασης ασφαλείας. Η συγκεκριμένη κατηγορία κινδύνου έχει μεγάλη συσχέτιση με το νομικό κόστος. Ο συνδυασμός τους μπορεί να προκαλέσει, ανάλογα από τα ιδιαίτερα χαρακτηριστικά ενός περιστατικού, πολύ υψηλότερες έμμεσες οικονομικές επιπτώσεις σε έναν οργανισμό από τις αθροιστικές επιπτώσεις που θα είχαν οι δύο αυτές κατηγορίες κινδύνων αν ήταν ανεξάρτητες μεταξύ τους.

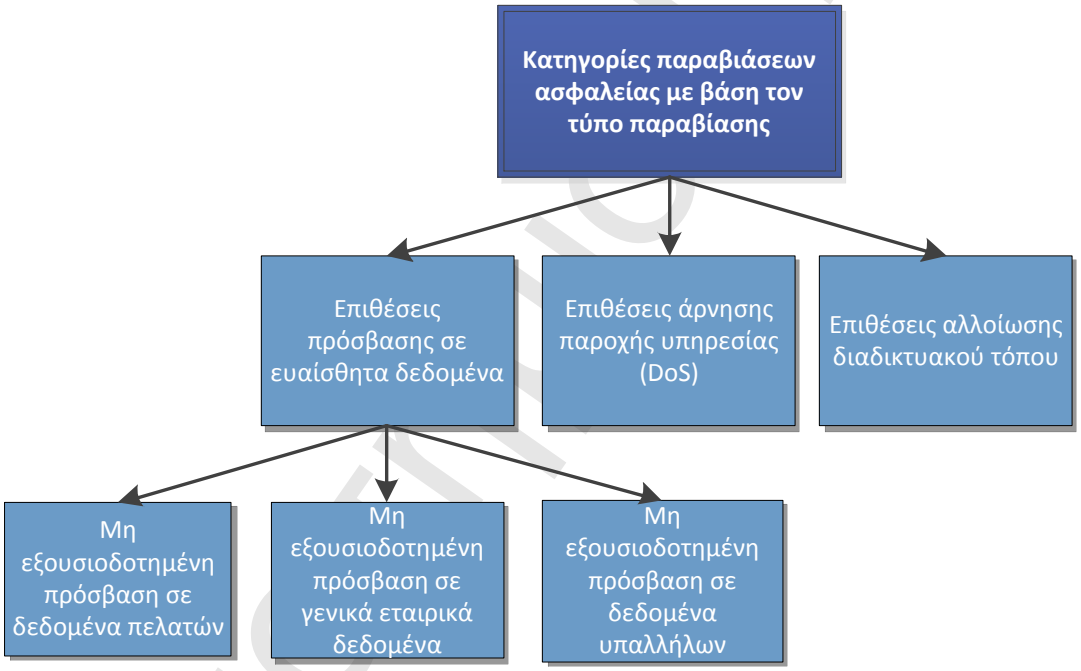
4.2.4 Κατηγορίες περιστατικών παραβίασης ασφαλείας

Η φύση μίας επίθεσης στα ΠΣ ενός οργανισμού χαρακτηρίζεται κατά κύριο λόγο από τον τύπο της παραβίασης ασφαλείας. Με βάση αυτό το κριτήριο, τα περιστατικά ασφαλείας μπορούν να διαχωριστούν σε τρεις γενικές κατηγορίες όπως αποτυπώνεται στην Εικόνα 11.

Πρώτη κατηγορία είναι η μη εξουσιοδοτημένη πρόσβαση και χρήση ευαίσθητων δεδομένων με αποτέλεσμα την παραβίασης της ασφάλειας εμπιστευτικότητας και ακεραιότητας. Το σύνολο των επιθέσεων αυτής της κατηγορίας ονομάζεται επιθέσεις πρόσβασης (access attacks). Αποτελεί την κυριότερη κατηγορία παραβιάσεων ασφαλείας σε βαθμό που σε πολλές μελέτες, ρυθμιστικά πλαίσια και στην νομοθεσία ταυτίζεται με τον ίδιο τον όρο της παραβίασης ασφαλείας. Όπως αναλύεται στα επόμενα κεφάλαια της διατριβής, το κόστος που επιφέρει αυτή η κατηγορία περιστατικών είναι πολύ μεγαλύτερο από τις άλλες δύο κατηγορίες. Επίσης, σε αριθμό περιπτώσεων, στην κατηγορία αυτή ανήκει η συντριπτική πλειοψηφία επί του συνόλου των περιστατικών. Επιμερίζεται περεταίρω σε τρεις υποκατηγορίες ανάλογα με το είδος των δεδομένων που υπόκειται σε κίνδυνο:

(1) Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών. Η συγκεκριμένη παραβίαση ασφαλείας συνήθως επιτελείται με την κλοπή κινητών μέσων αποθήκευσης και με την φυσική ή απομακρυσμένη πρόσβαση στο ΠΣ ενός οργανισμού. Η παραβίαση μπορεί

να προκληθεί από αμέλεια του προσωπικού που μπορεί να οδηγήσει είτε στην κλοπή υλικού με ευαίσθητη πληροφόρηση, είτε στην αποστολή πληροφοριών σε αποδέκτη για τις οποίες δεν έχει δικαίωμα πρόσβασης. Τα περιστατικά αυτά έχουν αυξηθεί σημαντικά μέσα στην τελευταία τριετία καθώς οι οργανισμοί παγκοσμίως, λόγω της Κρίσης του 2008, προκειμένου να μειώσουν το λειτουργικό τους κόστος, αύξησαν σταδιακά την χρήση τεχνολογιών απομακρυσμένης πρόσβασης και αποθήκευσης δεδομένων. Τα περιστατικά, που ανήκουν σε αυτή την κατηγορία, αφορούν κατά κύριο λόγο παραβιάσεις της ασφάλειας εμπιστευτικότητας και έχουν την δυναμική να δημιουργήσουν σοβαρό έμμεσο κόστος σε έναν οργανισμό μέσω δημιουργίας νομικών κινδύνων και κινδύνων φήμης και πελατείας.



Εικόνα 11: Κατηγορίες παραβιάσεων ασφαλείας με βάση τον τύπο παραβίασης

(2) Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων. Η συγκεκριμένη κατηγορία έχει πολλά κοινά χαρακτηριστικά με την προηγούμενη και αποτελεί κατά κύριο λόγο παραβίαση της ασφάλειας εμπιστευτικότητας. Το κόστος αυτών των επιθέσεων είναι συνήθως μικρότερο λόγω της συνήθης σχέσης μεγέθους που υπάρχει στις επιχειρήσεις μεταξύ του πελατολογίου και των υπαλλήλων με το πρώτο να είναι, στην πλειοψηφία

των περιπτώσεων, συντριπτικά μεγαλύτερο. Το κόστος αυτών των περιστατικών είναι κατά κύριο λόγο έμμεσο όπως συμβαίνει και στην προαναφερόμενη υποκατηγορία.

(3) Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα. Τα περιστατικά αυτής της κατηγορίας αποτελούν παραβίαση είτε της ασφάλειας εμπιστευτικότητας, είτε της ασφάλειας ακεραιότητας σε μεμονωμένο ή ταυτόχρονο επίπεδο. Το κόστος αυτών των περιστατικών είναι κατά κύριο λόγο έμμεσο και η υπόσταση του εξαρτάται από την μορφή των δεδομένων. Σοβαρά περιστατικά αυτής της κατηγορίας αφορούν την κλοπή κρατικών μυστικών και εταιρικών απορρήτων τα οποία μπορούν να οδηγήσουν σε ανεπανόρθωτες ζημιές κρατικούς και ιδιωτικούς φορείς.

Η δεύτερη κατηγορία περιστατικών παραβίασης ασφαλείας άφορα το τύπο επίθεσης άρνησης παροχής υπηρεσίας (Denial of Service – DoS). Στα περιστατικά αυτά ο εισβολέας στέλνει μεγάλο αριθμό πληροφοριών στους διακομιστές του στοχευόμενου οργανισμού προκειμένου να τους οδηγήσει σε υπερφόρτωση με σκοπό τον περιορισμό της εύρυθμης λειτουργίας τους για ένα χρονικό διάστημα. Εταιρίες όπου οι πωλήσεις τους εξαρτώνται από την εύρυθμη λειτουργία των διακομιστών τους, όπως είναι αυτές που ασχολούνται με το ηλεκτρονικό εμπόριο, μπορούν να επωμιστούν μεγάλο κόστος από τις επιθέσεις αυτού του τύπου ειδικά αν ο χρόνος δυσλειτουργίας είναι σχετικά μεγάλος. Τα περιστατικά αυτά αποτελούν χαρακτηριστικές περιπτώσεις παραβιάσεων της ασφάλειας διαθεσιμότητας.

Η τρίτη κατηγορία περιστατικών παραβίασης ασφαλείας περιλαμβάνει τις επιθέσεις αλλοίωσης εταιρικού διαδικτυακού τόπου (website alteration / defacement). Η κατηγορία αυτή αποτελεί επίσης παραβίαση της ασφάλειας διαθεσιμότητας και οι οργανισμοί που πλήττονται περισσότερο είναι πάλι οι οργανισμοί που εξαρτώνται από το διαδίκτυο για την προώθηση ή και εκτέλεση των πωλήσεων τους.

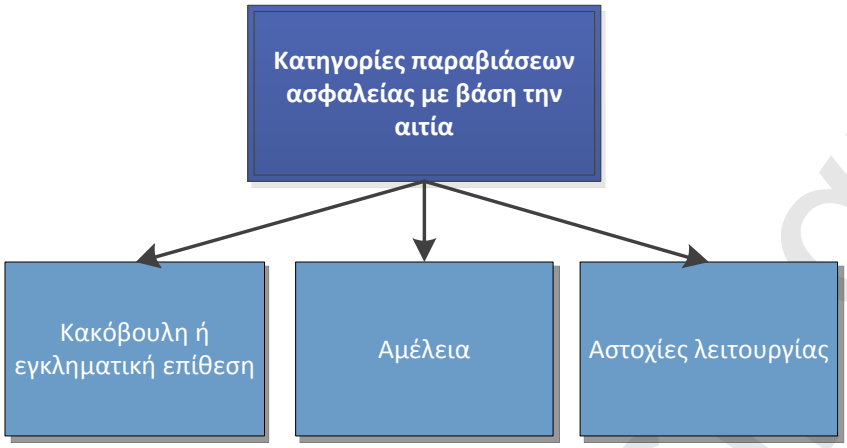
Όπως αναλύεται στις επόμενες ενότητες, τα περιστατικά τύπου παραβίασης της ασφάλειας διαθεσιμότητας, τα τελευταία χρόνια, έχουν μειωθεί σε αριθμό επιθέσεων και το κόστος που επιφέρουν έχει μειωθεί σημαντικά σε σχέση με το σύνολο του κόστους που επωμίζονται οι οργανισμοί από τις παραβιάσεις ασφαλείας γενικότερα. Πλέον, η παραβίαση κυρίως της εμπιστευτικότητας και δευτερευόντως της ακεραιότητας αποτελούν τα πρωτεύοντα προβλήματα ασφαλείας για τους οργανισμούς κάθε κατηγορίας.

Τα περιστατικά παραβίασης ασφαλείας μπορούν επίσης να διαχωριστούν με κριτήριο την αιτία που προκαλεί το περιστατικό. Οι αιτιάσεις ενός περιστατικού μπορούν να χωριστούν σε τρεις γενικές κατηγορίες όπως αποτυπώνεται στην Εικόνα 12:

(1) Κακόβουλη ή εγκληματική επίθεση (malicious or criminal attack) προερχόμενη από πρόσωπα που ανήκουν είτε στο εσωτερικό είτε στο εξωτερικό περιβάλλον ενός οργανισμού. Η συγκεκριμένη πηγή απειλής εκμεταλλεύεται ευπάθειες ασφαλείας, είτε με φυσική υπόσταση είτε σε επίπεδο λογισμικού, προκειμένου να εκδηλώσει μία επίθεση. Τα κίνητρα αυτών των επιθέσεων περιλαμβάνουν κυρίως οικονομικά οφέλη, βιομηχανική κατασκοπεία και χακτιβισμό (hactivism). Η κατηγορία αυτή περιλαμβάνει τα περιστατικά που ενέχουν την συγκριτικά μεγαλύτερη οικονομική απώλεια για τους οργανισμούς στο σύνολο τους.

(2) Αμέλεια (negligence) από τους υπαλλήλους ή τρίτους με πρόσβαση στα ΠΣ ενός οργανισμού η οποία μπορεί να οδηγήσει ακούσια σε ένα περιστατικό παραβίασης ασφαλείας. Οι ευπάθειες, που έχουν δημιουργηθεί με την ραγδαία αυξανόμενη χρήση τεχνολογιών απομακρυσμένης πρόσβασης και της χρήσης κινητών μονάδων αποθήκευσης, έχουν αυξήσει σημαντικά την επίπτωση που δύναται να προκαλέσουν οι χρήστες ενός ΠΣ, ως ακούσιες πηγές απειλής. Η αύξηση των επιπτώσεων συνεπάγεται παράλληλα την αύξηση του επιπέδου των κινδύνων παραβιάσεων ασφαλείας.

(3) Αστοχίες στην λειτουργία των ΠΣ (system glitch) το οποίο μπορεί να οδηγήσει κυρίως σε προβλήματα διαθεσιμότητας και ακεραιότητας των πληροφοριών.



Εικόνα 12: Κατηγορίες παραβιάσεων ασφαλείας με βάση την αιτία πρόκλησης

4.2.5 Διαδικασία αντιμετώπισης περιστατικών παραβίασης ασφαλείας

Η διαδικασία, που τυπικά πραγματοποιείται στα πλαίσια ενός οργανισμού, για την αντιμετώπιση ενός περιστατικού παραβίασης ασφαλείας απεικονίζεται στην Εικόνα 13. Η διαδικασία είναι κοινή ανεξαρτήτως του μεγέθους και του είδους του περιστατικού καθώς και του είδους του οργανισμού που προσβλήθηκε. Το σύνολο της διαδικασίας μπορεί να χωριστεί σε πέντε βήματα τα οποία αναλύονται στις παρακάτω παραγράφους.

4.2.5.1 Ανακάλυψη και ανάλυση ενός περιστατικού παραβίασης ασφαλείας

Η διαδικασία αντιμετώπισης περιστατικών παραβίασης ασφαλείας ξεκινάει με την ανακάλυψη ενός νέου περιστατικού από τον οργανισμό που προσβλήθηκε. Η επόμενη κίνηση περιλαμβάνει την συλλογή όλων των απαραίτητων στοιχείων σχετικά με το είδος του περιστατικού και την κατηγοριοποίηση του. Η κατηγοριοποίηση περιλαμβάνει τους τύπους παραβίασης ασφαλείας που περιγράφτηκαν στην Ενότητα 4.2.4. Στην περίπτωση που το περιστατικό ανήκει στην κατηγορία επίθεσης πρόσβασης, πρέπει να πραγματοποιηθεί περαιτέρω χαρακτηρισμός του τύπου της επίθεσης με κριτήριο το είδος των ευαίσθητων δεδομένων που προσβλήθηκαν.

Στην συνέχεια πρέπει να διερευνηθούν τα αίτια που οδήγησαν στο συγκεκριμένο περιστατικό προκειμένου να εξακριβωθεί αν προέρχεται από γεγονός ήδη προσδιορισμένο κατά την διαδικασία ΔΚΠΣ. Στην περίπτωση που το περιστατικό είναι όντως προσδιορισμένο, γίνεται διερεύνηση αν

έχει ήδη προβλεφθεί εφαρμογή συγκεκριμένων αντίμετρων ασφαλείας. Αν το συγκεκριμένο γεγονός δεν έχει ήδη προσδιορισθεί στην διαδικασία ΔΚΠΣ, τότε θα πρέπει να δοθούν τα απαραίτητα δεδομένα για την διερεύνηση του αρχικώς κατά το στάδιο αξιολόγησης και αποτίμησης κινδύνων της ΔΚΠΣ. Στην συνεχεία, κατά την επανάληψη του συνόλου της διαδικασίας ΔΚΠΣ, θα πρέπει να ενσωματωθεί στο σύνολο της διαδικασίας από το στάδιο του προσδιορισμού κινδύνων.

Η επόμενη σημαντική παράμετρος που πρέπει να αναλυθεί αφορά τον προσδιορισμό των άμεσων ενεργειών αντιμετώπισης του περιστατικού. Οι ενέργειες μπορούν να διακριθούν στην επικοινώνηση του περιστατικού είτε προς το εσωτερικό είτε προς το εξωτερικό περιβάλλον του οργανισμού και στις λοιπές ενέργειες με βραχυπρόθεσμο ορίζοντα υλοποίησης και άμεση ποσοτικοποίηση του κόστους που επιφέρουν. Η πρώτη κατηγορία ενεργειών πραγματοποιείται στα δύο επόμενα στάδια ενώ η δεύτερη στο τέταρτο.

4.2.5.2 Εσωτερική ενημέρωση για ένα περιστατικό παραβίασης ασφαλείας

Ανάλογα με το πορίσματα της διερεύνησης που περιγράφτηκε στην προηγούμενη παράγραφο γίνεται ενημέρωση, σχετικά με ένα περιστατικό παραβίασης ασφαλείας, συγκεκριμένων κλιμακίων στην διοικητική δομή ενός οργανισμού. Η κατηγορία στην οποία ανήκει το περιστατικό, καθώς και ο αντίκτυπος που προβλέπεται να επιφέρει σε άμεσο και έμμεσο επίπεδο το συγκεκριμένο γεγονός, καθορίζουν τη διάσταση ενημέρωσης και το επίπεδο ανάλυσης που πρέπει να πραγματοποιηθεί μέσα σε έναν οργανισμό.

Βασική παράμετρος στο συγκεκριμένο στάδιο είναι το αποτέλεσμα ανάλυσης σχετικά με την ύπαρξη πρόβλεψης από την ΔΚΠΣ για ένα περιστατικό. Στην περίπτωση που η πιθανότητα πραγμάτωσης, ενός συγκεκριμένου περιστατικού, έχει προσδιορισθεί και έχουν ήδη εφαρμοστεί μέτρα αντιμετώπισης, πρέπει να ενημερωθεί το κλιμάκιο διαχείρισης κινδύνων προκειμένου να προσδιορίσει τις τυχών διορθωτικές ενέργειες για την αποτροπή μελλοντικών παρόμοιων συμβάντων. Στο ενδεχόμενο που το συγκεκριμένο γεγονός δεν έχει προσδιορισθεί στους πιθανούς κινδύνους από την ΔΚΠΣ, πρέπει να γίνει ενημέρωση του κλιμακίου διαχείρισης κινδύνων προκειμένου να πραγματοποιηθούν οι ενέργειες που αναφέρονται στο πρώτο στάδιο της διαδικασίας αντιμετώπισης περιστατικών.

4.2.5.3 Εξωτερική ενημέρωση για ένα περιστατικό παραβίασης ασφαλείας

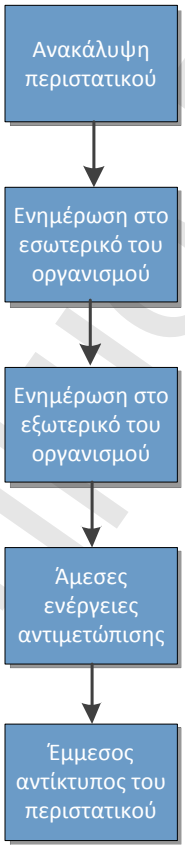
Το επόμενο βήμα αφορά την προετοιμασία και υλοποίηση ενημέρωσης του εξωτερικού περιβάλλοντος του οργανισμού. Το πρώτο θέμα που αναλύεται από έναν οργανισμό είναι αν υφίσταται υποχρέωση για την επίσημη ανακοίνωση ενός περιστατικού. Στην περίπτωση που δεν υφίσταται υποχρέωση ανακοίνωσης πραγματοποιείται ανάλυση την ύπαρξης σκοπιμότητας οικιοθελούς ανακοίνωσης από την πλευρά του οργανισμού. Όπως μπορεί να παρατηρηθεί στις οδηγίες διαχείρισης περιστατικών ασφαλείας διαφόρων κρατών, η ανακοίνωση ενός περιστατικού μπορεί να ωφελήσει μόνο υπό προϋποθέσεις τον οργανισμό και τα τρίτα μέρη που προσβλήθηκαν. Ο οδηγός της Αυστραλίας, σχετικά με την διαχείριση περιστατικών παραβίασης ασφαλείας, αναφέρει πως η ανακοίνωση ενός περιστατικού έχει πολύ περιορισμένη χρησιμότητα στην αντιμετώπιση ενός περιστατικού και πολύ βασικότερη από την ανακοίνωση είναι η εφαρμογή μέτρων ασφαλείας προκειμένου για την πρόληψη παρομοίων περιστατικών προσβολής της ασφαλείας [**53**].

Πρέπει να αναφερθεί επίσης πως η επίπτωση στην χρηματιστηριακή αξία των οργανισμών, από τις ανακοινώσεις περιστατικών ασφαλείας, είναι μία από τις μεθοδολογίες που ερευνούνται την τελευταία δεκαετία προκειμένου για τον προσδιορισμό της συνολικής οικονομικής επίπτωσης που επιφέρει ένα περιστατικό. Συνεπώς από την ερευνητική πλευρά, που ασχολείται με την ποσοτικοποίηση των επιπτώσεων που επιφέρουν αυτού του είδους τα περιστατικά, οι ανακοινώσεις αποφέρουν πολύ χρήσιμα δεδομένα. Εκτενής ανάλυση αυτής της μεθοδολογίας πραγματοποιείται στο κεφάλαιο 5.

Επίσης, από μελέτες δημοσκόπησης διαφαίνεται ότι ο χρόνος ανταπόκρισης ενός οργανισμού στην διαδικασία εξωτερικής ενημέρωσης, σχετικά με ένα περιστατικό παραβίασης ασφαλείας, διαδραματίζει σημαντικό ρόλο στην τελική οικονομική επίπτωση που θα του επιφέρει. Είναι χαρακτηριστικό το αποτέλεσμα έρευνας από την Ponemon Institute που εκπονήθηκε το 2011 όπου οργανισμοί, που έσπευσαν να ενημερώσουν άμεσα σχετικά με ένα περιστατικό, επιβαρύνθηκαν με 50% επιπλέον κόστος σε σχέση με άλλους οργανισμούς που κινήθηκαν προς την διαδικασία ενημέρωσης με πιο αργούς ρυθμούς [**27**]. Το συγκεκριμένο κόστος προέρχεται κατά κύριο λόγο από άμεσες και μετρήσιμες επιβαρύνσεις. Συνεπώς, είναι πολύ σημαντικό να προσδιορίζεται ο βέλτιστος χρόνος ενημέρωσης για ένα περιστατικό σύμφωνα με οικονομικά κριτήρια ώστε να

περιορίζονται στον μέγιστο βαθμό οι αντιοικονομίες που δύναται να προκύψουν από μία βεβιασμένη ανακοίνωση ενός γεγονότος.

Η ενημέρωση για ένα περιστατικό συνήθως αφορά δύο ομάδες ενδιαφερόμενων: (α) Ιδιώτες είτε με φυσική είτε με νομική υπόσταση και (β) τις κατάλληλες ρυθμιστικές αρχές οι οποίες προσδιορίζονται από την ανάλυση του περιστατικού που πραγματοποιήθηκε κατά την υλοποίηση του πρώτου σταδίου της συγκεκριμένης διαδικασίας. Ο τρόπος και η ταχύτητα ενημέρωσης επίσης είναι σε άμεση εξάρτηση με τα ιδιαίτερα χαρακτηριστικά του περιστατικού και του μεγέθους του όπως αυτό προσδιορίζεται με βάση των αριθμό των εκτεθειμένων εγγραφών.



Εικόνα 13: Διαδικασία αντιμετώπισης παραβιάσεων ασφαλείας

Στο [**28**] υποστηρίζεται πως η γνωστοποίηση ενός περιστατικού παραβίασης ασφαλείας προς τα άτομα, των οποίων τα προσωπικά δεδομένα περιήλθαν στην κατοχή μη εξουσιοδοτημένων φορέων, δεν επαρκεί για την αντιμετώπιση τους. Μάλιστα, η γνωστοποίηση πλέον σπάνια επιφέρει πραγματικά πλεονεκτήματα προς τα άτομα που έχουν εκτεθεί σε κίνδυνο και συνεπώς δικαιολογημένα πλέον η γνωστοποίηση θεωρείται ένα απαξιωμένο μέσο αντιμετώπισης των

περιστατικών παραβίασης ασφάλειας. Αυτό που προτείνεται, στην συγκεκριμένη μελέτη, είναι η έρευνα και εύρεση μέσων προστασίας της ασφάλειας και της ιδιωτικότητας των ευαίσθητων πληροφοριών. Η ποσοτικοποίηση του επιπέδου ασφαλείας, καθώς και των κινδύνων προερχόμενων από περιστατικά παραβίασης ασφαλείας, αποτελούν πολύ σημαντικές πηγές πληροφόρησης για την διοίκηση ενός οργανισμού προκειμένου για την λήψη των κατάλληλων αποφάσεων σε σχέση με επενδύσεις σε συστήματα ασφαλείας και διαδικασίες αντιμετώπισης των κινδύνων.

4.2.5.4 Άμεσες ενέργειες αντιμετώπισης

Στο τέταρτο στάδιο της συγκεκριμένης διαδικασίας, ο οργανισμός που προσβλήθηκε πραγματοποιεί τις άμεσες ενέργειες αντιμετώπισης, που προέκυψαν από την ανάλυση που προηγήθηκε στο πρώτο στάδιο. Στις ενέργειες αυτές δεν περιλαμβάνεται η επικοινώνηση του περιστατικού προς το εσωτερικό και εξωτερικό περιβάλλον του οργανισμού καθώς οι ενέργειες αυτές αφορούν αποκλειστικά τα δύο προηγούμενα στάδια. Οι ενέργειες, που αφορά αυτό το στάδιο, χαρακτηρίζονται ως άμεσες λόγω του βραχυπρόθεσμου ορίζοντα υλοποίησης τους και του σαφή προσδιορισμού του οικονομικού τους αντίκτυπου.

Όπως αναφέρθηκε και στις προηγούμενες παραγράφους, τα πορίσματα της ανάλυσης ενός περιστατικού πρέπει να επικοινωνούνται με τα κλιμάκια της ΔΚΠΣ. Επομένως, το σύνολο των άμεσων ενεργειών αντιμετώπισης ενός περιστατικού, πρέπει να πραγματοποιείται διαμέσου των διαδικασιών της ΔΚΠΣ. Το μεγαλύτερο ποσοστό των άμεσων ενεργειών πρέπει να σχετίζεται με τα μέτρα ελέγχου που συνθέτουν την ασφάλεια ΠΣ ενός οργανισμού. Συγκεκριμένα, περιλαμβάνουν την αναθεώρηση, τροποποίηση, κατάργηση και την εισαγωγή νέων μέτρων ελέγχου ασφαλείας, ενέργειες που μπορούν να πραγματοποιηθούν είτε στο στάδιο του προσδιορισμού κινδύνων είτε στο στάδιο αξιολόγησης και αποτίμησης κινδύνων που περιλαμβάνονται στο πλαίσιο ΔΚΠΣ.

4.2.5.5 Έμμεσος αντίκτυπος περιστατικού

Στο πέμπτο και τελευταίο στάδιο της διαδικασίας αντιμετωπίζεται ο έμμεσος οικονομικός αντίκτυπος που εκτιμήθηκε ότι θα επιφέρει ένα περιστατικό κατά το πρώτο στάδιο της ανάλυσης. Όπως περιγράφτηκε ήδη στις προηγούμενες ενότητες, το έμμεσο κόστος ενός περιστατικού προέρχεται από την ενεργοποίηση άλλων εταιρικών κινδύνων όπως είναι ο νομικός κίνδυνος.

Συνεπώς οι συσχετίσεις κινδύνων, που προσδιορίσθηκαν στο πρώτο στάδιο αντιμετώπισης ενός περιστατικού, οδηγούν στην εκτίμηση για το σύνολο του έμμεσου οικονομικού αντίκτυπου και στις αναγκαίες κινήσεις προκειμένου για τον περιορισμό του.

Η πλήρης διάσταση των αποτελεσμάτων αυτής της διαδικασίας και του τελικού έμμεσου αντίκτυπου δύναται να χρειαστούν χρόνια για προσδιορισθούν έστω με ένα ποσοστό περιορισμένης ακρίβειας. Όπως έχει ήδη αναλυθεί, το έμμεσο κόστος των παραβιάσεων ασφαλείας αποτελεί ένα από τα δυσκολότερα στοιχεία ποσοτικοποίησης στο σύνολο των κινδύνων ΠΣ και τα τελευταία χρόνια έχει λάβει την ιδιαίτερη ερευνητική προσοχή της ακαδημαϊκής και επιχειρηματική κοινότητας. Στην επόμενη ενότητα - μεταξύ άλλων - αναλύονται οι κυριότερες ερευνητικές προσπάθειες από διεθνής μελετητικούς οργανισμούς σχετικά με την ασφάλεια οι οποίοι τα τελευταία χρόνια έχουν πλέον ως βασικό στόχο την ακριβέστερη προσέγγιση του συνολικού κόστους που επιφέρουν οι παραβιάσεις ασφαλείας.

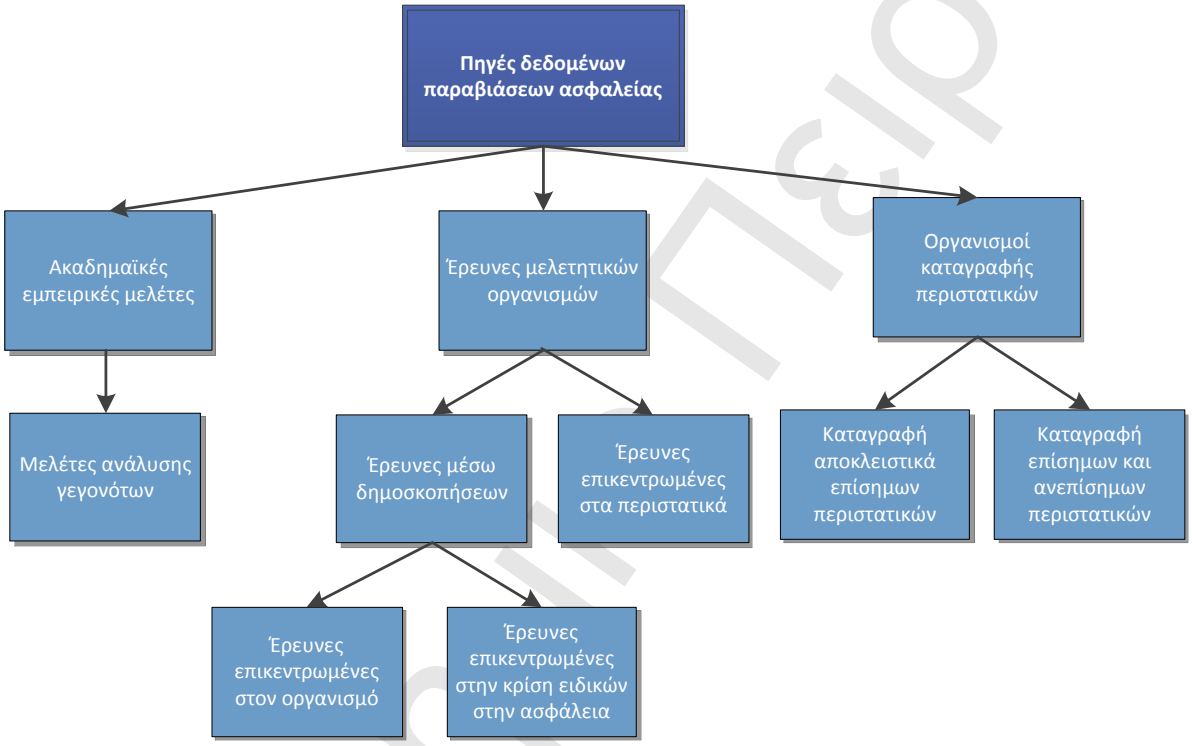
4.3 Πηγές δεδομένων παραβιάσεων ασφαλείας

Η ενότητα αυτή είναι αφιερωμένη στην ανάλυση των πηγών που περιέχουν δεδομένα σχετικά με τις παραβιάσεις ασφαλείας. Από το σύνολο της ερευνητικής προσπάθειας προέκυψε πως οι πηγές αυτές μπορούν να ταξινομηθούν σε τρεις γενικές κατηγορίες όπως αποτυπώνεται στην Εικόνα 14:

(1) Δεδομένα προερχόμενα από τα αποτελέσματα ακαδημαϊκών εμπειρικών μελετών. Οι μελέτες αυτές στο σύνολο τους εφαρμόζουν την μεθοδολογία ανάλυσης γεγονότων προκειμένου για την ποσοτικοποίηση του οικονομικού αντίκτυπου που επιφέρουν τα περιστατικά ασφαλείας σε έναν οργανισμό. Εκτενής ανάλυση των μελετών αυτής της κατηγορίας γίνεται στο κεφάλαιο 5.

(2) Δεδομένα προερχόμενα από έρευνες δημόσιων και ιδιωτικών μελετητικών οργανισμών. Οι έρευνες αυτές μπορούν να διακριθούν περαιτέρω σε έρευνες ανάλυσης δεδομένων προερχομένων από δημοσκοπήσεις και σε έρευνες επικεντρωμένες στα περιστατικά. Το μεγαλύτερο πλήθος των ερευνών γίνεται μέσω δημοσκοπήσεων και το σύνολο τους μπορεί να διαχωριστεί σε έρευνες επικεντρωμένες στον οργανισμό και σε έρευνες επικεντρωμένες στην κρίση ειδικών στην ασφάλεια ΠΣ. Τα δείγματα των

πρώτων συνθέτονται από πολλαπλές ανταποκρίσεις διαφορετικών ατόμων ανά οργανισμό ενώ τα δείγματα των δεύτερων συνθέτονται από την κρίση ενός υψηλόβαθμου στελέχους, σχετικού συνήθως με την ασφάλεια, ανά οργανισμό. Εκτενής ανάλυση των ερευνών προερχόμενων από μελετητικούς οργανισμούς πραγματοποιείται στις ενότητες 4.3.1 έως 4.3.3.



Εικόνα 14: Διαχωρισμός των πηγών δεδομένων παραβιάσεων ασφαλείας

(3) Δεδομένα προερχόμενα από οργανισμούς καταγραφής περιστατικών. Στην κατηγορία αυτή ανήκουν οργανισμοί αξιολόγησης, καταγραφής και στατιστικής ανάλυσης των περιστατικών παραβίασης ασφαλείας. Στα πλαίσια της παρούσας διατριβής έγινε περαιτέρω διαχωρισμός των οργανισμών αυτών σε αυτούς που έχουν υιοθετήσει αυστηρά κριτήρια για την επιλογή και καταγραφή των περιστατικών και σε αυτούς που καταγράφουν τα περιστατικά χωρίς την εφαρμογή κάποιας αυστηρής μεθοδολογίας. Οι βάσεις δεδομένων και οι διαδικτυακοί τόποι των πρώτων περιέχουν αποκλειστικά

επίσημα περιστατικά παραβίασης ασφαλείας[2] ενώ των δεύτερων περιέχουν και ανεπίσημα περιστατικά των οποίων η εγκυρότητα δεν είναι πλήρως επιβεβαιωμένη. Εκτενής ανάλυση των δεδομένων που προέρχονται από οργανισμούς καταγραφής περιστατικών πραγματοποιείται στην ενότητα 4.3.4.

4.3.1 Γενικά περί των ερευνών μελετητικών οργανισμών για την ασφάλεια

Οι βασικές πηγές ποσοτικοποιήσιμων δεδομένων σχετικά με τις παραβιάσεις ασφαλείας, σε διαθεσιμότητα στο ευρύ κοινό, προέρχονται από έρευνες δημοσκόπησης σχετικές με την ασφάλεια (security audits) και από έρευνες επικεντρωμένες στα περιστατικά (post-incident studies). Ο διαχωρισμός των δύο μεθοδολογιών προκύπτει από το αντικείμενο επικέντρωσης που επιλέγεται. Στην περίπτωση των μελετών δημοσκόπησης το αντικείμενο επικέντρωσης είναι είτε νομικά πρόσωπα, είτε φυσικά πρόσωπα με την ιδιότητα των ειδικών στην ασφάλεια ΠΣ που δέχονται να συμμετάσχουν. Η άλλη κατηγορία μελετών επικεντρώνεται σε συγκεκριμένα περιστατικά και κυρίως σε αυτά που έχει επιτελεστεί εγκληματολογική ανάλυση.

Οι έρευνες και των δύο κατηγοριών έχουν αυξηθεί τα τελευταία χρόνια γεγονός που αποτυπώνει την κλιμακούμενη εξάρτηση κρατών και οργανισμών στην εύρυθμη λειτουργία των ΠΣ και στην προστασία των ευαίσθητων δεδομένων που διαχειρίζονται. Η συχνότητα των ερευνών είναι συνήθως ετήσια ή διετής και πραγματοποιούνται κυρίως από μελετητικούς οργανισμούς ιδιωτικών συμφερόντων όπως οι Symantec, Ponemon Institute, Verizon, Ernst & Young, KPMG και PriceWaterHouseCoopers αλλά και οργανισμούς δημόσιων συμφερόντων όπως είναι οι CSI και FBI. Προκειμένου για την εκβάθυνση στα πλεονεκτήματα και μειονεκτήματα των ερευνών δημοσκόπησης ακολουθεί στο υπόλοιπο της συγκεκριμένης ενότητας ανάλυση της μεθοδολογίας που ακολουθούν.

Η διεξαγωγή των ερευνών δημοσκόπησης πραγματοποιείται είτε μέσω συνεντεύξεων, είτε μέσω ερωτηματολογίων είτε μέσω και των δύο μαζί. Η μεθοδολογία, στην οποία στηρίζεται η συλλογή των δεδομένων, είναι ένα βασικό μειονέκτημα για την στατιστική αξιοπιστία των συγκεκριμένων ερευνών. Ο δημόσιος ή ιδιωτικός φορέας που διεξάγει μία τέτοιου τύπου έρευνα, αποστέλλει ένα μεγάλο σύνολο από ερωτηματολόγια προς οργανισμούς κάθε κατηγορίας

[2] Στα πλαίσια της παρούσας διατριβής ως επίσημο περιστατικό παραβίασης ασφαλείας ορίζεται το περιστατικό το οποίο έχει ανακοινωθεί και συνεπώς επιβεβαιωθεί επίσημα από τον οργανισμό ή τους οργανισμούς τους οποίους αφορά.

συλλέγοντας ένα δείγμα όπου οι συμμετέχοντες, που τελικά ανταποκρίνονται στα ερωτηματολόγια και στις συνεντεύξεις, αυτοεπιλέγονται. Η σύνθεση συνεπώς του δείγματος δεν πραγματοποιείται μέσω τυχαίας διαδικασίας δειγματοληψίας ή μέσω της επιλογής κριτηρίων αντιπροσώπευσης του συνολικού πληθυσμού αλλά βασίζεται στη θέληση και το ενδιαφέρον των ερωτηθέντων.

Η μεθοδολογία σύνθεσης δείγματος, που ακολουθούν οι μελέτες αυτές, μπορεί να υπαχθεί στις ευρύτερη κατηγορία μεθοδολογιών στις οποίες δεν λαμβάνεται υπόψη η πιθανότητα ένα στοιχείο του πληθυσμού να περιληφθεί στο δείγμα (nonprobability samples). Πιο συγκεκριμένα, η συγκεκριμένα μεθοδολογία, μπορεί να υπαχθεί στις ειδικότερες κατηγορίες δειγμάτων ευκολίας (convenience samples) και δειγμάτων κρίσης (judgment samples).

Τα δείγματα ευκολίας προέρχονται κυρίως από ερωτηματολόγια που στέλνονται είτε μέσω ταχυδρομείου είτε συμπληρώνονται σε κάποιον διαδικτυακό τόπο. Ονομάζονται κατά αυτόν τον τρόπο καθώς παρέχουν ένα εύκολο, χαμηλού κόστους τρόπο συλλογής δεδομένων. Το πρόβλημα, όπως αναφέρθηκε και παραπάνω, είναι ότι οι ερωτηθέντες αυτοεπιλέγονται γεγονός που οδηγεί σε σοβαρή πιθανότητα ελλιπούς αντιπροσώπευσης του πληθυσμού με αποτέλεσμα τα πορίσματα της έρευνας να έχουν αμφίβολη αποτελεσματικότητα στην περιγραφή των ιδιαίτερων χαρακτηριστικών του. Το σύνολο των μελετών λαμβάνει τις παραδοχές ότι το εκάστοτε δείγμα αποτελεί αντιπροσωπευτική απεικόνιση του πληθυσμού και ότι η σύνθεση του πραγματοποιήθηκε μέσω τυχαίας δειγματοληψίας. Οι παραδοχές αυτές, σε πολλές περιπτώσεις μελετών, δεν είναι ρεαλιστικές και είναι αναγκαία η προσεκτική αξιολόγηση των αποτελεσμάτων που επιφέρουν.

Χαρακτηριστικό είναι ότι ακόμα και η αρχική επιλογή των παραληπτών των ερωτηματολογίων δεν πραγματοποιείται μέσω μεθοδολογιών τυχαίας δειγματοληψίας. Παραδείγματα αποτελούν οι έρευνες που διεξάγονται από τους οργανισμούς CSI/FBI [**10**], Ernst & Young [**54**], PriceWaterHouseCoopers [**8**] και Ponemon Institute [**11**]. Η Ponemon Institute επιλέγει ως παραλήπτες, και συνεπώς πιθανούς συμμετάσχοντες στο δείγμα, κυρίως εταιρίες με ωριμασμένες διαδικασίες ασφάλειας. Η ετήσια έρευνα από την Ernst & Young συλλέγει το μεγαλύτερο σύνολο δεδομένων σε σύγκριση με τις λοιπές παρόμοιες μελέτες, αλλά το σύνολο των ερωτηθέντων προέρχεται αποκλειστικά από το πελατολόγιο του συγκεκριμένου οργανισμού.

Η δεύτερη προαναφερόμενη κατηγορία μεθοδολογιών δειγματοληψίας, την οποία ακολουθούν οι συγκεκριμένες μελέτες, είναι τα δείγματα κρίσης. Οι παρατηρήσεις, που συνθέτουν αυτή την κατηγορία δειγμάτων, προέρχονται από τις γνώμες επιλεγμένων ειδικών πάνω σε ένα συγκεκριμένο ζήτημα. Αρκετές έρευνες πάνω στην ασφάλεια βασίζονται αποκλειστικά στην άποψη και στις θέσεις των ειδικών δημιουργώντας προβλήματα αντικειμενικότητας στα αποτελέσματα που εξάγονται. Παραδείγματα αποτελούν οι ετήσιες μελέτες από τους CSI/FBI και οι αντίστοιχες μελέτες που εκπονούνται από την Ernst & Young. Τα δεδομένα αποτελούν αποτέλεσμα της κρίσης ειδικών στα ΠΣ και σε θέματα ασφαλείας, στα ερωτήματα που θέτονται από τους προαναφερόμενους οργανισμούς. Οι ειδικοί αυτοί συνήθως κατέχουν τις θέσεις του CIO, CISO, CFO στους οργανισμούς που επιλέγονται να συμπεριληφθούν στα δείγματα.

Ένα ακόμα πρόβλημα που αντιμετωπίζουν αυτές οι έρευνες, αλλά και γενικότερα οι προσπάθειες ποσοτικοποίησης του κόστους παραβιάσεων ασφαλείας μέσω της εμπειρικής ανάλυσης δεδομένων προερχόμενων από την αγορά, είναι τα μικρά σχετικά ποσοστά των δημοσιευμένων περιστατικών σε σχέση με το υπολογιζόμενο σύνολο. Εκτιμάται ότι μόνο το 10%, εκ του συνόλου των περιστατικών, ανιχνεύεται από τους οργανισμούς που προσβάλλονται [**33**]. Το πρόβλημα αυτό κλιμακώνεται περαιτέρω καθώς υπολογίζεται ότι μόνο το 15% – 20%, εκ των διαπιστωμένων περιστατικών ανακοινώνεται από τους οργανισμούς στις αρχές, προς τον Τύπο ή έστω προς τις δικές τους νομικές υπηρεσίες. Ένας από τους βασικότερους λόγους αποφυγής ανακοίνωσης ενός περιστατικού είναι η ανησυχία ότι η αρνητική δημοσιότητα θα βλάψει την τιμή της μετοχής και θα αυξήσει σημαντικά τις έμμεσες οικονομικές επιπτώσεις που αναμένεται να επιφέρει.

Χαρακτηριστικό παράδειγμα αυτού του φαινομένου αποτελεί το εξαιρετικά χαμηλό ποσοστό ανταπόκρισης που έλαβε η πρόσφατη έρευνα από τους CSI/FBI [**10**]. Το ποσοστό συμμετοχής ανήλθε σε 6,4% έστω και αν η συγκεκριμένη έρευνα ήταν ανώνυμη. Η ίδια μελέτη, για πρώτη φορά, δεν μπόρεσε να εκδώσει εκτιμήσεις σχετικά με το μέσο κόστος ενός περιστατικού παραβίασης ασφαλείας. Η μελέτη που διεξήχθη το 2010 από την Ponemon Institute [**55**], για το κόστος παραβιάσεων ασφαλείας που αντιμετωπίζουν εταιρίες από τις ΗΠΑ, είχε ποσοστό ανταπόκρισης κάτω του 13% το οποίο μειώθηκε ακόμα περισσότερο στην αντίστοιχη μελέτη που διεξήχθη το 2011 [**27**].

Τα μεγέθη αυτά υποδηλώνουν ότι η ανασταλτικότατα των οργανισμών, σχετικά με την ανακοίνωση λεπτομερειών για περιστατικά ασφαλείας, έχει αυξανόμενη τάση τα τελευταία χρόνια. Όπως αναλύεται διεξοδικότερα στο κεφάλαιο 5, γίνεται προσπάθεια από το σύνολο των κρατών, που έχουν μεγάλη εξάρτηση στην εύρυθμη λειτουργία των ΠΣ, ενίσχυσης των κανονιστικών πλαισίων και της κείμενης νομοθεσίας προκειμένου, τα παραπάνω ποσοστά ανίχνευσης παραβιάσεων ασφαλείας και εν συνεχεία ανακοίνωσης τους, να αυξηθούν.

Ένα πλεονέκτημα που έχουν οι συγκεκριμένες έρευνες, σε σχέση με τις αντίστοιχες εμπειρικές μελέτες ανάλυσης γεγονότων, είναι ότι οι πρώτες μπορούν να εξετάσουν κάθε είδος παραβίασης ασφαλείας ανεξάρτητα από την φύση της απειλής και τα εργαλεία που χρησιμοποιούνται για την εκτέλεση της επίθεσης. Ένα εκ των σημαντικών εργαλείων που χρησιμοποιούνται από επίδοξους εισβολείς, προκειμένου για την εκτέλεση κακόβουλων επιθέσεων, είναι οι ιοί[3]. Σύμφωνα με έρευνες [**27**], το 50% των παραβιάσεων ασφαλείας από κακόβουλες επιθέσεις πραγματοποιείται μέσω ιών. Όπως όμως αναλύεται στο κεφάλαιο 5, η ένταξη περιστατικών προκαλούμενων από ιούς σε ένα δείγμα, το οποίο εξετάζεται μέσω της μεθοδολογίας ανάλυσης γεγονότων, προκαλεί προβλήματα στις βασικές δομές και παραδοχές στις οποίες βασίζεται η συγκεκριμένη εμπειρική μεθοδολογία. Συνεπώς, οι επιπτώσεις που επιφέρουν οι επιθέσεις μέσω ιών, μπορούν να αναλυθούν με μεγαλύτερη μεθοδολογική εγκυρότητα μέσω των δεδομένων που προκύπτουν από τις έρευνες που αναλύονται στην συγκεκριμένη ενότητα από ότι με δεδομένα που προκύπτουν από μελέτες ανάλυσης γεγονότων.

Το κυριότερο ζήτημα που αντιμετωπίζουν οι προσεγγίσεις ποσοτικοποίησης του κόστους παραβιάσεων ασφαλείας, από τις έρευνες μελετητικών οργανισμών και από τις εμπειρικές μελέτες ανάλυσης γεγονότων, είναι ο υπολογισμός του έμμεσου κόστους όπως αυτό αναλύεται στην ενότητα 4.2.3. Το έμμεσο κόστος, λόγω της φύσης του, είναι αδύνατο να υπολογιστεί με αντικειμενικότητα και ακρίβεια. Αποτελεί ωστόσο το σημαντικότερο μέρος επί του συνολικού κόστους μίας παραβίασης ασφαλείας [**27**]. Στο παρόν κεφάλαιο, μεταξύ άλλων, γίνεται συγκριτική ανάλυση των πορισμάτων από έρευνες ασφαλείας σχετικά με το κόστος των παραβιάσεων. Στο κεφάλαιο 5 αναλύεται εμπειρική μελέτη που διενεργήθηκε, στα πλαίσια της

[3] Προκειμένου για την ανάγκες της παρούσας διατριβής, αναφερόμενοι στους ιούς θα συμπεριλαμβάνουμε γενικότερα το κακόβουλο λογισμικό (malware) που σχετίζεται με σκουλήκια (warms) και δούρειους ίππους (trojan horses) το οποίο, στο σύνολο του, αποσκοπεί στην πρόκληση επιθέσεων μαζικού τύπου χωρίς επικέντρωση σε έναν συγκεκριμένο οργανισμό.

διατριβής, πάνω στο κόστος των παραβιάσεων με χρήση της μεθοδολογίας ανάλυσης γεγονότων. Επίσης πραγματοποιείται σύγκριση των ευρημάτων της συγκεκριμένης εμπειρικής μελέτης, με τα αποτελέσματα προγενέστερων μελετών. Ακολούθως, στο κεφάλαιο 7 πραγματοποιείται συγκριτική ανάλυση μεταξύ των αποτελεσμάτων προκειμένου να εξαχθούν συνολικά συμπεράσματα σχετικά με το κόστος που ενέχουν για τους οργανισμούς οι παραβιάσεις ασφαλείας.

4.3.2 Γενική περιγραφή των κυριότερων οργανισμών εκπόνησης ερευνών

Στην παράγραφο αυτή αναφέρονται περιληπτικά οι διεθνείς μελετητικοί οργανισμοί που εκπονούν τις κυριότερες μελέτες σχετικά με την ασφάλεια ΠΣ και τις παραβιάσεις ασφαλείας των οποίων μελέτες χρησιμοποιήθηκαν κατά την ερευνητική προσπάθεια. Καθώς στο κεφάλαιο 5 το δείγμα που μελετήθηκε αποτελείται αποκλειστικά από εταιρίες των ΗΠΑ και το διάστημα ανάλυσης είναι μεταξύ των ετών 2008 – 2011, οι μελέτες που αναλύθηκαν, για λόγους συγκρισιμότητας, αφορούν οργανισμούς με έδρα τις ΗΠΑ και την ίδια χρονική περίοδο. Κατά συνέπεια, οι μελέτες της PriceWaterHouseCoopers, έστω και αν χρησιμοποιούνται σε άλλες ενότητες της παρούσας διατριβής, δεν χρησιμοποιήθηκαν για την άντληση δεδομένων για τις παραβιάσεις ασφαλείας καθώς αφορούν αποκλειστικά οργανισμούς με έδρα το Ηνωμένο Βασίλειο.

Ο οργανισμός Computer Security Institute (CSI) μαζί με το Federal Bureau of Investigation (FBI) εκπονούν και δημοσιεύουν σε ετήσια βάση μελέτη δημοσκόπησης σχετικά με το ηλεκτρονικό έγκλημα και την ασφάλεια ΠΣ. Η συγκεκριμένη μελέτη είναι η μακροβιότερη σε σχέση με το σύνολο των μελετών του είδους. Βασικό πλεονέκτημα της μεθοδολογίας που ακολουθείται μπορεί να θεωρηθεί η σύνθεση των δειγμάτων από οργανισμούς που ανήκουν σε κάθε κατηγορία μεγέθους λαμβάνοντας ως κριτήριο μεγέθους τον ετήσιο κύκλο εργασιών. Αυτό οδήγησε στην συμβατότητα των αποτελεσμάτων των ερευνών αυτών με αυτά που προέκυψαν από την μελέτη ανάλυσης γεγονότων, που συστάθηκε στα πλαίσια της παρούσας διατριβής, και στην οποία χρησιμοποιήθηκε δείγμα περιστατικών που αφορούσε εταιρίες από κάθε επίπεδο κεφαλαιοποίησης.

Οι συγκεκριμένοι φορείς επισημαίνουν πως τα δείγματα που μελετήθηκαν δεν προέρχονται από μεθόδους τυχαίας δειγματοληψίας και οι παραλήπτες των ερωτηματολογίων είναι

αποκλειστικά μέλη του CSI. Επίσης, η μέση ανταπόκριση των συμμετασχόντων στις έρευνες δεν ξεπερνά το 10%, ποσοστό το οποίο είναι αρκετά μικρό ώστε να θεωρηθούν τα αποτελέσματα αντιπροσωπευτικά έστω του δείγματος που δημιουργούν οι συγκεκριμένοι φορείς. Το γεγονός ότι οι παρατηρήσεις προέρχονται από οργανισμούς μέλους μίας κοινότητας αφιερωμένης στην ασφάλεια των ΠΣ οδηγεί στο συμπέρασμα ότι οι συγκεκριμένοι φορείς έχουν ήδη συστήσει δομές διαχείρισης κινδύνων ΠΣ με καταρτισμένο στελεχιακό δυναμικό. Αυτό μπορεί να σημαίνει πως η επίπτωση καθώς και η συχνότητα ενός περιστατικού παραβίασης ασφαλείας, για αυτούς τους οργανισμούς, να είναι σε αρκετά μικρότερη κλίμακα από αυτή που θα υφίσταται σε οργανισμούς με μικρότερες δομές ασφαλείας. Συνεπώς, από τα παραπάνω προκύπτει πως, τα αποτελέσματα αυτών των ερευνών, δεν μπορούν να γενικευτούν στο σύνολο των οργανισμών χωρίς την ενίσχυση από τα πορίσματα άλλων μοντέλων και μεθόδων. Κατά την διάρκεια της ερευνητικής προσπάθειας αναλύθηκαν οι μελέτες που αφορούσαν τα έτη 2008, 2009, 2010 [**56**], [**57**], [**10**]. Πρέπει να σημειωθεί πως κατά την στιγμή συγγραφής του παρόντος δεν είχε εκδοθεί ακόμη μελέτη των οργανισμών αυτών για το 2011.

Ο φορέας Ponemon Institute ασχολείται με την έρευνα και εκπαίδευση πάνω στην ασφάλεια των ευαίσθητων δεδομένων. Τα τελευταία επτά έτη εκδίδει ετησίως μελέτες δημοσκόπησης σχετικά με την οικονομική επίπτωση των παραβιάσεων ασφαλείας σε δημόσιους και ιδιωτικούς οργανισμούς που εδρεύουν σε χώρες οι οποίες παρουσιάζουν μεγάλη ανάπτυξη στην χρήση τεχνολογιών πληροφόρησης. Οι μελέτες του συγκεκριμένου φορέα, που αναλύθηκαν στα πλαίσια της παρούσας, είναι οι ετήσιες δημοσκοπήσεις εταιριών με έδρα τις ΗΠΑ για τα έτη 2008, 2009, 2010 και 2011 [**58**], [**59**], [**55**], [**27**].

Η εταιρία Verizon ασχολείται μεταξύ άλλων με προϊόντα και υπηρεσίες ασφαλείας και τα τελευταία οκτώ έτη εκδίδει μελέτη ετήσιας συχνότητας αφιερωμένη στις παραβιάσεις ασφαλείας. Η μεθοδολογία που ακολουθεί είναι κατά κύριο λόγο επικεντρωμένη στο περιστατικό και δευτερευόντως στον οργανισμό που το επωμίστηκε. Η σύνθεση των δεδομένων προέρχεται από τα αρχεία καταγραφής πραγματικών περιστατικών του συγκεκριμένου οργανισμού και άλλων όπως είναι οι μυστικές υπηρεσίες των ΗΠΑ (US secret service). Αυτή είναι η κύρια διαφορά αυτών των μελετών από τις μελέτες των οποίων τα δεδομένα είναι προϊόν δημοσκόπησης.

Η εστίαση των μελετών της Verizon αποκλειστικά στα περιστατικά, για τα οποία έχει διεξαχθεί εγκληματολογική έρευνα, μας οδηγεί στην υπόθεση ότι η σύνθεση του δείγματος, σε

σημαντικό βαθμό, επικεντρώνεται σε μεγάλα περιστατικά. Συγκρίνοντας τον αριθμό των περιστατικών με τον αριθμό των προσβεβλημένων εγγραφών οδηγεί σε έναν μέσο αριθμό εγγραφών ανά περιστατικό ο οποίος ανέρχεται στο 1 εκατομ. Ακολουθώντας την μεθοδολογική προσέγγιση του CSI/FBI, σχετικά με το μέγεθος ενός περιστατικού, όταν ο αριθμός των εγγραφών που εκτίθενται ξεπερνάει τις 100.000, τότε το περιστατικό θεωρείται μεγάλο. Αυτό οδηγεί τα δείγματα των μελετών της Verizon να μην είναι αντιπροσωπευτικά του συνολικού πληθυσμού περιστατικών παραβίασης ασφαλείας αλλά μόνο μίας κατηγορίας εξ αυτών.

Ένα επιπλέον μειονέκτημα των μελετών της Verizon είναι η έλλειψη εκτιμήσεων για το μέγεθος των οικονομικών επιπτώσεων που επέφεραν τα περιστατικά που αναλύθηκαν. Οι οργανισμοί που προσβλήθηκαν καθώς και οι οργανισμοί που διεξήγαν την εγκληματολογική έρευνα δεν αποκαλύπτουν εκτιμήσεις για τον οικονομικό αντίκτυπο που επέφεραν ή προβλέπεται να επιφέρουν τα περιστατικά που αναλύθηκαν. Κατά την ερευνητική προσπάθεια αναλύθηκαν οι μελέτες του συγκεκριμένου οργανισμού που αφορούσαν τα έτη 2009, 2010, 2011 [**60**], [**13**], [**61**]. Δεν συμπεριλήφθηκε η ανάλυση για το έτος 2008 προκειμένου να τηρηθεί ομοιογένεια στα αντλούμενα δεδομένα καθώς από το 2009 ξεκίνησε η προαναφερόμενη συνεργασία της Verizon με την μυστική υπηρεσία των ΗΠΑ το οποίο οδήγησε σε πλήρη αλλαγή της σύνθεσης των δεδομένων.

Ο διεθνής μελετητικός οργανισμός Ernst & Young εκδίδει ετησίως μελέτη δημοσκόπησης σχετικά με την ασφάλεια ΠΣ. Σε συνδυασμό με τις αντίστοιχες μελέτες του CSI/FBI, οι μελέτες του συγκεκριμένου φορέα αποτελούν τις μακροβιότερες μελέτες του είδους. Βασικό χαρακτηριστικό των μελετών της Ernst & Young είναι το μέγεθος του δείγματος το οποίο ξεπερνάει τα αντίστοιχα δείγματα όλων των υπολοίπων μελετών που αναλύθηκαν κατά την διάρκεια της διατριβής. Κατά την διάρκεια την ερευνητικής προσπάθειας αναλύθηκαν οι μελέτες του οργανισμού που αφορούσαν τα έτη 2010 και 2011 [**54**], [**6**].

4.3.3 Ανάλυση των μελετών ανά κατηγορία δεδομένων

Στην συγκεκριμένη ενότητα γίνεται ανάλυση των δεδομένων που προέρχονται από τις μελέτες για την ασφάλεια. Η δομή της ανάλυσης βασίζεται στα ιδιαίτερα χαρακτηριστικά των παραβιάσεων ασφαλείας στα οποία επικεντρώθηκε η έρευνα και όχι ανά μελετητικό φορέα. Η μεθοδολογία ανάλυσης των παραβιάσεων ασφαλείας που χρησιμοποιήθηκε ως βάση είναι το

Veris A^4 Threat Model που έχει δημιουργηθεί από την Verizon [**62**]. Σύμφωνα με το συγκεκριμένο μοντέλο, ένα περιστατικό ασφαλείας αναλύεται ως μία σειρά γεγονότων τα οποία προκαλούν αρνητικό αντίκτυπο στις ευαίσθητες πληροφορίες ενός οργανισμού. Το συνθετικό A^4 στο όνομα του μοντέλου παραπέμπει στον διαχωρισμό των βασικών στοιχείων που συνθέτουν ένα περιστατικό ασφαλείας σε τέσσερις κατηγορίες: (α) Πηγή απειλής (agent), (β) τρόπος επίθεσης (actions), (γ) στοιχεία ενεργητικού που επηρεάζονται (assets) και (δ) είδος επίπτωσης (attribute).

Η πηγή απειλής κυρίως αναφέρεται στο περιβάλλον προέλευσης του επιτιθέμενου και ο βασικός διαχωρισμός της είναι μεταξύ του εσωτερικού και εξωτερικού περιβάλλοντος ενός οργανισμού. Τα στοιχεία των ερευνών σχετικά με την πηγή απειλής αναλύονται στην παράγραφο 4.3.3.4. Ο τρόπος επίθεσης αναφέρεται στα εργαλεία και την μεθοδολογία που χρησιμοποιείται από την πηγή απειλής προκειμένου να εκδηλώσει μία επίθεση. Όπως αναφέρθηκε στην ενότητα 4.2.4 ένα κριτήριο με βάση το οποίο μπορούμε να διακρίνουμε τα περιστατικά ασφαλείας σε κατηγορίες είναι ο τρόπος επίθεσης. Η σημαντικότητα που προκύπτει, από τα δεδομένα των μελετών, σχετικά με κάθε κατηγορία παραβίασης ασφαλείας αναλύεται στην παράγραφο 4.3.3.3. Τα δεδομένα που προέρχονται από τις μελέτες σχετικά με τα στοιχεία ενεργητικού που προσβάλλονται αφορούν κυρίως το είδος των δεδομένων καθώς και το είδος του υλικού που διαχειρίζεται τα δεδομένα που προσβλήθηκαν. Το είδος της επίπτωσης αναφέρεται στα χαρακτηριστικά της ασφάλειας δεδομένων που παραβιάστηκαν όπως είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Οι μελέτες δεν παρέχουν επαρκή στοιχεία για το συγκεκριμένο στοιχείο των περιστατικών ασφαλείας και μεγαλύτερα περιθώρια ανάλυσης παρέχουν οι εμπειρικές αναλύσεις.

Τα δύο βασικά συνθετικά χαρακτηριστικά των περιστατικών ασφαλείας, τα οποία εξαρτώνται από τις τέσσερις προαναφερόμενες κατηγορίες, είναι ο οικονομικός αντίκτυπος και η συχνότητα εμφάνισης. Τα δεδομένα που προέρχονται από τις μελέτες ασφαλείας για τα δύο αυτά χαρακτηριστικά αναλύονται στις δύο επόμενες παραγράφους.

4.3.3.1 Ανάλυση του οικονομικού αντίκτυπου παραβιάσεων ασφαλείας

Οι μελέτες που έχουν συνταχθεί από τους φορείς CSI/FBI και Ponemon Institute αποτελούν τις πιο ολοκληρωμένες πηγές, για τον οικονομικό αντίκτυπο των παραβιάσεων ασφαλείας, που προέρχονται από μελέτες ασφαλείας. Στην παρούσα ενότητα η ανάλυση επικεντρώνεται κυρίως

στα δεδομένα που προέρχονται από τις μελέτες των συγκεκριμένων φορέων. Αρχικώς παραθέτουμε κάποιες γενικές διαπιστώσεις που πηγάζουν από τις μελέτες αυτές.

Οι μελέτες από τους CSI/FBI, κατά τα τελευταία δύο έτη, οδηγούνται στην διαπίστωση ότι οι οργανισμοί γενικά δεν μπορούν να προσεγγίσουν με επαρκή ακρίβεια ούτε τον οικονομικό αντίκτυπο που επιφέρουν οι παραβιάσεις ασφαλείας, ούτε το αποτέλεσμα που επιτυγχάνεται από την εφαρμογή συγκεκριμένων αντίμετρων ασφαλείας. Μπορεί να εξαχθεί το συμπέρασμα ότι η απροθυμία των οργανισμών να παραχωρήσουν δεδομένα σχετικά με τις οικονομικές επιπτώσεις των παραβιάσεων ασφαλείας δεν προέρχεται αποκλειστικά από την ανησυχία αρνητικής αντίδρασης από την πλευρά των αγορών αλλά και από την αδυναμία ποσοτικοποίησης των ίδιων των επιπτώσεων. Η διαπίστωση αυτή αποδεικνύει ότι το επίπεδο ακρίβειας των υπαρχουσών μεθοδολογιών ποσοτικοποίησης των κινδύνων παραβιάσεων ασφαλείας είναι αρκετά ανεπαρκές και η ερευνητική προσπάθεια που καταβάλει η ακαδημαϊκή και επαγγελματική κοινότητα έχει μεγάλα περιθώρια βελτίωσης. Μέρος αυτής της προσπάθειας αποτελεί και η παρούσα διδακτορική διατριβή.

Οι μελέτες των προαναφερόμενων φορέων αποτυπώνουν το κόστος ανά περιστατικό κατά δήλωση των προσβληθέντων οργανισμών. Η απροθυμία αποκάλυψης, από την πλευρά των οργανισμών, των οικονομικών επιπτώσεων από παραβιάσεις ασφαλείας μπορεί να προσδιορισθεί ξεκάθαρα από τις συγκεκριμένες μελέτες καθώς περιλαμβάνουν το μεγαλύτερο μέγεθος υποψήφιων συμμετεχόντων. Είναι χαρακτηριστικό το επίπεδο ανταπόκρισης στην έρευνα της CSI/FBI μειώθηκε σταδιακά τα τρία τελευταία χρόνια και από 10,4% όπου ανήλθε το 2009 μειώθηκε σε 6,4% το 2011.

Στον Πίνακα 2 παρουσιάζονται τα βασικά δεδομένα των μελετών της Ponemon για την περίοδο 2008 – 2011. Στην πρώτη στήλη αναγράφεται η εκτίμηση για το μέσο κόστος ανά περιστατικό παραβίασης ασφαλείας. Στην δεύτερη στήλη αναγράφεται το συνολικό κόστος ανά εγγραφή που εκτίθεται με τα δεδομένα για τον επιμερισμό του κόστους σε άμεσο και έμμεσο να αναγράφονται στην τρίτη και τέταρτη στήλη αντιστοίχως. Οι μελέτες τις Ponemon αποτελούν τις μοναδικές μελέτες του είδους με κάποια σχετική πληρότητα δεδομένων σχετικά με τον οικονομικό αντίκτυπο των παραβιάσεων ασφαλείας. Όπως προκύπτει από τα δεδομένα του πίνακα, το μέσο συνολικό κόστος ανά εγγραφή ανέρχεται σε 204 $ και επιμερίζεται σε 61 $ άμεσου κόστους και 143 $ έμμεσου κόστους. Η αναλογία συνεπώς μεταξύ άμεσου και έμμεσου κόστους, που

προτείνεται από τις συγκεκριμένες αναλύσεις, είναι περίπου 30 / 70. Στο Διάγραμμα 1 αποτυπώνεται χαρακτηριστικά η προαναφερόμενη αναλογία καθώς και η εξέλιξη της στην διάρκεια της τελευταίας τετραετίας. Η προτεραιότητα που δίνουν πλέον οι οργανισμοί στην αντιμετώπιση των περιστατικών ασφαλείας αποτυπώνεται μεταξύ άλλων και από την σχετική αύξηση του άμεσου κόστους σε σχέση με το έμμεσο κόστος μέσα στα τελευταία χρόνια. Η αύξηση του άμεσου κόστους καταδεικνύει την τάση των οργανισμών προς την αντιμετώπιση των περιστατικών με μεγαλύτερα χρηματικά και οργανωτικά μέσα.

Πίνακας 2: Κόστος παραβιάσεων ασφαλείας από την Ponemon Institute

Έτος	Κόστος ανά περιστατικό (.000 $)	Συνολικό κόστος ανά εγγραφή σε έκθεση ($)	Άμεσο κόστος ανά εγγραφή σε έκθεση ($)	Έμμεσο κόστος ανά εγγραφή σε έκθεση ($)
2008	6.660	202	50	152
2009	6.750	204	60	144
2010	7.240	214	73	141
2011	5.500	194	59	135
Μέσες τιμές	**6.538**	**204**	**61**	**143**

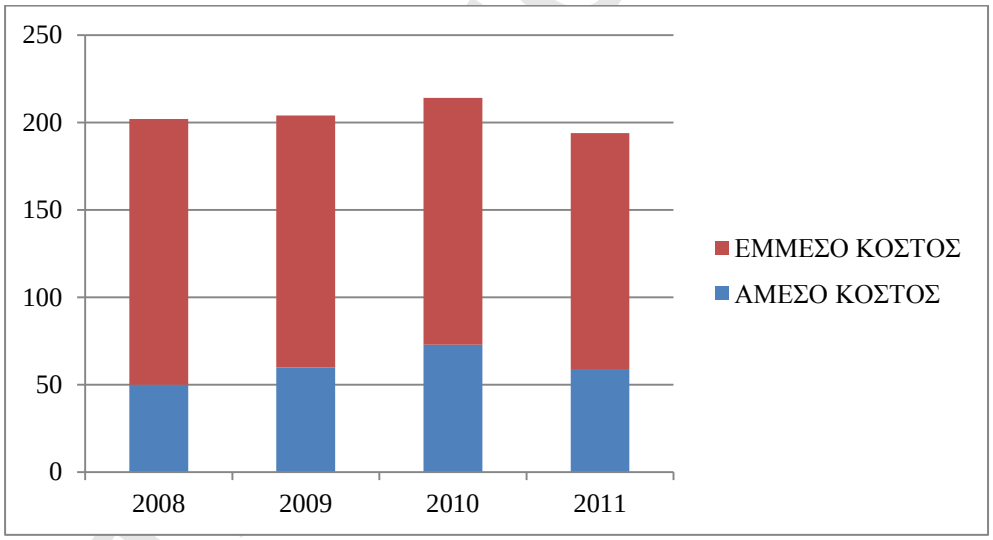
Στον Πίνακα 3 παρουσιάζονται τα δεδομένα για την εκτίμηση του συνολικού αντίκτυπου ανά περιστατικό από τις αντίστοιχες μελέτες του CSI/FBI. Πρέπει να σημειωθεί πως οι μελέτες αυτές δεν παρέχουν δεδομένα σχετικά με τον αριθμό των εγγραφών που εκτίθενται στο δείγμα που ερευνήθηκε. Επιπλέον, δεν παρέχουν εκτιμήσεις σχετικά με το κόστος ανά εγγραφή. Συνεπώς η μόνη ακριβής εκτίμηση για το κόστος ανά εγγραφή, σε σχέση με το σύνολο των μελετών του είδους, προέρχεται από την Ponemon Institute.

Πίνακας 3: Κόστος παραβιάσεων ασφαλείας από το CSI/FBI

Έτος	Κόστος ανά περιστατικό (.000 $)
2008	289
2009	234
2010	100

Στο Διάγραμμα 2 παρουσιάζεται η κλιμάκωση του μέσου συνολικού κόστους που προκαλείται ανά περιστατικό ασφαλείας στην περίοδο 2008 – 2011 από τις CSI/FBI και Ponemon Institute. Αυτό που διακρίνεται εμφανώς είναι η εξαιρετικά μεγάλη απόκλιση που παρουσιάζουν οι δύο προσεγγίσεις μεταξύ τους με την μέση εκτίμηση της CSI/FBI να τεκμαίρεται ως εξαιρετικά χαμηλή. Πρέπει να σημειωθεί πως στην τελευταία μελέτη των συγκεκριμένων φορέων η συμμετοχή των εταιριών στην αποκάλυψη δεδομένων κόστους ήταν σε τόσο χαμηλό επίπεδο που ο φορέας δεν μπορούσε να εξάγει κάποια ασφαλή προσέγγιση για τις οικονομικές επιπτώσεις από τις παραβιάσεις ασφαλείας. Είναι χαρακτηριστικό πως αν το μέσο πραγματικό κόστος ήταν κατώτερο των $300.000, τότε η αντιμετώπιση των παραβιάσεων ασφαλείας δεν θα αποτελούσε μία από τις προτεραιότητες των οργανισμών παγκοσμίως. Επίσης, δεν θα αποτελούσε το αντικείμενο μελέτης μεγάλου πλήθους ακαδημαϊκών και επαγγελματιών κατά την διάρκεια της τελευταίας δεκαετίας.

Διάγραμμα 1: Ανάλυση κόστους ανά περιστατικό σε άμεσο και έμμεσο από Ponemon

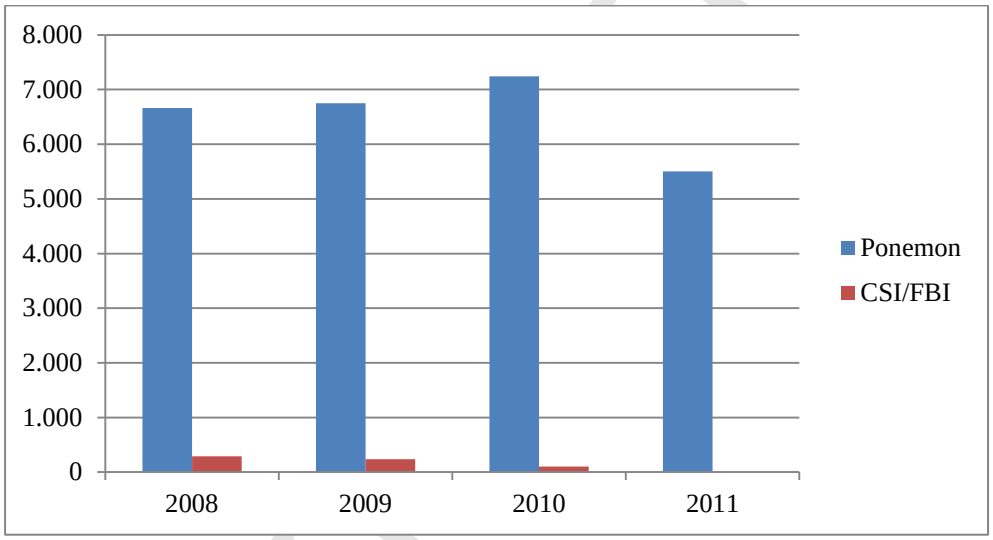


Το μέσο κόστος που προκύπτει και από τους δύο οργανισμούς είναι σε αρκετά χαμηλά επίπεδα συγκρινόμενο με τα αποτελέσματα των αντίστοιχων εμπειρικών μελετών που παρουσιάζονται στο κεφάλαιο 5[4]. Μπορούμε να εκφέρουμε δύο πιθανές αιτιάσεις για το μέγεθος αυτών των αποτελεσμάτων: (α) Οι οργανισμοί που αποκαλύπτουν τις οικονομικές επιπτώσεις από

[4] Λεπτομερής συγκριτική ανάλυση των δεδομένων κόστους μεταξύ των μελετών συμβουλευτικών οργανισμών και εμπειρικών μελετών της ακαδημαϊκής κοινότητας πραγματοποιείται στο κεφάλαιο 7.

παραβιάσεις ασφαλείας αναφέρονται κατά κύριο λόγο σε περιστατικά χαμηλής σημασίας τα οποία προκαλούν σχεδόν αποκλειστικά άμεσα και σαφώς μετρήσιμα κόστη. (β) Το μεγαλύτερο μέρος των οργανισμών έχει αδυναμία ποσοτικοποίησης της πλήρης διάστασης των οικονομικών επιπτώσεων αναφερόμενοι κατά κύριο λόγο στο κομμάτι των έμμεσων επιπτώσεων. Αυτό αποδεικνύεται από την αδυναμία των CSI/FBI να εκδώσουν αποτελέσματα με ακρίβεια στην τελευταία μελέτη της λόγω της εξαιρετικά μικρής ανταπόκρισης των οργανισμών που συμμετείχαν.

Διάγραμμα 2: Προσέγγιση συνολικού κόστους ανά περιστατικό από Ponemon & FBI/CSI (ποσά σε .000 $)



Η διαπίστωση αυτή μπορεί να συνδυαστεί με τις σημαντικές αλλαγές που επήλθαν στην φύση των κινδύνων παραβιάσεων ασφαλείας καθώς και στην εξαιρετική αύξηση στην πολυπλοκότητα των επιθέσεων τα οποία αναπόφευκτα οδηγούν σε περαιτέρω δυσκολίες για την ανεύρεση και ποσοτικοποίηση των επιπτώσεων των παραβιάσεων ασφαλείας. Η προαναφερόμενη αλλαγή στην φύση των κινδύνων μπορεί να αποτυπωθεί και από την άποψη της πλειοψηφίας των οργανισμών ότι το περιβάλλον των κινδύνων ΠΣ αλλάζει δραστικά λόγω των ραγδαίων εξελίξεων της τεχνολογίας [**54**].

Από τις μελέτες του Ponemon Institute προκύπτει η σταδιακή μείωση του κόστους απώλειας πελατείας ως συνέπεια μίας παραβίασης ασφαλείας. Αυτό οδηγεί στο συμπέρασμα ότι ο κίνδυνος απώλειας πελατείας, ως συνέπεια των κινδύνων παραβιάσεων ασφαλείας, σταδιακά μειώνεται. Βέβαια, η μείωση δεν είναι ανάλογη για κάθε κλάδο δραστηριότητας και εξαρτάται από το είδος

του οργανισμού. Καθώς το κόστος απώλειας πελατείας είναι ένα από τα πλέον σημαντικά στοιχεία του έμμεσου κόστους ενός περιστατικού ασφαλείας, η σταδιακή μείωση του έμμεσου κόστους τα τελευταία χρόνια μπορεί να αποδοθεί κυρίως σε αυτόν τον λόγο.

Τα στοιχεία που αναφέρουν οι έρευνες αυτές, σχετικά με τον κόστος σε συνολικό επίπεδο ή ανά κατηγορία κόστους, με διάσπαση του δείγματος ανά κλάδο δραστηριότητας δεν θα χρησιμοποιηθούν καθώς δεν έχουν στατιστική εγκυρότητα. Συγκεκριμένα, ο μέσος αριθμός παρατηρήσεων που χρησιμοποιήθηκε για κάθε δείγμα ανά κλάδο ήταν το ανώτερο 3,5. Το μέγεθος αυτό κρίνεται ως εξαιρετικά ανεπαρκές προκειμένου να χρησιμοποιηθούν τα στοιχεία αυτά για έκδοση συμπερασμάτων. Προφανώς το μικρό δείγμα είναι που οδήγησε σε αποτελέσματα τα οποία αντίκειται στις υποθέσεις που προέρχονται βάση της θεωρίας. Συγκεκριμένα το συνολικό κόστος και το έμμεσο κόστος προερχόμενο από απώλεια πελατείας για τις εταιρίες τεχνολογίας εμφανίζεται ως χαμηλότερο σε σύγκριση με άλλους κλάδους, οι οποίοι λόγω της φύσης τους, δεν έχουν τόσο μεγάλη εξάρτηση στα ΠΣ. Η υπόθεση που πραγματοποιείται βάση της θεωρίας είναι ότι οι οργανισμοί τεχνολογίας πρέπει να υπόκειται σε μεγαλύτερο έμμεσο κόστος από τις παραβιάσεις ασφαλείας σε σύγκριση με τους λοιπούς οργανισμούς. Εμπειρικές μελέτες, συμπεριλαμβανομένης αυτής που εκπονήθηκε στα πλαίσια της παρούσας διατριβής, επιβεβαιώνουν την συγκεκριμένη υπόθεση.

4.3.3.2 Ανάλυση της συχνότητας εμφάνισης των παραβιάσεων ασφαλείας

Από τις μελέτες των CSI/FBI μπορούν να εξαχθούν δεδομένα προκειμένου για την προσέγγιση της ετήσιας συχνότητας εμφάνισης παραβιάσεων ασφαλείας. Συγκεκριμένα, από τις μελέτες των συγκεκριμένων φορέων, προκύπτει πως στο διάστημα ανάλυσης κατά μέσο όρο το 43% των οργανισμών δέχθηκε τουλάχιστον μία παραβίαση ασφαλείας μέσα σε διάστημα δώδεκα μηνών. Το συγκεκριμένο ποσοστό πρέπει να ερμηνευθεί σε συνδυασμό με ένα άλλο μέγεθος το οποίο αναφέρθηκε αρχικώς στην ενότητα 4.3.1. Το μέγεθος αυτό αφορά το εκτιμώμενο μέρος των παραβιάσεων ασφαλείας που διαπιστώνεται από έναν οργανισμό σε σχέση με το σύνολο των πετυχημένων επιθέσεων που δέχεται. Εμπειρικές μελέτες προσεγγίζουν το ποσοστό αυτό σε 10% επί του συνόλου των παραβιάσεων ασφαλείας το οποίο είναι αρκετά χαμηλό. Συνδυάζοντας τα δύο αυτά μεγέθη μεταξύ τους μπορούμε να οδηγηθούμε στην εύλογη υπόθεση ότι σχεδόν το σύνολο των οργανισμών σήμερα δέχεται μία τουλάχιστον παραβίαση ασφαλείας σε ετήσια βάση. Με άλλα λόγια το ποσοστό των οργανισμών που δέχθηκε σε ετήσια βάση ένα περιστατικό

ασφαλείας προκύπτει εξαιρετικά υψηλό, όταν συνδυαστεί με το εκτιμώμενο ποσοστό των διαγνωσμένων παραβιάσεων ασφαλείας το οποίο είναι εξαιρετικά χαμηλό.

Σύμφωνα με τις δύο τελευταίες δημοσκοπήσεις από την Ernst & Young, πάνω από το 70% των οργανισμών θεωρεί ότι οι κίνδυνοι παραβιάσεων ασφαλείας αυξάνονται. Συνδυάζοντας τα αποτελέσματα των συγκεκριμένων μελετών μπορούμε να ξεχωρίσουμε δύο κύριους λόγους που οδηγούν σε αλλαγές το περιβάλλον κινδύνων που καλούνται να αντιμετωπίσουν οι οργανισμοί: Ο πρώτος λόγος έγκειται στην αύξηση των κινδύνων που προέρχονται από το εξωτερικό περιβάλλον. Οι κίνδυνοι αυτοί αναλύονται στην παράγραφο 4.3.3.4. Ο δεύτερος λόγος προέρχεται από την ραγδαία εξέλιξη της τεχνολογίας και την άμεση υιοθέτηση της από τους οργανισμούς προκειμένου να πετύχουν μείωση του κόστους και να ανταπεξέλθουν μέσα στην οικονομική κρίση των τελευταίων ετών. Το σύνολο σχεδόν των οργανισμών θεωρεί ότι η χρήση τεχνολογιών τύπου "cloud computing" και κινητών υπολογιστικών συσκευών δεν μειώνει τους κινδύνους παραβιάσεων ασφαλείας με το 60% να εκτιμάει ότι οι συγκεκριμένοι κίνδυνοι αυξάνονται.

Μπορούμε συνεπώς να συμπεράνουμε ότι η αύξηση των κινδύνων, ανεξαρτήτως του λόγου από τον οποίο προέρχεται, έχει την δυναμική να οδηγήσει σε αύξηση την συχνότητα των παραβιάσεων ασφαλείας. Τα προαναφερόμενα δεδομένα δεν μπορούν να μας οδηγήσουν στην προσέγγιση του επιπέδου στο οποίο ανέρχεται η συχνότητα των παραβιάσεων αλλά μας δίνουν σαφή ένδειξη για την αυξητική τάση τους.

Στις αντίστοιχες μελέτες από την Ponemon Institute, τα δείγματα που χρησιμοποιούνται αποτελούνται αποκλειστικά από οργανισμούς που έχουν δεχθεί τουλάχιστον μία παραβίαση ασφαλείας και συνεπώς δεν μπορούν να χρησιμοποιηθούν προκειμένου να προκύψουν συμπεράσματα σχετικά με την συχνότητα παραβιάσεων ασφαλείας.

4.3.3.3 Ανάλυση κατηγοριών περιστατικών ασφαλείας

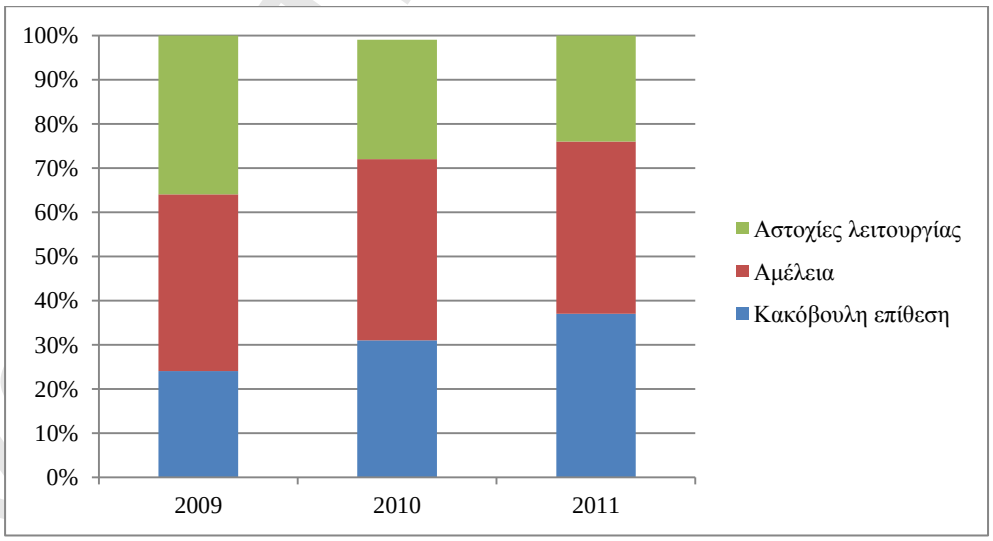
Προκειμένου για την ανάλυση των κατηγοριών στις οποίες μπορούν να ενταχθούν τα περιστατικά ασφαλείας έγινε χρήση των κριτηρίων που τέθηκαν στην ενότητα 4.2.4. Οι μελέτες του Ponemon Institute περιέχουν τα δεδομένα με τη μεγαλύτερη πληρότητα προκειμένου για την ποσοτικοποίηση των εξεταζόμενων κατηγοριών. Στον Πίνακα 4 παρουσιάζεται η εξέλιξη που είχε στην τελευταία τριετία ο επιμερισμός των παραβιάσεων ασφαλείας μεταξύ των τριών βασικών κατηγοριών.

Από το Διάγραμμα 3, στο οποίο παρουσιάζονται τα δεδομένα του Πίνακα 4, φαίνεται καθαρά η μείωση των περιστατικών που προκαλούνται από αστοχίες στην λειτουργία των ΠΣ ενός οργανισμού ενώ παράλληλα διαπιστώνεται η ραγδαία αύξηση των περιστατικών που προκαλούνται από κακόβουλες ή εγκληματικές επιθέσεις. Η διαπίστωση αυτή επιβεβαιώνει τις αλλαγές που επιτελούνται στο περιβάλλον κινδύνων στο οποίο οφείλουν να λειτουργήσουν και να ανταπεξέλθουν οι οργανισμοί. Επίσης επιβεβαιώνει τους οργανισμούς σχετικά με την προτεραιότητα που επιδίδουν πλέον στους κινδύνους παραβιάσεων ασφαλείας. Η κατηγορία των περιστατικών που προέρχονται από αμέλεια του ανθρώπινου παράγοντα, που συσχετίζεται άμεσα ή έμμεσα με έναν οργανισμό, παραμένει σταθερή τα τελευταία χρόνια υποδεικνύοντας ότι οι εξελίξεις που έχουν συντελεστεί δεν την επηρεάζουν.

Πίνακας 4: Επιμερισμός περιστατικών παραβίασης ασφαλείας ανά κατηγορία από Ponemon

Κατηγορία περιστατικού	2009	2010	2011
Κακόβουλη επίθεση	24%	31%	37%
Αμέλεια	40%	41%	39%
Αστοχίες λειτουργίας	36%	27%	24%

Διάγραμμα 3: Επιμερισμός περιστατικών παραβίασης ασφαλείας ανά κατηγορία από Ponemon



Οι μελέτες της Verizon παρουσιάζουν μία άλλη διάσταση σχετικά με τις κατηγορίες που επιμερίζονται τα περιστατικά ασφαλείας. Όπως φαίνεται στον Πίνακα 5 η χρήση κακόβουλου λογισμικού σε συνδυασμό με μεθόδους hacking, προκειμένου για την επίτευξη επιθέσεων πρόσβασης, αποτελούν την συντριπτική πλειονότητα των περιστατικών. Τα περιστατικά επομένως φυσικής παραβίασης, κλοπής υλικού και κατάχρησης δεδομένων από το ανθρώπινο στοιχείο στο εσωτερικό περιβάλλον ενός οργανισμού σταδιακά μειώνονται οδηγώντας την βαρύτητα σε επιθέσεις στον κυβερνοχώρο προερχόμενες κυρίως από απειλές που πηγάζουν από το εξωτερικό περιβάλλον ενός οργανισμού. Εκτενέστερη περιγραφή αυτού του φαινομένου γίνεται στην παράγραφο 4.3.3.4 όπου αναλύεται η προέλευση των απειλών που προκαλούν παραβιάσεις ασφαλείας.

Πίνακας 5: Τρόπος επίθεσης σε σχέση με τον αριθμό των επιθέσεων σύμφωνα με την Verizon

Τρόπος επίθεσης	2009	2010	2011
Κακόβουλο λογισμικό	38%	49%	69%
Hacking	40%	50%	81%
Χρήση κοινωνικής δικτύωσης	28%	11%	7%
Κατάχρηση δεδομένων	48%	17%	5%
Φυσική επίθεση	15%	29%	10%
Σφάλμα	2%	1%	1%

Στον Πίνακα 6 παρουσιάζεται η ίδια κατανομή των περιστατικών ασφαλείας με την διαφοροποίηση ότι τα δεδομένα αφορούν τον αριθμό των προσβεβλημένων εγγραφών χωρίς να λαμβάνεται υπόψη ο αριθμός των περιστατικών από τον οποίο προήλθαν. Σχεδόν το σύνολο των εγγραφών, των οποίων η ασφάλεια παραβιάστηκε, προέρχεται από επιθέσεις στις οποίες χρησιμοποιήθηκε hacking με εργαλεία κακόβουλου λογισμικού. Πλέον, η αμέλεια του ανθρώπινου στοιχείου, σε συνδυασμό με την χρήση της κοινωνικής δικτύωσης, δημιουργούν εστίες σοβαρών ευπαθειών προς εκμετάλλευση μέσω hacking για την επιτέλεση επιθέσεων στον κυβερνοχώρο. Η συντριπτική πλειοψηφία των περιστατικών που προκλήθηκαν από το ανθρώπινο στοιχείο στο εσωτερικό περιβάλλον του οργανισμού αφορούσε αμέλεια και όχι κακόβουλη πράξη. Προκύπτει επομένως πως η αμέλεια κατά κύριο λόγο δεν αποτελεί απειλή αλλά ευπάθεια η οποία δύναται να γίνει αντικείμενο εκμετάλλευσης από ενέργειες hacking και χρήσης κακόβουλου λογισμικού. Στις μελέτες των CSI/FBI και Ponemon προκύπτει ξεκάθαρα η αυξητική τάση των

περιστατικών ασφαλείας που προκαλούνται από την χρήση hacking και κακόβουλου λογισμικού επιβεβαιώνοντας τα προαναφερόμενα πορίσματα που προήλθαν από την χρήση των δεδομένων της Verizon.

Πίνακας 6: Τρόπος επίθεσης σε σχέση με τον αριθμό των προσβεβλημένων εγγραφών σύμφωνα με την Verizon

Τρόπος επίθεσης	2009	2010	2011
Κακόβουλο λογισμικό	94%	79%	95%
Hacking	96%	89%	99%
Χρήση κοινωνικής δικτύωσης	3%	1%	37%
Κατάχρηση δεδομένων	3%	1%	1%
Φυσική επίθεση	1%	10%	1%
Σφάλμα	0%	0%	0%

Οι μελέτες των CSI/FBI επιβεβαιώνουν ότι οι κατηγορίες παραβιάσεων ασφαλείας, που ανήκουν στις κατηγορίες άρνησης παροχής υπηρεσίας και αλλοίωσης διαδικτυακού τόπου, έχουν μειωθεί αισθητά τα τελευταία χρόνια και πλέον η πλειοψηφία των περιστατικών, είτε λαμβάνοντας τον αριθμό των περιπτώσεων είτε το μέσο επίπεδο επίπτωσης με κριτήριο τον αριθμό των εκτιθέμενων εγγραφών, ανήκει στα περιστατικά επιθέσεων πρόσβασης. Στην τελευταία μελέτη μάλιστα των δύο φορέων προκύπτει πως οι κατηγορίες άρνησης παροχής υπηρεσίας και αλλοίωσης διαδικτυακού τόπου έχουν περιοριστεί στο μισό σε σχέση με το μέσο επίπεδο των τελευταίων ετών.

Από την τελευταία μελέτη της Verizon προκύπτει πως τα συνηθέστερα περιστατικά αφορούν εξωτερικούς παράγοντες, χρήση κακόβουλου λογισμικού και hacking καθώς και επίθεση πρόσβασης με στόχο την παραβίαση της εμπιστευτικότητας και ακεραιότητας ευαίσθητων δεδομένων. Όπως επιβεβαιώνεται από εμπειρικές μελέτες, σχετικά με την ποσοτικοποίηση του κόστους παραβιάσεων ασφαλείας, οι επιθέσεις που συνδυάζουν αυτά τα χαρακτηριστικά αποτελούν τις πλέον επικίνδυνες με την δυναμική πρόκλησης των μεγαλύτερων οικονομικών επιπτώσεων σε έναν οργανισμό. Στην εμπειρική μελέτη που έγινε στα πλαίσια της παρούσας διατριβής και παρουσιάζεται στο κεφάλαιο 5 οι παραβιάσεις εμπιστευτικότητας ευαίσθητων δεδομένων πελατών αποτελούν το 46% επί του συνολικού δείγματος και περιλαμβάνουν τα περιστατικά που επέφεραν το μεγαλύτερο κόστος. Στις μελέτες από την Ernst & Young

επιβεβαιώνονται τα προαναφερόμενα, καθώς προκύπτει πως οι οργανισμοί πλέον θεωρούν ότι οι εστίες των σημαντικότερων κινδύνων ΠΣ προέρχονται από την εμπιστευτικότητα των πληροφοριών που διαχειρίζονται και από την διατήρηση της διαθεσιμότητας των ΠΣ.

4.3.3.4 Ανάλυση προέλευσης των απειλών για την ασφάλεια

Στην τελευταία μελέτη από την Ernst & Young προκύπτει πως η συντριπτική πλειοψηφία των οργανισμών θεωρεί τις απειλές από το εξωτερικό περιβάλλον ως τις πλέον βασικές και αποδίδουν λιγότερη βαρύτητα στις αντίστοιχες απειλές προερχόμενες από το εσωτερικό περιβάλλον. Η προτεραιότητα που επιδίδουν οι οργανισμοί στην αντιμετώπιση των εξωτερικών απειλών αποδεικνύεται από τα δεδομένα που προέρχονται από τις έρευνες της Verizon και τα οποία αποτυπώνονται στον Πίνακα 7 και Πίνακα 8. Συγκεκριμένα, στον Πίνακα 7 προκύπτει χαρακτηριστικά η εναλλαγή της βαρύτητας, στην πρόκληση περιστατικών ασφαλείας, μεταξύ των εσωτερικών και εξωτερικών απειλών. Τα τελευταία τρία χρόνια οι εσωτερικές απειλές παρουσιάζουν ραγδαία μείωση με τους κινδύνους παραβιάσεων ασφαλείας να εστιάζονται σχεδόν αποκλειστικά στις απειλές που δημιουργεί το εξωτερικό περιβάλλον ενός οργανισμού.

Πίνακας 7: Κατανομή του αριθμού περιστατικών σύμφωνα με την πηγή απειλής με στοιχεία της Verizon

Πηγή απειλής	2009	2010	2011
Εξωτερική	72%	86%	98%
Εσωτερική	48%	12%	4%
Συνεργάτης	6%	2%	1%
Πολλαπλή	27%	9%	2%

Η βαρύτητα των εξωτερικών απειλών στην σύνθεση των κινδύνων παραβιάσεων ασφαλείας μπορεί να διαπιστωθεί ακόμη περισσότερο από τον Πίνακα 8, στον οποίο παρουσιάζεται η κατανομή του συνολικού αριθμού προσβεβλημένων εγγραφών ανά πηγή απειλής[5]. Ο αριθμός των δεδομένων, που προσβλήθηκαν από εξωτερικές απειλές, αυξάνεται διαρκώς σε όλο το διάστημα ανάλυσης με αποκορύφωμα το έτος 2011 όπου σχεδόν το σύνολο των δεδομένων προσβλήθηκαν

[5] Τα δεδομένα που αφορούσαν τον αριθμό των προσβεβλημένων εγγραφών στο έτος 2010 εξαιρέθηκαν καθώς είχαν πολύ μεγάλη απόκλιση σε σχέση με το σύνολο των υπολοίπων δεδομένων και επέφεραν μεγάλη αλλοίωση στον υπολογισμό των μέσων τιμών. Αξίζει να σημειωθεί πως η ποσοστιαία κατανομή του αριθμού των εγγραφών ανά πηγή απειλής ήταν στα ίδια επίπεδο με το μέσο επίπεδο του υπολοίπου χρονικού διαστήματος.

από επιθέσεις προερχόμενες από το εξωτερικό περιβάλλον των οργανισμών. Κατά μέσο όρο το 89% των δεδομένων προσβάλλεται από εξωτερικές απειλές με το υπόλοιπο μέρος να επιμερίζεται σχεδόν ισόποσα στις υπόλοιπες κατηγορίες πηγών απειλών.

Πίνακας 8: Κατανομή του αριθμού των προσβεβλημένων εγγραφών ανά πηγή απειλής με στοιχεία της Verizon

Πηγή απειλής	2004-2008	2009	2011	Μέσες τιμές
Εξωτερική	662.154.296	138.566.355	173.874.419	139.227.867
Εσωτερική	27.589.587	1.264.240	55.493	4.129.903
Συνεργάτης	43.744.443	130	153.002	6.271.082
Πολλαπλή	44.015.607	2.436.297	403	6.636.044
Σύνολα	**777.503.933**	**142.267.022**	**174.083.317**	**156.264.896**

Συνδυάζοντας τα παραπάνω αποτελέσματα με τα αντίστοιχα αποτελέσματα της προηγούμενης ενότητας καταλήγουμε σε ένα γενικό πόρισμα: Οι εξωτερικές απειλές είναι οι πλέον σοβαρές για έναν οργανισμό και επιπλέον η επίδραση των εσωτερικών απειλών είναι κατά κύριο λόγο από αμέλεια η οποία δεν επιφέρει άμεση επίθεση αλλά δημιουργεί ευπάθειες που δύναται να εκμεταλλευθούν εξωτερικοί παράγοντες.

4.3.3.5 Ανάλυση λοιπών θεμάτων σχετικά με τις παραβιάσεις ασφαλείας

Εξίσου σημαντικός με τα προαναφερθέντα στις προηγούμενες παραγράφους είναι ο προβληματισμός, που αποτυπώνουν οι οργανισμοί, σχετικά με την κατάλληλη επικοινώνηση με την ανώτερη διοίκηση θεμάτων ασφαλείας που περιλαμβάνουν κατά κύριο λόγο τον προσδιορισμό του επιπέδου επένδυσης σε δομές ασφαλείας. Το πρόβλημα αυτό προκαλείται κατά κύριο λόγο από την έλλειψη μεθόδων αντικειμενικής ποσοτικοποίησης του επιπέδου της ασφάλειας, των οικονομικών επιπτώσεων που επιφέρουν περιστατικά παραβίασης και γενικότερα του μεγέθους των κινδύνων ΠΣ.

Η έλλειψη αυτή στερεί την δυνατότητα, στα κλιμάκια διαχείρισης κινδύνων, στην επικοινωνία θεμάτων ασφαλείας μέσω απλών μεγεθών και δεικτών που μπορεί να κατανοήσει η διοίκηση ενός οργανισμού και να πεισθεί στην διοχέτευση επιπλέον κεφαλαίων σε δομές ασφαλείας. Το σύνολο της ερευνητικής προσπάθειας της παρούσας διατριβής επικεντρώνεται στην σύνθεση μεθοδολογιών για την αντικειμενική ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας

προκειμένου για την αποτελεσματικότερη ενημέρωση των αποφασιζόντων σε έναν οργανισμό και την εν κατακλείδι επίτευξη του βέλτιστου επιπέδου επενδύσεων σε δομές ασφαλείας.

4.3.4 Οργανισμοί καταγραφής και ανάλυσης περιστατικών ασφαλείας

Στην συγκεκριμένη ενότητα γίνεται περιγραφή των οργανισμών που είναι αφιερωμένοι στην καταγραφή και ανάλυση γνωστοποιημένων περιστατικών παραβίασης ασφαλείας. Οι οργανισμοί που καταγράφονται είναι όλοι κοινωφελούς σκοπού και χρησιμοποιήθηκαν για την άντληση δεδομένων κατά την διάρκεια της ερευνητικής προσπάθειας. Μπορούν να χωριστούν σε δύο γενικές κατηγορίες: (α) Οργανισμοί καταγραφής περιστατικών που έχουν επισήμως ανακοινωθεί. (β) Οργανισμοί που καταγράφουν το σύνολο των περιστατικών χωρίς να θεωρούν απαραίτητη την επίσημη αποδοχή από τον φορέα που προσβλήθηκε.

4.3.4.1 Οργανισμοί καταγραφής επίσημων περιστατικών ασφαλείας

Από το σύνολο της ερευνητικής προσπάθειας οδηγηθήκαμε στο πόρισμα ότι οι τρεις βασικότεροι οργανισμοί, που ανήκουν στην πρώτη εκ των δύο προαναφερομένων κατηγοριών, είναι οι DatalossDB [**63**], Identity Theft Resource Center (ITRC) [**64**] και Privacy Rights Clearing House (PRH) [**65**].

Η βάση DatalossDB αποτελεί συλλογική προσπάθεια της κοινότητας των φυσικών και νομικών προσώπων που ενδιαφέρονται για την ασφάλεια των ΠΣ και επικουρείται από το Open Security Foundation. Θεωρούμε ότι είναι η εγκυρότερη βάση και η καταγραφή των περιστατικών γίνεται με το πλέον αξιόπιστο τρόπο. Όπως αναφέρεται αναλυτικά στην ενότητα 5.5, η βάση αυτή αποτέλεσε την κύρια πηγή δεδομένων για την εμπειρική ανάλυση του κόστους παραβιάσεων ασφαλείας που πραγματοποιήθηκε στα πλαίσια της παρούσας διατριβής.

Το ITRC είναι ένας κοινωφελής οργανισμός με σκοπό την έρευνα και ενημέρωση σε θέματα αντιμετώπισης παραβιάσεων ασφαλείας και προσβολής ευαίσθητων δεδομένων καταναλωτών και οργανισμών. Εκδίδει σε ετήσια βάση εκθέσεις με τα περιστατικά παραβίασης ασφαλείας τα οποία κατέγραψε και ανάλυσε καθώς και στατιστικά στοιχεία με κριτήριο τα βασικά χαρακτηριστικά των περιστατικών όπως είναι ο αριθμός των προσβεβλημένων εγγραφών και ο κλάδοι στους οποίους ανήκουν οι εκτεθειμένοι οργανισμοί. Θεωρείται από το πιο αξιόπιστους οργανισμούς και χρησιμοποιήθηκε κατά την εμπειρική ανάλυση που εκπονήθηκε.

Το PRH είναι ένας κοινωφελής οργανισμός με ευρεία αποδοχή στις ΗΠΑ και με σκοπό την προστασία των προσωπικών δεδομένων των καταναλωτών. Ένα από τα κύρια ερευνητικά θέματα του συγκεκριμένου οργανισμού είναι οι παραβιάσεις ασφαλείας και περιέχει δεδομένα περιστατικών από το 2005. Η καταγραφή των περιστατικών θεωρείται αρκετά έγκυρη και κατά την εμπειρική ανάλυση που πραγματοποιήθηκε χρησιμοποιήθηκαν δεδομένα και από αυτή την βάση.

4.3.4.2 Οργανισμοί καταγραφής επίσημων και ανεπίσημων περιστατικών ασφαλείας

Στην δεύτερη κατηγορία επιμερισμού των οργανισμών καταγραφής περιστατικών ασφαλείας κατατάσσονται οι οργανισμοί που δεν θέτουν ιδιαίτερα αυστηρά κριτήρια προκειμένου για την καταχώρηση και ανάλυση ενός περιστατικού. Η βασικότερη διαφοροποίηση έγκειται στο ότι τα περιστατικά που καταγράφονται δεν θεωρείται απαραίτητο να έχουν αναγνωρισθεί από τους οργανισμούς που τα επωμίστηκαν.

Ο IdentityTheft.info [**66**] είναι ένας διαδικτυακός οργανισμός ο οποίος παρέχει πληροφορίες σχετικά με περιστατικά παραβίασης ασφαλείας και κλοπής προσωπικών δεδομένων από το 2008. Παρέχει αποκλειστικά πληροφόρηση σχετικά με τα περιστατικά που καταγράφει σε καθημερινή βάση χωρίς να επιχειρεί την περαιτέρω ανάλυση τους. Το databreaches.net [**67**] είναι ένας διαδικτυακός τόπος ο οποίος καταγράφει περιστατικά από το 2009 και συνεργάζεται με το DatalossDB. Καταγράφει περιστατικά σε καθημερινή βάση και επιχειρεί την κατάταξη τους ανάλογα με τον τύπο του οργανισμού που προσβάλλεται και το είδος του περιστατικού. Το BankinfoSecurity [**68**] είναι ένας οργανισμός που εστιάζει στην καταγραφή περιστατικών που σχετίζονται με τον χρηματοπιστωτικό κλάδο. Επίσης καταγράφει τις εξελίξεις σχετικά με τις μεθοδολογίες και τα εργαλεία αντιμετώπισης κινδύνων παραβιάσεων ασφαλείας. Το DataBreachToday [**69**] είναι ένας διαδικτυακός τόπος ο οποίος έχει δημιουργηθεί από το Information Security Media Group και αποσκοπεί στην καταγραφή περιστατικών και εξελίξεων στην διαχείριση κινδύνων ΠΣ λαμβάνοντας στοιχεία από πολλαπλές πηγές.

Καθώς οι προαναφερόμενες πηγές δεδομένων δεν χρησιμοποιούν αυστηρά κριτήρια στην καταχώρηση των περιστατικών, χρησιμοποιήθηκαν μόνο επικουρικά κατά την διάρκεια της ερευνητικής προσπάθειας. Τα δεδομένα αντλήθηκαν κατά κύριο λόγο από τα δεδομένα που

παρέχουν οι οργανισμοί που κατατάχθηκαν στην πρώτη κατηγορία. Οι πηγές που ανήκουν στην δεύτερη κατηγορία χρησιμοποιήθηκαν κατά κύριο λόγο για την επαλήθευση και συμπλήρωση ελλείψεων στα δεδομένα που προέρχονταν από τις πηγές της πρώτης κατηγορίας.

5 Μέτρηση της οικονομικής επίπτωσης παραβιάσεων ασφάλειας μέσω της μεθοδολογίας ανάλυσης γεγονότων

5.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο αναλύεται η μεθοδολογία ανάλυσης γεγονότων, υφιστάμενες εμπειρικές μελέτες που χρησιμοποιούν την συγκεκριμένη μεθοδολογία και κατά κύριο λόγο η έρευνα που διεξήχθη, στα πλαίσια της παρούσας διατριβής, σχετική με την μέτρηση της οικονομικής επίπτωσης των παραβιάσεων ασφαλείας μέσω της χρήσης εμπειρικών δεδομένων. Σε αντίθεση με τα δεδομένα που συλλέγονται από τις μελέτες συμβουλευτικών οργανισμών για την ασφάλεια ΠΣ, που προέρχονται από εθελοντική ανταπόκριση των οργανισμών, τα δεδομένα που μελετήθηκαν στις συγκεκριμένες εμπειρικές μελέτες προέρχονται από πληροφόρηση που υφίσταται δημόσια στην αγορά. Η πληροφόρηση αυτή συνθέτεται από την πορεία των μετοχών εισηγμένων εταιριών στις χρηματαγορές οι οποίες δέχθηκαν περιστατικά παραβίασης ασφαλείας.

Η έλλειψη αντικειμενικών ποσοτικών δεδομένων, προκειμένου για την χρήση τους στην εκτίμηση των κινδύνων ασφαλείας, οδήγησε την ακαδημαϊκή κοινότητα, τα τελευταία είκοσι χρόνια, στην ανάπτυξη μίας εναλλακτικής μεθοδολογίας για τον προσδιορισμό του συνολικού κόστους, προερχόμενο από τις επιθέσεις στον κυβερνοχώρο. Η μεθοδολογία αυτή, βασιζόμενη στην μεθοδολογία ανάλυσης γεγονότων (event study methodology), προσεγγίζει το σύνολο των οικονομικών επιπτώσεων εμμέσως μέσω της δημιουργίας ενός αντιπροσωπευτικού μέτρου το οποίο προέρχεται από την στατιστική ανάλυση των επιπτώσεων στην τιμή της μετοχής από την ανακοίνωση παραβιάσεων ασφαλείας.

Η μεθοδολογία αυτή επιχειρεί την σύνδεση μεταξύ της θεωρίας ασφάλειας πληροφόρησης με την ανάλυση γεγονότων και την θεωρεία χρηματοοικονομικής. Η χρήση της στην επιστήμη της Πληροφορικής εφαρμόστηκε αρχικώς για την διερεύνηση της συσχέτισης μεταξύ της ανακοίνωσης επένδυσης πρόσθετων κεφαλαίων σε ΠΣ και πιθανών ασυνήθη αποδόσεων (abnormal returns) στην μετοχή. Ασυνήθεις αποδόσεις ορίζονται ως η διαφορά μεταξύ της πραγματικής και της αναμενόμενης απόδοσης μίας μετοχής. Η αναμενόμενη απόδοση υπολογίζεται με βάση κάποιο επιλεγμένο μοντέλο αποτίμησης επενδυτικών κεφαλαίων.

Αναλυτική περιγραφή της μεθοδολογίας υπολογισμού των ασυνήθη αποδόσεων πραγματοποιείται στην ενότητα 5.4.3.

Προκειμένου για συγκριτικούς λόγους στην ανάλυση προηγούμενων μελετών, εισάγεται ένας τελεστής ο οποίος υπολογίζεται από τον λόγο του αριθμού των γεγονότων που περιλαμβάνονται στο δείγμα προς το μέγεθος της περιόδου, από την οποία προέρχονται τα γεγονότα, μετρούμενη σε χρόνια. Ένα δείγμα που περιλαμβάνει μεγάλο αριθμό παρατηρήσεων αλλά παράλληλα μεγάλη περίοδο ανάλυσης υπάρχει περίπτωση να μην μπορεί να χρησιμοποιηθεί στο σύνολο του καθώς η περίοδος ανάλυσης δύναται να περιλαμβάνει ραγδαίες εξελίξεις σε θέματα τεχνολογίας, της οικονομικής ανάπτυξης και της αποτελεσματικότητας των αγορών στην διάχυση της πληροφόρησης. Σε αυτή την περίπτωση ένα δείγμα πρέπει να διαχωριστεί σε περιόδους με κοινά χαρακτηριστικά ώστε να υπάρχει συνοχή στα δεδομένα που αντλούνται. Η προαναφερόμενη διαπίστωση αποτελεί τον βασικό λόγο για την χρήση του παραπάνω τελεστή προκειμένου για την αξιολόγηση, σε κοινή βάση, των δεδομένων που χρησιμοποίησαν ανάλογες υφιστάμενες μελέτες.

Στο κεφάλαιο αυτό αρχικώς περιγράφονται προηγούμενες σημαντικές μελέτες οι οποίες συγκρίνονται με κριτήριο τα ιδιαίτερα χαρακτηριστικά της μεθοδολογίας που εφαρμόζουν. Στην συνέχεια περιγράφεται η εμπειρική συνεισφορά της συγκεκριμένης ερευνητικής προσπάθειας. Στην επόμενη ενότητα αναλύεται η μεθοδολογία που ακολουθήθηκε στην παρούσα ερευνητική προσπάθεια. Ακολουθεί η περιγραφή της μεθοδολογίας και της διαδικασίας επιλογής του δείγματος που αναλύθηκε. Στην επόμενη ενότητα γίνεται ανάλυση των στατιστικών υποθέσεων που εξετάστηκαν και σε αυτήν που ακολουθεί περιγράφονται τα αποτελέσματα τα οποία συγκρίνονται με τα αντίστοιχα προηγούμενων μελετών προκειμένου για την εξαγωγή συμπερασμάτων με τα οποία κλείνει το παρόν κεφάλαιο.

5.2 Μελέτες ανάλυσης γεγονότων σχετικών με Πληροφοριακά Συστήματα

Στον Πίνακα 9 παρουσιάζονται τα κυριότερα χαρακτηριστικά διαφόρων σημαντικών μελετών που έκαναν χρήση της μεθοδολογίας ανάλυσης γεγονότων προκειμένου για την διερεύνηση των αντιδράσεων της αγοράς στην δημοσίευση γεγονότων σχετικών με την τεχνολογία πληροφόρησης.

Σύμφωνα με την έρευνα που διεξήχθη, η πρώτη μελέτη που χρησιμοποίησε την μεθοδολογία ανάλυσης γεγονότων έγινε από τους Dos Santos et. al. [**70**]. Η συγκεκριμένη μελέτη ήταν αφιερωμένη στην εξέταση της αντίδρασης των χρηματαγορών στις εταιρικές ανακοινώσεις επενδύσεων σε ΠΣ. Η μεθοδολογία της μελέτης ήταν, στο μεγαλύτερο μέρος της, βασισμένη στην αντίστοιχη μελέτη των Loderer et. al. σχετικά με την επίδραση της ανακοίνωσης παροχής μερισμάτων στις αποδώσεις των μετοχών [**71**]. Μία από τις πρώτες μελέτες που αφιερώθηκαν στην ανάλυση των αντιδράσεων της αγοράς σε ανακοινώσεις παραβιάσεων ασφαλείας δημιουργήθηκε από τους Ettredge et. al. [**72**]. Η μελέτη αυτή ήταν επικεντρωμένη σε επιθέσεις τύπου distributed Denial-of-Service (dDoS) και τα γεγονότα αντλήθηκαν από ένα πολύ στενό χρονικό ορίζοντα. Επίσης, η ανάλυση εστιάστηκε μόνο σε εταιρίες του διαδικτύου. Ειδικότερα, αναλύθηκαν οι επιθέσεις που εξαπέλυσαν hackers εναντίων εταιριών του διαδικτύου τον Φεβρουάριο του 2000. Το πόρισμα της μελέτης ήταν μεγάλες απώλειες, για τις εταιρίες διαδικτύου ως αποτέλεσμα επιθέσεων τύπου dDoS, με στατιστική σημαντικότητα. Ωστόσο, ο εξαιρετικά στενός χρονικός ορίζοντας ανάλυσης και η περιορισμένη επιλογή των εκτιθέμενων εταιριών, περιορίζουν σημαντικά τις δυνατότητες γενίκευσης των πορισμάτων της συγκεκριμένης μελέτης.

Η πρώτη μελέτη που εξέτασε την συσχέτιση μεταξύ των παραβιάσεων ασφαλείας και της αντίδρασης των αγορών, με μεγαλύτερο εύρος δεδομένων και ανάλυσης, πραγματοποιήθηκε από τους Campbell et. al. [**73**]. Οι συγκεκριμένοι μελετητές διαχώρισαν τις παραβιάσεις ασφαλείας μεταξύ αυτών που εμπλέκουν αυθαίρετη πρόσβαση σε δεδομένα εμπιστευτικού χαρακτήρα και των υπολοίπων. Κατέληξαν σε αρνητικές ασυνήθεις αποδώσεις με στατιστική σημαντικότητα προκαλούμενες από παραβιάσεις ασφαλείας εμπιστευτικών δεδομένων. Σε αντίθεση με την προαναφερόμενη μελέτη από τους Ettredge et. al., οι συγκεκριμένοι συγγραφείς δεν υποστηρίζουν την πιθανότητα σοβαρών οικονομικών επιπτώσεων προκαλούμενων από άλλους τύπους παραβιάσεων ασφαλείας συμπεριλαμβανομένων και των επιθέσεων τύπου DoS. Η κύρια διαφοροποίηση μεταξύ των δύο μελετών, η οποία περιορίζει την δυνατότητα σύγκρισης τους, είναι η χρήση εξαιρετικά συγκεκριμένου δείγματος αποτελούμενο από γεγονότα που επηρέασαν αποκλειστικά εταιρίες του διαδικτύου σε πολύ στενό χρονικό πλαίσιο από την πλευρά των Ettredge et al.

Πίνακας 9: Βασικά χαρακτηριστικά μελετών της επίδρασης στην μετοχή από ανακοινώσεις παραβιάσεων ασφαλείας

Έτος δημοσίευσης	Βασικός συγγραφέας	Περίοδος ανάλυσης	Αριθμός γεγονότων στο συνολικό δείγμα	Παράθυρα ανάλυσης	Αποτελέσματα ερευνών	Παρατηρήσεις	Δείκτης αντιπροσώπευσης του αγοραίου χαρτοφυλακίου	Περίοδος εκτίμησης παραμέτρων παλινδρόμησης
1993	Dos Santos et. al.	1981-1988	97	[-1,0]	Αποτελέσματα χωρίς στατιστική σημαντικότητα για το σύνολο του δείγματος. Μη σημαντικά αποτελέσματα για τα υπό-δείγματα με βάση τον κλάδο. Στατιστικά σημαντικά αποτελέσματα για τις επενδύσεις σε νεωτερισμούς ΠΣ	Η ανάλυση επικεντρώθηκε στην επίπτωση που έχουν οι επενδύσεις ΠΣ στην αξία ενός οργανισμού.	Chicago Center for Research in Security Prices (CRSP) Index	[-201,-2]
2002	Ettredge et. al.	Φεβρουάριος 2000	166	[0,3], [0,6]	Αρνητικά αποτελέσματα με στατιστική σημαντικότητα για όλα τα παράθυρα ανάλυσης. Μεγαλύτερη επίπτωση των παραβιάσεων ασφαλείας στην περίπτωση ηλεκτρονικού εμπορίου και της επακόλουθης εμφάνισης υψηλότερων κινδύνων.	Η ανάλυση επικεντρώνεται μόνο σε επιθέσεις τύπου dDoS οι οποίες συνέβησαν σε στενό χρονικό ορίζοντα αποκλειστικά σε εταιρίες του διαδικτύου. Επιπλέον, η αντίδραση των αγορών στο σύνολο του κλάδου ηλεκτρονικού εμπορίου διερευνήθηκε.	Δεν αναφέρεται	Δεν αναφέρεται
2003	Campbell et. al.	1995-2000	43	[-1,1]	Στατιστικά σημαντικά αποτελέσματα σχετικά με την διαφοροποίηση αντίδρασης των αγορών σε διαφορετικούς τύπους παραβιάσεων ασφαλείας. Στατιστικά σημαντικά αρνητικά αποτελέσματα σχετικά με παραβιάσεις ασφαλείας της εμπιστευτικότητας δεδομένων. Στατιστικά ασήμαντη αντίδραση των αγορών στις άλλες κατηγορίες παραβιάσεων ασφαλείας. Περιορισμένη στατιστική σημαντικότητα για τα αρνητικά αποτελέσματα στο σύνολο του δείγματος.	Το δείγμα χωρίστηκε σε δύο υπό-δείγματα με κριτήριο τον τύπο των παραβιάσεων ασφαλείας. Το πρώτο περιελάμβανε τα γεγονότα παραβίασης εμπιστευτικότητας και το δεύτερο όλα τα υπόλοιπα.	Ισόποσα επιμερισμένος δείκτης με χρήση των NYSE/AMEX/Nasdaq	[-121,-2]
2003	Garg et. al.	1996-2002	22	[0,3]	Στατιστικά σημαντικά αποτελέσματα για το παράθυρο ανάλυσης [0,3]. Στατιστικά σημαντικά αποτελέσματα ελέγχοντας διαφορετικούς τύπους παραβιάσεων ασφαλείας	Η ανάλυση δεν επικεντρώθηκε σε μεμονωμένους τύπους παραβιάσεων ασφαλείας. Εγκάρσια (cross-sectional) επισκόπηση της περιόδου ανάλυσης. Η επίδραση των παραβιάσεων ασφαλείας σε προμηθευτές λογισμικού ασφαλείας αναλύθηκε επίσης.	Δεν αναφέρεται	Δεν αναφέρεται
2003	Hovav et. al.	1998-2002	23	[-1,0],[-1,1], [-1,5], [-1,10], [-1,25]	Μη στατιστικά σημαντικά αποτελέσματα για το σύνολο του δείγματος. Στατιστικά σημαντικά αποτελέσματα για τις εταιρίες διαδικτύου.	Η ανάλυση επικεντρώνεται μόνο σε επιθέσεις τύπου dDoS.	S&P 500	[-201,-2]

2004	Cavusoglu et. al.	1996-2001	66	[0,1]	Στατιστικά σημαντικά αποτελέσματα για το σύνολο του δείγματος. Στατιστικά σημαντικά αποτελέσματα για την επίδραση σε εταιρίες του διαδικτύου. Σημαντική άνοδος στην τιμή μετοχής των εταιριών προμήθειας λογισμικού ασφαλείας. Ασήμαντα αποτελέσματα σχετικά με το κόστος επιμερίζοντας το δείγμα με κριτήριο το είδος της παραβίασης ασφαλείας.	Η ανάλυση δεν επικεντρώθηκε σε μεμονωμένους τύπους παραβιάσεων ασφαλείας. Εγκάρσια (cross-sectional) επισκόπηση της περιόδου ανάλυσης. Η επίδραση των παραβιάσεων ασφαλείας σε προμηθευτές λογισμικού ασφαλείας αναλύθηκε επίσης.	Nasdaq	[-160,-1]
2010	Patel	2001-2009	34	[0,3], [0,8], [0,30]	Στατιστικά σημαντικά αρνητικά αποτελέσματα μόνο στο παράθυρο ανάλυσης [0,8] ως αποτέλεσμα ανακοινώσεων παραβίασης ασφαλείας. Τα αποτελέσματα που αφορούν τον τύπο των δεδομένων που εκτέθηκαν καθώς και το μέγεθος του οργανισμού δεν εμφανίζουν στατιστική σημαντικότητα σε κανένα παράθυρο ανάλυσης.	Εξέταση των παραβιάσεων ασφαλείας τα οποία οδηγούν στην έκθεση εμπιστευτικών πληροφοριών οι οποίες περιλαμβάνουν είτε αριθμούς κοινωνικής ασφάλισης ή πληροφορίες πιστωτικών καρτών.	S&P 500	[-50,-1]
2010	Gatzlaff et. al.	2004-2006	77	Διάφορα παράθυρα ανάλυσης από [-5,0] έως [0,180]	Στατιστικά σημαντικά αρνητικά αποτελέσματα στα παράθυρα ανάλυσης από το [0,1] έως το [0,35]. Στατιστικά σημαντική μεγαλύτερη επίπτωση των παραβιάσεων ασφαλείας για τις μικρότερες εταιρίες. Μεγαλύτερο κόστος για τους οργανισμούς που εμφανίζουν μεγαλύτερες επενδυτικές ευκαιρίες. Σημαντικές ενδείξεις διαρροής εσωτερικής πληροφόρησης.	Η μελέτη εξετάζει αποκλειστικά παραβιάσεις ασφαλείας οι οποίες εμπλέκουν εμπιστευτική πληροφόρηση και ιδίως πληροφορίες σχετιζόμενες με τους υπαλλήλους και πελάτες ενός οργανισμού.	Δείκτης CRSP	[-252,-7]
2011	Yayla et. al.	1994-2006	123	[-1,1],[-1,5], [-1,10]	Στατιστικά σημαντικά αρνητικά αποτελέσματα για το συνολικό δείγμα. Αρνητικά αποτελέσματα με στατιστική σημαντικότητα για εταιρίες ηλεκτρονικού εμπορείου και εταιρίες τεχνολογίας. Μεγαλύτερος αντίκτυπος από επιθέσεις τύπου DoS σε σχέση με τους λοιπούς τύπους. Η προαναφερόμενη στατιστική σημαντικότητα δεν ίσχυσε για όλα τα παράθυρα ανάλυσης.	Η μελέτη αυτή εξετάζει όλους τους τύπους παραβιάσεων ασφαλείας εκτός από τις επιθέσεις ιών. Πραγματοποιείται ανάλυση του είδους οργανισμού, ανά τομέα οικονομίας και με βάση παράγοντες έκτακτης ανάγκης.	Ισόποσα επιμερισμένος δείκτης με χρήση των NYSE/AMEX/Nasdaq	[-130,-10]
2011	Gordon et. al.	1995-2007	121	[-1,1]	Στατιστικά σημαντικά αρνητικά αποτελέσματα για το σύνολο του δείγματος. Τα αρνητικά αποτελέσματα προερχόμενα από παραβιάσεις στην κατηγορία της διαθεσιμότητας πληροφόρησης εμφανίζουν μεγαλύτερη σημαντικότητα. Τα αποτελέσματα οδηγούνται κυρίως από την υπό-περίοδο μεταξύ 1995-2001 υποδεικνύοντας την σταδιακή μείωση των επιπτώσεων που επιφέρουν οι παραβιάσεις ασφαλείας.	Η μελέτη αυτή εξετάζει περιστατικά παραβίασης ασφαλείας με κριτήρια το είδος της παραβίασης και τον χρόνο που πραγματοποιήθηκε. Οι μελετητές επιχειρούν να επεξηγήσουν τα ανάμικτα αποτελέσματα προηγούμενων μελετών. Κάνουν χρήση, εκτός του CAPM, του μοντέλου τριών-παραμέτρων των Fama-French.	Σταθμισμένος δείκτης με χρήση των NYSE/AMEX/Nasdaq	[-121,-2]

Τα περιστατικά ασφαλείας, που δεν επηρεάζουν εμπιστευτικές πληροφορίες, μπορούν να κατηγοριοποιηθούν ως λειτουργικά περιστατικά ασφαλείας υποδηλώνοντας ότι επηρεάζουν μόνο λειτουργικά έναν οργανισμό. Οι εταιρίες διαδικτύου δύναται να απολέσουν σημαντικά μεγέθη χρηματοροών και φήμης από σημαντικά λειτουργικά περιστατικά ασφαλείας σε αντίθεση με εταιρίες παραδοσιακού τύπου (brick-and-mortar firms). Ωστόσο, η ανάλυση από τους Campbell et al. έχει το μειονέκτημα χρήσης σχετικά μικρού δείγματος καθώς, από το πλήθος των 43 γεγονότων στο σύνολο του δείγματος, μόνο 11 γεγονότα αφορούν παραβίαση ασφάλειας εμπιστευτικών πληροφοριών.

Σε άλλη μελέτη οι Hovav et. al. [**74**] ερεύνησαν την επίπτωση των επιθέσεων τύπου DoS επιβεβαιώνοντας τα κοινά αποτελέσματα των μελετών από τους Ettredge et. al. και Campbell et. al. Συγκεκριμένα, κατέληξαν σε στατιστικά σημαντικά αρνητικά αποτελέσματα για το σύνολο του δείγματος, καθώς και εξατομικευμένα για τις εταιρίες διαδικτύου υποδηλώνοντας ότι οι εταιρίες παραδοσιακού τύπου δεν επηρεάζονται σημαντικά από επιθέσεις αυτού του τύπου. Ωστόσο, όπως και οι ίδιοι οι συγγραφείς σημειώνουν, το δείγμα που χρησιμοποιήθηκε είναι πολύ μικρό περιλαμβάνοντας μόνο 23 παρατηρήσεις γεγονός που δύναται να περιορίζει την εγκυρότητα των αποτελεσμάτων.

Νεώτερη μελέτη από τους ίδιους συγγραφείς [**75**] εξέτασε ένα πολύ μεγαλύτερο σύνολο δεδομένων αποτελούμενο από 186 παρατηρήσεις αλλά περιορίστηκε μόνο σε ανάλυση επιθέσεων προερχόμενες από ιούς. Τα αποτελέσματα της μελέτης αυτής όχι μόνο δεν είχαν στατιστική σημαντικότητα αλλά οι υπολογιζόμενες μέσες σωρευτικές ασυνήθεις αποδόσεις ήταν θετικές γεγονός που έρχεται σε αντίθεση με τις υποθέσεις βάση θεωρίας. Ο λόγος που οδήγησε σε αυτά τα αποτελέσματα αυτήν την μελέτη θεωρούμε ότι έχει να κάνει με την ίδια την υπόσταση των ιών και με τα ιδιαίτερα χαρακτηριστικά των επιθέσεων παραβίασης ασφαλείας που επιφέρουν σε έναν οργανισμό.

Μία επίθεση προερχόμενη από ιό, εξ ορισμού, επιρρεάζει ένα σύνολο οργανισμών ταυτόχρονα το οποίο έρχεται σε αντίθεση με την μεθοδολογία ανάλυσης γεγονότων με την οποία εξετάζεται η αντίδραση της αγοράς στην ανακοίνωση ενός γεγονότος επικεντρωμένου σε μία επιχείρηση. Αντιθέτως, έναν ιός έχει την δυναμική να επηρεάσει έναν ολόκληρο τομέα ή ακόμα και το σύνολο μίας οικονομίας. Χαρακτηριστικά παραδείγματα είναι ο ιός “Melissa” τον Μάρτιο του 1999, ο ιός “Love Bug” τον Μάιο του 2000 και ο ιός “Code Red” τον Αύγουστο του 2001 που έπληξαν έναν

τεράστιο αριθμό ΠΣ με σημαντικό μέρος αυτών να ανήκει σε επιχειρήσεις της υψηλής κεφαλαιοποίησης. Εκτιμάται ότι μόνο οι ιοί που εμφανίστηκαν το 1999, οδήγησαν οργανισμούς σε παγκόσμιο επίπεδο σε οικονομικές απώλειες ύψους $7,6 δις λόγω μειωμένης παραγωγικότητας [**76**]. Καμιά όμως από τις αναρίθμητες επιθέσεις, που προκλήθηκαν από αυτούς τους ιούς, δεν μπορεί να χαρακτηρισθεί ως στοχευόμενη επίθεση σε κάποιον μεμονωμένο οργανισμό. Λαμβάνουμε την παραδοχή επομένως, ότι σε μία μαζική επίθεση ενός ιού οι αγορές δεν θα αντιδράσουν απέναντι σε κάθε μεμονωμένη επιχείρηση που προσβλήθηκε.

Επομένως, για τον προαναφερόμενο λόγο, από την παρούσα έρευνα αμφισβητείται η εγκυρότητα μίας μελέτης ανάλυσης γεγονότων η οποία περιλαμβάνει περιστατικά ιών και από το δείγμα που δημιουργήθηκε εξαιρέθηκαν όλα τα περιστατικά που προκλήθηκαν από επιθέσεις ιών. Μία πρόσφατη μελέτη από τους Yayla et. al. [**77**] υποστηρίζει πως η προσθήκη περιστατικών επιθέσεων ιών μειώνει την εγκυρότητα των αποτελεσμάτων μίας μελέτης ανάλυσης γεγονότων. Οι συγκεκριμένοι μελετητές εξαίρεσαν από το δείγμα τους όλα τα περιστατικά που προκλήθηκαν από ιούς. Επιπρόσθετα, έρευνες που έχουν γίνει από οργανισμούς όπως ο CSI αποτυπώνουν μία βαθμιαία μείωση της σημαντικότητας των περιστατικών παραβίασης ασφαλείας προκαλούμενων από ιούς, με κριτήρια την συχνότητα και το επίπεδο επίπτωσης, γεγονός το οποίο οδηγεί στο συμπέρασμα πως οι οργανισμοί πλέον έχουν εφοδιαστεί με τα κατάλληλα μέτρα αντιμετώπισης τους και δεν αποτελούν πλέον αιτιάσεις γεγονότων με την δυναμική επιπτώσεων που είχαν προγενέστερα [**56**]. Μάλιστα στην τελευταία μελέτη του συγκεκριμένου οργανισμού [**10**] τα περιστατικά από ιούς έχουν ενσωματωθεί πλέον στην γενικότερη κατηγορία πρόκλησης επιθέσεων μέσω της χρήσης κακόβουλου λογισμικού το οποίο αποτυπώνει περαιτέρω τον βαθμιαίο περιορισμό του αντίκτυπου που επιφέρουν οι ιοί στην ασφάλεια ΠΣ τα τελευταία χρόνια.

Οι Garg et. al. [**78**] εξέτασαν περιστατικά παραβίασης ασφαλείας στην περίοδο μεταξύ των ετών 1996 - 2002 χωρίς επικέντρωση σε συγκεκριμένους τύπους περιστατικών. Μελέτησαν μόνο έναν παράθυρο ανάλυσης γεγονότων το οποίο περιελάμβανε την ημέρα γεγονότος και τις τρεις ακόλουθες. Τα αποτελέσματα τους, για το σύνολο των δεδομένων και για υποσύνολα με κριτήριο τους διαφορετικούς τύπους παραβιάσεων ασφαλείας, παρουσίασαν στατιστική σημαντικότητα. Το πρόβλημα με την συγκεκριμένη μελέτη είναι το μικρό μέγεθος δείγματος το οποίο αποτελείται από 22 παρατηρήσεις παρότι εξετάστηκε ένα χρονικό διάστημα έξι ετών. Το μέγεθος του δείγματος δύναται να οδηγήσει σε θέματα στατιστικής υπόστασης των παραδοχών που

λαμβάνονται προκειμένου για την εφαρμογή της μεθοδολογίας ανάλυσης γεγονότων. Οι μελετητές δεν αναφέρουν λεπτομέρειες σχετικά με την εξέταση της κανονικότητας για την κατανομή που ακολουθούν οι ασυνήθεις αποδόσεις το οποίο, λόγω του μεγέθους του δείγματος, κρίνεται απαραίτητο. Για τους λόγους αυτούς τα αποτελέσματα αυτής της μελέτης χρησιμοποιήθηκαν μόνο για συγκριτικούς λόγους με άλλες μελέτες που εξέτασαν την ίδια χρονική περίοδο όπως αναλύεται παρακάτω.

Μία άλλη μελέτη που διεξήχθη από τους Cavusoglu et al. [**79**], εξέτασε την ίδια περίπου χρονική περίοδο με τους Garg et. al. [**78**], Campbell et. al. [**73**] και Hovav et. al. [**74**] αλλά με ένα μεγαλύτερο δείγμα 66 παρατηρήσεων. Όπως οι συγγραφείς υποστηρίζουν, η περίοδος που ανέλυσαν (1996 - 2001) χαρακτηρίστηκε από υψηλές αποτιμήσεις και διακυμάνσεις στις χρηματαγορές το οποίο δύναται να οδηγήσει σε λανθασμένα συμπεράσματα μία μελέτη βασισμένη στην μεθοδολογία ανάλυσης γεγονότων. Επιπλέον, το μέγεθος του δείγματος, σταθμισμένο με το εύρος της χρονικής περιόδου που αναλύθηκε είναι σχετικά μικρό ενισχύοντας περαιτέρω το προαναφερόμενο πρόβλημα της υψηλής διακύμανσης των χρηματαγορών. Οι μελετητές χρησιμοποίησαν ένα παράθυρο ανάλυσης μεγέθους δύο ημερών, υποδεικνύοντας εμμέσως μεγαλύτερη υποστήριξη στην υπόθεση πληροφοριακά αποτελεσματικών αγορών ημι-ισχυρού τύπου, καταλήγοντας σε στατιστικά σημαντικές αρνητικές ασυνήθεις αποδόσεις για το συνολικό δείγμα[6]. Συνεπείς με τις υπόλοιπες - προαναφερόμενες - μελέτες υποστήριξαν την υπόθεση ότι τα περιστατικά ασφαλείας πλήττουν περισσότερο τις εταιρίες διαδικτύου αλλά δεν βρήκαν σημαντικές αποδείξεις για την υποστήριξη της υπόθεσης ύπαρξης διαφορών στις επιπτώσεις από τους διαφορετικούς τύπους παραβιάσεων ασφαλείας.

Σε πρόσφατη μελέτη ο Patel [**80**] εξέτασε την επίδραση περιστατικών παραβίασης ασφαλείας τα οποία εξέθεσαν δεδομένα με εμπιστευτικότητα τα οποία περιελάμβαναν είτε αριθμούς κοινωνικής ασφάλισης, είτε στοιχεία πιστωτικών καρτών. Ο συγγραφέας χρησιμοποίησε ένα ευρύ αριθμό παραθύρων ανάλυσης τα οποία περιελάμβαναν μέχρι και 30 ημέρες το οποίο αντίκειται στην υπόθεση πληροφοριακά αποτελεσματικών αγορών. Η συγκεκριμένη μελέτη παρέχει στατιστικά σημαντικά αποτελέσματα, για το σύνολο του δείγματος, μόνο στο παράθυρο ανάλυσης οκτώ ημερών το οποίο θεωρούμε ότι είναι σχετικά μεγάλο καθώς αντίκειται – όπως

[6] Ανάλυση των υποθέσεων αποτελεσματικότητας πληροφόρησης των αγορών πραγματοποιείται στην ενότητα 5.4.1.

προαναφέρθηκε - στην υπόθεση αποτελεσματικότητας των αγορών. Τα αποτελέσματα, σχετικά με τον τύπο των δεδομένων που προσβλήθηκαν και το μέγεθος του οργανισμού, δεν είναι στατιστικώς σημαντικά σε κανένα παράθυρο ανάλυσης. Χρησιμοποιώντας το τελεστή που ορίστηκε στην εισαγωγική ενότητα του συγκεκριμένου κεφαλαίου, το μέγεθος του δείγματος (39) σε σχέση με τον σχετικά μεγάλο ορίζοντα ανάλυσης εννέα ετών (2001 – 2009) περιορίζει σημαντικά την στατιστική εγκυρότητα των αποτελεσμάτων της συγκεκριμένης έρευνας.

Οι Gatzlaff et. al. [**81**] εξέτασαν παραβιάσεις ασφαλείας που περιορίστηκαν μόνο στην εμπιστευτικότητα πληροφόρησης και πιο συγκεκριμένα σε δεδομένα υπαλλήλων και πελατών. Το δείγμα της παρούσας έρευνας αποτελείται από παραβιάσεις ασφαλείας αυτών των κατηγοριών κατά το αξιοπρόσεκτο μέγεθος του 97% όπως φαίνεται και από τον Πίνακα 12 στην ενότητα 5.5. Το γεγονός αυτό επιβεβαιώνει την συγκριτική σημαντικότητα που οι συγκεκριμένες κατηγορίες παραβιάσεων ασφαλείας έχουν σήμερα. Το μέγεθος του δείγματος της μελέτης των Gatzlaff et. al. σταθμισμένο κατά τον προαναφερόμενο τελεστή (77 παρατηρήσεις προς περίοδο ανάλυσης 3 ετών) είναι το μεγαλύτερο σε σύγκριση με τα αντίστοιχα δείγματα των προαναφερόμενων μελετών. Δυστυχώς, η χρονική περίοδος ανάλυσης δεν είναι ιδιαίτερα πρόσφατη (2004 – 2006) λαμβάνοντας υπόψη την χρονική στιγμή δημοσίευσης.

Οι συγκεκριμένοι μελετητές υποστηρίζουν ότι περιστατικά ασφαλείας που πλήττουν την εμπιστευτικότητα έχουν την δυναμική να προκαλέσουν σοβαρότερες έμμεσες οικονομικές απώλειες σε έναν οργανισμό από ότι οι λοιπές κατηγορίες περιστατικών. Η άποψη αυτή ταυτίζεται με την προαναφερόμενη μελέτη των Campbell et. al. όπου το δείγμα χωρίστηκε σε δύο υπό-δείγματα σύμφωνα με τον τύπο του περιστατικού ασφαλείας. Το πρώτο περιείχε περιστατικά αυθαίρετης πρόσβασης σε εμπιστευτικές πληροφορίες και το δεύτερο όλα τα υπόλοιπα. Συνεπώς, μπορούμε να εξάγουμε το συνολικό συμπέρασμα, ότι η ακαδημαϊκή κοινότητα ταυτίζεται πλέον με την θεωρητική άποψη ότι τα περιστατικά παραβίασης ασφάλειας εμπιστευτικών πληροφοριών είναι περισσότερο επώδυνα για έναν οργανισμό σε σύγκριση με τις λοιπές κατηγορίες περιστατικών και επιχειρείται η εμπειρική της επιβεβαίωση. Οι ίδιοι ερευνητές διαφωνούν με την εγκυρότητα των αποτελεσμάτων προηγούμενων μελετών που λαμβάνουν γεγονότα από εξαιρετικά διευρυμένες χρονικές περιόδους ενώ εκείνοι χρησιμοποιούν σχετικά μικρό χρονικό ορίζοντα δειγματοληψίας. Όπως προκύπτει από το σύνολο της ανάλυσης στην παρούσα ενότητα, η ερευνητική προσπάθεια της διατριβής ακολουθεί πιστά αυτήν την άποψη. Οι ερευνητές

χρησιμοποίησαν μία μεγάλη ποικιλία παραθύρων ανάλυσης το οποίο συναντήθηκε και στην προαναφερόμενη μελέτη από τον Patel. Τα αποτελέσματα τους είχαν στατιστική σημαντικότητα για τα παράθυρα ανάλυσης μεταξύ [0,0] και [0,35].

Στην παρούσα έρευνα, υποστηρίζεται πως η χρήση παραθύρων ανάλυσης μεγαλύτερων των τριών ημερών αντίκειται στις βασικές παραδοχές της μεθοδολογίας ανάλυσης γεγονότων και επομένως αμφισβητείται η εγκυρότητα χρήσης τους. Επιπλέον, υποστηρίζουμε ότι η χρήση μεγάλων σχετικά παραθύρων ανάλυσης δεν είναι η κατάλληλη μέθοδος ανάλυσης της μακροβιότητας των αρνητικών επιπτώσεων που επιφέρει ένα περιστατικό ασφαλείας για δύο λόγους που πηγάζουν από τις βασικές παραδοχές της μεθοδολογίας ανάλυσης γεγονότων: (α) Τα σχετικά μεγάλα παράθυρα ανάλυσης δεν συνάδουν με την υπόθεση των πληροφοριακά αποτελεσματικών αγορών. (β) Καθώς απομακρυνόμαστε από την ημέρα συμβάντος, η πιθανότητα άλλα τυχαία συμβάντα να επηρεάσουν τις αντιδράσεις τις αγοράς αυξάνεται, υποβαθμίζοντας ταυτόχρονα την εγκυρότητα των αποτελεσμάτων.

Στην ερευνητική προσπάθεια της παρούσας, τα περιστατικά παραβίασης ασφάλειας εμπιστευτικών πληροφοριών, όπως αναφέρθηκε και παραπάνω, αποτελούν το σύνολο σχεδόν του δείγματος προσδίδοντας μία αρχική επιβεβαίωση της υπόθεσης ότι αποτελούν πλέον την κατηγορία περιστατικών με την μεγαλύτερη συχνότητα εμφάνισης. Το μέγεθος της συχνότητας εμφάνισης περιστατικών που προσβάλουν εμπιστευτικές πληροφορίες εμφανίζεται σε πρόσφατες στατιστικές αναλύσεις συμβουλευτικών οργανισμών όπου πλέον το σύνολο σχεδόν των καταγεγραμμένων περιστατικών αφορά την παραβίαση της εμπιστευτικότητας ευαίσθητων πληροφοριών [**13**], [**61**][7]. Στην στατιστική ανάλυση, που αναλύεται στην ενότητα 5.7, επιχειρείται η εμπειρική επιβεβαίωση της συγκριτικά μεγαλύτερης σοβαρότητας των συγκεκριμένων περιστατικών.

Οι Yayla et. al. [**77**] μελέτησαν την περίοδο ανάμεσα στο 1994 – 2006 και κατέληξαν σε ένα δείγμα 123 περιστατικών. Οι συγγραφείς, χρησιμοποίησαν το μεγαλύτερο δείγμα σε σχέση με το σύνολο των προαναφερόμενων μελετών, και ταυτόχρονα ανέλυσαν την μεγαλύτερη συγκριτικά χρονική περίοδο. Συνεπώς, χρησιμοποιώντας πάλι τον τελεστή στάθμισης του μεγέθους του

[7] Εκτενής ανάλυση των μελετών για την ασφάλεια ΠΣ και των περιστατικών παραβίασης ασφαλείας, που εκπονούνται από συμβουλευτικούς οργανισμούς, πραγματοποιείται στο κεφάλαιο 4.

δείγματος, το δείγμα των Gatzlaff et. al. είναι το σχετικά μεγαλύτερο από το σύνολο των μελετών που αναλύθηκαν. Η μελέτη των Yayla et. al. κατέληξε σε αρνητικές ασυνήθεις αποδόσεις με στατιστική σημαντικότητα για το σύνολο του δείγματος. Επιβεβαίωσαν τα αποτελέσματα προηγούμενων μελετών τα οποία αφορούσαν την πρόκληση μεγαλύτερων επιπτώσεων στις εταιρίες ηλεκτρονικού εμπορίου σε σχέση με τις παραδοσιακές εταιρίες. Παρουσιάζει ενδιαφέρον, το αποτέλεσμα της συγκεκριμένη μελέτης κατά το οποίο προκύπτει μεγαλύτερη επίπτωση από τις επιθέσεις τύπου DoS σε σύγκριση με άλλα είδη επιθέσεων. Το αποτέλεσμα αυτό έρχεται σε αντίθεση με προγενέστερες μελέτες. Επιπλέον, οι συγγραφείς εξήγαγαν το συμπέρασμα ότι λιγότερες εταιρίες επηρεάζονται πλέον από περιστατικά ασφαλείας σε σύγκριση με το παρελθόν. Το αποτέλεσμα αυτό έρχεται σε αντίθεση με ότι προβλέπεται από την θεωρεία και λοιπές εμπειρικές ενδείξεις για την εξέλιξη των παραβιάσεων ασφαλείας και πιθανότατα να είναι απόρροια του σχετικά μικρού δείγματος σε σχέση με το εύρος του ορίζοντα ανάλυσης. Τέλος, έστω και αν η συγκεκριμένη μελέτη είναι αρκετά πρόσφατη, δεν αναλύθηκαν τα τελευταία έτη στην διάρκεια των οποίων τα θέματα ασφαλείας εισήλθαν σε μία νέα εποχή και πλέον οι παραβιάσεις ασφαλείας θεωρούνται ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζει ένας σύγχρονος οργανισμός.

Στην πιο πρόσφατη μελέτη, που αναλύθηκε κατά την διάρκεια της παρούσας ερευνητικής προσπάθειας, οι Gordon et. al. [**82**] ανέλυσαν σχεδόν την ίδια περίοδο με την μελέτη των Yayla et. al. και κατέληξαν με ένα δείγμα σχεδόν εφάμιλλο σε μέγεθος, περιλαμβάνοντας 121 παρατηρήσεις. Το μέγεθος του δείγματος σταθμισμένο με το εύρος σε χρόνια του διαστήματος ανάλυσης είναι και πάλι μικρότερο από το δείγμα των Gatzlaff et. al. Οι συγγραφείς ερεύνησαν τις σημαντικές διαφορές στα εμπειρικά αποτελέσματα προηγούμενων μελετών και διερεύνησαν την επεξήγηση τους. Υποστήριξαν πως η διακύμανση του εύρους χρόνου ανάλυσης καθώς και οι ανεπάρκειες του Μοντέλου Αποτίμησης Κεφαλαιουχικών Αγαθών (Capital Asset Pricing Model) είναι οι πιθανότερες βασικές αιτιάσεις των ανάμικτων αποτελεσμάτων προγενέστερων μελετών[8]. Οι Gordon et. al. - όπως και οι Gatzlaff et. al. - χρησιμοποίησαν κατά την εξέταση του δείγματος επιπρόσθετα το μοντέλο τριών-μεταβλητών των Fama-French. Τα αποτελέσματα της ανάλυσης τους είναι πολύ διαφορετικά μεταξύ των μοντέλων που χρησιμοποιήθηκαν. Συγκεκριμένα, βρήκαν

[8] Ανάλυση των Μοντέλων Αποτίμησης Επενδυτικών Κεφαλαίων, ιδιαιτέρως του Μοντέλου Αποτίμησης Κεφαλαιουχικών Αγαθών και του μοντέλου τριών-μεταβλητών των Fama-French πραγματοποιείται στην 5.4.3.

στατιστική σημαντικότητα στο επίπεδο του 1%, για το σύνολο του δείγματος, χρησιμοποιώντας το μοντέλο τριών-μεταβλητών ενώ το αντίστοιχο αποτέλεσμα προερχόμενο από το μοντέλο μία μεταβλητής ήταν στατιστική σημαντικότητα στο επίπεδο του 8%. Η κατηγορία παραβίασης ασφάλειας με την μεγαλύτερη επίπτωση προέκυψε να είναι η διαθεσιμότητα πληροφόρησης με 1% επίπεδο σημαντικότητας προερχόμενο και πάλι από το μοντέλο τριών-μεταβλητών.

Πρέπει βέβαια να αναφερθεί πως η υπό-περίοδος που κατά κύριο λόγο οδηγεί τα συμπεράσματα της έρευνας στο [**82**] είναι μεταξύ των ετών 1995 – 2001 όπου σχεδόν το ήμισυ των παρατηρήσεων προήλθε από περιστατικά που προκλήθηκαν από επιθέσεις ιών. Όπως υποστηρίχθηκε και παραπάνω, η χρήση επιθέσεων ιών στην ανάλυση γεγονότων είναι αντίθετη προς τις θεμελιώδεις αρχές της συγκεκριμένης μεθοδολογίας και επιπλέον δύναται να επηρεάσει αρνητικά τις παραδοχές στις οποίες βασίζεται η περιγραφική γραμμική παλινδρόμηση η οποία χρησιμοποιείται για την εφαρμογή των μοντέλων αποτίμησης επενδυτικών κεφαλαίων. Συγκεκριμένα, η χρήση γεγονότων με ταυτόχρονη επίδραση σε μεγάλο αριθμό επιχειρήσεων μπορεί να οδηγήσει σε αλληλοσυσχέτιση των γεγονότων το οποίο μπορεί να έχει ως αποτέλεσμα την εμφάνιση αυτοσυσχέτισης με συνεπακόλουθη αποδυνάμωση της εγκυρότητας των στατιστικών αποτελεσμάτων.

5.3 Εμπειρική συνεισφορά της παρούσας έρευνας

Η συγκεκριμένη ερευνητική προσπάθεια επιχειρεί να συμπληρώσει το κενό ανάλυσης που υφίσταται για την χρονική περίοδο από το 2008 μέχρι σήμερα. Προς αυτήν την κατεύθυνση το δείγμα απαρτίζεται από γεγονότα που συνέβησαν την περίοδο μεταξύ Ιανουαρίου 2008 και Ιανουαρίου 2012. Επιπρόσθετα, το μικρό μέγεθος του δείγματος προηγούμενων μελετών, το οποίο σε πολλές περιπτώσεις είναι μικρότερο των 30 περιστατικών, δεν διασφαλίζει την κανονικότητα της κατανομής των ασυνήθη αποδόσεων. Καθώς δεν είναι ρεαλιστική η θεώρηση ότι ο πληθυσμός των ασυνήθη αποδόσεων, προερχόμενων από παραβιάσεις ασφαλείας, ακολουθεί την κανονική κατανομή, πρέπει να δημιουργηθεί ένα ελάχιστο απαιτούμενο μέγεθος δείγματος. Οι στατιστικολόγοι γενικά συμφωνούν ότι σε ένα δείγμα άνω των 30 παρατηρήσεων το κεντρικό οριακό θεώρημα μπορεί να εφαρμοστεί για ένα μεγάλο αριθμό πληθυσμιακών κατανομών. Καθώς η παρούσα μελέτη περιλαμβάνει έναν αριθμό παρατηρήσεων ο οποίος είναι πολύ πάνω από αυτό το κατώτατο όριο και λαμβάνοντας υπόψη ότι η χρονική περίοδος που αναλύθηκε είναι σχετικά

μικρή (4 έτη), μπορούμε να υποθέσουμε ότι η κατανομή δειγματοληψίας προσεγγίζει με μικρές αποκλίσεις την κανονική κατανομή.

Ακολουθώντας την μεθοδολογία των Gatzlaff et. al και Gordon et. al. έγινε ανάλυση του δείγματος χρησιμοποιώντας δύο μοντέλα αποτίμησης επενδυτικών κεφαλαίων: Το Μοντέλο Αποτίμησης Κεφαλαιουχικών Αγαθών και το μοντέλο τριών-παραμέτρων των Fama-French. Με αυτόν τον τρόπο γίνεται εμπειρική επαλήθευση των ενδεχόμενης χρησιμότητας του πολυμεταβλητού μοντέλου στην ανάλυση περιστατικών ασφαλείας χρησιμοποιώντας ένα πρόσφατο δείγμα με στατιστικά επαρκές μέγεθος.

Επιχειρήθηκε στην μελέτη να επεκταθεί η μεθοδολογία των Gordon et. al. για την επεξήγηση των παραγόντων που έχουν οδηγήσει το σύνολο των προηγούμενων ανάλογων μελετών σε ανάμικτα συμπεράσματα. Συνεπώς, πέραν από τις δύο παραμέτρους που έθεσαν οι Gordon et. al., σχετικά με τις διαφορετικές χρονικές περιόδους ανάλυσης και των ανεπαρκειών του μοντέλου αποτίμησης κεφαλαιουχικών αγαθών, προσθέτουμε τις εξής:

(α) Η διαφορετική θεώρηση και μεταχείριση των περιστατικών επιθέσεων προερχόμενων από ιούς το οποίο αναλύθηκε εκτενώς στην εξέταση υφιστάμενων μελετών στην ενότητα 5.2.

(β) Ποικίλα μεγέθη δειγμάτων κυμαινόμενα από 23 έως 120 γεγονότα. Όπως αναλύθηκε παραπάνω και αναπτύσσεται περεταίρω στις επόμενες ενότητες του παρόντος κεφαλαίου, μικρά δείγματα συνδυαζόμενα με σχετικά ευρύ χρονικό ορίζοντα ανάλυσης δύναται να αποδυναμώσουν την θεωρητική εγκυρότητα μίας μελέτης ανάλυσης γεγονότων.

(γ) Χρήση διαφορετικών δεικτών για την αντιπροσώπευση του αγοραίου χαρτοφυλακίου στα μοντέλα αποτίμησης επενδυτικών κεφαλαίων που χρησιμοποιήθηκαν από τις μελέτες ανάλυσης γεγονότων. Οι δείκτες ποίκιλλαν μεταξύ των S&P 500, Nasdaq, CRSP και συνθετικών δεικτών προερχόμενων από την χρήση διάφορων μεμονωμένων.

(δ) Η μέθοδος δειγματοληψίας που υιοθετήθηκε. Αρκετοί μελετητές χρησιμοποίησαν, ως πηγές άντλησης παρατηρήσεων, αποκλειστικά μέσα ενημέρωσης με απήχηση στο ευρύ κοινό. Το γεγονός αυτό μπορεί να περιορίσει την αντικειμενικότητα και διεύρυνση των αποτελεσμάτων μίας μελέτης. Στην ενότητα 5.5 αναλύεται περεταίρω η άποψη αυτή η

οποία οδήγησε την ανάπτυξη της μεθοδολογίας δειγματοληψίας που ακολουθήθηκε από την παρούσα ερευνητική προσπάθεια.

Στον Πίνακα 9 παρουσιάζονται αναλυτικά τα χαρακτηριστικά των κυριότερων μελετών, που ερευνήθηκαν στα πλαίσια της παρούσας διατριβής. Φαίνεται καθαρά η μεγάλη διαφοροποίηση που έχουν οι μελέτες μεταξύ τους στις βασικότερες τους πτυχές το οποίο έχει οδηγήσει στα ανάμικτα συμπεράσματα που έχουν αποδώσει. Στην παρούσα έρευνα έγινε προσπάθεια σύνθεσης των ιδιαίτερων χαρακτηριστικών που εμπειρικά έχουν αποδώσει τα εγκυρότερα αποτελέσματα με παράλληλες προσθήκες η οποίες, κατά την άποψη του εγγράφοντος, οδηγούν στην επίτευξη μίας αποδοτικότερης μεθοδολογίας.

5.4 Ανάλυση της μεθοδολογίας σε χρήση στην παρούσα μελέτη

5.4.1 Περιγραφή της μεθοδολογίας ανάλυσης γεγονότων

Η μεθοδολογία ανάλυσης γεγονότων (event study methodology) είναι ένα πανίσχυρο εργαλείο το οποίο έχει ευρέως εφαρμοστεί από την ερευνητική κοινότητα με στόχο την ποσοτικοποίηση της οικονομικής επίπτωσης απρόβλεπτων περιστατικών σε έναν οργανισμό. Η κύρια επικέντρωση της μεθοδολογίας είναι στην ποσοτικοποίηση των έμμεσων οικονομικών επιπτώσεων, προκαλούμενων από ένα απρόβλεπτο γεγονός, οι οποίες έχουν μεγάλο χρονικό ορίζοντα πραγμάτωσης και είναι μακράν δυσκολότερη η ποσοτικοποίηση τους σε σχέση με τις άμεσες επιπτώσεις. Κατά την διάρκεια των τελευταίων δεκαετιών, η μεθοδολογία ανάλυσης γεγονότων εφαρμόστηκε στο ερευνητικό πεδίο της διοίκησης επιχειρήσεων ως ένα μέσο διερεύνησης διαφόρων περιστάσεων που παρουσιάζονται στο εταιρικό περιβάλλον. Προς αυτή την κατεύθυνση ερευνήθηκαν περιστατικά κρίσης, εντολών επιστροφής ελαττωματικών προϊόντων, αντικατάστασης ηγετικών στελεχών οργανισμών, ατυχήματα, ανακοινώσεις απόφασης παροχής μερίσματος προς μετόχους και λοιπά περιστατικά ανάλογης βαρύτητας.

Βασική απαίτηση της μεθοδολογίας είναι ο διερευνώμενος οργανισμός, τον οποίο αφορά ένα συγκεκριμένο περιστατικό, να είναι εισηγμένος σε κάποια χρηματαγορά. Με αυτόν τον τρόπο δίνεται η δυνατότητα στην αγορά να τροποποιήσει την κεφαλαιακή αξία ενός οργανισμού αποτυπώνοντας την πληροφορία, για το συγκεκριμένο περιστατικό, στις μελλοντικές προσδοκώμενες χρηματοροές του. Μέσω της μεθοδολογίας ανάλυσης γεγονότων, οι προσδοκίες

των συμμετεχόντων στις χρηματαγορές, σχετικά με την μακροχρόνια επίπτωση ενός δημοσιευμένου περιστατικού ασφαλείας, εκτιμώνται. Οι πιθανές αλλαγές της τιμής μετοχής ενός οργανισμού εξετάζονται προκειμένου για την διερεύνηση ασυνήθη αποδόσεων, σε συγκεκριμένη χρονική περίοδο η οποία επικεντρώνεται στην ημέρα ανακοίνωσης του γεγονότος. Η περίοδος αυτή αποκαλείται παράθυρο περιόδου ανάλυσης γεγονότος (event window). Η βασικότερη ίσως παραδοχή της συγκεκριμένης μεθοδολογίας είναι ότι, οι υπολογιζόμενες ασυνήθεις αποδόσεις, δεν είναι αποτέλεσμα ενός τυχαίου γεγονότος αλλά προϊόν του συγκεκριμένου γεγονότος που αναλύεται.

Στην παρούσα έρευνα, τα γεγονότα που ερευνώνται είναι περιστατικά παραβίασης ασφαλείας όπως ορίστηκαν στην ενότητα 4.2. Είναι σημαντικό να ορισθεί ο χρόνος πραγμάτωσης ενός γεγονότος όπου, για τις ανάγκες τις παρούσας μελέτης, ορίζεται ως η ημέρα της πρώτης επίσημης δημόσιας ανακοίνωσης. Αυτό ισχύει ακόμα και στις περιπτώσεις που ένα γεγονός έπληξε έναν οργανισμό μήνες ή και χρόνια πριν από την δημοσίευση του. Πρέπει να αναφερθεί ότι η έννοια επίσημη προσδίδεται από το μέσο δημοσίευσης το οποίο απαιτείται να αφορά ένα μέσο ενημέρωσης με ευρεία αναγνώριση της αξιοπιστίας του. Καταχώρηση ενός πραγματικού γεγονότος σε αμφιβόλου αξιοπιστίας μέσων ενημέρωσης δεν θεωρείται ως πρώτη δημοσίευση από την παρούσα μελέτη καθώς λαμβάνεται η παραδοχή ότι οι αγορές είτε δεν παρακολουθούν μέσα ενημέρωσης αυτού του είδους, είτε δεν αντιδρούν μέχρι την επιβεβαίωση της υπόστασης ενός γεγονότος που θα προέλθει από την δημοσίευσή του σε ένα έγκυρο μέσο. Η λέξη δημόσια για την ανακοίνωση ενός γεγονότος παραπέμπει στον αναγκαίο διαχωρισμό από την πιθανή γνώση εμπιστευτικών πληροφοριών μιας σχετικά μικρής ομάδας ενδιαφερόμενων και από την πιθανή διαρροή της. Η περίπτωση αυτή αφορά την διαρροή εσωτερικής πληροφόρησης η οποία αναλύεται διεξοδικά στην συνέχεια.

Πρέπει να τονισθεί η σημασία της οριοθέτησης του χρόνου της πρώτης δημόσιας επίσημης ανακοίνωσης ενός γεγονότος με ακρίβεια καθώς, κατά την θεωρεία της αποτελεσματικής αγοράς (efficient market theory), η αντίδραση της αγοράς σε νέα πληροφόρηση πρέπει να είναι άμεση. Επιπρόσθετα, ο ακριβής προσδιορισμός της ημέρας πραγμάτωσης ενός γεγονότος είναι σημαντικός για την σύνθεση των παράθυρων περιόδου ανάλυσης γεγονότων που χρησιμοποιήθηκαν στην μελέτη.

5.4.2 Προσδιορισμός παραθύρων περιόδου ανάλυση γεγονότων

Το μέγεθος ενός παράθυρου περιόδου ανάλυσης γεγονότων είναι κρίσιμης σημασίας προκειμένου για την λήψη αμερόληπτων και αντικειμενικών αποτελεσμάτων. Το αυξανόμενο μέγεθος του παράθυρου μεγεθύνει την πιθανότητα ανακάλυψης εξακολουθητικών οικονομικών επιπτώσεων από ένα γεγονός αλλά παράλληλα μεγεθύνει την πιθανότητα εμφάνισης άλλων τυχαίων, σχετικών με τον οργανισμό, γεγονότων τα οποία έχουν την δυναμική μεταβολής της κεφαλαιακής του υπόστασης. Το πρόβλημα είναι ότι η οικονομική επίδραση γεγονότων, που λαμβάνουν χώρα ή έρχονται στην δημοσιότητα σε κοινό χρόνο, δεν μπορεί να εξατομικευθεί. Συνεπώς, η ισχύς της μεθοδολογίας ανάλυσης γεγονότων μειώνεται καθώς το παράθυρο ανάλυσης αυξάνεται.

Σύμφωνα με την θεωρεία, όταν η ημέρα πραγμάτωσης ενός γεγονότος είναι προσδιορισμένη με ακρίβεια, τότε ένα παράθυρο ανάλυσης μεγέθους δύο ημερών είναι κατάλληλο [**83**]. Επιπρόσθετα, η χρήση ενός σχετικά μεγάλου παράθυρου ανάλυσης είναι ανακόλουθη προς την υπόθεση αποτελεσματικών αγορών (efficient market hypothesis). Στην παρούσα μελέτη, γίνεται η παραδοχή ότι οι αγορές χαρακτηρίζονται από αποτελεσματικότητα πληροφόρησης ημι-ισχυρού τύπου (informationally semi-strong efficient). Σύμφωνα με την θεωρεία, μία αγορά θεωρείται ότι είναι αποτελεσματική, σχετικά με την διάχυση πληροφόρησης σε ημι-ισχυρό επίπεδο, όταν το σύνολο της δημόσια διαθέσιμης πληροφόρησης αποτυπώνεται σε άμεσο χρόνο στην τιμή μετοχής μίας εταιρίας. Το σύνολο των πληροφοριών, με διαθεσιμότητα στο ευρύ κοινό, χωρίζεται σε δύο κατηγορίες [**84**]:

(1) Πληροφόρηση που δημιουργείται από τις αγορές όπως οι ιστορικές αποδόσεις των μετοχών, η σχέση ξένα προς ιδία κεφάλαια σε μία εταιρία ή έναν κλάδο και το επίπεδο της αξίας κεφαλαιοποίησης μίας εταιρίας ανά το χρόνο.

(2) Πληροφόρηση που δεν δημιουργείται από τις αγορές και περιλαμβάνει ανακοινώσεις αποφάσεων, δεδομένων και γεγονότων που αφορούν εταιρίες, κλάδους ή το σύνολο της οικονομίας. Ανακοινώσεις αποφάσεων περιλαμβάνουν για παράδειγμα την αντικατάσταση ενός διευθυντικού στελέχους, της εξαγορά ενός οργανισμού και την στρατηγική συμμαχία δύο οργανισμών. Ανακοινώσεις δεδομένων είναι για παράδειγμα τα περιοδικά οικονομικά αποτελέσματα που ανακοινώνει στον τύπο ένας οργανισμός.

Η ανακοίνωση γεγονότων, που περιλαμβάνεται σε αυτήν την κατηγορία, αποτελεί το είδος πληροφοριών που ενδιαφέρει την παρούσα μελέτη. Η επίδραση τους στην τιμή της μετοχής ενός οργανισμού είναι αυτό που αξιολογείται προκειμένου να ποσοτικοποιηθούν εμμέσως μεγέθη τα οποία είναι δύσκολο ή αδύνατο να ποσοτικοποιηθούν άμεσα.

Υποθέτοντας ότι οι αγορές είναι ημι-ισχυρού τύπου, από πλευράς αποτελεσματικότητας πληροφόρησης, η επίδραση ενός γεγονότος στην τιμή μίας μετοχής θα πρέπει να αποτυπώνεται άμεσα ή, διατυπώνοντας το διαφορετικά, την ημέρα ανακοίνωσης του γεγονότος[9]. Αυτό οδηγεί στην επιλογή ενός παραθύρου ανάλυσης το οποίο περιλαμβάνει μόνο την ημέρα ανακοίνωσης του γεγονότος. Ορίζουμε ως t_o την ημέρα ανακοίνωσης ενός γεγονότος και το παράθυρο ανάλυσης, που περιλαμβάνει αποκλειστικά αυτή την ημέρα, ορίζεται ως [0,0].

Προηγούμενες παρόμοιες μελέτες συμπεριέλαβαν την ημέρα πριν την ημέρα γεγονότος προκειμένου να ληφθεί υπόψη και εξεταστεί η περίπτωση διαρροής εσωτερικής πληροφόρησης (insider information leakage) [**73**], [**74**], [**81**], [**77**]. Επιπροσθέτως, πλήθος ερευνών χρησιμοποίησε παράθυρα ανάλυσης τα οποία συμπεριελάμβαναν την επόμενη ημέρα από την ημέρα γεγονότος προκειμένου να ληφθεί υπόψη η πιθανότητα της δημοσίευσης του να πραγματοποιήθηκε μετά το κλείσιμο της χρηματαγοράς στην οποία διαπραγματεύεται η μετοχή του οργανισμού που αφορά ένα συγκεκριμένο γεγονός. Επιπλέον, μελέτες έχουν αναλύσει παράθυρα τα οποία περιελάμβαναν επιπρόσθετες ημέρες πέραν της επόμενης από την ημέρα γεγονότος προκειμένου να ερευνηθεί η περίπτωση επίπτωσης ενός γεγονότος στη χρηματιστηριακή αξία ενός οργανισμού με σχετικά μεγάλη διάρκεια.

Το γενικό συμπέρασμα που προκύπτει, από την ανάλυση παρόμοιων μελετών που διεξήχθησαν κατά την τελευταία δεκαετία, είναι η σταδιακή μείωση των παράθυρων περιόδου ανάλυσης γεγονότων. Με αυτόν τον τρόπο, οι μελετητές υποθέτουν ότι στις αγορές σταδιακά επέρχεται περαιτέρω ωρίμανση με αποτέλεσμα να προσεγγίζουν την αποτελεσματικότητα πληροφόρησης ημι-ισχυρού τύπου. Σύμφωνα με αυτή την λογική, η χρήση μικρότερων παράθυρων ανάλυσης οδηγεί σε αποτελέσματα με μεγαλύτερη θεωρητική υπόσταση.

[9] Στο υπόλοιπο της μελέτης, η ημέρα ανακοίνωσης γεγονότος θα αναφέρεται, χάριν συντομίας ως ημέρα γεγονότος.

Το μεγαλύτερο παράθυρο περιόδου ανάλυσης γεγονότων που χρησιμοποιήθηκε στην παρούσα έρευνα ήταν τριών ημερών και συμπεριελάμβανε την προηγούμενη ημέρα από την ημέρα γεγονότος, την ημέρα γεγονότος και την επόμενη ημέρα από την ημέρα γεγονότος. Στο παράθυρο αυτό θα αναφερόμαστε, χάριν συντομίας, ως [-1,1]. Η χρήση του συγκεκριμένου παραθύρου ανάλυσης έγινε περισσότερο για λόγους σύγκρισης και συνοχής με προηγούμενες μελέτες όπως θα υποστηριχθεί αναλυτικά στην ενότητα 5.7.

Στο υπόλοιπο της μελέτης χρησιμοποιούνται οι ακόλουθοι ορισμοί: Ορίζουμε ως τ_k την ημέρα πραγμάτωσης ενός γεγονότος k. Ακολούθως, ορίζουμε $t_1 = \tau_k - 1$ και $t_2 = \tau_k + 1$ ως τα όρια ενός παραθύρου ανάλυσης τριών ημερών όπως αυτό αναφέρθηκε στην προηγούμενη παράγραφο. Επιπροσθέτως, στην παρούσα μελέτη χρησιμοποιήθηκαν τα ακόλουθα παράθυρα ανάλυσης:

(1) Παράθυρο ανάλυσης το οποίο περιείχε μόνο την ημέρα γεγονότος με τα όρια του να είναι μόνο το $t_1 = t_2 = \tau_k$ και περιγράφεται ως [0,0].

(2) Παράθυρο ανάλυσης το οποίο περιείχε την προηγούμενη από την ημέρα γεγονότος και την ημέρα γεγονότος με τα όρια του να είναι τα $t_1 = \tau_k - 1$ και $t_2 = \tau_k$. Περιγράφεται επίσης ως [-1,0].

(3) Παράθυρο ανάλυσης το οποίο περιείχε την ημέρα γεγονότος και την επόμενη από την ημέρα γεγονότος με τα όρια του να είναι τα $t_1 = \tau_k$ και $t_2 = \tau_k + 1$. Περιγράφεται επίσης ως [0,1].

5.4.3 Ανάλυση των μοντέλων αποτίμησης επενδυτικών κεφαλαίων

Η εξέταση για την ύπαρξη ασυνήθη αποδόσεων σε ένα δεδομένο χρονικό διάστημα πραγματοποιείται μέσω της χρήσης ενός μοντέλου υπολογισμού της προσδοκώμενης απόδοσης μίας μετοχής. Τα μοντέλα αυτά καλούνται γενικά μοντέλα αποτίμησης επενδυτικών κεφαλαίων (asset pricing models) και μπορούν να χωριστούν σε δύο κατηγορίες: (α) Μοντέλα μονού δείκτη (single-index) και (β) μοντέλα πολλαπλών δεικτών (multi-index). Κοινός σκοπός των μοντέλων αυτών είναι η αποτίμηση μίας μετοχής προκειμένου να προσδιορισθεί αν είναι υποεκτιμημένη, είναι στην κανονική της τιμή ή είναι υπερεκτιμημένη. Συγκρίνοντας την προσδοκώμενη απόδοση μίας μετοχής, με βάση τους υπολογισμούς των παραπάνω μοντέλων, με την πραγματική ιστορική

απόδοση, μπορεί να διακριθεί η ύπαρξη ασυνήθεις αποδόσεων. Οι αποδόσεις αυτές λαμβάνονται ως ένδειξη του κόστους ή της ωφέλειας ενός γεγονότος το οποίο γνωστοποιήθηκε στην αγορά.

Στην περίπτωση που το γεγονός είναι η παραβίαση ασφαλείας ενός οργανισμού, υποθέτουμε ότι η αγορά θα διορθώσει την τιμή της μετοχής του, σε αντίδραση προς την γνωστοποίηση του γεγονότος, προκειμένου να αποτυπώσει δύο κατηγορίες απώλειας μελλοντικών χρηματοροών. Η πρώτη αφορά την πεποίθηση ότι ο οργανισμός θα δεχθεί παρόμοιες επιθέσεις στο μέλλον οι οποίες θα πλήξουν τις μελλοντικές χρηματοροές του. Πρέπει εδώ να αναφερθεί, πως θεωρώντας ότι ένας οργανισμός που ανήκει στον τομέα τεχνολογίας έχει μεγαλύτερη πιθανότητα να δεχθεί και άλλες πετυχημένες επιθέσεις στον κυβερνοχώρο μετά από μία ήδη πετυχημένη, έγινε η σύνθεση αντίστοιχης στατιστικής υπόθεσης στην ενότητα 5.6.2. Η δεύτερη κατηγορία απώλειας μελλοντικών χρηματοροών αφορά την αναμονή μελλοντικών άυλων οικονομικών επιπτώσεων ως συνέπεια ενός περιστατικού ασφαλείας. Οι επιπτώσεις αυτές απαρτίζουν το έμμεσο κόστος που επιφέρει ένα γεγονός παραβίασης ασφαλείας, και η πραγμάτευση τους αναμένεται σε μεσοπρόθεσμο ή ακόμα και μακροπρόθεσμο ορίζοντα. Παραδείγματα κόστους αυτής της κατηγορίας είναι νομικά έξοδα και το κόστος εφαρμογής κανονιστικών πλαισίων.

Βασική παράμετρος, στην χρήση μοντέλων αποτίμησης επενδυτικών κεφαλαίων, είναι η επιλογή της περιόδου εκτίμησης. Ως περίοδο εκτίμησης (estimation period) ορίζουμε το χρονικό πλαίσιο στα όρια του οποίου λαμβάνονται τα δεδομένα που χρησιμοποιούνται για την ανάλυση παλινδρόμησης μεταξύ των δεδομένων αποδόσεων μίας μετοχής και των αποδόσεων των δεικτών που συμπεριλαμβάνονται στο μοντέλο, όπως είναι ο δείκτης που αντιπροσωπεύει το αγοραίο χαρτοφυλάκιο. Στα πλαίσια της παρούσας μελέτης, το μέγεθος της περιόδου εκτίμησης ορίζεται ως T και μετράται σε ημέρες. Το αριστερό όριο της περιόδου εκτίμησης τέθηκε σε t=-201 ημέρες ενώ το αντίστοιχο δεξιό όριο σε t=-2 ημέρες καταλήγοντας σε ένα μέγεθος 200 ημερών. Το δεξιό όριο τέθηκε ως δύο ημέρες πριν την ημέρα γεγονότος ώστε να αποφθεχθεί η αλληλοεπικάλυψη μεταξύ περιόδου εκτίμησης και τουλάχιστον ενός εκ των παραθύρων ανάλυσης. Η επιλογή αυτή, για το δεξιό όριο της περιόδου, είναι σε συμφωνία με άλλες μελέτες ανάλυσης γεγονότων όπως οι [**70**], [**85**], [**74**].

Καθώς ένα μέρος των ημερών που περιλαμβάνονται στα χρονικά πλαίσια της περιόδου εκτίμησης αφορά αργίες, κατά τις οποίες οι χρηματαγορές είναι κλειστές, το τελικό μέγεθος παρατηρήσεων για την ανάλυση παλινδρόμησης είναι αρκετά μικρότερο. Οι περίοδοι εκτίμησης

των γεγονότων στο συνολικό δείγμα είχαν, κατά μέσο όρο, 137 παρατηρήσεις κλεισίματος τιμής μετοχής, οι οποίες απέδωσαν 136 τιμές απόδοσης. Γενικά είναι αποδεκτό η περίοδος εκτίμησης, όπου στην περίπτωση αναλύσεων γεγονότων είναι σε ημερήσια βάση, όταν γίνεται αξιολόγηση αποδόσεων που προσεγγίζουν την κανονική κατανομή, να κυμαίνεται μεταξύ 100 και 300 ημέρες [**86**]. Στην ανάλυση αυτή περιορίστηκε το μέγεθος της περιόδου εκτίμησης κοντά στο αποδεκτό αριστερό όριο προκειμένου για την αποφυγή εξαίρεσης γεγονότων λόγω της μη διαπραγμάτευσης της μετοχής για όλο το διάστημα[10].

5.4.3.1 Μοντέλο Αποτίμησης Κεφαλαιουχικών Αγαθών (Capital Asset Pricing Model)

Το μοντέλο που έχει χρησιμοποιηθεί σχεδόν από το σύνολο των μελετών που έχουν εφαρμόσει την μεθοδολογία ανάλυσης γεγονότων είναι το Μοντέλο Αποτίμησης Κεφαλαιουχικών Αγαθών (Capital Asset Pricing Model). Το μοντέλο αυτό, το οποίο χάριν συντομίας θα αναφέρεται στην παρούσα μελέτη ως CAPM, προσδιορίζει την αναμενόμενη ή απαιτούμενη απόδοση μίας μετοχής με βάση την συσχέτιση που έχει η μετοχή με την αγορά καθώς και την πρόσθετη απόδοση που απαιτείται από τους επενδυτές για ένα χαρτοφυλάκιο που περιλαμβάνει όλες τις αξίες σε σχέση με μία επένδυση μηδενικού κινδύνου [**87**]. Η μορφή του CAPM, που χρησιμοποιείται στην παρούσα μελέτη, είναι ως ακολούθως:

$$R_{it} - R_f = a_i + \beta_i(R_{mt} - R_f) + \varepsilon_{it} \qquad (1)$$

Αναλυτικότερα, το CAPM είναι ένα μοντέλο μονού δείκτη με το οποίο προσδιορίζεται η αναμενόμενη απόδοση μίας μετοχής i στην διάρκεια μίας περιόδου t ως γραμμική συνάρτηση της απόδοσης που επιφέρει η αγορά R_{mt} και της συσχέτισης της μετοχής με την αγορά εκφρασμένη ως β_i το οποίο αποκαλείται συντελεστής βήτα. Η μεταβλητή R_f αντιπροσωπεύει την απόδοση μηδενικού κινδύνου και συνήθως αντιπροσωπεύεται με την χρήση των αποδόσεων κρατικών ομολόγων. Στη μελέτη αυτή, ακλουθώντας πλήθος μελετών που έχουν χρησιμοποιήσει το CAPM στο παρελθόν, η συγκεκριμένη μεταβλητή υπολογίστηκε χρησιμοποιώντας τις μηνιαίες αποδόσεις των γραμματίων του Δημοσίου των ΗΠΑ (treasury bills). Τα γραμμάτια αυτά είναι βραχυπρόθεσμα κρατικά χρεόγραφα που διατίθενται στην αγορά για την κάλυψη αναγκών

[10] Πρέπει να σημειωθεί πως σχεδόν το σύνολο των μελετών ανάλυσης γεγονότων, που μελετήθηκαν στα πλαίσια της παρούσας, είχε ανώτερο μέγεθος περιόδου εκτίμησης τις 200 ημέρες.

ρευστότητας του Δημοσίου των ΗΠΑ. Η μηνιαίες αποδόσεις, που έχουν δημοσιευθεί, μετατράπηκαν σε ημερήσιες αποδόσεις για το σύνολο της περιόδου εκτίμησης του μοντέλου.

Το μοντέλο είναι εκφρασμένο σε όρους πλεονασματικών αποδόσεων (excess returns) των αποδόσεων από μία μετοχή σε σχέση με τις αποδόσεις μηδενικού κινδύνου προκειμένου η υπολογιζόμενη αναμενόμενη απόδοση να σταθμιστεί σε σχετικούς όρους. Ο συντελεστής βήτα είναι επικεντρωμένος στην εταιρία που αντιπροσωπεύει (firm-dependent) και μέσω αυτού εκτιμάται ο συστηματικός κίνδυνος (systematic risk) μίας μετοχής. Υπολογίζεται μέσω του λόγου της συνδιακύμανσης των αποδόσεων μίας μετοχής με τις αποδόσεις των αγοραίου χαρτοφυλακίου προς την διακύμανση των αποδόσεων του αγοραίου χαρτοφυλακίου. Αποκαλείται επίσης και ως Ordinary Least Squares (OLS) βήτα καθώς η μέθοδος που χρησιμοποιείται για τον υπολογισμό του είναι η περιγραφική γραμμική παλινδρόμηση με την κλασσική μέθοδο ελαχίστων τετραγώνων. Ο δεύτερος συντελεστής, επικεντρωμένος στην εταιρία, είναι ο a_i και υπολογίζεται με την ίδια μέθοδο ενώ αναμένεται κατά μέσο όρο να προσεγγίζει την μονάδα. Ο παράγοντας ε_{it} αντιπροσωπεύει τα υπόλοιπα ή κατάλοιπα, που προέρχονται από την ανάλυση παλινδρόμησης, για την μετοχή i την ημέρα t με τις OLS ιδιότητες.

Τα υπόλοιπα αντιπροσωπεύουν την επίδραση που έχουν ανακοινώσεις αποφάσεων δεδομένων και γεγονότα, τα οποία αφορούν αποκλειστικά έναν συγκεκριμένο οργανισμό, στην συνολική του αναμενόμενη απόδοση. Μπορούμε να τα θεωρήσουμε ως το σύνολο του μη συστηματικού κινδύνου (non-systematic risk) μίας μετοχής το οποίο έχει απομείνει στο συνολικό της επίπεδο κινδύνου όταν αυτή η μετοχή είναι μέρος ενός χαρτοφυλακίου υπό πλήρη διασπορά (diversification). Στην ορολογία της μεθοδολογίας ανάλυσης γεγονότων, τα υπόλοιπα είναι οι ασυνήθεις αποδόσεις που προέρχονται από απρόβλεπτα γεγονότα, τα οποία υπό την μορφή των παραβιάσεων ασφαλείας, αποτελούν το αντικείμενο ανάλυσης της παρούσας έρευνας.

Μία σημαντική απόφαση στην εφαρμογή του CAPM είναι η επιλογή του δείκτη που θα χρησιμοποιηθεί ως μεταβλητή αντιπροσώπευσης (proxy) του αγοραίου χαρτοφυλακίου. Μεγάλο πλήθος μελετών ανάλυσης γεγονότων έχουν χρησιμοποιήσει είτε τον Standards & Poor's 500 Composite Index (S&P 500) ή έναν συνθετικό δείκτη ισόποσης στάθμισης που περιλαμβάνει τους δείκτες NYSE, AMEX και Nasdaq. Στην παρούσα μελέτη χρησιμοποιήθηκε ο δείκτης Russell 3000 ο οποίος είναι ένας δείκτης με στάθμιση κεφαλαιακής αξίας (value-weighted) και περιλαμβάνει τις 3000 μεγαλύτερες μετοχές των χρηματαγορών των ΗΠΑ. Από τα πορίσματα της

παρούσας έρευνας προέκυψε πως η χρήση αυτού του δείκτη γίνεται για πρώτη φορά σε μελέτη αυτού του είδους και στόχος είναι η αντιπροσώπευση του αγοραίου χαρτοφυλακίου με έναν, από θεωρητικής και πρακτικής πλευράς, περισσότερο ολοκληρωμένο δείκτη.

Ο Russell 3000 περιλαμβάνει το 98% περίπου του συνόλου της κεφαλαιοποίησης των χρηματαγορών των ΗΠΑ. Επιπλέον, οι μετοχές που τον συνθέτουν προέρχονται από όλα τα επίπεδα κεφαλαιοποίησης ήτοι υψηλής-, μεσαίας- και μικρής-κεφαλαιοποίησης[11]. Συνεπώς, μπορεί να θεωρηθεί ότι καλύπτει σε μεγάλο βαθμό τις απαιτήσεις εύρους αξιών και διασποράς του θεωρητικού αγοραίου χαρτοφυλακίου.

Αφού υπολογίστηκαν οι αποδόσεις, για κάθε εταιρία στην περίοδο εκτιμήσεων που αφορά κάθε γεγονός του δείγματος, καθώς και των αποδόσεων του δείκτη αντιπροσώπευσης του αγοραίου χαρτοφυλακίου, εφαρμόστηκε η κλασσική ανάλυση παλινδρόμησης ελαχίστων τετραγώνων μίας ανεξάρτητης μεταβλητής στο μοντέλο της εξίσωσης 1. Έγινε προσέγγιση των εκτιμητών για τους πραγματικούς συντελεστές a_i και β_i οι οποίοι υποδηλώνονται ως a_s και β_s. Τοποθετώντας τους εκτιμητές στην εξίσωση 1 καταλήγουμε στην χαρακτηριστική γραμμή για την κάθε μετοχή που περιλαμβάνεται στο δείγμα (security characteristic line). Οι ασυνήθεις αποδόσεις υπολογίζονται με τον ακόλουθο τύπο:

$$AR_{it} = (R_{it} - R_f) - [a_s + \beta_s(R_{mt} - R_f)] \qquad (2)$$

Με AR_{it} υποδηλώνονται οι ασυνήθεις αποδόσεις για την εταιρία i την ημέρα t. R_{it} ορίζεται ως η πραγματική απόδοση που επετεύχθη από την μετοχή i την ημέρα t. Επομένως, η ασυνήθης απόδοση, μίας συγκεκριμένης μετοχής σε μία δεδομένη χρονική περίοδο, είναι η διαφορά μεταξύ της πραγματικής και αναμενόμενης απόδοσης με την παραδοχή ότι προέρχεται από την ανακοίνωση ενός συγκεκριμένου γεγονότος και όχι από ένα τυχαίο γεγονός το οποίο συνέβη ταυτόχρονα.

[11] Ο δείκτης Russell 3000 περιλαμβάνει τις μετοχές που συνθέτουν τον δείκτη Russell 1000 ο οποίος μετράει τις επιδόσεις της μεγάλης και μεσαίας κεφαλαιοποίησης και τις μετοχές που συνθέτουν τον δείκτη Russell 2000 ο οποίος μετράει τις επιδόσεις την μικρής κεφαλαιοποίησης της αγοράς.

5.4.3.2 Μοντέλο τριών-μεταβλητών Fama-French

Σε συνδυασμό με την χρήση του CAPM, για τον υπολογισμό των ασυνήθη αποδόσεων, χρησιμοποιήθηκε το μοντέλο τριών-μεταβλητών των Fama-French. Το συγκεκριμένο πολυμεταβλητό μοντέλο είναι βασισμένο στο CAPM και αποτελεί επέκταση του επιχειρώντας την πληρέστερη επεξήγηση των αναμενόμενων αποδόσεων μίας μετοχής. Πέρα της ανεξάρτητης μεταβλητής που αντιπροσωπεύει την αγορά, χρησιμοποιούνται επιπλέον μεταβλητές οι οποίες αντιπροσωπεύουν θεμελιώδη χαρακτηριστικά ενός οργανισμού προκειμένου για την πληρέστερη επεξήγηση του συστηματικού κινδύνου. Οι θεμελιώδεις οικονομικές μεταβλητές που χρησιμοποιούνται από το μοντέλο είναι ο λόγος μεταξύ λογιστικής-αγοραίας-αξίας της μετοχής (book-to-market ratio) και η αξία της συνολικής κεφαλαιοποίησης της. Έχει αποδειχθεί εμπειρικά ότι ο λόγος λογιστικής-αγοραίας-αξίας μπορεί να αποτελέσει ένα αξιόπιστο κριτήριο για την κατηγοριοποίηση των μετοχών μεταξύ μετοχών χαμηλής τιμής (value stocks) και μετοχών υπεραξίας (growth stocks). Επιπλέον, η χρήση αυτής της μεταβλητής έχει αποδειχθεί ότι υποδεικνύει την επίδραση άλλων θεμελιωδών μεγεθών όπως είναι η μόχλευση (leverage) και ο δείκτης λογιστικών κερδών προς την τρέχουσα χρηματιστηριακή τιμή μετοχής (earnings-to-price ratio). Η δεύτερη πρόσθετη παράμετρος του μοντέλου, η αξία της συνολικής κεφαλαιοποίησης, αντιπροσωπεύει το μέγεθος ενός οργανισμού [**88**], [**89**], [**90**]. Το μοντέλο τριών-μεταβλητών είναι ως ακολούθως:

$$R_{it}\text{-}R_f = a_i + \beta_i(R_{mt}\text{-}R_f) + s_i SMB_t + h_i HML_t + \varepsilon_{it} \qquad (3)$$

Το μοντέλο προσδιορίζει την αναμενόμενη απόδοση μίας μετοχής i, κατά την διάρκεια μίας περιόδου t, ως μία γραμμική συνάρτηση με τις ακόλουθες ανεξάρτητες μεταβλητές: (α) Τη συσχέτιση των αποδόσεων της μετοχής με τις αγοραίες αποδόσεις R_{mt} όπως υπολογίζεται από τον συντελεστή βήτα και υποδηλώνεται ως β_i, (β) το περιθώριο μεταξύ των μέσων αποδόσεων των μετοχών της μικρής κεφαλαιοποίησης σε σχέση με τις μέσες αποδόσεις των μετοχών της μεγάλης κεφαλαιοποίησης το οποίο υποδηλώνεται ως SMB (Small Minus Big) και (γ) το περιθώριο μεταξύ των μέσων αποδόσεων των μετοχών χαρακτηρισμένων ως χαμηλής τιμής και των μετοχών χαρακτηρισμένων ως υπεραξίας το οποίο υποδηλώνεται ως HML (High Minus Low). Οι μετοχές που έχουν σχετικά υψηλό λόγο λογιστικής-αγοραίας-αξίας ταξινομούνται ως χαμηλής τιμής ενώ οι μετοχές, με χαμηλή τιμή σε αυτό τον λόγο, ταξινομούνται ως μετοχές υπεραξίας. Η μεταβλητή

HML αποκαλείται επίσης και ως πρόσθετη απόδοση αξίας (value premium). Ο δείκτης που χρησιμοποιείται για την αντιπροσώπευση του αγοραίου χαρτοφυλακίου είναι ο ίδιος που χρησιμοποιήθηκε και στο CAPM. Οι δύο πρόσθετες ανεξάρτητες μεταβλητές, που εισάγει το συγκεκριμένο μοντέλο, SMB και HML, αντιπροσωπεύουν άγνωστα θεμελιώδη μεγέθη και βασίζονται σε εμπειρικά αποτελέσματα μελετών. Όπως αποτυπώνεται στην εξίσωση 3, στην παρούσα μελέτη, χρησιμοποιείται και αυτό το μοντέλο στην μορφή των πλεονασματικών αποδόσεων.

Τα δεδομένα που χρησιμοποιήθηκαν στην παρούσα μελέτη σχετικά με τις ανεξάρτητες μεταβλητές SMB και HML λήφθηκαν από τον διαδικτυακό τόπο του καθηγητή Kenneth R. French [**91**]. Τα αποτελέσματα των δημοσιευμένων ερευνών των Fama-French σχετικά με τις εμπειρικές μελέτες χαρτοφυλακίων, που μεταξύ άλλων έχουν χρησιμοποιηθεί για τον υπολογισμό των παραμέτρων του μοντέλου τριών-μεταβλητών, δημοσιεύονται σε αυτόν τον διαδικτυακό τόπο.

Τα ασυνήθη αποτελέσματα, στην περίπτωση του μοντέλου τριών-μεταβλητών, υπολογίζονται μέσω του ακόλουθου τύπου:

$$AR_{it} = (R_{it} - R_f) - [a_s + \beta_s(R_{mt} - R_f) + s_i SMB_t + h_i HML_t] \qquad (4)$$

Μέσω της ανάλυσης παλινδρόμησης πολλών μεταβλητών γίνεται προσέγγιση των συντελεστών, οι οποίοι υποδηλώνονται ως a_s, β_s, s_i, h_i σύμφωνα με την εξίσωση 4. Σύμφωνα με την έρευνα που διεξήχθη, η μελέτη από τους Gatzlaff et. al. [**81**] είναι η πρώτη ανάλυση γεγονότων παραβίασης ασφαλείας που χρησιμοποίησε το μοντέλο τριών-μεταβλητών των Fama-French, σε συνδυασμό με το CAPM, για τον υπολογισμό των ασυνήθη αποδόσεων. Οι συγκεκριμένοι ερευνητές δεν βρήκαν σημαντικές διαφοροποιήσεις στα αποτελέσματα που προέκυψαν από την χρήση των δύο μοντέλων. Μία πρόσφατη μελέτη από τους Gordon et. al. [**82**] έκανε χρήση του μοντέλου τριών-μεταβλητών και εξήγαγε διαφορετικά αποτελέσματα με στατιστική σημαντικότητα σε σχέση με το CAPM. Στην μελέτη αυτή, έγινε εφαρμογή και των δύο μοντέλων σε ένα πιο επίκαιρο δείγμα, σε σχέση με τις προαναφερόμενες μελέτες, προκειμένου για την αποσαφήνιση των ανάμικτων αποτελεσμάτων που έχουν προκύψει. Στην παρούσα μελέτη επιχειρείται η περαιτέρω αποσαφήνιση της σχετικής χρησιμότητας των δύο μοντέλων στην μεθοδολογία ανάλυσης γεγονότων χρησιμοποιώντας ένα πιο πρόσφατο δείγμα από το σύνολο των προηγούμενων μελετών.

5.4.4 Μεθοδολογία στατιστικής ανάλυσης δεδομένων

Προκειμένου για την επαλήθευση των παραδοχών που θέτονται από την ανάλυση γραμμικής παλινδρόμησης, έγινε ανάλυση καταλοίπων (residual analysis) στα αποτελέσματα κάθε γεγονότος που συμπεριελήφθη στο τελικό δείγμα. Η ανάλυση που έγινε ήταν κοινή και για τα δύο μοντέλα που αναφέρθηκαν στην παραπάνω ενότητα.

Αναλυτικότερα, η παραδοχή της ομοσκεδαστικότητας αξιολογήθηκε με την χρήση γραφήματος καταλοίπων (residual plots). Κανένα από τα γεγονότα που αναλύθηκαν δεν παρουσίασε εμφανή απόκλιση από την παραδοχή της ομοσκεδαστικότητας. Η κανονικότητα της κατανομής που ακολουθούν τα κατάλοιπά αξιολογήθηκε χρησιμοποιώντας γραφήματα κανονικών πιθανοτήτων (normal probability plots) στα οποία η γραμμικότητα, μεταξύ των συνόλων από δεδομένα τα οποία απαρτίζονταν από τα κατάλοιπα και τις τιμές των τυποποιημένων κανονικών μορίων (standardized normal quantiles), αξιολογήθηκε. Τα αποτελέσματα κατέδειξαν μικρού μεγέθους αποκλίσεις από την κανονικότητα όπου, λαμβάνοντας υπόψη το μέγεθος του δείγματος που αναλύθηκε καθώς και την σθεναρότητα σε σφάλματα της ανάλυσης παλινδρόμησης, θεωρήθηκαν ότι δεν αλλοιώνουν τα αποτελέσματα που προέκυψαν. Τελικώς, δημιουργήθηκαν γραφήματα καταλοίπων στο χρόνο και χρησιμοποιήθηκε το κριτήριο των Durbin-Watson προκειμένου για το έλεγχο ύπαρξης αυτοσυσχέτισης πρώτου βαθμού. Τα αποτελέσματα έδειξαν πως τα κατάλοιπα δεν είχαν συσχέτιση σε κανένα από τα γεγονότα που αναλύθηκαν.

Στην μεθοδολογία ανάλυσης γεγονότων, όπως έχει πλέον διαμορφωθεί, είναι κοινή πρακτική να τυποποιείται η διακύμανση των καταλοίπων ώστε να διασφαλίζεται η παραδοχή της ομοσκεδαστικότητας, που προϋποθέτει κοινή διακύμανση για το σύνολο των ασυνήθη αποδόσεων που περιλαμβάνονται σε ένα παράθυρο ανάλυσης. Η τυποποίηση πραγματοποιείται χρησιμοποιώντας το επονομαζόμενο σφάλμα πρόβλεψης (prediction error) το οποίο υποδηλώνεται ως $\mathrm{var}(\mathrm{AR}_{it})$ και ορίζεται από τον ακόλουθο τύπο [**92**]:

$$\mathrm{var}(\mathrm{AR}_{it}) = s_i^2 \left[1 + \frac{1}{T} + \frac{(R_{mt} - \bar{R}_m)^2}{\sum_{\tau=1}^{T} (R_{m\tau} - \bar{R}_m)^2}\right] \qquad (5)$$

Η μεταβλητή s_i^2 είναι η διακύμανση των καταλοίπων στην περίοδο εκτίμησης ενώ ο δεύτερος όρος μέσα στις αγκύλες είναι ο τελεστής τυποποίησης της διακύμανσης. Ως $\bar{R}_m$ ορίζεται η μέση απόδοση του δείκτη αγοραίου χαρτοφυλακίου, κατά την περίοδο εκτίμησης και $R_{m\tau}$ είναι η

απόδοση του ίδιου δείκτη σε κάθε μέρα που περιλαμβάνεται στο διάστημα εκτίμησης. Εφαρμόζοντας τον συγκεκριμένο τύπο, η διακύμανση των καταλοίπων, σε κάθε μέρα που περιλαμβάνεται στο παράθυρο περιόδου ανάλυσης γεγονότων, προσαρμόζεται με βάση δύο παραμέτρους: (α) Τον μέγεθος της διαφοράς μεταξύ της αγοραίας απόδοσης, στην συγκεκριμένη μέρα, και της μέσης αγοραίας απόδοσης στο σύνολο του διαστήματος εκτίμησης. (β) Το μέγεθος Τ του διαστήματος εκτίμησης. Συνεπώς, όταν η απόκλιση των ημερήσιων αγοραίων αποδόσεων σε σχέση με την μέση απόδοση είναι μικρότερη και η περίοδος εκτίμησης είναι μεγαλύτερη, τότε η τυποποιημένη διακύμανση καταλοίπων αναμένεται να είναι χαμηλότερη και το αντίστροφο.

Η εξαρτημένη μεταβλητή, σωρευτική ασυνήθης απόδοση (Cumulative Abnormal Return – CAR) υπολογίζεται ως το άθροισμα των ασυνήθη αποδόσεων για κάθε γεγονός k μέσα στο δείγμα, το οποίο αφορά μία εταιρία i, για κάθε ημέρα που περιλαμβάνεται στο παράθυρο περιόδου ανάλυσης γεγονότων μεγέθους $[t_1, t_2]$:

$$\mathrm{CAR_k} = \sum_{t_1}^{t_2} \mathrm{AR_{it}} \qquad (6)$$

Στην παρούσα μελέτη οι σωρευτικές ασυνήθεις αποδόσεις ορίζονται με επικέντρωση στο γεγονός (event-oriented) προκειμένου να λαμβάνεται υπόψη με μεγαλύτερη ακρίβεια η ύπαρξη περισσότερων του ενός γεγονότος μέσα στο δείγμα για κάθε οργανισμό. Ο ορισμός αυτός έρχεται σε αντίθεση με τον αντίστοιχο ορισμό προηγούμενων ανάλογων μελετών ο οποίος μπορεί να χαρακτηρισθεί ως επικεντρωμένος στην εταιρία (firm-oriented). Το μέσο CAR για το σύνολο των N γεγονότων, που περιλαμβάνονται στο δείγμα, υπολογίζεται ως ακολούθως:

$$\overline{\mathrm{CAR}} = \frac{1}{\mathrm{N}} \sum_{\mathrm{k}=1}^{\mathrm{N}} \mathrm{CAR}_k \qquad (7)$$

Η διακύμανση των $\mathrm{CAR_k}$ ορίζεται από τον ακόλουθο τύπο θέτοντας την παραδοχή ότι οι ημερήσιες ασυνήθεις αποδόσεις είναι ανεξάρτητες μεταξύ τους για κάθε παράθυρο περιόδου ανάλυσης γεγονότων:

$$\mathrm{var}(\mathrm{CAR}_k) = \sum_{t_1}^{t_2} \mathrm{var}(\mathrm{AR_{it}}) \qquad (8)$$

Κάνοντας χρήση του παραπάνω τύπου μπορεί να υπολογιστεί η μέση διακύμανση των CAR_k, για το σύνολο του δείγματος, ως ακολούθως:

$$\mathrm{var}(\overline{\mathrm{CAR}}) = \frac{1}{N^2}\sum_{k=1}^{N}\mathrm{var}(\mathrm{CAR_k}) \qquad (9)$$

Προκειμένου για τον έλεγχο των στατιστικών υποθέσεων της παρούσας μελέτης, χρησιμοποιήθηκε η στατιστική Student t ακολουθώντας την μεθοδολογία που δημιουργήθηκε από τον Patell [92]. Η στατιστική t ακολουθεί την κατανομή Student με T-1 βαθμούς ελευθερίας. Οι βαθμοί ελευθερίας προσδιορίζονται από τον αριθμό των παρατηρήσεων αποδόσεων που περιλαμβάνονται στην περίοδο εκτίμησης μετά την αφαίρεση ενός. Πλήθος σημαντικών μελετών ανάλυσης γεγονότων βάσισαν την στατιστική ανάλυση τους στην συγκεκριμένη μεθοδολογία όπως οι [93], [79], [81]. Η μορφή της στατιστικής t είναι ως εξής:

$$t = \frac{\overline{\mathrm{CAR}}}{\sqrt{\mathrm{var}(\overline{\mathrm{CAR}})}} \sim t_{(a,df=T-1)} \qquad (10)$$

5.5 Μεθοδολογία επιλογής δείγματος

Βασικό κριτήριο στην διαμόρφωση της μεθοδολογίας επιλογής δείγματος ήταν το χρονικό διάστημα από το οποίο λήφθηκαν οι υποψήφιες παρατηρήσεις προς επιλογή στο τελικό σύνολο δεδομένων προς ανάλυση. Στην παρούσα μελέτη χρησιμοποιήθηκαν δύο σημαντικές παράμετροι για την συγκεκριμένη επιλογή. Η πρώτη αφορά την δραστική αλλαγή, ιδίως στα τελευταία χρόνια, στην φύση και στον βαθμό επίπτωσης των περιστατικών παραβίασης ασφαλείας στους οργανισμούς που προσβάλλονται. Η δεύτερη αφορά τον βαθμό ωρίμανσης της αγοράς σε σχέση με την αντιμετώπιση δημόσιων ανακοινώσεων περιστατικών ασφαλείας.

Σχετικά με την πρώτη παράμετρο, όπως αναφέρθηκε εκτενώς στην ενότητα 4.3.3, τα τελευταία τρία χρόνια οι επιθέσεις στον κυβερνοχώρο έχουν μεταβληθεί σημαντικά σε σχέση με την μορφή τους και τα κίνητρα που τις οδηγούν. Ο πόλεμος και η κατασκοπία στον κυβερνοχώρο έχουν αυξηθεί σε μεγάλο βαθμό τα τελευταία χρόνια [**94**] και η πλειοψηφία των επιθέσεων πλέον εφαρμόζει εξαιρετικά εξελιγμένες μεθόδους.

Σχετικά με την δεύτερη παράμετρο, υιοθετήθηκε από την παρούσα μελέτη η παραδοχή ότι το επίπεδο ωρίμανσης της αγοράς, σχετικά με θέματα ασφαλείας ΠΣ, είναι προοδευτικά αναλογικό με την διαχρονική αύξηση της εξάρτησης των επιχειρήσεων σε τεχνολογίες πληροφορικής, εξάρτηση που οδηγείται από τα κίνητρα διατήρησης ανταγωνιστικών πλεονεκτημάτων, την θέση

τους στην αγορά και τα επίπεδα κερδοφορίας. Η εταιρία McAffe και άλλοι οργανισμοί που δραστηριοποιούνται στον κλάδο της ασφάλειας πληροφορικής, τα τελευταία τρία χρόνια, έχουν δημοσιεύσει έναν σημαντικό αριθμό εμπεριστατωμένων μελετών οι οποίες επικεντρώνονται στον εξαιρετικά μεγάλο όγκο στοχευόμενων κυβερνητικών επιθέσεων που έχουν λάβει χώρα παγκοσμίως. Πρωταρχικός στόχος αυτών των μελετών εμφανίζεται να είναι η αφύπνιση των αγορών και η αύξηση στο ευρύ κοινό της επίγνωσης ενός φαινομένου το οποίο θέτει σε εξαιρετική έκθεση κινδύνου τα θεμέλια της εθνικής ασφάλειας και οικονομίας. Επομένως, σύμφωνα με τα προαναφερθέντα, μπορούμε να συνάγουμε την διαπίστωση ότι το επίπεδο πληροφόρησης και ωρίμανσης των αγορών είναι σημαντικά υψηλότερο σε σχέση με πέντε ή περισσότερα χρόνια πριν.

Λαμβάνοντας υπόψη τους προαναφερόμενους παράγοντες και παρόμοιες μελέτες που πραγματοποιήθηκαν κατά την διάρκεια της τελευταίας δεκαετίας, τα χρονικά όρια ανάλυσης της παρούσας μελέτης επιλέχθηκαν μεταξύ 1^{η} Ιανουαρίου 2008 και 31 Ιανουαρίου 2012. Όπως διαπιστώθηκε από την έρευνα που διεξάχθηκε, στο συγκεκριμένο χρονικό διάστημα εμφανίστηκαν στην δημοσιότητα ένας μεγάλος αριθμός σημαντικών περιπτώσεων παραβίασης ασφαλείας.

Τα γεγονότα παραβίασης ασφαλείας, όπως ορίστηκαν στην ενότητα 4.2, έπρεπε να εκπληρώνουν τα παρακάτω κριτήρια προκειμένου να συμπεριληφθούν στο τελικό δείγμα:

1. Οι εταιρίες που ανακοινώνουν ένα περιστατικό ασφαλείας πρέπει να είναι εισηγμένες στην κεφαλαιαγορά των ΗΠΑ. Εμπειρικές μελέτες έχουν αποδείξει ότι οι παράμετροι που χρησιμοποιούνται από τα μοντέλα αποτίμησης επενδυτικών κεφαλαίων (CAPM, Fama-French three-factor model) περιορίζονται σε επίπεδο κράτους [**95**]. Για αυτό τον λόγο ακολουθείται στην παρούσα μελέτη η μεθοδολογία προηγούμενων μελετών οι οποίες χρησιμοποιούν δεδομένα σε επίπεδο κράτους αντί δεδομένων σε παγκόσμιο επίπεδο. Επίσης η πλειονότητα προηγούμενων μελετών, βασισμένων στην ανάλυση γεγονότων, έχει επικεντρωθεί στην ανάλυση της συμπεριφοράς των κεφαλαιαγορών των ΗΠΑ καθώς θεωρείται ως η αγορά με την μεγαλύτερη επάρκεια πληροφόρησης (information efficiency). Όπως αναφέρθηκε στην ενότητα 5.4.1, βασική προϋπόθεση για την θεωρητική υπόσταση των αποτελεσμάτων της ανάλυσης γεγονότων είναι η ρεαλιστικότητα της υπόθεσης για την επάρκεια πληροφόρησης των αγορών.

2. Η μετοχή μίας εισηγμένης εταιρίας, που δέχθηκε επίθεση ασφαλείας, πρέπει να είναι εισηγμένη και να έχει διαπραγμάτευση σε όλη την περίοδο εκτίμησης όπως αυτή καθορίστηκε στην ενότητα 5.4.3.

3. Γεγονότα τα οποία συμπίπτουν χρονικά με λοιπές σημαντικές δημόσιες ανακοινώσεις του ίδιου οργανισμού, μέσα στο χρονικό πλαίσιο που θέτεται από το παράθυρο περιόδου ανάλυσης γεγονότων (event window period), εξαιρούνται. Σημαντικό προαπαιτούμενο που θέτεται από την μεθοδολογία ανάλυσης γεγονότων είναι ένα γεγονός, του οποίου η επίδραση αναλύεται, να μην συμπίπτει χρονικά με άλλα γεγονότα τα οποία έχουν την δυναμική να επηρεάσουν την αξία της μετοχής ενός οργανισμού. Σε μία τέτοια περίπτωση η υπόσταση της μεθοδολογίας αποδυναμώνεται καθώς είναι εξαιρετικά δύσκολος ο διαχωρισμός της μεμονωμένης επίδρασης δύο ταυτόχρονων γεγονότων στην αξία ενός οργανισμού. Σοβαρά γεγονότα τα οποία μπορούν να επηρεάσουν την χρηματιστηριακή αξία ενός οργανισμού, τα οποία λήφθηκαν υπόψη από την παρούσα έρευνα, είναι τα εξής: Συγχωνεύσεις, εξαγορές, διασπάσεις μετοχών (stock splits), ανακοινώσεις μερισμάτων, ανακοινώσεις οικονομικών αποτελεσμάτων, ανακοινώσεις αντικατάστασης διευθυντικών στελεχών και άλλα γεγονότα παραβίασης ασφαλείας τα οποία συμπίπτουν χρονικά με το υπό εξέταση γεγονός.

4. Γεγονότα τα οποία αφορούν εταιρίες μη κερδοσκοπικού χαρακτήρα εξαιρούνται. Ο βασικός λόγος για την προσθήκη αυτού του κριτήριου είναι ότι οι εταιρίες που δεν αναζητούν το κέρδος αλλά την παροχή κοινωνικής ωφέλειας αποτιμούνται με τελείως διαφορετικά κριτήρια από την αγορά. Η προσθήκη γεγονότων που αφορούν εταιρίες αυτής της μορφής θα αλλοίωνε την συνοχή του τελικού δείγματος.

Το σύνολο των δεδομένων της παρούσας μελέτης συγκεντρώθηκε κυρίως με την χρήση της βάσης δεδομένων DatalossDB του οργανισμού κοινής ωφέλειας Open Security Foundation [**63**]. Η συγκεκριμένη βάση δεδομένων είναι αποτέλεσμα κοινής προσπάθειας της κοινότητας που αποτελείται από ερευνητές και επαγγελματίες οι οποίοι ασχολούνται με την ασφάλεια ΠΣ και σκοπός της είναι η έρευνα, καταγραφή και αναφορά ευπαθειών ΠΣ και περιστατικών παραβίασης ασφαλείας. Ο λόγος που επιλέχθηκε η συγκεκριμένη πηγή δεδομένων είναι (α) η πληρότητα και η ακρίβεια που εμφανίζει σε στατιστικά στοιχεία (β) ο αριθμός καταγραμμένων περιστατικών παραβίασης ασφαλείας και (γ) η ελεύθερη προσβασιμότητα της. Σύμφωνα με την έρευνα που

έγινε, καμία άλλη διαδικτυακή βάση δεδομένων αυτού του είδους δεν συνδυάζει τα παραπάνω πλεονεκτήματα. Επιπρόσθετα, η έρευνα συμπληρώθηκε από τις περιοδικές αναφορές που συντάσσει και δημοσιεύει ο οργανισμός Identity Theft Report Center (ITRC) [**64**] και ο οργανισμός Privacy Rights Clearing House (PRC) [**65**] οι οποίοι είναι και οι δύο κοινής ωφέλειας. Τέλος, έγινε έρευνα στις δημοσιεύσεις των διαδικτυακών τόπων που είναι αφιερωμένοι αποκλειστικά στην δημοσίευση περιστατικών παραβίασης ασφαλείας όπως οι BankinfoSecurity [**68**] και Databreaches.net [**67**]. Ο πρώτος είναι ένας διεθνής οργανισμός με στόχο την ενημέρωση του χρηματοπιστωτικού τομέα σε θέματα ασφάλειας ΠΣ. Το δεύτερο είναι ένα ανεξάρτητο blog αναγνωρισμένο από την κοινότητα των ειδικών στην ασφάλεια.

Οι παραπάνω αναφερόμενοι οργανισμοί, παρότι είναι ιδιαιτέρως γνωστοί στην κοινότητα των ανθρώπων που ασχολούνται με την ασφάλεια ΠΣ, δεν είναι ιδιαιτέρως γνωστοί στο ευρύ κοινό όπως είναι οι επενδυτές και αναλυτές που παρακολουθούν την πορεία των εισηγμένων εταιριών και αποτυπώνουν τις προσδοκίες και εκτιμήσεις τους με βάση την πληροφόρηση που έχουν στην διάθεση τους. Συνεπώς, έπρεπε να επιβεβαιωθεί ότι η πληροφόρηση που παρέχουν οι προαναφερόμενες διαδικτυακές πηγές δεδομένων έχει αποτυπωθεί και σε πηγές πληροφόρησης με μεγαλύτερη απήχηση στο ευρύ κοινό. Επομένως, για κάθε περιστατικό που αντλήθηκε από τις συγκεκριμένες πηγές δεδομένων, έγινε έλεγχος του «επιπέδου δημοσιότητας» που έλαβε. Στην παρούσα έρευνα έγινε η παραδοχή πως περιστατικά που έχουν λάβει επαρκή δημοσιότητα χρησιμοποιούνται από την αγορά ως στοιχείο πληροφόρησης, για την αξιολόγηση της πορείας ενός οργανισμού και της σημερινής του αξίας.

Ο βαθμός δημοσιότητας επιβεβαιώθηκε από την διερεύνηση ύπαρξης των επιλεγμένων περιστατικών στο CNET και στο ZDNET οι οποίοι είναι διεθνής οργανισμοί παροχής πληροφόρησης τεχνολογίας προς τον επιχειρηματικό κόσμο και χρήζουν ευρείας αποδοχής και εκτίμησης. Η έρευνα δεν επικεντρώθηκε στην χρήση μεγάλων μέσων μαζικής ενημέρωσης προκειμένου για την άντληση του δείγματος, όπως είναι τα Wall Street Journal και USA Today, προκειμένου να αποφθεχθεί με αυτόν τον τρόπο η συλλογή δεδομένων που να αφορούν κατά πλειοψηφία πολύ μεγάλες εταιρίες. Γεγονότα παραβίασης ασφαλείας που αφορούν εταιρίες με μικρή κεφαλαιοποίηση, ανεξάρτητα από το επίπεδο σημαντικότητας τους, πολλές φορές δεν καταγράφονται από τα μεγάλα μέσα μαζικής ενημέρωσης. Στο [**82**] η έρευνα που πραγματοποιήθηκε χρησιμοποίησε αποκλειστικά γεγονότα που αποτυπώθηκαν μόνο από γνωστά

μέσα ενημέρωσης. Όπως αναφέρεται χαρακτηριστικά στην ίδια μελέτη, το δείγμα που δημιουργήθηκε ενδεχομένως να μην είναι αντιπροσωπευτικό του πληθυσμού των περιστατικών παραβίασης ασφαλείας λόγω της πιθανότητας να περιλαμβάνει μόνο μεγάλου μεγέθους περιστατικά.

Όπως καταγράφεται από στατιστικές μελέτες περιπτώσεων παραβίασης ασφαλείας, η κατανομή των περιστατικών με βάση το μέγεθος του οργανισμού που προσβάλλεται προσεγγίζει την κανονική κατανομή [**60**]. Με βάση αυτήν την παρατήρηση μπορούμε να συμπεράνουμε ότι το μέγεθος ενός οργανισμού επιρρεάζει ελάχιστα την πιθανότητα να δεχθεί μία παραβίαση ασφαλείας. Τα χαρακτηριστικά που μπορούν να κάνουν ελκυστικό έναν οργανισμό σε μία πηγή απειλής είναι περισσότερο η αξία των δεδομένων που διαχειρίζεται και το επίπεδο ασφαλείας που έχει εγκαταστήσει παρά το μέγεθος του ίδιου του οργανισμού. Στις δύο τελευταίες μελέτες της Verizon, σχετικά με τις παραβιάσεις ασφαλείας, καταγράφεται μία χαρακτηριστική αλλαγή των ισορροπιών σχετικά με την κατανομή του αριθμού των περιστατικών ανά κατηγορία μεγέθους οργανισμού. Συγκεκριμένα, η κατηγορία μεγέθους μεταξύ 11-100 εργαζομένων καταλαμβάνει πλέον άνω του 50% των διαπιστωμένων περιστατικών [**13**], [**61**]. Καθώς σκοπός την παρούσας έρευνας ήταν η ανάλυση περιστατικών ασφαλείας που διαδραματίστηκαν στα τελευταία έτη, η προαναφερόμενη αλλαγή στην κατανομή των περιστατικών ανά κατηγορία μεγέθους οργανισμού έπρεπε να ληφθεί υπόψη.

Επιχειρήθηκε συνεπώς στην έρευνα να διατηρηθεί μία ισορροπία μεταξύ του βαθμού δημοσιότητας των γεγονότων που επιλέχτηκαν και του επιπέδου μεροληπτικότητας επιλογής (selection bias) στην διαδικασία δειγματοληψίας. Ο τελικός στόχος ήταν η επίτευξη αντιπροσώπευσης στο δείγμα όλων των μεγεθών εταιρικής κεφαλαιοποίησης με παράλληλη εισαγωγή περιστατικών που να τηρούσαν έναν ελάχιστο βαθμό δημοσιότητας.

Τα κριτήρια που χρησιμοποιήθηκαν για την λήψη δεδομένων από τις προαναφερόμενες επιλεγμένες πηγές δεδομένων ήταν (α) απώλεια δεδομένων κάθε τύπου, (β) πηγή απειλής προερχόμενη είτε από το εσωτερικό είτε από το εξωτερικό περιβάλλον ενός οργανισμού, (γ) γεγονότα που αφορούν κερδοσκοπικούς οργανισμούς και (δ) παραβιάσεις ασφαλείας κάθε τύπου με εξαίρεση αυτές που αφορούσαν ιούς. Όπως υποστηρίχθηκε στην ενότητα 5.2, περιστατικά τα οποία προκαλούνται από ιούς δεν μπορούν να αναλυθούν επαρκώς από την μεθοδολογία ανάλυσης γεγονότων και για αυτόν τον λόγο κατά την διαδικασία δειγματοληψίας εξαιρέθηκαν.

Με βάση τα προαναφερόμενα κριτήρια άντλησης δεδομένων, δημιουργήθηκε μία αρχική συλλογή γεγονότων απαρτιζόμενη από 125 παρατηρήσεις εμπεριέχοντας τις προϋποθέσεις για τον τύπο των προσβαλλόμενων οργανισμών και τους περιορισμούς στον χρόνο και τον τύπο παραβίασης ασφαλείας. Στην συνέχεια έγινε εφαρμογή των κριτηρίων, όπως αναλύθηκαν παραπάνω, για την επιλογή των παρατηρήσεων στο τελικό δείγμα. Η συνολική εφαρμογή των κριτηρίων αποτυπώνεται στον Πίνακα 10. Δύο περιστατικά αφαιρέθηκαν λόγω της ύπαρξης γεγονότων που συνέπεσαν χρονικά στο παράθυρο περιόδου ανάλυσης γεγονότων [-1,1]. Ακολούθως, έντεκα περιστατικά αφαιρέθηκαν καθώς οι εμπλεκόμενες εταιρίες δεν είχαν πλήρη χρηματιστηριακή διαπραγμάτευση στο διάστημα εκτίμησης. Τελικώς, ένα πρόσθετο σύνολο από επτά περιστατικά αφαιρέθηκε καθώς οι εταιρίες, που προσβλήθηκαν από τα συγκεκριμένα περιστατικά, δεν ήταν εισηγμένες στις χρηματαγορές των ΗΠΑ. Το εναπομείναν δείγμα περιελάμβανε 105 γεγονότα. Συγκρίνοντας το συγκεκριμένο μέγεθος δείγματος με το εύρος της περιόδου που διερευνήθηκε, είναι ένα από τα μεγαλύτερα δείγματα που έχουν χρησιμοποιηθεί σε ανάλογη μελέτη ανάλυσης γεγονότων.

Πλήρης παράθεση των γεγονότων που χρησιμοποιήθηκαν από την παρούσα μελέτη, με τα βασικά χαρακτηριστικά τους, παραθέτεται στο παράρτημα ΙΙ. Επίσης, ενδεικτικά αποσπάσματα από δημοσιεύσεις γεγονότων παραβίασης ασφαλείας στα μέσα ενημέρωσης, τα οποία τοποθετήθηκαν στο δείγμα, παραθέτονται στο παράρτημα ΙΙΙ.

Πίνακας 10: Εφαρμογή κριτηρίων επιλογής δείγματος

Κριτήριο επιλογής	Αναμόρφωση μεγέθους δείγματος	Εναπομείναν μέγεθος δείγματος
Αρχική συλλογή γεγονότων	125	125
Ύπαρξη γεγονότων που συμπίπτουν χρονικά	(2)	123
Ανεπαρκή δεδομένα για το διάστημα εκτίμησης	(11)	112
Εισηγμένος οργανισμός σε χρηματαγορά εκτός των ΗΠΑ	(7)	105

Στον Πίνακα 11 αποτυπώνονται τα χαρακτηριστικά των εταιριών που συμπεριλαμβάνονται στο τελικό δείγμα. Καθώς το δείγμα περιλαμβάνει γεγονότα τα οποία πρόσβαλαν την ίδια εταιρία, ο συνολικός αριθμός των εταιριών στο δείγμα ανέρχεται σε 92. Η μέση κεφαλαιοποίηση των

εταιριών που συμπεριλαμβάνονται στο δείγμα ανέρχεται σε $48 δις ενώ η διάμεσος της κεφαλαιοποίησης σε $17,5 δις. Η διαφορά μεταξύ μέσης τιμής και διαμέσου κεφαλαιοποίησης αποτυπώνει την εύρος του μεγέθους των εταιριών που συμπεριλήφθησαν στο δείγμα και την επίτευξη αποφυγής μεμονωμένης χρήσης εταιριών που ανήκουν στην μεγάλη κεφαλαιοποίηση. Λόγω της μεγάλης διασποράς των δεδομένων κεφαλαιοποίησης στο δείγμα επιλέχθηκε στο υπόλοιπο της μελέτης η χρήση της διαμέσου προκειμένου για το σύνολο των υπολογισμών και την έκδοση συμπερασμάτων.

Όπως φαίνεται στον ίδιο πίνακα, οι εταιρίες παροχής χρηματοοικονομικών υπηρεσιών έχουν την μεγαλύτερη διάμεση κεφαλαιοποίηση ενώ ακολουθούν οι εταιρίες καταναλωτικών αγαθών και προϊόντων υγείας. Επίσης, οι εταιρίες τεχνολογίας σε συνδυασμό με τις εταιρίες που ανήκουν στο τομέα υπηρεσιών, καταλαμβάνουν άνω του 50% των γεγονότων παραβιάσεων ασφαλείας που αναλύθηκαν. Επιπρόσθετα, όπως προκύπτει από την σύγκριση των μέσων τιμών και των διαμέσων, για τους δύο προαναφερόμενους τομείς, οι εταιρίες που περιλαμβάνονται ανήκουν σε κάθε κατηγορία κεφαλαιοποίησης.

Ο Πίνακας 12 παραθέτει τα γεγονότα που συμπεριλήφθησαν στο τελικό δείγμα ανά κατηγορία παραβίασης ασφαλείας. Σχεδόν το 84% των γεγονότων παραβίασης ασφαλείας αφορά είτε μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα, είτε μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών. Σχεδόν το σύνολο του δείγματος (97%) αφορά γεγονότα σχετικά με παραβίαση της ασφάλειας ευαίσθητων δεδομένων.

Η συγκεκριμένη παρατήρηση επιβεβαιώνει προηγούμενες εμπειρικές μελέτες που αναφέρθηκαν στην Ενότητα 5.2 και που επιδόθηκαν κατά κύριο λόγο στην έκθεση ευαίσθητων δεδομένων. Επίσης, μας οδηγεί στο συμπέρασμα ότι η παραβίαση της εμπιστευτικότητας θα πρέπει να συγκεντρώνει το μεγαλύτερο ενδιαφέρον των ειδικών στην ασφάλεια ΠΣ σε σχέση με τα θέματα παραβίασης της διαθεσιμότητας και παραβίασης της ακεραιότητας. Η παραπάνω παρατήρηση οδήγησε την επικέντρωση της διατριβής σε θέματα παραβίασης ασφαλείας που αφορούν την εμπιστευτικότητα ευαίσθητων δεδομένων.

Πίνακας 11: Βασικά χαρακτηριστικά εταιριών δείγματος

Τομέας οικονομίας	Αριθμός γεγονότων ανά τομέα οικονομίας	Ποσοστό γεγονότων σε σύνολο δείγματος	Μέση κεφαλαιοποίηση ανά τομέα οικονομίας (000.000 $)	Διάμεσος κεφαλαιοποίησης ανά τομέα οικονομίας (000.000 $)
Καταναλωτικά αγαθά	14	13,33%	35.825,50	22.695,00
Χρηματοοικονομικές υπηρεσίες	17	16,19%	48.621,04	35.220,00
Προϊόντα υγείας	11	10,48%	41.340,00	23.090,00
Βιομηχανικά αγαθά	5	4,76%	19.760,00	15.180,00
Γενικές υπηρεσίες	33	31,43%	43.403,40	7.895,00
Τεχνολογίας	23	21,90%	74.796,48	16.170,00
Πρώτων υλών	2	1,90%	9.645,00	9.645,00
Συνολικός αριθμός γεγονότων	105	100,00%	48.017,37	17.460,00

Πίνακας 12: Γεγονότα ανά κατηγορία παραβίασης ασφαλείας

Κατηγορία παραβίασης ασφαλείας	Αριθμός γεγονότων	Ποσοστό γεγονότων σε σύνολο δείγματος
Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	48	45,71%
Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	40	38,10%
Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	14	13,33%
Λοιπές κατηγορίες παραβιάσεων	3	2,86%
Σύνολο	105	100,00%

5.6 Ανάπτυξη υποθέσεων προς ανάλυση

Η μεθοδολογία που χρησιμοποιήθηκε στην ανάλυση υποθέσεων αφορά στατιστικούς ελέγχους ενός άκρου (one-tail tests). Οι έλεγχοι αυτοί, οι οποίοι ονομάζονται και κατευθυντήριοι (directional), διαχωρίζουν την κατανομή πιθανοτήτων με την περιοχή απόρριψης της H_0 στο αριστερό της άκρο. Η επιλογή αυτή γίνεται προκειμένου να αποτυπωθεί η παραδοχή ότι ένα περιστατικό παραβίασης ασφαλείας αναμένεται να προκαλέσει αποκλειστικά αρνητικές

επιπτώσεις σε έναν οργανισμό. Αντίθετο αποτέλεσμα έρχεται σε διαφωνία με το προσδοκώμενο αποτέλεσμα βάση θεωρίας.

Πίνακας 13: Στατιστική μεθοδολογία μελετών ανάλυσης γεγονότων

Έτος δημοσίευσης	Κύριος συγγραφέας	Στατιστική μεθοδολογία που χρησιμοποιήθηκε
1993	Dos Santos et. al.	Z statistic χρησιμοποιώντας CSAR[12] ακολουθώντας την Student's-t κατανομή
2001	Subramani et. al.	Student's -t κατανομή
2001	Im et. al.	Z statistic χρησιμοποιώντας CSAR ακολουθώντας την Student's-t κατανομή
2002	Ettredge et. al.	Z statistic χρησιμοποιώντας CSAR ακολουθώντας την Student's-t κατανομή
2003	Campbell et. al.	Z statistic χωρίς να προσδιορίζουν λεπτομερώς την κατανομή. Χρήση OLS και SUR.
2003	Garg et. al.	Δεν αναφέρουν
2003	Hovav et. al.	Z statistic χρησιμοποιώντας CSAR ακολουθώντας την Student's-t κατανομή
2004	Cavusoglu et. al.	Student's -t κατανομή
2004	Hovav et. al.	Z statistic χρησιμοποιώντας CSAR ακολουθώντας την Student's-t κατανομή
2006	Ko et. al.	Παραμετρικοί και μη παραμετρικοί έλεγχοι για την αξιολόγηση της διαφοράς των διαφορών μεταξύ εταιριών που έχουν δεχθεί παραβίαση ασφαλείας και εταιριών που δεν έχουν δεχθεί.
2009	Bharadwaj et. al.	Student's -t κατανομή. Η μεθοδολογία OLS χρησιμοποιήθηκε για την ανάλυσης υποθέσεων των στατιστικών βασισμένο στα CAR. Η μεθοδολογία GLS χρησιμοποιήθηκε για τον έλεγχο ύπαρξης σημαντικών διαφορών στην επίπτωση που προκαλείται από διαφορετικά είδη παραβιάσεων ασφαλείας.
2010	Patel	Student's -t κατανομή
2010	Gatzlaff et. al.	Student's t-test κατά τον Patell (1976)
2011	Yayla et. al.	Student's -t κατανομή
2011	Gordon et. al.	Z statistic χωρίς περισσότερες διευκρινήσεις.

[12] Η ορολογία CSAR αποτελεί σύντμηση του Cumulative Standardized Abnormal Returns.

Όπως αναπτύχθηκε στην ενότητα 5.4.4, η κατανομή πιθανοτήτων που χρησιμοποιήθηκε είναι η t-Student με T-1 βαθμούς ελευθερίας. Το μεγαλύτερο μέρος των μελετών ανάλυσης γεγονότων έχουν χρησιμοποιήσει την συγκεκριμένη κατανομή ενώ ένα μικρό μέρος την z-standardized κανονική κατανομή προκειμένου για την ανάλυση στατιστικών υποθέσεων. Ο Πίνακας 13 αναφέρει τις κατανομές που χρησιμοποιήθηκαν από τις κυριότερες μελέτες που αναλύθηκαν προκειμένου για την μεθοδολογική ανάλυση της έρευνας και για την σύγκριση των αποτελεσμάτων.

Όταν οι παρατηρήσεις ενός δείγματος αποτελούνται από ημερήσια δεδομένα ασυνήθη αποδόσεων, εμφανίζεται ισχυρή ροπή μη κανονικότητας στην κατανομή που σχηματίζεται. Ωστόσο, όταν ένα δείγμα είναι επαρκώς μεγάλο, ήτοι άνω των 50 παρατηρήσεων, παρουσιάζεται μικρή διαφοροποίηση μεταξύ των αποτελεσμάτων που προέρχονται από την κανονική και την Student-t κατανομή. Καθώς το μέγεθος του δείγματος μεγαλώνει, η κατανομή των παρατηρήσεων, αποτελούμενων από ημερήσιες αποδόσεις, τείνει προς την κανονική κατανομή ειδικά όταν το μέγεθος υπερβαίνει τις 50 παρατηρήσεις [**96**]. Όπως αναφέρθηκε στην ενότητα 5.2, ένας μεγάλος αριθμός προηγούμενων μελετών έχει ως βασικό περιορισμό το αρκετά μικρό μέγεθος δείγματος το οποίο είναι μικρότερο του προαναφερόμενου επιπέδου των 50 παρατηρήσεων.

Στην παρούσα μελέτη χρησιμοποιήθηκαν descriptive summary measures σε συνδυασμό με normal probability plots προκειμένου να εκτιμηθεί η υπόθεση κανονικότητας της κατανομής δειγματοληψίας. Τα στοιχεία που προέκυψαν, από τα προαναφερόμενα στατιστικά εργαλεία, υπόδειξαν αποκλίσεις από την κανονικότητα σε αποδεκτά επίπεδα τα οποία δεν επηρεάζουν την στατιστική εγκυρότητα της μεθοδολογίας ανάλυσης γεγονότων.

5.6.1 Υπόθεση στο συνολικό δείγμα

Η πρώτη υπόθεση που αναλύθηκε σχετίζεται με την αντίδραση της αγοράς σε μία παραβίαση ασφαλείας λαμβάνοντας υπόψη το σύνολο του δείγματος. Η υπόθεση γίνεται δεκτή όταν δεν υπάρχει ένδειξη αρνητικής αντίδρασης με στατιστική σημαντικότητα, από την πλευρά των αγορών, στις δημόσιες ανακοινώσεις περιστατικών παραβίασης ασφαλείας.

Η υπόθεση που αναλύθηκε παραπάνω συνοψίζεται στην παρακάτω πρόταση:

$H1_0$: *Ένα περιστατικό παραβίασης ασφαλείας δεν θα έχει αρνητική επίπτωση σε έναν οργανισμό ανεξαρτήτως του μεγέθους και του είδους του οργανισμού.*

5.6.2 Υπόθεση σε επιμέρους δείγματα με βάση το είδος οργανισμού

Η δεύτερη υπόθεση αφορά την ύπαρξη διαφοροποίησης για το μέγεθος της επίπτωσης μίας παραβίασης ασφαλείας με βάση τον τομέα της οικονομίας στον οποίο υπάγεται η δραστηριοποίηση ενός οργανισμού. Προς αυτή την κατεύθυνση το συνολικό δείγμα επιμερίστηκε σε δυο υπό-δείγματα όπου το πρώτο περιελάμβανε τις εταιρίες που άνηκαν στο τομέα τεχνολογίας και το δεύτερο περιελάμβανε τις εταιρίες που άνηκαν σε όλους τους υπόλοιπους τομείς. Το μέγεθος του δείγματος εταιριών τεχνολογίας ήταν μεγέθους 23 παρατηρήσεων, ενώ το δείγμα με τις λοιπές εταιρίες ήταν μεγέθους 82 παρατηρήσεων.

Η θεωρητική προσέγγιση, στην οποία βασίζεται η συγκεκριμένη υπόθεση, προέρχεται από την αντίληψη ότι οι χρηματοδότες ενός οργανισμού θεωρούν ότι οι επιχειρήσεις τεχνολογίας επηρεάζονται περισσότερο από ένα περιστατικό παραβίασης ασφαλείας. Διατυπώνοντας το διαφορετικά, οι αγορές αναμένεται να «τιμωρήσουν» περισσότερο μία επιχείρηση τεχνολογίας, που επωμίστηκε μία παραβίαση ασφαλείας, από ότι μία επιχείρηση που δραστηριοποιείται σε άλλους τομείς της οικονομίας. Οι αγορές αναμένουν από τις επιχείρησης τεχνολογίας να είναι περισσότερο ικανές να διατηρήσουν ένα επαρκές επίπεδο ασφάλειας το οποίο να τις καθιστά συγκριτικά περισσότερο ικανές να προστατεύσουν τα πληροφοριακά τους συστήματα από μία εσωτερική ή εξωτερική πηγή απειλής. Επομένως, ένα αρνητικό περιστατικό ασφαλείας αναμένεται να επηρεάσει περισσότερο την αξιοπιστία μίας επιχείρησης τεχνολογίας και την εμπιστοσύνη της αγοράς στην ικανότητα της να προστατεύσει τα ευαίσθητα δεδομένα που διαχειρίζεται, από την επίδραση που θα ασκήσει σε μία επιχείρηση εκτός τεχνολογικής δραστηριοποίησης. Τέλος μία ακόμη παράμετρος, που λαμβάνεται σοβαρά από τις αγορές, είναι ο σοβαρός βαθμός εξάρτησης των εταιριών τεχνολογίας στα συστήματα τεχνολογίας πληροφόρησης προκειμένου να επιτελέσουν τις βασικές πτυχές λειτουργίας τους.

Σύμφωνα με την έρευνα των υφιστάμενων παρόμοιων μελετών που πραγματοποιήθηκε η παρούσα είναι η πρώτη που εστιάζει στον προαναφερόμενο διαχωρισμό ανάλυσης. Το σύνολο σχεδόν προηγούμενων σημαντικών μελετών εστίασε σε επίπεδο κλάδου δραστηριοποίησης αντί για τον περισσότερο διευρυμένο διαχωρισμό που προτείνεται στην παρούσα μελέτη που

χρησιμοποιεί το κριτήριο του τομέα δραστηριοποίησης. Στο [**72**] το δείγμα διαχωρίζεται σε εταιρίες που πραγματοποιούν ηλεκτρονικό εμπόριο και σε εταιρίες που η κύρια εμπορική τους δραστηριότητα πραγματοποιείται με παραδοσιακά μέσα. Στο [**79**] το δείγμα εστιάζεται στις εταιρίες προμήθειας προϊόντων ασφαλείας (security vendors). Θεωρούμε πως η γενικότερη βάση διαχωρισμού που χρησιμοποιήθηκε στα πλαίσια της παρούσας διατριβής οδηγεί σε περισσότερο εμπεριστατωμένη γενίκευση των στατιστικών αποτελεσμάτων.

Η υπόθεση που αναλύθηκε παραπάνω συνοψίζεται στην παρακάτω πρόταση:

$H2_0$: *Ένα περιστατικό παραβίασης ασφαλείας δεν θα έχει ισχυρότερη επίπτωση σε έναν οργανισμό τεχνολογίας σε σχέση με έναν οργανισμό που δραστηριοποιείται σε οποιοδήποτε άλλο τομέα της οικονομίας.*

5.6.3 Υπόθεση σε επιμέρους δείγματα με βάση το μέγεθος του περιστατικού

Η επόμενη υπόθεση που αναλύθηκε αφορά την διερεύνηση ύπαρξης διαφοροποίησης στην επίπτωση ενός περιστατικού σε συνάρτηση με το μέγεθος του. Το κριτήριο που χρησιμοποιήθηκε για τον προσδιορισμό του μεγέθους ενός περιστατικού ασφαλείας είναι ο αριθμός των εγγραφών που επηρεάστηκαν. Το συγκεκριμένο κριτήριο είναι η πρώτη φορά που χρησιμοποιείται από ανάλογη εμπειρική μελέτη. Η βασική αρνητική συνέπεια που προκαλείται από την χρήση αυτού του κριτήριου είναι ότι εξαιρείται ένας αριθμός περιστατικών είτε λόγω έλλειψης στοιχείων, είτε λόγω της μορφής του περιστατικού. Πλέον όμως υπάρχει η τάση τα περισσότερα περιστατικά που δημοσιεύονται, να συνοδεύονται από επαρκή στοιχεία συμπεριλαμβάνοντας εκτίμηση του εύρους των εγγραφών που επηρεάστηκαν. Το δείγμα που αναλύθηκε περιλαμβάνει επαρκή στοιχεία επηρεασμένων εγγραφών κατά το 74%. Τα 78 περιστατικά, που περιλαμβάνουν επαρκή στοιχεία, αναλύονται περαιτέρω στον Πίνακα 14.

Στην υπόθεση αυτή αναμένεται τα περιστατικά, που περιλαμβάνουν την έκθεση μεγαλύτερου όγκου ευαίσθητων δεδομένων, να επιφέρουν μεγαλύτερο αντίστοιχα συνολικό κόστος σε έναν οργανισμό. Σύμφωνα με τα δεδομένα υπολογισμού του άμεσου κόστους ανά περιστατικό ασφαλείας, όπως αποτυπώνονται στο παράρτημα ΙΙ, παρατηρείται μία αναλογική σχέση μεταξύ του αριθμού προσβεβλημένων εγγραφών και του άμεσου κόστους. Η παρατήρηση αυτή κυρίως οδήγησε την παρούσα μελέτη στην επιλογή του αριθμού των εγγραφών σε έκθεση ως κριτήριο για το μέγεθος ενός περιστατικού ασφαλείας. Στην ανάλυση της συγκεκριμένης στατιστικής υπόθεσης

διερευνείται η ύπαρξη ανάλογης σχέσης μεταξύ του αριθμού προσβεβλημένων εγγραφών και του έμμεσου κόστους ανά περιστατικό ασφαλείας. Με άλλα λόγια μελετάται η υπόθεση αν το μέρος του κόστους, από ένα περιστατικό ασφαλείας, που προκύπτει σε μεσοπρόθεσμο ή μακροπρόθεσμο ορίζοντα εξαρτάται από τον αριθμό των εγγραφών των οποίων η εμπιστευτικότητα κινδύνευσε.

Πίνακας 14: Ανάλυση αριθμού επιρρεασμένων εγγραφών - περιστατικών

Αριθμός επηρεασμένων εγγραφών	Αριθμός περιστατικών	Ποσοστό επί του συνόλου
>0 και <10.000	24	30,77%
>10.000 και <100.000	24	30,77%
>100.000 και <1.000.000	13	16,67%
>1.000.000	17	21,79%
Σύνολα	78	100,00%

Η υπόθεση που αναλύθηκε παραπάνω συνοψίζεται στην παρακάτω πρόταση:

$H3_0$: *Ένα περιστατικό παραβίασης ασφαλείας δεν θα έχει ισχυρότερη επίπτωση σε μία επιχείρηση όταν εκτίθεται η εμπιστευτικότητα περισσότερων εγγραφών δεδομένων από ότι σε ένα άλλο με έκθεση λιγότερων εγγραφών.*

5.7 Ανάλυση αποτελεσμάτων

Προκειμένου για την υλοποίηση των υπολογισμών που περιγράφονται στην ενότητα 5.4.4, αρχικώς έγινε η δημιουργία μίας βάσης δεδομένων με τα στοιχεία αποδόσεων για το σύνολο των διαστημάτων εκτίμησης τα οποία αφορούσαν όλα τα γεγονότα που επιλέχτηκαν στο τελικό δείγμα. Στην συνέχεια έγινε επεξεργασία των δεδομένων με την χρήση ενός προγράμματος που δημιουργήθηκε ειδικά για το σκοπό αυτό και ο κώδικας του παραθέτεται στο παράρτημα IV. Το πρόγραμμα είναι γραμμένο σε Visual Basic και τρέχει σε περιβάλλον Excel. Δίνεται η δυνατότητα επιλογής του μοντέλου αποτίμησης επενδυτικών κεφαλαίων που θα χρησιμοποιηθεί μεταξύ του CAPM και του μοντέλου τριών μεταβλητών των Fama-French. Επίσης μπορεί να γίνει επιλογή των γεγονότων με βάση των αριθμό τον εκτεθειμένων εγγραφών τοποθετώντας κριτήρια σχετικά με τον κατώτατο και ανώτατο αριθμό τους.

Αρχικά έγινε ανάλυση γραμμικής παλινδρόμησης μίας ανεξάρτητης μεταβλητής και εν συνεχεία τριών μεταβλητών χρησιμοποιώντας την βάση δεδομένων με τα στοιχεία αποδόσεων προκειμένου να υπολογιστούν οι συντελεστές των παραμέτρων των δύο μοντέλων που χρησιμοποιήθηκαν. Ακολούθως έγινε υπολογισμός των ασυνήθη αποδόσεων, για τα δύο μοντέλα, χρησιμοποιώντας τους τύπους 2 και 4 για όλες τις ημέρες που συνθέτουν κάθε παράθυρο περιόδου ανάλυσης γεγονότων για κάθε γεγονός στο δείγμα. Στην συνέχεια υπολογίστηκαν οι αντίστοιχες ημερήσιες διακυμάνσεις χρησιμοποιώντας τον τύπο 5. Τα δεδομένα αυτά ακολούθως χρησιμοποιήθηκαν για το υπολογισμό των σωρευτικών ασυνήθη αποδόσεων καθώς και των σωρευτικών διακυμάνσεων τους, για κάθε παράθυρο ανάλυσης σε κάθε γεγονός, με την χρήση των τύπων 6 και 8 τα οποία, στην συνέχεια, με την χρήση των τύπων 7 και 9, απέδωσαν τις αντίστοιχες μέσες σωρευτικές ασυνήθεις αποδόσεις και τις μέσες σωρευτικές διακυμάνσεις. Από τα δεδομένα αυτά προέκυψε η στατιστική t για κάθε στατιστική υπόθεση και παράθυρο ανάλυσης προκειμένου για την εξέταση κάθε υπόθεσης όπως αναλύεται στις ακόλουθες ενότητες.

5.7.1 Ανάλυση συνολικού δείγματος

Η ανάλυση του πλήρους δείγματος αφορά την πρώτη υπόθεση, σχετικά με την ύπαρξη αρνητικών ασυνήθη αποδόσεων με στατιστική σημαντικότητα, για τις εταιρίες που δέχθηκαν μία δημοσιευμένη παραβίαση ασφαλείας. Τα στατιστικά αποτελέσματα, για το πλήρες δείγμα χρησιμοποιώντας το CAPM, αποτυπώνονται στον Πίνακα 15. Από τα αποτελέσματα προκύπτει αρνητικό μέσο CAR για τα παράθυρα ανάλυσης [-1,0] και [0,0] αλλά χωρίς στατιστική σημαντικότητα. Το μέσο CAR για τα υπόλοιπα παράθυρα ανάλυσης είναι κοντά στο μηδέν επίσης χωρίς στατιστική σημαντικότητα.

Πίνακας 15: CAPM - Ανάλυση συνολικού δείγματος

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	105	0,0018	0,4633	0,6781
[-1,0]	105	-0,0006	-0,1981	0,4216
[0,0]	105	-0,0003	-0,1325	0,4474
[0,1]	105	0,0021	0,6694	0,7478

Τα στατιστικά αποτελέσματα για το πλήρες δείγμα, χρησιμοποιώντας το μοντέλο τριών-μεταβλητών, αποτυπώνονται στον Πίνακα 16. Η πρώτη σημαντική διαπίστωση που εξάγεται είναι ότι όλοι οι μέσοι CARs είναι αρνητικοί ανεξάρτητα του παραθύρου ανάλυσης που εξετάζεται. Τα αποτελέσματα συνεπώς, προερχόμενα από την χρήση του συγκεκριμένου μοντέλου, επιβεβαιώνουν την θεωρητική προσδοκία της αρνητικής επίπτωσης στην κεφαλαιακή αξία ενός οργανισμού προερχόμενη από την ανακοίνωση ενός περιστατικού παραβίασης ασφαλείας. Αναλυτικότερα, στο παράθυρο ανάλυσης [-1,0], το μέσο CAR είναι -0,0039 με στατιστική σημαντικότητα στο επίπεδο του 10%. Το μέγεθος αυτό αποκαλύπτει πως στην περίοδο ανάμεσα t_{-1} και t_0, οι προσβαλλόμενοι οργανισμοί χάνουν κατά μέσο όρο το 0,39% της χρηματιστηριακής κεφαλαιοποίησης τους. Λαμβάνοντας υπόψη ότι η διάμεσος κεφαλαιοποίησης, του συνόλου των εταιριών στο συνολικό δείγμα, ανέρχεται σε $17,5 δις, από το παραπάνω ποσοστό απώλειας προκύπτει μέση οικονομική επίπτωση ανά περιστατικό ίση με $68 εκατομμύρια. Πρέπει να σημειωθεί πως αν χρησιμοποιηθεί ο μέσος όρος αντί της διαμέσου, η μέση απώλεια αυξάνεται σε $187 εκατομμύρια. Ο λόγος της σημαντικής διαφοράς μεταξύ των δύο αποτελεσμάτων είναι οι σημαντικές αποκλίσεις μεταξύ των μεγεθών των εταιριών που εξετάστηκαν. Οι αποκλίσεις αυτές αποτυπώνουν το εύρος αντιπροσώπευσης των εταιριών, που ανήκουν σε κάθε κατηγορία κεφαλαιοποίησης, στο δείγμα.

Είναι γενικά αποδεκτό στην περίπτωση σημαντικών αποκλίσεων, μεταξύ των δεδομένων σε ένα δείγμα, ότι η αξιοπιστία του μέσου όρου αποδυναμώνεται και η διάμεσος αποτελεί περισσότερο αξιόπιστο μέτρο καθώς δεν επηρεάζεται από ακραίες τιμές. Στην παρούσα μελέτη, λαμβάνοντας υπόψη την σύνθεση των τιμών των παρατηρήσεων που περιλαμβάνονται στο δείγμα, επιλέγεται η χρήση της διαμέσου ως περισσότερο αξιόπιστο και αντιπροσωπευτικό μέτρο για την τάση των δεδομένων. Από την έρευνα που έγινε σε προηγούμενες ανάλογες μελέτες, το σύνολο τους έκανε χρήση της μέσης κεφαλαιοποίησης προκειμένου για την εξαγωγή συμπερασμάτων. Χαρακτηριστικό παράδειγμα είναι η πρόσφατη έρευνα από τους Yayla et. al. [**77**] όπου, παρότι η τυπική απόκλιση για την κεφαλαιοποίηση σε όλες τις περιπτώσεις υπερβαίνει σε μέγεθος τον μέσο όρο, απουσιάζει ο υπολογισμός της διαμέσου. Σε άλλη πρόσφατη έρευνα από τους Gordon et. al. [**82**] γίνεται, παράλληλα με τον μέση κεφαλαιοποίηση, υπολογισμός της διαμέσου όμως χωρίς να γίνεται αναφορά ποιο από τα δύο στατιστικά μέτρα είναι περισσότερο αξιόπιστο για την εξαγωγή συμπερασμάτων. Η εξαγωγή των αποτελεσμάτων, στο συγκεκριμένο κεφάλαιο και στο υπόλοιπο

στην παρούσας διατριβής, όπως αναφέρθηκε και στην ενότητα 5.5, πραγματοποιήθηκε με την χρήση της διαμέσου.

Πίνακας 16: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	105	-0,0021	-0,5749	0,2832
[-1,0]	105	-0,0039	-1,3121	0,0959
[0,0]	105	-0,0033	-1,5534	0,0613
[0,1]	105	-0,0015	-0,4919	0,3118

Συνεχίζοντας την ανάλυση των δεδομένων του Πίνακα 16, το παράθυρο ανάλυσης [0,0] έχει μέσο CAR ίσο με -0,0033 και με τιμή p ίση με 0,0613 το οποίο παραπέμπει σε στατιστική σημαντικότητα κοντά στο επίπεδο του 5%. Το μέγεθος αυτό υποδεικνύει ότι την ημέρα γεγονότος η προσβαλλόμενη εταιρία έχασε κατά μέσο όρο 0,33% της κεφαλαιακής της αξίας. Χρησιμοποιώντας την διάμεσο κεφαλαιοποίησης, όπως αναλύθηκε παραπάνω, προκύπτει εκτίμηση της μέσης οικονομικής απώλειας, ανά περιστατικό παραβίασης ασφαλείας, της τάξης των $57 εκατομμυρίων. Τα άλλα δύο παράθυρα που αναλύθηκαν, μέσω του μοντέλου τριών-μεταβλητών, αποδίδουν μεν αρνητικά αποτελέσματα χωρίς όμως στατιστική σημαντικότητα. Η ανάλυση της συγκεκριμένης στατιστικής υπόθεσης οδήγησε την παρούσα μελέτη σε έναν αριθμό σημαντικών παρατηρήσεων όπως αναλύεται παρακάτω.

Η πρώτη παρατήρηση αφορά την έγκαιρη αντίδραση των αγορών στις ανακοινώσεις παραβιάσεων ασφαλείας. Στην περίπτωση του CAPM, τα παράθυρα ανάλυσης που περιλαμβάνουν την ημέρα t_1, αποφέρουν θετικό μέσο CAR ενώ τα παράθυρα, ανάλυσης που περιλαμβάνουν τις ασυνήθεις αποδόσεις μέχρι την ημέρα γεγονότος, παρότι δεν έχουν στατιστική σημαντικότητα, τουλάχιστον αποφέρουν αρνητικό μέσο CAR. Στην περίπτωση του μοντέλου τριών-μεταβλητών, τα αποτελέσματα είναι παρόμοια. Όπως προαναφέρθηκε το μέσο CAR, με την χρήση του συγκεκριμένου μοντέλου, είναι αρνητικό για όλα τα παράθυρα ανάλυσης. Στις περιπτώσεις όμως που συμπεριλαμβάνεται η ημέρα t_1, τα αποτελέσματα στερούνται σε στατιστική σημαντικότητα. Μπορούμε να συμπεράνουμε, με βάση τα προαναφερόμενα αποτελέσματα, ότι η εξέταση επιπρόσθετων ημερών, μετά την ημέρα γεγονότος, στα παράθυρα

ανάλυσης δεν παρέχει πρόσθετη πληροφόρηση προκειμένου για την εκτίμηση της οικονομικής απώλειας που επιφέρουν οι παραβιάσεις ασφαλείας.

Η δεύτερη παρατήρηση της παραπάνω ανάλυσης αφορά την χρήση την ημέρας t_{-1} στα παράθυρα ανάλυσης. Αναλύοντας τα αποτελέσματα, που προκύπτουν από το μοντέλο τριών-μεταβλητών, το παράθυρο ανάλυσης [-1,0] έχει μέσο αρνητικό CAR το οποίο υπερβαίνει το αντίστοιχο αρνητικό μέσο CAR που αντιστοιχεί στο παράθυρο ανάλυσης [0,0]. Από το αποτέλεσμα αυτό συνάγεται η πιθανότητα διαρροής εσωτερικής πληροφόρησης. Το αποτέλεσμα αυτό είναι αντίθετο με μελέτες που διενεργήθηκαν σε προγενέστερο χρόνο, ο οποίος υπερέβαινε τα πέντε έτη, ενώ συμφωνεί με μελέτες ειδικά των τελευταίων τριών ετών όπως των Gatzlaff et. al. [**81**] και των Yayla et. al. [**77**] οδηγώντας στο τελικό συμπέρασμα ότι οι αγορές προοδευτικά οδηγούνται σε μεγαλύτερη αποτελεσματικότητα πληροφόρησης. Συνεπώς, η προσθήκη της ημέρας t_{-1} παρέχει επιπρόσθετη πληροφόρηση στην ανάλυση γεγονότων και επιβεβαιώνει την πλειονότητα των προηγούμενων ανάλογων μελετών που συμπεριέλαβαν αυτήν την ημέρα στα παράθυρα ανάλυσης που χρησιμοποίησαν.

Η τρίτη παρατήρηση της παραπάνω ανάλυσης αφορά το επίπεδο διαφοροποίησης των αποτελεσμάτων προερχόμενων από το CAPM και το μοντέλο τριών-μεταβλητών των Fama-French. Τα αποτελέσματα δεν συμπίπτουν σε κανένα παράθυρο ανάλυσης. Τα αποτελέσματα του CAPM είναι αντίθετα προς την θεωρεία καθώς σε δύο παράθυρα παρατηρούμε θετικό μέσο CAR και επιπλέον δεν υπάρχει σε κανένα αποτέλεσμα έστω αδύναμη στατιστική σημαντικότητα. Αντίθετα, τα αποτελέσματα από το μοντέλο τριών μεταβλητών είναι σύμφωνα με την θεωρεία καθώς όλα τα CAR είναι αρνητικά με δύο παράθυρα να παρουσιάζουν στατιστική σημαντικότητα. Το συμπέρασμα που εξάγεται είναι πως η χρήση ενός περισσότερο πολύπλοκου μοντέλου επεξήγησης των αναμενόμενων αποδόσεων ενός οργανισμού, οδηγεί σε περισσότερο αξιόπιστα αποτελέσματα.

Η πιο πρόσφατη μελέτη που έκανε χρήση και των δύο μοντέλων, από τους Gordon et. al. [**82**], παρότι αναλύει διαφορετική χρονική περίοδο, κατέληξε σε παρόμοια συμπεράσματα για την συγκριτική αξιοπιστία των δύο μοντέλων. Μάλιστα η μείωση της αξιοπιστίας του CAPM είναι περισσότερο εμφανής στην δεύτερη χρονική περίοδο που αναλύουν οι συγκεκριμένοι συγγραφείς μεταξύ του 2002 – 2007. Στην συγκεκριμένη περίοδο τα αποτελέσματα του CAPM έχουν ακόμα λιγότερη στατιστική σημαντικότητα σε σχέση με την πρώτη περίοδο ανάλυσης του 1995 – 2001.

Το αποτέλεσμα αυτό επιβεβαιώνει και συμπληρώνει παράλληλα η έρευνα της παρούσας διατριβής που αναλύει παραβιάσεις ασφαλείας των τελευταίων ετών.

Η μοναδική παρόμοια μελέτη που βρέθηκε, κατά την διάρκεια της έρευνας, με περίοδο ανάλυσης που να περιλαμβάνει ένα μέρος της περιόδου που αναλύεται από την παρούσα είναι του Patel [**80**]. Τα αποτελέσματα αυτής της έρευνας δεν έχουν στατιστική σημαντικότητα σχεδόν σε όλα τα παράθυρα ανάλυσης που χρησιμοποιήθηκαν και η αξιοπιστία τους περιορίζεται αρκετά από το μικρό δείγμα των 34 παρατηρήσεων που αναλύθηκε.

Λαμβάνοντας υπόψη τα αποτελέσματα του συνόλου των μελετών που αναλύθηκαν, το γενικό συμπέρασμα στο οποίο καταλήγουμε είναι ότι η οικονομική επίπτωση των παραβιάσεων ασφαλείας είναι αρνητική, στατιστικά σημαντική και σταδιακά μειώνεται. Οι Yayla et. al. ανάλυσαν την περίοδο μεταξύ των ετών 1994 – 2006 και κατέληξαν σε μία μέση αρνητική επίπτωση της τάξης του 0,92%. Οι Gatzlaff et. al. μελέτησαν μία υποπερίοδο της προηγούμενης μελέτης μεταξύ των ετών 2004 – 2006 και κατέληξαν σε μία αρνητική επίπτωση της τάξης του 0,57%. Οι Gordon et. al. ανάλυσαν την περίοδο μεταξύ των ετών 1995 – 2007, χωρισμένη σε δύο υποπεριόδους, και συμφωνούν επίσης με το συμπέρασμα των μειούμενων αρνητικών επιπτώσεων που επιφέρουν οι παραβιάσεις ασφαλείας. Συγκεκριμένα, για την περίοδο μεταξύ 1995 – 2001 η μέση οικονομική επίπτωση υπολογίστηκε στο επίπεδο του 2,4%, ενώ για την περίοδο μεταξύ 2002 – 2007 η επίπτωση μειώθηκε στο επίπεδο του 0,34%. Το συγκεκριμένο αποτέλεσμα προσεγγίζει ιδιαίτερα τα αποτελέσματα που αναφέρονται στον Πίνακα 16 στα παράθυρα [-1,0] και [0,0]. Οι Cavusoglu et. al. βρήκαν παρόμοια αποτελέσματα για την περίοδο του 1996 – 2001 καθώς το μέσο κόστος υπολογίστηκε στο επίπεδο του 2,1% επιβεβαιώνοντας την μεγάλη διαφοροποίηση που έχει διαδραματιστεί, μέσα στην τελευταία δεκαετία, στο επίπεδο των επιπτώσεων που επιφέρουν τα περιστατικά παραβίασης ασφαλείας.

Η παρούσα διατριβή, αναλύοντας ένα πιο πρόσφατο χρονικό διάστημα σε σύγκριση με την προαναφερόμενες μελέτες, επιβεβαιώνει το συμπέρασμα ότι οι οικονομικές επιπτώσεις των παραβιάσεων ασφαλείας είναι στατιστικώς σημαντικά αρνητικές και παρουσιάζουν βάσιμες ενδείξεις σταθεροποίησης σε ένα συγκεκριμένο επίπεδο. Το επίπεδο των μέσων CAR, με την χρήση του μοντέλου τριών-μεταβλητών, ανέρχεται σε 0,39% και 0,33% για τα παράθυρα [-1,0] και [0,0] αντιστοίχως. Το υπολογιζόμενο αυτό επίπεδο οικονομικής επίπτωσης προσεγγίζει τα αντίστοιχα αποτελέσματα πρόσφατων προαναφερόμενων μελετών των Gatzlaff et. al. και Gordon

et. al. Συνολικά μπορούμε να εκφέρουμε ότι οι αγορές κατά την διάρκεια της τελευταίας δεκαετίας, αναφορικά με την αντίδραση τους στις ανακοινώσεις περιστατικών ασφαλείας, σταδιακά ωρίμασαν και πλέον το επίπεδο της μέσης οικονομικής επίπτωσης παρουσιάζει βάσιμη τάση σταθεροποίησης σε ένα συγκεκριμένο επίπεδο.

5.7.2 Ανάλυση με κριτήριο το είδος οργανισμού

Προκειμένου για την ανάλυση της δεύτερη υπόθεσης, το δείγμα χωρίστηκε σε δύο υπό-δείγματα. Οι εταιρίες που ανήκουν στο τομέα τεχνολογίας αποτέλεσαν το πρώτο υπό-δείγμα και οι λοιπές εταιρίες το δεύτερο.

Στον Πίνακα 17 αποτυπώνονται τα στατιστικά αποτελέσματα για τις εταιρίες τεχνολογίας, ενώ στον Πίνακα 18 αποτυπώνονται τα στατιστικά αποτελέσματα για τις υπόλοιπες εταιρίες χρησιμοποιώντας και στις δύο περιπτώσεις το CAPM. Τα ίδια παράθυρα ανάλυσης, που χρησιμοποιήθηκαν στην ανάλυση του πρώτου στατιστικού ερωτήματος, χρησιμοποιήθηκαν και στο παρόν. Το μέσο CAR για το παράθυρο ανάλυσης [-1,0], για τον τομέα τεχνολογίας, είναι πολύ χαμηλότερο και με μεγάλη στατιστική σημαντικότητα σε σχέση με το ίδιο παράθυρο για τις λοιπές εταιρίες. Το αποτέλεσμα αυτό επαληθεύει εμπειρικά την πεποίθηση ότι οι οργανισμοί τεχνολογίας επηρεάζονται περισσότερο από τις παραβιάσεις ασφαλείας σε σχέση με τις λοιπές εταιρίες.

Η ίδια ανάλυση, όπως παραπάνω, πραγματοποιήθηκε χρησιμοποιώντας το μοντέλο τριών-μεταβλητών με τα αποτελέσματα να παρουσιάζονται στον Πίνακα 19 και στον Πίνακα 20 για τις εταιρίες τεχνολογίας και τις λοιπές εταιρίες αντιστοίχως. Παρατηρείται για μία ακόμα φορά, ότι η χρήση του πολυμεταβλητού μοντέλου ανάλυσης παράγει εντελώς διαφοροποιημένα αποτελέσματα από το μοντέλο μίας μεταβλητής. Το μέσο CAR είναι αρνητικό για όλα τα παράθυρα ανάλυσης και για τα δύο δείγματα. Επιπροσθέτως, το παράθυρο ανάλυσης [-1,0] παράγει αποτελέσματα με έντονη στατιστική σημαντικότητα για τις εταιρίες τεχνολογίας, όπως και στην περίπτωση του CAPM. Η διαφοροποίηση εδώ σε σχέση με το CAPM, αφορά το αποτέλεσμα για τις εταιρίες εκτός του τεχνολογικού τομέα όπου παρουσιάζει αρνητική επίπτωση σε συνδυασμό με αδύναμη στατιστική σημαντικότητα. Στην περίπτωση του CAPM έχουμε θετικό αποτέλεσμα και καθόλου στατιστική σημαντικότητα. Για μία ακόμα φορά προκύπτει πως το μοντέλο πολλών μεταβλητών οδηγεί σε περισσότερο αξιόπιστα αποτελέσματα.

Πίνακας 17: CAPM - Ανάλυση τομέα εταιριών τεχνολογίας

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	23	-0,0048	-0,6499	0,2584
[-1,0]	23	-0,0042	-3,1701	0,0009
[0,0]	23	0,0006	0,1417	0,5563
[0,1]	23	0,0000	0,0037	0,5015

Πίνακας 18: CAPM - Ανάλυση εταιριών εκτός τομέα τεχνολογίας

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	82	0,0036	0,8146	0,7916
[-1,0]	82	0,0004	0,1395	0,5554
[0,0]	82	-0,0005	-0,2131	0,4158
[0,1]	82	0,0027	0,7359	0,7685

Συγκεκριμένα, έχουμε μέση οικονομική επίπτωση για τις εταιρίες τεχνολογίας ίση με 0,45% και αντίστοιχη επίπτωση για τις λοιπές εταιρίες ίση με 0,37%. Με άλλα λόγια η επίπτωση μίας παραβίασης ασφαλείας εκτιμάται ότι επιρρεάζει τον τεχνολογικό τομέα περισσότερο κατά 21,6% σε σχέση με το σύνολο της υπόλοιπης οικονομίας.

Πίνακας 19: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση τομέα εταιριών τεχνολογίας

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	23	-0,0018	-0,2500	0,4015
[-1,0]	23	-0,0045	-3,4765	0,0003
[0,0]	23	-0,0031	-0,7404	0,2302
[0,1]	23	-0,0004	-0,0663	0,4736

Πίνακας 20: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση εταιριών εκτός τομέα τεχνολογίας

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	82	-0,0022	-0,5177	0,3027
[-1,0]	82	-0,0037	-1,3951	0,0826
[0,0]	82	-0,0033	-1,3676	0,0868
[0,1]	82	-0,0018	-0,5127	0,3045

Λαμβάνοντας υπόψη την μέση κεφαλαιοποίηση του τεχνολογικού τομέα και των υπολοίπων, η οικονομική επίπτωση που υπολογίζεται με βάση το CAPM, για τις εταιρίες τεχνολογίας ανέρχεται σε $68 εκατομμύρια ενώ για τις λοιπές δεν είναι αρνητική όπως παρουσιάζεται και στον Πίνακα 21. Το αποτέλεσμα αυτό καταδεικνύει ότι στην περίπτωση του CAPM, τα γενικότερα αποτελέσματα οδηγούνται από τις εταιρίες τεχνολογίας. Στην περίπτωση του μοντέλου τριών-μεταβλητών, το επίπεδο οικονομικής επίπτωσης υπολογίζεται σε $73 εκατομμύρια το οποίο είναι πολύ κοντά με το αντίστοιχο επίπεδο επίπτωσης που υπολογίστηκε μέσω του CAPM. Η διαφορά στην οικονομική επίπτωση των παραβιάσεων ασφαλείας μεταξύ των δύο υποσυνόλων εταιριών, στη περίπτωση του πολυμεταβλητού μοντέλου, είναι αρκετά μικρότερη καθώς το κόστος για τις εταιρίες εκτός τομέα τεχνολογίας υπολογίζεται σε $66 εκατομμύρια. Το αποτέλεσμα που παρουσιάζεται στον Πίνακα 21, αναφορικά με το παράθυρο ανάλυσης [0,0], έχει αδύναμη στατιστική σημαντικότητα και δεν υπάρχει συγκρίσιμο μέγεθος για τις εταιρίες τεχνολογίας. Συνεπώς δεν μπορούμε να το χρησιμοποιήσουμε προκειμένου να εξάγουμε συμπεράσματα.

Πρέπει να αναφερθεί πως το δείγμα τεχνολογικού τομέα που χρησιμοποιήθηκε περιείχε 23 παρατηρήσεις το οποίο είναι αρκετά μικρότερο σε σχέση με το δείγμα λοιπών εταιρών που περιείχε 82 παρατηρήσεις. Το μέγεθος του πρώτου δείγματος είναι πιθανόν να οδηγήσει σε αποκλίσεις από την κανονικότητα για την κατανομή των καταλοίπων. Επομένως, το δείγμα που χρησιμοποιήθηκε από την παρούσα έρευνα, παρότι είναι από τα μεγαλύτερα που έχουν δημιουργηθεί, όταν διασπάται σε υπό-δείγματα με βάση τον τομέα οικονομίας οδηγεί σε σύνολα δεδομένων που πιθανότατα δεν καλύπτουν τις στατιστικές απαιτήσεις για την παραδοχή κανονικότητας στην κατανομή των δεδομένων. Αυτό το πρόβλημα υφίσταται και σε άλλες μελέτες με μεγάλο συνολικό δείγμα όπως η πρόσφατη μελέτη από τους Yayla et. al. Στην μελέτη

αυτή παρότι το συνολικό δείγμα ανέρχεται σε 123 παρατηρήσεις, το υπό-δείγμα των εταιριών ηλεκτρονικού εμπορίου ανέρχεται σε 23 και το υπό-δείγμα των εταιριών τεχνολογίας σε 38. Τα δείγματα αυτά είναι επίσης μικρά γεγονός που οδηγεί σε πιθανότητα αποκλίσεων των κατανομών από την κανονικότητα. Η παραπάνω μελέτη καταλήγει, για την περίοδο 1994 – 2006, ότι οι εταιρίες ηλεκτρονικού εμπορίου και τεχνολογίας γενικότερα δέχθηκαν μεγαλύτερη επίπτωση από τις παραβιάσεις ασφαλείας σε σχέση με τις λοιπές εταιρίες. Η μελέτη της παρούσας διατριβής επιβεβαιώνει εμπειρικά ότι το φαινόμενο αυτό συνεχίζει να υφίσταται αλλά πλέον με μία αποκλιμάκωση της διαφοράς στα τελευταία έτη. Το τελευταίο συμπέρασμα είναι ανάλογο με αυτό της ενότητας 5.7.1 σχετικά με την διαπίστωση σταδιακής ωρίμανσης των αγορών στον χειρισμό πληροφόρησης που αφορά γεγονότα παραβίασης ασφαλείας.

Πίνακας 21: Εκτιμήσεις οικονομικής απώλειας για παράθυρα ανάλυσης με στατιστική σημαντικότητα

Δείγμα	CAPM		Fama-French 3-factor model	
Γενικό δείγμα	-		[-1,0]	[0,0]
	-		-68	-57
Εταιρίες τεχνολογίας	[-1,0]	-	[-1,0]	-
	-68		-73	-
Εταιρίες εκτός τεχνολογικού τομέα	-		[-1,0]	[0,0]
	-		-66	-59

5.7.3 Ανάλυση με κριτήριο το μέγεθος της παραβίασης ασφάλειας

Προκειμένου για την ανάλυση της τρίτης υπόθεσης, το δείγμα χωρίστηκε σε τρία υπό-δείγματα με κριτήριο το μέγεθος των περιστατικών ασφαλείας όπως αυτό ορίστηκε στην ενότητα 5.6.3. Το πρώτο δείγμα περιελάμβανε τα περιστατικά ασφαλείας που εξέθεσαν μέχρι 100.000 εγγραφές. Το μέγεθος του ανήλθε στις 48 παρατηρήσεις το οποίο ήταν αρκετά ικανοποιητικό από στατιστικής πλευράς. Οι παραβιάσεις ασφαλείας, που αφορούν περισσότερες των 100.000 εγγραφών, χαρακτηρίζονται ως καταστροφικές και εκτός των συνηθισμένων ορίων στα πλαίσια των οποίων κυμαίνεται ένα μέσο περιστατικό σύμφωνα με συμβουλευτικούς οργανισμούς που σχετίζονται με την ασφάλεια όπως η Ponemon Institute. Επίσης, περιστατικά που αφορούν την έκθεση άνω των

1000 εγγραφών θεωρούνται μεγάλα και ικανά να προκαλέσουν σημαντικές οικονομικές επιπτώσεις σε έναν οργανισμό. Στο δείγμα που χρησιμοποιήθηκε το μικρότερο περιστατικό αφορούσε την έκθεση 1.500 εγγραφών. Προκειμένου να υφίσταται συνοχή με τις μελέτες των συγκεκριμένων οργανισμών, που αναλύθηκαν στο κεφάλαιο 4, επιλέχτηκε αυτό το όριο για τον διαχωρισμό του δείγματος.

Το δεύτερο δείγμα περιελάμβανε τα περιστατικά ασφαλείας που εξέθεσαν από 100.000 έως 1.000.000 εγγραφές. Το μέγεθος του δεν ήταν ικανοποιητικό καθώς περιελάμβανε μόνο 13 παρατηρήσεις. Το τρίτο δείγμα περιελάμβανε τα περιστατικά ασφαλείας που οδήγησαν σε έκθεση άνω των 1.000.000 εγγραφών. Αναλόγως με το δεύτερο δείγμα, το μέγεθος και του τρίτου δείγματος, ίσο με 17 παρατηρήσεις, ήταν αρκετά μικρό από στατιστικής πλευράς. Συναντάμε το ίδιο πρόβλημα, που διαπιστώθηκε στην ενότητα 5.7.2, όπου το συνολικό δείγμα πάλι διαχωρίστηκε σύμφωνα με κάποιο κριτήριο. Το συμπέρασμα είναι κοινό και αναφέρεται στην αναγκαιότητα χρήσης ακόμα μεγαλύτερων δειγμάτων προκειμένου για την διατήρηση σε ισχύ των στατιστικών παραδοχών και την διατήρηση της εγκυρότητας των αποτελεσμάτων.

Η ανάλυση της συγκεκριμένης υπόθεσης έγινε αρχικώς με την χρήση και των δύο μοντέλων αποτίμησης επενδυτικών κεφαλαίων. Επιλέχθηκε στην συνέχεια να γίνει χρήση των αποτελεσμάτων, που προέρχονται από το μοντέλο τριών-μεταβλητών προκειμένου για την ανάλυση της συγκεκριμένης στατιστικής υπόθεσης καθώς, για τους λόγους που αναφέρθηκαν στις ενότητες 5.7.1 και 5.7.2, τα αποτελέσματα που εξάγονται με την χρήση αυτού του μοντέλου είναι πιο αξιόπιστα. Τα αποτελέσματα, που προέρχονται από την χρήση του CAPM, μπορούν να βρεθούν στο παράρτημα V.

Στον Πίνακα 22 αποτυπώνονται τα στατιστικά αποτελέσματα για τα περιστατικά ασφαλείας με έκθεση, σε κίνδυνο παραβίασης εμπιστευτικότητας, έως 100.000 εγγραφών. Το μέσο CAR είναι αρνητικό σε κάθε παράθυρο ανάλυσης αλλά με εξαιρετικά ασθενή στατιστική σημαντικότητα, στο επίπεδο του 20%, για τα παράθυρα ανάλυσης [-1,0] και [0,0]. Στον Πίνακα 23 αποτυπώνονται τα αντίστοιχα αποτελέσματα που αφορούν περιστατικά με αριθμό εγγραφών μεταξύ 100.000 και 1.000.000. Τα αποτελέσματα είναι ενάντια προς τα αναμενόμενα καθώς το μέσο CAR είναι θετικό για κάθε παράθυρο ανάλυσης. Παρόμοια αποτελέσματα απέδωσε η ανάλυση του τρίτου δείγματος, που αφορά περιστατικά με εμπλεκόμενες εγγραφές άνω του 1.000.000 και αποτυπώνονται στον Πίνακα 24. Το μειονέκτημα του δεύτερου και τρίτου δείγματος, όπως

αναφέρθηκε και παραπάνω, είναι το σχετικά μικρό μέγεθος τους. Ωστόσο, η διαφορά των αποτελεσμάτων μεταξύ των περιστατικών που αφορούν περιστατικά κάτω των 100.000 εγγραφών και αυτά που αφορούν περισσότερες εγγραφές είναι αρκετά μεγάλη ώστε να εξάγουμε συμπεράσματα με αρκετή ασφάλεια.

Πίνακας 22: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος περιστατικών προσβολής μέχρι 100.000 εγγραφών

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	48	-0,0048	-0,4851	0,3142
[-1,0]	48	-0,0073	-0,8794	0,1904
[0,0]	48	-0,0057	-0,9864	0,1629
[0,1]	48	-0,0032	-0,4122	0,3404

Πίνακας 23: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος περιστατικών προσβολής 100.000 - 1.000.000 εγγραφών

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	13	0,0046	0,0858	0,5341
[-1,0]	13	0,0075	0,3765	0,6464
[0,0]	13	0,0045	0,9724	0,8337
[0,1]	13	0,0016	0,4161	0,6610

Πίνακας 24: Μοντέλο Fama-French τριών-μεταβλητών - Ανάλυση συνολικού δείγματος περιστατικών προσβολής άνω των 1.000.000 εγγραφών

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	17	0,0015	0,5999	0,7252
[-1,0]	17	0,0023	0,7056	0,7592
[0,0]	17	0,0029	0,4301	0,6661
[0,1]	17	0,0021	0,3332	0,6303

Το βασικό πόρισμα, από την εμπειρική ανάλυση της συγκεκριμένης στατιστικής υπόθεσης, αφορά το συνολικό κόστος μίας παραβίασης ασφαλείας το οποίο δεν αυξάνεται αναλογικά με τον αριθμό των εγγραφών που προσβάλλονται από μία παραβίαση ασφαλείας όταν το περιστατικό αφορά αριθμό εγγραφών άνω των 100.000. Στην πραγματικότητα το έμμεσο κόστος είναι ανεξάρτητο από τον αριθμό των εγγραφών σε κίνδυνο εμπιστευτικότητας, όταν το περιστατικό δεν είναι τυπικού μεγέθους, σε αντίθεση με το άμεσο κόστος που είναι σε ευθεία συνάρτηση με το επίπεδο των εμπλεκόμενων εγγραφών.

Τα αποτελέσματα από την συγκεκριμένη ανάλυση οδηγούν στην εμπειρική επιβεβαίωση διαπιστώσεις που έχουν καταγραφεί στον τύπο σχετικά με συγκεκριμένα περιστατικά παραβίασης ασφαλείας που περιλαμβάνουν έκθεση πολύ μεγάλου όγκου πληροφοριών. Χαρακτηριστική περίπτωση αποτελεί η κλοπή ενός laptop τον Μάιο του 2005 το οποίο περιείχε μία κυβερνητική βάση δεδομένων των ΗΠΑ με προσωπικά δεδομένα 26,5 ανθρώπων. Το μέγεθος της παραβίασης ασφάλειας, σε εγγραφές που εκτέθηκαν, μέχρι τότε ήταν το μεγαλύτερο που είχε συμβεί στον Δημόσιο τομέα των ΗΠΑ. Το άμεσο κόστος ήταν ανάλογο του μεγέθους του αριθμού των εγγραφών καθώς μόνο για την παρακολούθηση των λογαριασμών του τεράστιου αριθμού ανθρώπων που εμπλέκονταν χρειάστηκαν περίπου $160 εκατομμύρια. Το έμμεσο κόστος όμως δεν ήταν ανάλογο. Ο λόγος ήταν το κίνητρο που οδήγησε στην απώλεια των δεδομένων το οποίο οδηγήθηκε από το ίδιο το υλικό και όχι από την πιθανή αξία εκμετάλλευσης των δεδομένων [**97**].

Το παραπάνω περιστατικό, όπως και άλλα ανάλογα, συμφωνεί με το αποτέλεσμα της ανάλυσης της παρούσας ενότητας όπου το έμμεσο κόστος είναι ανεξάρτητο από το μέγεθος ενός περιστατικού ασφαλείας και εξαρτάται από άλλους παράγοντες που δεν έχουν συσχέτιση με τον αριθμό των εγγραφών που εκτίθενται.

Επίσης, τα παραπάνω οδηγούν στην ενδεχόμενη αμφισβήτηση της προσθήκης παραβιάσεων ασφαλείας που προέρχονται από την κλοπή υλικού σε ένα δείγμα ανάλυσης γεγονότων. Η κλοπή δεν είναι απαραίτητο να οδηγεί σε προσπέλαση και εκμετάλλευση των ευαίσθητων δεδομένων που πιθανόν να υφίσταται σε μία κινητή συσκευή καταχώρησης. Σχετικά με το θέμα αυτό δεν έχει μέχρι σήμερα υπάρξει μνεία από τους μελετητές σχετικά με την αντιμετώπιση περιστατικών προερχόμενων από κλοπή υλικού. Το δείγμα στο οποίο βασίστηκε η έρευνα της παρούσας διατριβής, περιείχε 14 περιστατικά κλοπής τα οποία, στο βαθμό που επέτρεπε το εύρος δημοσιότητας του κάθε περιστατικού, αναλύθηκαν προκειμένου να διαπιστωθεί ότι πρόκειται για

πραγματικές παραβιάσεις ασφαλείας. Επίσης ο αριθμός των γεγονότων κλοπής υλικού αντιπροσωπεύει μόνο το 13% του συνολικού δείγματος και συνεπώς η εν δυνάμει αλλοίωση των αποτελεσμάτων είναι αρκετά μικρή.

Επιπλέον, περιστατικά που αφορούν περισσότερες των 100.000 εγγραφών, δεν αφορούν τον μέσο όρο, όπως αναφέρθηκε στην αρχή της συγκεκριμένης ενότητας, και συνεπώς δεν είναι απαραίτητο η συμπεριφορά τους να είναι ανάλογη με ένα μέσο περιστατικό. Η υπόθεση αυτή επιβεβαιώνεται εμπειρικά από την ανάλυση που έγινε με κριτήριο το μέγεθος του περιστατικού. Μπορούμε να αναμένουμε μία αναλογική κλιμάκωση του άμεσου και έμμεσου κόστους ενός περιστατικού το οποίο όμως αφορά προσβολή ενός αριθμού εγγραφών που δεν υπερβαίνουν τις 100.000. Γεγονότα που αφορούν περισσότερες εγγραφές παρουσιάζουν άλλη συμπεριφορά. Το έμμεσο κόστος τους δύναται να είναι είτε εξαιρετικά μικρό σε σχέση με το άμεσο κόστος, όπως στην περίπτωση του κλεμμένου laptop που αναφέρθηκε παραπάνω, είτε εξαιρετικά υψηλό οδηγώντας ένα γεγονός στον χαρακτηρισμό του ως καταστροφικό. Συνεπώς, δεν μπορούμε να υποθέσουμε ανάλογη σχέση μεταξύ αριθμού εκτεθειμένων εγγραφών και κόστους σε αυτού του είδους τα περιστατικά.

Εκτενέστερη ανάλυση της σχέσης μεταξύ του μεγέθους ενός περιστατικού ασφαλείας και του επιπέδου οικονομικής επίπτωσης που επιφέρει πραγματοποιείται στο κεφάλαιο 7. Τέλος, τα συμπεράσματα της συγκεκριμένη παραγράφου αποτελούν εμπειρική επιβεβαίωση των όσων αναφέρονται στον εννοιολογικό προσδιορισμό, που δίνεται στην ενότητα 4.2, για τα περιστατικά παραβιάσεων ασφαλείας.

5.8 Συμπεράσματα

Η μελέτη που αναλύθηκε στο παρόν κεφάλαιο διερεύνησε την επίπτωση που έχουν οι ανακοινώσεις παραβιάσεων ασφαλείας στην χρηματιστηριακή αξία ενός οργανισμού. Η επίδραση ενός περιστατικού παραβίασης ασφαλείας, στην αγοραία αξία κεφαλαιοποίησης ενός οργανισμού, θεωρείται ως ένα αντιπροσωπευτικό μέτρο του συνολικού κόστους που θα επιφέρει το συγκεκριμένο περιστατικό στο βραχυπρόθεσμο και μακροπρόθεσμο ορίζοντα. Η ποσοτικοποίηση της οικονομικής επίπτωσης που επιφέρουν οι παραβιάσεις ασφαλείας είναι πολύ σημαντική για την λήψη αποφάσεων, σε αντικειμενική βάση, σχετικά με το κεφάλαια που πρέπει να επενδυθούν στην ασφάλεια ΠΣ. Η επίπτωση κινδύνου μπορεί να ποσοτικοποιηθεί με αντικειμενικότητα

οδηγώντας σε περισσότερο αξιόπιστες προσεγγίσεις σχετικά με το συνολικό επίπεδο των κινδύνων ΠΣ από παραβιάσεις ασφαλείας όπως αυτό αναλύεται στο κεφάλαιο 7.

Σύμφωνα με την έρευνα που διεξήχθη, η παρούσα μελέτη είναι η πρώτη που ανάλυσε την επίδραση των περιστατικών ασφαλείας στην εταιρική αξία για την περίοδο 2008 – 2011. Η περίοδος αυτή χαρακτηρίστηκε από ραγδαία αύξηση των επιθέσεων στον κυβερνοχώρο και παράλληλα από αύξηση στην πολυπλοκότητα και ανωτερότητα των μέσων επίθεσης. Το τελευταίο έτος ανάλυσης έχει χαρακτηριστεί ως "year of the hack" αποτυπώνοντας την σημαντικότητα που έχει πλέον αποκτήσει το συγκεκριμένο ζήτημα [**98**]. Ωστόσο, στην περίοδο αυτή οι αγορές παρουσίασαν ιδιαιτέρως υψηλή διακύμανση ως αποτέλεσμα της παγκόσμιας οικονομικής Κρίσης. Παρόλο που η συγκεκριμένη διαπίστωση δεν ανατρέπει τα αποτελέσματα της μεθοδολογίας ανάλυσης γεγονότων, μειώνει την στατιστική εγκυρότητα τους. Είναι επιθυμητό επομένως μελλοντική έρευνα να επιδιώξει την χρήση ενός ακόμα μεγαλύτερου δείγματος.

Η συνολική μέση οικονομική επίπτωση, από ένα περιστατικό παραβίασης ασφαλείας, λαμβάνοντας υπόψη το συνολικό δείγμα, υπολογίζεται μεταξύ των $57 - $68 εκατομμυρίων. Το δείγμα που περιλαμβάνει τις εταιρίες τεχνολογίας παρουσιάζει ένα μέσο κόστος που κυμαίνεται μεταξύ $68 - $73 εκατομμυρίων. Το κόστος αυτό υπολογίζεται ως υπέρτερο, σε σχέση με το κόστος για τις λοιπές εταιρίες, κατά $7 εκατομμύρια ανά περιστατικό. Τα αποτελέσματα της συγκεκριμένης έρευνας είναι σύμφωνα με την θεωρεία και τα μεγέθη σε χρηματικούς όρους είναι σημαντικά. Αξίζει να σημειωθεί πως με την χρήση των μέσω τιμών κεφαλαιοποίησης τα αποτελέσματα κόστους είναι πολύ μεγαλύτερα αλλά για τους λόγους που αναφέραμε στην ενότητα 5.4.4 προτιμήθηκε η χρήση της διαμέσου.

Τα αποτελέσματα, συγκρινόμενα με προγενέστερες ανάλογες μελέτες, καταδεικνύουν το γεγονός ότι οι αγορές έχουν σταδιακά, την τελευταία δεκαετία, γίνει λιγότερο ευαίσθητες σε πληροφορίες σχετιζόμενες με περιστατικά παραβίασης ασφαλείας και ότι γενικά έχουν ανέλθει σε πολύ μεγαλύτερο επίπεδο ωρίμανσης σχετικά με την αντίδραση τους σε τέτοιου είδους γεγονότα. Ωστόσο οι μέσες οικονομικές επιπτώσεις είναι αρκετά σημαντικές και οι οργανισμοί οφείλουν να τις λαμβάνουν σοβαρά υπόψη τους στις αποφάσεις τους σχετικά με τις επενδύσεις στην ασφάλεια ΠΣ. Περεταίρω, παρατηρώντας τα χαρακτηριστικά των γεγονότων στο παράρτημα ΙΙ, διακρίνουμε συγκεκριμένα περιστατικά όπου μόνο το άμεσο υπολογιζόμενο κόστος είναι τεράστιο και σε

κάποιες περιπτώσεις ανέρχεται σε σημαντικό ποσοστό της συνολικής αξίας κεφαλαιοποίησης ενός οργανισμού.

Το περιστατικό με α/α 66 που αφορούσε την Sony οδήγησε σε παραβίαση της εμπιστευτικότητας 24,6 εκατομμυρίων εγγραφών. Το άμεσο κόστος υπολογίστηκε στο ποσό των $1,47 δις το οποίο αποτελούσε το 7% της χρηματιστηριακής αξίας της εταιρίας κατά την στιγμή του συμβάντος. Περίπου 7% άμεσο κόστος δέχθηκε και η εταιρία SAIC στο περιστατικό με α/α 92. Υπάρχουν επίσης περιπτώσεις που απειλήθηκε η ίδια η ύπαρξη ενός οργανισμού ή ο οργανισμός οδηγήθηκε στην χρεοκοπία. Στο περιστατικό με α/α 29 η Heartland payment systems επωμίστηκε μία τεράστια προσβολή ασφαλείας όπου η εμπιστευτικότητα 130 εκατομμυρίων εγγραφών παραβιάστηκε. Υπολογίζεται ότι ο οργανισμός δέχθηκε ως άμεση οικονομική απώλεια από το συμβάν το ποσό των $7,8 δις το οποίο αποτελούσε επτά φορές την κεφαλαιοποίηση του. Σε άλλο περιστατικό η θυγατρική DigiNotar της εταιρίας Vasco δέχθηκε μία πολύ σοβαρή παραβίαση ασφαλείας η οποία τελικά την οδήγησε στην χρεοκοπία.

Συμπερασματικά, το γεγονός ότι οι αγορές πλέον έχουν ωριμάσει και η οικονομική απώλεια των περιστατικών ασφαλείας έχει περιοριστεί δεν πρέπει να καθησυχάζει τις διοικήσεις των εταιριών καθώς πάντα υπάρχει η πιθανότητα ενός πολύ σοβαρού περιστατικού που μπορεί να θέσει σε κίνδυνο τα ίδια τα θεμέλια του οργανισμού. Η πιθανότητα ακραίων περιστατικών που μπορεί να δεχθεί κάθε οργανισμός οδηγεί σε μεγάλο βαθμό το συνολικό μέγεθος των κινδύνων παραβιάσεων ασφαλείας όπως αναλύεται διεξοδικά στο κεφάλαιο 7.

Στο συγκεκριμένο κεφάλαιο αναλύθηκαν τα ανάμεικτα αποτελέσματα που προέρχονται από σχετικές μελέτες προτείνοντας έναν αριθμό αιτιάσεων. Τα αποτελέσματα της παρούσα έρευνας υποδεικνύουν πως η χρήση του CAPM, σε συνδυασμό με ένα πολυμεταβλητό μοντέλο όπως το μοντέλο τριών-μεταβλητών των Fama-French, μπορεί να αποδώσει τελείως διαφορετικά συμπεράσματα για το ίδιο σύνολο δεδομένων. Τα πολυμεταβλητά μοντέλα αποδίδουν πιο αξιόπιστα αποτελέσματα τα οποία επεξηγούν με μεγαλύτερη σαφήνεια τις τιμές των μετοχών. Επιπρόσθετα, η διαφορετική προσέγγιση από την ακαδημαϊκή κοινότητα συγκεκριμένων τύπων παραβίασης ασφαλείας, όπως επιθέσεις ιών, έχει οδηγήσει επίσης σε ανάμικτα αποτελέσματα. Για παράδειγμα η μελέτη των Gordon et. al. [**82**] έχει ένα δείγμα από 121 περιστατικά εκ των οποίων τα 51 είναι επιθέσεις ιών. Αντιθέτως, η μελέτη των Yayla et. al. [**77**] δεν δέχεται ότι τα συγκεκριμένα περιστατικά μπορούν να εξεταστούν από μία μελέτη ανάλυσης γεγονότων και τα

εξαιρούν. Η διαφοροποίηση αυτή στην μεθοδολογία σύνθεσης του δείγματος μπορεί να οδηγήσει δύο μελέτες σε πολύ διαφορετικά συμπεράσματα.

Σχετικά με την περίοδο ανάλυσης, οι περισσότερες μελέτες χρησιμοποίησαν περιόδους οι οποίες υπερέβαιναν τα πέντε έτη και έφτασαν το ανώτερο μέχρι το 2009. Η μελέτη αυτή χρησιμοποίησε μία σχετικά στενή χρονική περίοδο τεσσάρων ετών καλύπτοντας το κενό που υπήρχε από τις υφιστάμενες μελέτες, αναφορικά με την ανάλυση των τελευταίων ετών, προκειμένου να αποσαφηνιστεί η σταδιακή διαμόρφωση του τρόπου με τον οποίο οι αγορές μεταχειρίζονται τα περιστατικά παραβίασης ασφαλείας.

Το κύριο αποτέλεσμα της ερευνητικής προσπάθειας, που αναλύθηκε στο συγκεκριμένο κεφάλαιο, είναι οι σαφείς ενδείξεις ωρίμανσης των αγορών σχετικά με τον χειρισμό περιστατικών παραβίασης ασφαλείας και η σταθεροποίηση της μέσης οικονομικής επίπτωσης κάθε συμβάντος σε ένα συγκεκριμένο εύρος κόστους. Η χρήση ενός ακόμα μεγαλύτερου δείγματος συμβάντων θα πρέπει να χρησιμοποιηθεί από μελλοντικές ερευνητικές προσεγγίσεις του θέματος προκειμένου για την ισχυρότερη διασφάλιση της παραδοχής κανονικότητας των κατανομών των ασυνήθη αποδόσεων και κυρίως για την μείωση της επίδρασης που ενέχει η εξαιρετική διακύμανση που χαρακτηρίζει τις παγκόσμιες αγορές τα τελευταία χρόνια.

Μεγάλες και φημισμένες επιχειρήσεις όπως η Symantec [**99**] αναγκάζονται πλέον να δημοσιεύσουν παλιότερα και νέα περιστατικά παραβίασης ασφαλείας που επωμίστηκαν τα ΠΣ τους. Στις ΗΠΑ από το 2004 περισσότερες από 45 πολιτείες έχουν θεσπίσει νόμους που επιβάλουν στους οργανισμούς την δημόσια ανακοίνωση περιστατικών ασφαλείας. Μόνο το 2008 περισσότερες από 18 πολιτείες των ΗΠΑ θέσπισαν νομοθεσία σχετικά με τις παραβιάσεις ασφαλείας [**100**]. Είναι επίσης χαρακτηριστική η πρόσφατη ρυθμιστική κίνηση στην οποία προχώρησε η επιτροπή κεφαλαιαγοράς των ΗΠΑ (SEC) κατά την οποία οι εισηγμένες εταιρίες υποχρεούνται να ανακοινώνουν δημόσια ακόμα και πιθανά περιστατικά παραβίασης ασφαλείας [**101**]. Ανάλογη τάση παρατηρείται και σε άλλες προηγμένες χώρες με πλέον μεγάλη εξάρτηση στα ΠΣ. Οι εξελίξεις αυτές αναμένεται να αυξήσουν περεταίρω το ποσοστό των περιστατικών ασφαλείας που δημοσιεύεται και να δώσουν συνεπώς την δυνατότητα σύνθεσης, στις μελέτες ανάλυσης γεγονότων, περισσότερο ολοκληρωμένων δειγμάτων. Περισσότερο ολοκληρωμένα δείγματα θα δώσουν την δυνατότητα προσέγγισης, με μεγαλύτερη εγκυρότητα, του ακριβές μεγέθους των οικονομικών επιπτώσεων που επιφέρουν τα περιστατικά ασφαλείας.

Η αυξανόμενη δημοσιότητα ομάδων «χακτιβιστών» (hacktivists) όπως οι Anonymous και LuzSec διαμορφώνουν μία μεγαλύτερη αντίληψη των αγορών σχετικά με το πραγματικό μέγεθος των κινδύνων που εγκυμονούν οι παραβιάσεις ασφαλείας. Παράλληλα με την αύξηση των επιπέδων δημοσίευσης των περιστατικών ασφαλείας από τους οργανισμούς, αναμένεται παράλληλα περαιτέρω αύξηση του επιπέδου ωρίμανσης των αγορών και αυτό θα αποτυπωθεί από μελλοντικές μελέτες πάνω στις χρηματιστηριακές αποδόσεις των προσβεβλημένων εταιριών.

6 Μέτρηση του επιπέδου ασφαλείας με την χρήση στοχαστικών μεθόδων

6.1 Εισαγωγή

Η μέτρηση μεγεθών μέσω της χρήσης στοχαστικών μεθόδων πραγματοποιείται εδώ και αρκετά χρόνια σε αρκετά πεδία ενδιαφέροντος της Οικονομικής Επιστήμης και κυρίως στην μελέτη της διαχείρισης κινδύνων. Τα εργαλεία της στοχαστικής ανάλυσης είναι ιδιαιτέρως σημαντικά στην μαθηματική μοντελοποίηση των οικονομικών φαινομένων. Η σημαντικότητα αυτή προέρχεται από το γεγονός ότι οι στοχαστικές μέθοδοι λαμβάνουν την παραδοχή ότι η λειτουργία των οικονομικών αγορών συνθέτεται από ένα σύνολο τυχαίων φαινομένων. Χαρακτηριστικό παράδειγμα αποτελεί η μοντελοποίηση της τιμολόγησης των παραγώγων προϊόντων δικαιώματος προαίρεσης (options) των Black-Scholes και του Merton τα οποία ουσιαστικά έδωσαν άλλες διαστάσεις στην χρηματοοικονομική επιστήμη και άλλαξαν ριζικά τον τρόπο προσέγγισης των οικονομικών μεγεθών.

Οι παραβιάσεις ασφαλείας δείχνουν να ακολουθούν τυχαία μοτίβα μέσα στον χρόνο όπως συμβαίνει με τις οικονομικές μεταβλητές. Τα επιτόκια, οι συναλλαγματικές ισοτιμίες και οι τιμές των μετοχών ακολουθούν στο σύνολο τους τυχαία μοτίβα των οποίων η συμπεριφορά έχει επιχειρηθεί να αναλυθεί μέσω της χρήσης στοχαστικών μεθόδων. Εργαλεία όπως η κίνηση Brown, η οποία έχει χρησιμοποιηθεί για την περιγραφή του «τυχαίου περίπατου» που ακολουθούν οι μετοχές, και η στοχαστική ολοκλήρωση μπορούν να εφαρμοστούν στην ποσοτικοποίηση της ασφάλειας των ΠΣ.

Στο κεφάλαιο αυτό αναλύεται η χρήση στοχαστικών μεθόδων προκειμένου για την αντικειμενική και ακριβέστερη ποσοτικοποίηση του επιπέδου ασφαλείας ενός ΠΣ. Οι υφιστάμενες προσεγγίσεις για την ποσοτικοποίηση της ασφάλειας, βασίζονται κατά κύριο λόγο σε δεδομένα ποιοτικής φύσεως τα οποία είναι προϊόν υποκειμενικής κρίσης. Η μεθοδολογία που αναπτύσσεται στην παρούσα μελέτη βασίζεται σε ποσοτικά αποτελέσματα που προέρχονται από κατάλληλη και αντικειμενική επεξεργασία των ιστορικών δεδομένων που αφορούν τις ευπάθειες λογισμικού.

Οι ευπάθειες αποτελούν το βασικό δομικό στοιχείο του επιπέδου ασφαλείας ενός συστήματος. Χωρίς την ύπαρξη ευπαθειών, στα συστατικά μέρη ενός συστήματος, δεν θα υπήρχε λόγος να προσεγγιστεί το επίπεδο ασφαλείας καθώς δεν θα υπήρχαν κίνδυνοι. Η βασική ιδέα είναι πως κάθε ευπάθεια αποτελείται από μία σειρά τυχαίων γεγονότων που συντελούνται μέσα στα στάδια του κύκλου ύπαρξης της. Το τυχαίο αυτό γεγονός θεωρούμε ότι ακολουθεί έναν «τυχαίο περίπατο» κατά αναλογία – όπως προαναφέρθηκε – με τις οικονομικές μεταβλητές και δύναται να προσομοιωθεί μέσω της κίνησης Brown.

Επεκτείνοντας την εστίαση στο επίπεδο του συστατικού στοιχείου ενός συστήματος, η ολότητα των ευπαθειών που εμφανίζονται μπορούν να αναλυθούν ως μία συνολική σειρά τυχαίων γεγονότων η οποία μπορεί να προσδιορισθεί επίσης μέσω της κίνησης Brown. Η ανάλυση του συνόλου των συστατικών στοιχείων ενός συστήματος η οποία επιτυγχάνεται μέσω στοχαστικής ολοκλήρωσης μπορεί να οδηγήσει στην προσέγγιση του επιπέδου ασφαλείας που παρουσιάζει ένα σύστημα σε μία δεδομένη χρονική περίοδο.

Στην επόμενη ενότητα αναλύεται η θεωρεία της εντροπίας πληροφόρησης η οποία χρησιμοποιήθηκε προκειμένου να λυθεί το πρόβλημα της αντικειμενικής προσέγγισης του συντελεστή βαρύτητας που έχει κάθε συστατικό στοιχείο ενός συστήματος στον προσδιορισμό του επιπέδου ασφαλείας. Στην συνέχεια αναλύονται οι μηχανισμοί καταχώρησης ευπαθειών ανοικτού κώδικα που χρησιμοποιήθηκαν προκειμένου να αντληθούν τα απαραίτητα δεδομένα για την ανάπτυξη του μοντέλου και την εμπειρική επιβεβαίωση του. Στην επόμενη ενότητα γίνεται συνοπτική ανάλυση των υφιστάμενων μεθοδολογιών ποσοτικοποίησης του επιπέδου ασφαλείας ενός συστήματος και της έννοιας του τεχνικού παράγοντα κινδύνου που αποτελεί την βάση για την προτεινόμενη μεθοδολογία. Στις επόμενες τρεις ενότητες αναλύεται η σταδιακή ανάπτυξη του προτεινόμενου μοντέλου. Τέλος, στην τελευταία ενότητα αναφέρονται τα συμπεράσματα από το σύνολο της ερευνητικής εργασίας που παρουσιάζεται στο παρόν κεφάλαιο.

6.2 Βάσεις καταχώρησης ευπαθειών και η χρήση τους στην μεθοδολογία

Οι βάσεις δεδομένων στις οποίες καταχωρούνται και ανακοινώνονται καθημερινά νέες ευπάθειες, καθώς και το γενικό πλαίσιο λειτουργίας τους, ορίζονται ως μηχανισμοί καταχώρησης ευπαθειών (reporting vulnerabilities mechanisms). Οι βάσεις αυτές υποστηρίζονται και

συντηρούνται είτε από ιδιωτικούς φορείς που συνήθως ασχολούνται με την παραγωγή λογισμικού, είτε από μη κοινωφελείς οργανισμούς όπως είναι οι Open Security Foundation, Security Focus, National Vulnerabilities Database και ο MITRE.

Καθώς η παρούσα ερευνητική προσπάθεια εστίασε αποκλειστικά στις βάσεις που προέρχονται από μη κοινωφελής οργανισμούς η ανάλυση επικεντρώνεται σε αυτές. Στην επόμενη παράγραφο αναφέρονται οι βάσεις που χρησιμοποιήθηκαν και τα βασικά χαρακτηριστικά που οδήγησαν στην επιλογή τους. Οι επόμενες δύο παράγραφοι αφιερώνονται στην ανάλυση κάθε μίας από της βάσεις και των ιδιαίτερων χαρακτηριστικών τους ενώ η τελευταία παράγραφος περιγράφει τον τύπο των δεδομένων που χρησιμοποιήθηκε για την έρευνα.

6.2.1 Βάσεις καταχώρησης ευπαθειών ανοικτού κώδικα

Σημαντική κατηγορία βάσεων καταχώρησης ευπαθειών είναι οι λεγόμενες ανοικτού κώδικα (open source) οι οποίες είναι αποτελέσματα μη κερδοσκοπικών εγχειρημάτων και είναι προσβάσιμες στο ευρύ κοινό. Στην παρούσα ερευνητική προσπάθεια αντλήθηκαν δεδομένα από τις δύο μεγαλύτερες, και περισσότερο αναγνωρισμένες παγκοσμίως βάσεις ανοικτού κώδικα, οι οποίες είναι η Open Source Vulnerability Database (OSVDB) και η National Vulnerability Database (NVD). Οι δύο αυτές βάσεις, εκτός του ότι είναι ανοικτού κώδικα, έχουν άλλα δύο σημαντικά κοινά χαρακτηριστικά τα οποία αποτέλεσαν βασικά κριτήρια για την επιλογή τους κατά την διάρκεια της έρευνας.

(α) Το πρώτο κοινό χαρακτηριστικό αφορά την υποστήριξη του μηχανισμού καταγραφής ευπαθειών Common Vulnerabilities and Exposures (CVE) και κατά συνέπεια την καταχώρηση ευπαθειών τύπου CVE. Ο CVE είναι ένας μηχανισμός καταχώρησης μέσω του οποίου εξελίσσεται διαρκώς μία ενοποιημένη λίστα με τυποποιημένα ονόματα ευπαθειών και εκθέσεων κινδύνου με σκοπό την βελτίωση αναγνώρισης, εύρεσης και αντιμετώπισης τους. Ο φορέας που υλοποιεί το συγκεκριμένο μη εμπορικό εγχείρημα δημιουργίας ενός κοινού συστήματος ονομασίας ευπαθειών και εκθέσεων είναι ο μη κερδοσκοπικός οργανισμός MITRE. Στην δημιουργία του CVE και στην συνεχή ενημέρωση του συμβάλουν πρωτεργάτες της κοινότητας ασφάλειας ΠΣ, εταιρίες δημιουργίας λογισμικού και ερευνητές. Η λίστα CVE (CVE List) περιλαμβάνει μοναδικές καταχωρήσεις ευπαθειών και εκθέσεων κινδύνου όπου κάθε

μία καταχώρηση αποτελείται από έναν μοναδικό κωδικό ονομασίας, περιγραφή και αναφορά παραπομπών.

(β) Το δεύτερο σημαντικό κοινό χαρακτηριστικό των δύο βάσεων είναι η χρήση του συστήματος βαθμολόγησης ευπαθειών CVSS για το οποίο έγινε αναφορά στην ενότητα 2.4.2.1. Το CVSS v2 είναι το πλέον αναγνωρισμένο σύστημα βαθμολόγησης ευπαθειών και η μεθοδολογία που ακολουθείται θεωρείται επαρκώς αμερόληπτη και αντικειμενική. Επομένως, η επακόλουθη χρήση των δεδομένων καταγραφής ευπαθειών από τις συγκεκριμένες βάσεις, προκειμένου για την μέτρηση και μοντελοποίηση μεγεθών που αφορούν τις ευπάθειες, διατήρησε την απαιτούμενη αντικειμενικότητα στα τελικά αποτελέσματα το οποίο αποτελούσε τον βασικό στόχο του συνόλου της έρευνας.

6.2.2 Η βάση ανοικτού κώδικα OSVDB

Η OSVDB είναι, κατά την διάρκεια συγγραφής του παρόντος, η μεγαλύτερη βάση ανοικτού κώδικα και δημιουργήθηκε το 2002 από παράγοντες της αγοράς με σκοπό την παροχή αμερόληπτης και ακριβής πληροφόρησης σχετικά με τις ευπάθειες των ΠΣ [**102**]. Προκειμένου για την εξασφάλιση επαρκούς υποστήριξης του εν λόγο εγχειρήματος, δημιουργήθηκε το 2005 ο μη κερδοσκοπικός οργανισμός Open Security Foundation (OSF). Το μέγεθος της συγκεκριμένης βάσης είναι τεράστιο αφού καλύπτει λεπτομερώς σχεδόν 82.000 ευπάθειες για πάνω από 45.300 διαφορετικά προϊόντα λογισμικού, μεγέθη τα οποία μεταβάλλονται ανοδικά με σημαντικούς ρυθμούς. Η βάση αυτή υποστηρίζει το πρωτόκολλο καταγραφής τύπου CVE, για το οποίο έγινε αναφορά παραπάνω, από το 2004. Επίσης από το 2009 υιοθετήθηκε η μεθοδολογία βαθμολογίας των ευπαθειών του CVSS v2.

Στην προσπάθεια σύνθεσης του μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας, τα δεδομένα για τις ευπάθειες των προϊόντων λογισμικού που μελετήθηκαν αντλήθηκαν κατά κύριο λόγο από αυτή την βάση. Οι βασικότεροι λόγοι που μας οδήγησαν σε αυτήν την επιλογή αναλύονται παρακάτω:

(α) Ο κυριότερος λόγος επιλογής αυτής της βάσης είναι η παγκόσμια αναγνώριση που έχει επιτύχει το οποίο αποδεικνύεται από τον αριθμό των ερευνητών που παρέχουν σε καθημερινή βάση δεδομένα για την καταχώρηση νέων ευπαθειών. Κατά την στιγμή

συγγραφής του παρόντος, ο αριθμός των συνεργαζόμενων ερευνητών με τον OSF ξεπερνούσε τους 4.700.

(β) Ο δεύτερος λόγος έγκειται στο μέγεθος της βάσης καθώς είναι η μεγαλύτερη βάση ανοικτού κώδικα γεγονός που μας επιτρέπει να υποθέσουμε πως μέσω της μελέτης των δεδομένων της λαμβάνουμε την μέγιστη δυνατή εικόνα για την συνολική συμπεριφορά των ευπαθειών που εμφανίζει κάθε προϊόν λογισμικού.

(γ) Ο τρίτος λόγος έγκειται στην μεθοδολογία καταχώρησης νέων ευπαθειών που την καθιστά την πλέον αντικειμενική και αμερόληπτη βάση του είδους της. Η προϋπόθεση της αντικειμενικότητας ήταν σημαντική καθώς, σε συνδυασμό με τα υπόλοιπα εργαλεία κατασκευής του προτεινόμενου μοντέλου, κατέστη δυνατή η τελική εκροή αντικειμενικών και αμερόληπτων αποτελεσμάτων για την ποσοτικοποίηση του επιπέδου ασφαλείας ενός ΠΣ.

(δ) Βασικός επίσης λόγος επιλογής είναι η ελεύθερη πρόσβαση στην βάση χωρίς κανένα περιορισμό και επομένως τα απαραίτητα δεδομένα για την εφαρμογή του μοντέλου που συνθέσαμε είναι στην διάθεση κάθε ενδιαφερόμενου.

(ε) Τέλος, ένας επιπλέον ευνοϊκός παράγοντας στην χρήση της OSVDB ήταν η σχετική ευκολία άντλησης των στοιχείων που χρειάστηκαν κατά την διάρκεια της έρευνας λόγω του τρόπου κατασκευής της βάσης. Η αναλυτική σύνθεση του σχήματος της βάσης είναι διαθέσιμη στον διαδικτυακό τόπο που την φιλοξενεί το οποίο βοήθησε σε μεγάλο βαθμό την άντληση στοιχείων που πραγματοποιήθηκε.

6.2.3 Η βάση ανοικτού κώδικα NVD

Η δεύτερη βάση καταγραφής ευπαθειών ανοικτού κώδικα που χρησιμοποιήθηκε στα πλαίσια της παρούσας διατριβής ήταν η National Vulnerability Database (NVD). Όπως αναφέρθηκε αρχικώς στην ενότητα 2.4.2.1, η NVD σχεδιάστηκε και λειτουργεί υπό την εποπτεία και ενίσχυση του τμήματος ασφαλείας υπολογιστών του NIST και υποστηρίζεται επικουρικά από το Computer Emergency Readiness Team (CERT) των ΗΠΑ [**37**], [**103**]. Η συγκεκριμένη βάση προσφέρει έναν εξαιρετικό μηχανισμό αναζήτησης ευπαθειών από το 1997. Οι ευπάθειες που καταγράφονται αφορούν αποκλειστικά αυτές που καταχωρούνται στις λίστες του CVE.

Όπως στην περίπτωση της OSVDB, στην συγκεκριμένη βάση οι καταχωρήσεις πραγματοποιούνται κατόπιν αυστηρού ελέγχου των στοιχείων αναφοράς των ευπαθειών. Η ταξινόμηση των ευπαθειών που αντλούνται από το CVE, πραγματοποιείται μέσω του συστήματος βαθμολόγησης ευπαθειών CVSS v2. Το μέγεθος της συγκεκριμένης βάσης είναι αρκετά μεγάλο με της καταγραμμένες ευπάθειες τύπου CVE να ξεπερνάνε τις 51.000 καλύπτοντας ένα χρονικό διάστημα ανάλυσης το οποίο υπερβαίνει τα 20 έτη.

Ένα σοβαρό πρόβλημα της βάσης NVD το οποίο την καθιστά δύσχρηστη σε σχέση με την OSVDB είναι ο τρόπος κατασκευής της και συγκεκριμένα η δομή των .xml αρχείων στα οποία είναι καταχωρημένες οι πληροφορίες των καταγραμμένων ευπαθειών. Τα αρχεία αυτά δεν έχουν κοινές εκδόσεις και, προκειμένου να ξεπεραστεί το πρόβλημα αυτό και να αντληθούν τα αναγκαία δεδομένα, δημιουργήθηκε μία νέα βάση δεδομένων τύπου SQL Server.

6.2.4 Χρήση βάσεων καταχώρησης ευπαθειών ανοικτού κώδικα

Τα δεδομένα που λήφθηκαν από τις συγκεκριμένες βάσεις, κατά την διάρκεια της ερευνητικής προσπάθειας, αποσκοπούσαν κατά κύριο λόγο στην περιγραφή των δύο σημαντικότερων ιδιοτήτων των ευπαθειών: Η συχνότητα εμφάνισης και η σοβαρότητα που παρουσιάζουν. Επιπλέον στοιχεία που λήφθηκαν αφορούσαν τον αριθμό τους ανά προϊόν καθώς και την ημερομηνία ολοκλήρωσης της καταχώρησης και ανακοίνωσης τους. Τα στοιχεία αυτά χρησιμοποιήθηκαν προκειμένου να μελετηθεί η ύπαρξη μοτίβων στην εμφάνιση των ευπαθειών κατά την διάρκεια του χρόνου ανά προϊόν, ανά εταιρία κατασκευής λογισμικού και σε επίπεδο ΠΣ λαμβάνοντας το τελευταίο ως σύνολο διαφορετικών προϊόντων λογισμικού.

Πρέπει να αναφερθεί πως καμία από τις δύο προαναφερόμενες βάσεις δεν είναι πλήρης στην αποτύπωση των ευπαθειών που διαπιστώνονται για το σύνολο των προγραμμάτων λογισμικού. Κάθε μία από τις βάσεις δεν υποστηρίζει την καταγραφή ευπαθειών για συγκεκριμένα πακέτα λογισμικού καθώς δεν εμπίπτουν στα κριτήρια καταχώρησης που θέτουν. Επιπλέον, η NVD καταχωρεί αποκλειστικά ευπάθειες τύπου CVE σε αντίθεση με την OSVDB η οποία έχει μεγαλύτερο εύρος καταχώρησης. Συνεπώς, ένας από τους βασικούς λόγους που μας οδήγησαν στην χρήση δεδομένων και από τις δύο βάσεις, ήταν η επίτευξη πιο ολοκληρωμένης μελέτης των μεγεθών που αφορούν την τάση, την επίπτωση και την συχνότητα των ευπαθειών στην διάρκεια

του χρόνου προκειμένου για την αντικειμενικότερη μοντελοποίηση του επιπέδου ασφαλείας ενός ΠΣ.

Η βασικότερη αξιοποίηση των δεδομένων που παρέχουν οι δύο προαναφερόμενες βάσεις, στα πλαίσια της παρούσας ερευνητικής προσπάθειας, αφορούσε την προσέγγιση των στοχαστικών συναρτήσεων, που ακολουθούνται από τους παράγοντες κινδύνου, από τους οποίους εξαρτάται η ασφάλεια ενός συστήματος. Επιπλέον, τα δεδομένα χρησιμοποιήθηκαν για τον προσδιορισμό των συντελεστών βαρύτητας κάθε παράγοντα κινδύνου όπως αυτοί προσδιορίζονται με βάση την μεθοδολογία χρήσης της εντροπίας πληροφόρησης.

6.3 Τεχνικοί παράγοντες κινδύνου

Το βασικό δομικό στοιχείο της μεθοδολογίας που προτείνεται στο συγκεκριμένο κεφάλαιο αποτελείται από την θεώρηση των κύριων παραγόντων κινδύνου που προσδιορίζουν την ασφάλεια ενός συστήματος. Το σημαντικότερο βήμα, κατά την μοντελοποίηση του επιπέδου ασφαλείας ενός συστήματος, είναι ο ορισμός των παραγόντων κινδύνου των οποίων η συμπεριφορά πρέπει να επεξηγηθεί. Κατά την παρούσα ερευνητική προσπάθεια, η επιλογή αυτή πραγματοποιήθηκε με γνώμονα τα εξής:

(α) Επίτευξη της μέγιστης δυνατής αντικειμενικότητας.

(β) Αξιοπιστία στα αποτελέσματα του μοντέλου ποσοτικοποίησης της ασφάλειας.

(γ) Δυνατότητα εφαρμογής του μοντέλου σε διαφορετικές καταστάσεις.

(δ) Εξαγωγή κατανοητών αποτελεσμάτων για το σύνολο της διοίκησης ενός οργανισμού.

Προκειμένου για την εκπλήρωση των προαναφερόμενων στόχων, κατά την δημιουργία του μοντέλου, επιλέχθηκε ως παράγων κινδύνου κάθε τεχνικός παράγοντας που μετέχει στην σύνθεση ενός συστήματος. Η θεώρηση αυτή προσέδωσε στην μεθοδολογία που συστάθηκε ένα επιχειρησιακό περίγραμμα με χαρακτηριστικά περισσότερο κατανοητά στην διοίκηση ενός οργανισμού και με την όσο το δυνατόν λιγότερη χρήση εξειδικευμένων τεχνικών όρων. Αποτυπώνοντας το διαφορετικά, υιοθετήθηκε μία γενική προσέγγιση των ευπαθειών ενός συστήματος όπου το σημείο εστίασης δεν είναι η ευπάθεια αλλά το κάθε συστατικό μέρος ενός συστήματος. Η εννοιολογική θεώρηση της δεύτερης έννοιας είναι περισσότερο κατανοητή στην

διοίκηση ενός οργανισμού σε σχέση με την πρώτη. Κατά αναλογία μία μεθοδολογία που δομείται με βάση την επεξήγηση των τεχνικών παραγόντων κινδύνου μπορεί να προσδώσει αποτελέσματα με επιχειρησιακή προσέγγιση και αντικειμενικότητα.

6.3.1 Κατηγορίες μεθοδολογιών ποσοτικοποίησης της ασφάλειας

Στην παρούσα ενότητα παραθέτεται συνοπτική ανάλυση των υφιστάμενων μεθοδολογιών ποσοτικοποίησης της ασφάλειας προκειμένου να καταστεί σαφέστερη η μεθοδολογία που προτείνεται από την παρούσα ερευνητική προσπάθεια. Αρχικώς πρέπει να αναφερθεί ότι το σύνολο των υφιστάμενων μεθοδολογιών ποσοτικοποίησης της ασφάλειας επικεντρώνει την ανάλυση σε επίπεδο ευπάθειας. Οι μεθοδολογίες αυτές μπορούν να διαχωριστούν σε δύο γενικές κατηγορίες με κριτήριο την θεώρηση που επιδίδουν στις ευπάθειες [**104**]:

(1) Η πρώτη κατηγορία μεθοδολογιών περιλαμβάνει αυτές που αναλύουν την ασφάλεια ενός συστήματος εξετάζοντας κάθε ευπάθεια χωρίς να επιχειρείται ταξινόμηση των ευπαθειών και κατά συνέπεια ανάλυση σε υψηλότερο επίπεδο [**105**], [**106**], [**107**].

(2) Η δεύτερη κατηγορία μεθοδολογιών περιλαμβάνει αυτές που επιχειρούν ανάλυση της ασφάλειας εστιάζοντας στις ευπάθειες σε επίπεδο ταξινόμησης. Στις μεθοδολογίες αυτές πρωτεύοντα ρόλο έχουν τα κοινά χαρακτηριστικά και η συνολική συμπεριφορά των ευπαθειών ενός συστήματος ανά κατηγορία ταξινόμησης [**41**], [**108**].

Το βασικό μειονέκτημα των δύο παραπάνω κατηγοριών ανάλυσης, με μεγαλύτερη έμφαση να επιδίδεται στην πρώτη κατηγορία, αφορά την πολυπλοκότητα και τον χρόνο ανάλυσης που απαιτείται προκειμένου για την εξέταση κάθε μίας από τις ευπάθειες που περιλαμβάνονται σε ένα σύστημα οι οποίες συνήθως ανέρχονται σε χιλιάδες. Στο [**109**] οι ερευνητές αναγνωρίζουν το μέγεθος των υφιστάμενων ευπαθειών και του ρυθμού με τον οποίο αυξάνονται και προτείνουν μία μεθοδολογία για την ανταπόκριση μέσω αυτόματης ειδοποίησης ασφαλείας (automated security alert responding). Η συγκεκριμένη μελέτη έμμεσα προτείνει ότι οι αναλύσεις που είναι επικεντρωμένες σε επίπεδο ευπάθειας στερούνται αποδοτικότητας λαμβάνοντας υπόψη το εξαιρετικά υψηλό μέγεθος στο οποίο ανέρχονται οι ευπάθειες. Επιπλέον, καθώς η τεχνολογία αναπτύσσεται, νέες κατηγορίες ευπαθειών εμφανίζονται σε ολοένα μικρότερα χρονικά διαστήματα καθιστώντας τις μεθοδολογίες της πρώτης κατηγορίας σταδιακά λιγότερο αποδοτικές.

Στο [**108**] οι ερευνητές υποστηρίζουν την χρήση ανοικτών βάσεων δεδομένων για την ποσοτικοποίηση της ασφάλειας ΠΣ καθώς αναφέρουν πως επαρκώς εξειδικευμένες, διεξοδικές και επαναλαμβανόμενες μεθοδολογίες δεν έχουν ακόμα επιτύχει την ωριμότητα που απαιτείται και την καθολική αποδοχή. Η μεθοδολογία που προτείνουν υπάγεται στην δεύτερη κατηγορία καθώς η εστίαση γίνεται κυρίως σε επίπεδο κατηγοριών ευπαθειών. Αναλύεται η τάση που παρουσιάζουν οι κατηγορίες ευπαθειών με την υψηλότερη ταξινόμηση επίπτωσης στην πορεία του χρόνου. Παρόλο που μελέτες αυτού του είδους παρέχουν χρήσιμη πληροφόρηση σχετικά με την σημαντικότητα κάθε κατηγορίας ευπαθειών, στερούνται παροχής πρακτικών δεδομένων για την ποσοτικοποίηση του επιπέδου ασφαλείας που έχουν είτε συγκεκριμένα πακέτα λογισμικού είτε το σύνολο ενός ΠΣ.

6.3.2 Τεχνικοί παράγοντες κινδύνου σε σχέση με το σύνολο κινδύνων ενός ΠΣ

Η εννοιολογική προσέγγιση του τεχνικού παράγοντα κινδύνου, στην οποία βασίστηκε η ερευνητική προσπάθεια, είναι αυτή που προτάθηκε στο [**40**] και αναλύθηκε στην ενότητα 2.4.3. Πρέπει να αναφερθεί πως οι τεχνικοί παράγοντες κινδύνου αποτελούν μία από τις κατηγορίες κινδύνων που επηρεάζουν το επίπεδο ασφαλείας ενός ΠΣ και εντάσσονται στους λειτουργικούς ενδογενείς συστημικούς κινδύνους. Οι λοιπές μορφές κινδύνων, που επηρεάζουν το επίπεδο ασφαλείας, μπορούν να διακριθούν στις εξής κατηγορίες:

(α) Κίνδυνοι σχετιζόμενοι άμεσα με το ανθρώπινο δυναμικό. Οι κίνδυνοι αυτοί είναι ενδογενείς λειτουργικοί και, όπως αναλύθηκε στην ενότητα 2.3.1 και αποτυπώθηκε στην Εικόνα 2, αποτελούν μαζί με τους συστημικούς κινδύνους το σύνολο των λειτουργικών κινδύνων που προκαλούν τους κινδύνους παραβιάσεων ασφαλείας. Η ποσοτικοποίηση των κινδύνων που προκαλούνται από το ανθρώπινο δυναμικό είναι εξαιρετικά δύσκολο να προσεγγιστεί με αντικειμενικότητα. Ο παράγοντας αυτός ουσιαστικά εκμεταλλεύεται ευπάθειες ενός συστήματος ΠΣ, λειτουργώντας ως πηγή απειλής και συνεπώς η ποσοτικοποίηση του επιπέδου ασφαλείας, με την μελέτη των τεχνικών παραγόντων κινδύνου, μπορεί να συμπεριλάβει εμμέσως την επίδραση του ανθρώπινου παράγοντα.

(β) Φυσικοί κίνδυνοι οι οποίοι προκαλούνται κατά κύριο λόγο από φυσικές καταστροφές και μπορούν να χαρακτηριστούν ως λειτουργικοί εξωγενείς κίνδυνοι όπως επίσης αναλύθηκε στην ενότητα 2.3.1 και αποτυπώθηκε στην Εικόνα 2. Η ποσοτικοποίηση αυτών των κινδύνων πραγματοποιείται μέσω αρκετά διαφορετικών μεθοδολογιών σε σχέση με αυτές που χρησιμοποιούνται για την προσέγγιση των τεχνικών παραγόντων κινδύνου. Οι μεθοδολογίες αυτές κυρίως βασίζονται στην ανάλυση δεδομένων προερχόμενων από γεωγραφικά συστήματα πληροφοριών (Geographic Information Systems – GIS) [**110**].

Όπως προέκυψε από την ανάλυση των ερευνών για την ασφάλεια των ΠΣ στην ενότητα 4.3.3, οι κίνδυνοι παραβιάσεων ασφαλείας προκαλούνται κατά κύριο λόγο από τους τεχνικούς παράγοντες κινδύνου και η πλειοψηφία των οργανισμών κάθε κατηγορίας διεθνώς θεωρεί την αντιμετώπιση αυτών των παραγόντων πρώτης προτεραιότητας. Συγκεκριμένα, η πλειοψηφία των περιστατικών παραβίασης ασφαλείας τείνει να προέρχεται από εξωτερικούς παράγοντες οι οποίοι πραγματοποιούν επιθέσεις εκμεταλλευόμενοι τεχνικές ευπάθειες των ΠΣ. Όπως προέκυψε από την ανάλυση της προαναφερόμενης ενότητας τα περιστατικά ασφαλείας που προκαλούνται από εσωτερικούς παράγοντες βαίνουν τα τελευταία χρόνια μειωμένα ειδικά αν ληφθεί υπόψη ο αντίκτυπος που προκαλούν με βάση τον αριθμό των προσβεβλημένων εγγραφών.

Ο μεγαλύτερος κίνδυνος που προκαλείται από τους εσωτερικούς παράγοντες αφορά την αμέλεια του ανθρώπινου παράγοντα που προκαλεί ευπάθειες στα ΠΣ προς εκμετάλλευση από μία εξωτερική απειλή. Όπως όμως προκύπτει από τις μελέτες που αναλύθηκαν στην ενότητα 4.3.3, τα περιστατικά που προκαλούνται από την ανθρώπινη αμέλεια είναι σημαντικά σχεδόν αποκλειστικά λόγω του αριθμού τους και πολύ λιγότερο λόγω της επίπτωσης που εκτιμάται ότι επιφέρουν. Υπολογίζεται πως ο αριθμός των εγγραφών που προσβάλλεται από εξωτερικούς παράγοντες, εκμεταλλευόμενοι ευπάθειες των ΠΣ που προκαλούνται από αμέλεια, είναι αρκετά μικρότερος από τις επιθέσεις που εκμεταλλεύονται ευπάθειες προερχόμενες από τους τεχνικούς παράγοντες. Τέλος, η πιθανότητα και ο αντίκτυπος από κακόβουλες πράξεις προερχόμενες από εσωτερικούς παράγοντες ενός οργανισμού, έχουν επίσης μειωθεί δραστικά τα τελευταία χρόνια.

Συνεπώς, με βάση τα παραπάνω, μπορούμε να συνάγουμε ως γενικό συμπέρασμα πως το επίπεδο ασφαλείας ενός οργανισμού εξαρτάται κατά κύριο λόγο από τους λειτουργικούς ενδογενείς συστημικούς κινδύνους οι οποίοι αποτελούνται από τους τεχνικούς παράγοντες

κινδύνου ως αυτοί έχουν οριστεί στα πλαίσια της παρούσας διατριβής. Ο ανθρώπινος και ο φυσικός παράγοντας έχουν αθροιστικά ένα μικρό ποσοστό επίδρασης και μπορούν να ληφθούν υπόψη στην μοντελοποίηση ποσοτικοποίησης του επιπέδου ασφαλείας ως μία επιπρόσθετη τυχαία μεταβλητή. Με βάση τα παραπάνω η παραδοχή που λαμβάνεται είναι πως, υπό κανονικές συνθήκες, η τυχαία αυτή μεταβλητή δεν επιρρεάζει τα αποτελέσματα του μοντέλου σε τέτοιο βαθμό που να αλλοιώνει τα συμπεράσματα που προκύπτουν για το επίπεδο ασφάλειας των ΠΣ ενός οργανισμού και για το μέγεθος των κινδύνων παραβιάσεων ασφαλείας[13].

6.4 Βασικό μοντέλο ποσοτικοποίησης της ασφάλειας με την χρήση στοχαστικών μεθόδων

6.4.1 Η χρήση στοχαστικών μεθόδων στην ασφάλεια ΠΣ

Η χρήση στοχαστικών μεθόδων στην μέτρηση της ασφάλειας των ΠΣ μπορεί να οδηγήσει στον ακριβή προσδιορισμό και στην ποσοτικοποίηση του συνολικού επιπέδου επικινδυνότητας που αντιμετωπίζει ένας οργανισμός από την υιοθέτηση νέων τεχνολογιών στην διαχείριση της πληροφόρησης. Ο βασικός στόχος της χρήσης στοχαστικών μεθόδων, για την ποσοτικοποίηση του επιπέδου ασφαλείας, είναι η πληροφόρηση της Διεύθυνσης Πληροφορικής και της ανώτερης Διοίκησης ενός οργανισμού σχετικά με την ασφάλεια μέσω αντικειμενικών και κατανοητών αποτελεσμάτων. Το βασικό συνεπώς πλεονέκτημα που επιτυγχάνεται είναι η πληροφόρηση για τους κινδύνους ΠΣ κατά κύριο λόγο μέσω κατανοητών αριθμών και λιγότερο μέσω εξειδικευμένων επιστημονικών προσεγγίσεων οι οποίες είναι κατανοητές κυρίως από τα στελέχη της Διεύθυνσης Πληροφορικής. Οι τελευταίοι, μέσω αντικειμενικών ποσοτικών αποτελεσμάτων, έχουν την δυνατότητα να πείσουν την ανώτερη Διοίκηση ενός οργανισμού για τα απαιτούμενα κεφάλαια που απαιτούνται προκειμένου για την επίτευξη του βέλτιστου επιπέδου ασφαλείας των ΠΣ.

Επιπλέον, η επικοινωνία των δεδομένων για το επίπεδο ασφαλείας, παράλληλα με την κατανοητή υπόσταση που επιτυγχάνεται, πραγματοποιείται σε πιο άμεσο χρόνο. Είναι γενικά παραδεκτό πως οι αναγκαίες βελτιώσεις για την ασφάλεια ενός οργανισμού πρέπει, εκτός της

[13] Λόγω των αναφερθέντων στην συγκεκριμένη ενότητα, χάριν συντομίας, στο υπόλοιπο της παρούσας διατριβής η αναφορά στους παράγοντες κινδύνου θα ισοδυναμεί με τους τεχνικούς παράγοντες κινδύνου εκτός και αν διατυπώνεται διαφορετικά.

ακριβής μέτρησης τους, να υλοποιούνται στον κατάλληλο χρόνο ώστε, τα απαραίτητα ΠΣ ενός οργανισμού, να εκτίθενται σε κινδύνους στον μικρότερο δυνατό χρόνο. Συνολικά, μπορούμε να προσδιορίσουμε τα εξής πλεονεκτήματα που απορρέουν από την χρήση στοχαστικών μεθόδων στην προσέγγιση της ασφάλειας των ΠΣ:

(1) Προσδιορισμός με μεγαλύτερη ακρίβεια της αξίας των στοιχείων ενεργητικού που συνθέτουν τα ΠΣ που χρησιμοποιεί ένας οργανισμός.

(2) Προσδιορισμός της ευαισθησίας των στοιχείων ενεργητικού ΠΣ στις ευπάθειες που περιλαμβάνουν και σε τελική ανάλυση στους κινδύνους που απειλούν της αποτελεσματική λειτουργία τους και την ασφάλεια των δεδομένων που διαχειρίζονται.

(3) Ποσοτικοποίηση με αντικειμενικά κριτήρια του επιπέδου ασφαλείας μεμονωμένων στοιχείων των ΠΣ ή του συνόλου των ΠΣ ενός οργανισμού στην διάρκεια του χρόνου προκειμένου για την αποτελεσματικότερη και έγκαιρη πληροφόρηση όλων των επιπέδων Διοίκησης ενός οργανισμού.

(4) Αντικειμενική ποσοτικοποίηση της βαρύτητας που έχει κάθε παράγοντας κινδύνου στον προσδιορισμό του επιπέδου ασφαλείας ενός ΠΣ. Με την χρήση στοχαστικών μεθόδων και της μεθοδολογίας της εντροπίας έγινε δυνατή η ενσωμάτωση στο μοντέλο του συντελεστή βαρύτητας για κάθε τεχνικό παράγοντα κινδύνου με ποσοτικό προσδιορισμό αντί του ποιοτικού που ακολουθεί η πλειοψηφία των υφιστάμενων μεθοδολογιών.

(5) Χρήση των μετρήσεων για το επίπεδο ασφάλειας σε συγκεκριμένα χρονικά διαστήματα προκειμένου για τον προσδιορισμό της πιθανότητας πραγμάτωσης περιστατικών παραβίασης ασφαλείας η οποία αποτελεί μία από τις βασικές παραμέτρους που προσδιορίζουν το επίπεδο των κινδύνων παραβιάσεων ασφαλείας που αντιμετωπίζει ένας οργανισμός σε μία δεδομένη χρονική στιγμή. Η εκμετάλλευση του μοντέλου προσδιορισμού του επιπέδου ασφαλείας των ΠΣ ενός οργανισμού σε δεδομένο χρόνο ως μέτρο αναφοράς για την πιθανότητα υλοποίησης κινδύνων παραβιάσεων ασφαλείας αναλύεται εκτενώς στο κεφάλαιο 7 της παρούσας διατριβής.

Η ανάλυση του NIST στο [**111**] τονίζει το πρόβλημα που προκαλείται από την εξάρτηση σε υποκειμενικά και ποιοτικής φύσεως δεδομένα για την εκτίμηση των κινδύνων το οποίο

χαρακτηρίζει την πλειοψηφία των υφιστάμενων μεθοδολογιών ποσοτικοποίησης της ασφάλειας. Η ανάλυση αυτή υποστηρίζει την χρήση ιστορικών δεδομένων και την εφαρμογή κατάλληλων τεχνικών ανάλυσης για τον προσδιορισμό των τάσεων που χαρακτηρίζουν τους κινδύνους ασφαλείας και τις αλληλοσυσχετίσεις που έχουν. Επίσης, προτείνει ότι η βασική εστίαση, μίας μεθοδολογίας ποσοτικοποίησης της ασφάλειας, πρέπει να είναι στα στοιχεία λογισμικού και λιγότερο στις κατηγορίες ευπαθειών ή στις μεμονωμένες ευπάθειες.

Ο βασικότερος στόχος της μεθοδολογίας που αναλύεται στο παρόν κεφάλαιο είναι η προσπάθεια επίλυσης του προβλήματος της υποκειμενικότητας με την επίτευξη αντικειμενικότητας σε ικανοποιητικό επίπεδο. Η έρευνα εστιάζεται στο επίπεδο των συστατικών στοιχείων ενός συστήματος και προτείνεται συγκεκριμένη μεθοδολογία για την επεξεργασία ιστορικών δεδομένων με σκοπό την δημιουργία ενός μοντέλου ποσοτικοποίησης της ασφάλειας το οποίο βασίζεται στις δομές και παραδοχές που αναλύονται στην επόμενη παράγραφο.

6.4.2 Βασικό μοντέλο ποσοτικοποίησης της ασφάλειας

Προκειμένου για την επίτευξη των πλεονεκτημάτων που αναφέρθηκαν στην προηγούμενη παράγραφο, από της ποσοτικοποίηση της ασφάλειας μέσω στοχαστικών μεθόδων, μπορούμε να εισάγουμε το παρακάτω αρχικό μοντέλο το οποίο θα αποτελέσει τη βάση για την ανάπτυξη ενός ολοκληρωμένου μοντέλου προσέγγισης της ασφάλειας και το οποίο προτάθηκε αρχικώς στο [**112**]:

$$\mathrm{Sec\_status_t} = \int_0^t \prod_{i=1}^{k} f_i(x)\, dx \qquad (11)$$

Η τυχαία μεταβλητή που ορίζουμε ως Sec_status αφορά το επίπεδο ασφαλείας το οποίο υπολογίζεται μέσω ορισμένου στοχαστικού ολοκληρώματος. Τα όρια του ολοκληρώματος [0,t] θέτονται από τα χρονικά όρια του διαστήματος στο οποίο επιθυμούμε να υπολογίσουμε το επίπεδο ασφαλείας. Με f_i ορίζουμε την στοχαστική συνάρτηση που περιγράφει την συμπεριφορά έκαστου παράγοντα κινδύνου i. Τέλος, με k ορίζουμε το σύνολο των παραγόντων κινδύνου που εισάγουμε στο μοντέλο προκειμένου για τον υπολογισμό του επιπέδου ασφαλείας που επιφέρουν στο σύνολο τους.

Βασικό στοιχείο στην δομή του παραπάνω μοντέλου είναι ο συνδυασμός των παραγόντων κινδύνων που πραγματοποιείται μέσω του γινομένου τους. Με βάση την επιλογή αυτή γίνονται οι εξής παραδοχές:

(1) Όταν ένας παράγοντας κινδύνου έχει μηδενικό επίπεδο ασφαλείας τότε το σύνολο του συστήματος, του οποίου αποτελεί αναπόσπαστο μέρος, θεωρούμε ότι έχει μηδενικό επίπεδο ασφαλείας.

(2) Η προσθήκη ενός επιπλέον παράγοντα κινδύνου σε ένα σύστημα οδηγεί σε δύο πιθανές καταστάσεις: Το τρέχον επίπεδο ασφαλείας του συστήματος δεν επηρεάζεται στην περίπτωση που ο επιπλέον παράγοντας έχει άριστο επίπεδο ασφαλείας το οποίο ισούται με την μονάδα. Το τρέχον επίπεδο ασφαλείας του συστήματος μειώνεται σύμφωνα με την απόκλιση που έχει ο επιπλέον παράγοντας από την μονάδα.

(3) Η τρίτη παραδοχή είναι απόρροια της δεύτερης και σύμφωνα με αυτή ένας επιπλέον παράγοντας κινδύνου δεν μπορεί να μειώσει το τρέχον επίπεδο ασφαλείας ενός συστήματος.

(4) Οι παράγοντες κινδύνου, που απαρτίζουν ένα σύστημα, είναι ανεξάρτητοι μεταξύ τους.

Προκειμένου να επεξηγηθεί η πρώτη παραδοχή μπορούμε να αναφέρουμε πως όταν έχουμε την ακραία περίπτωση όπου ένας παράγοντας κινδύνου έχει μηδενικό επίπεδο ασφαλείας τότε το σύνολο του συστήματος έχει ουσιαστικά 100% πιθανότητα να δεχθεί μία επιτυχημένη παραβίαση ασφαλείας. Η βεβαιότητα όμως της προσβολής ενός συστήματος καταργεί τον παράγοντα κινδύνου καθώς ο κίνδυνος, όπως ορίστηκε στην ενότητα 2.2, αναφέρεται στην έλευση ενός αβέβαιου γεγονότος. Άρα η παραβίαση του συστήματος θεωρείται ένα βέβαιο γεγονός το οποίο πλέον δεν μπορεί να προσεγγιστεί μέσω της έννοιας του κινδύνου. Συνεπώς, καταλήγουμε στο συμπέρασμα πως στην ακραία αυτή περίπτωση ένα σύστημα πρέπει να θεωρηθεί ότι έχει μηδενικό επίπεδο ασφαλείας.

Η δεύτερη και η τρίτη παραδοχή μπορούν να επεξηγηθούν ταυτόχρονα καθώς και οι δύο βασίζονται στην φύση των τεχνικών παραγόντων κινδύνου. Όπως αναλύθηκε στην ενότητα 2.4, οι κίνδυνοι παραβιάσεων ασφαλείας, που προκαλούνται μεταξύ άλλων από τους τεχνικούς παράγοντες κινδύνου, είναι ανόργανοι κίνδυνοι και ως εκ τούτου είναι μη συμμετρικοί. Αυτό συνεπάγεται ότι μπορούν να προκαλέσουν μόνο αρνητικές συνέπειες σε έναν οργανισμό.

Συνεπώς, η εισαγωγή ενός επιπλέον παράγοντα κινδύνου σε ένα σύστημα στην καλύτερη των περιπτώσεων θα αφήσει στο ίδιο επίπεδο το τρέχον επίπεδο ασφαλείας είτε γιατί ο συγκεκριμένος παράγοντας δεν περιλαμβάνει ακόμα κάποια διαγνωσμένη ευπάθεια, είτε γιατί οι γνωστές ευπάθειες έχουν πλήρως αντιμετωπιστεί μέσω κατάλληλων αντιμέτρων ασφαλείας.

Η τέταρτη παραδοχή είναι απαραίτητη προκειμένου για την δημιουργία του συγκεκριμένου μοντέλου καθώς η ύπαρξη αλληλοσυσχέτισης μεταξύ των παραμέτρων κινδύνου διαφοροποιεί τελείως την μαθηματική απεικόνιση της ασφάλειας. Η φύση των επιλεγμένων παραμέτρων κινδύνου όμως οδηγεί την θεωρητική υπόσταση της συγκεκριμένης παραδοχής. Είναι ένα επιπλέον πλεονέκτημα που επιτυγχάνεται μέσω της χρήσης των συγκεκριμένων παραμέτρων κινδύνου. Μπορούμε να θεωρήσουμε πως το επίπεδο ασφαλείας προϊόντων ακόμα και του ίδιου κατασκευαστή, που όμως επιτελούν διαφορετικές λειτουργίες, είναι ανεξάρτητο μεταξύ τους.

Τέλος, από τα παραπάνω προκύπτει πως η τυχαία μεταβλητή Sec_status μπορεί να λάβει τιμές μεταξύ του μηδενός και της μονάδος. Όταν είναι ίση με την μονάδα τότε ένα σύστημα θεωρείται απόλυτα ασφαλές και εξαιρετικά απίθανη η πετυχημένη προσβολή του από κάποια πηγή απειλής. Η ιδεατή αυτή περίπτωση επιτυγχάνεται μόνο όταν όλα τα συστατικά μέρη ενός συστήματος έχουν επίπεδο ασφαλείας ίσο με την μονάδα. Το γεγονός ότι η μέγιστη ασφάλεια επιτυγχάνεται μόνο όταν το σύνολο των επιμέρους παραγόντων έχει υψηλή ασφάλεια ενώ ένα χαμηλό επίπεδο ασφαλείας μπορεί να προκληθεί από έναν μεμονωμένο παράγοντα, τονίζει την δυσκολία επίτευξης ενός αποδεκτού επιπέδου ασφαλείας για ένα σύστημα και ταυτόχρονα την ευκολία μείωσης του σε εξαιρετικά χαμηλά επίπεδα.

Στις επόμενες ενότητες αναλύεται η περαιτέρω διαμόρφωση του αρχικού προτεινόμενου μοντέλου. Αρχικώς αναλύεται η μεθοδολογία υπολογισμού του συντελεστή βαρύτητας με την χρήση της σταθμισμένης εντροπίας πληροφόρησης. Στην συνέχεια παραθέτεται η ανάλυση της κατανομής πιθανοτήτων των ευπαθειών που παρουσιάζουν οι παράγοντες κινδύνου. Τέλος αναλύεται το προτεινόμενο μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας με βάση τα αποτελέσματα της εμπειρικής ανάλυσης των δεδομένων που παρέχονται από τις βάσεις καταγραφής ευπαθειών ανοικτού κώδικα.

6.5 Χρήση της σταθμισμένης εντοπίας στο υπολογισμό του συντελεστή βαρύτητας των παραγόντων κινδύνου

Στην συγκεκριμένη ενότητα αναλύεται η μεθοδολογική προσέγγιση που ακολουθήθηκε για τον αντικειμενικό προσδιορισμό των συντελεστών βαρύτητας των τεχνικών παραγόντων κινδύνου που μετέχουν στην σύνθεση ενός ΠΣ για το οποίο επιχειρείται προσέγγιση του επίπεδου ασφαλείας σε μία δεδομένη χρονική στιγμή. Η προσέγγιση βασίζεται στην εντροπία πληροφόρησης η οποία αποτελεί μία από τις θεμελιώδης έννοιες της Πληροφορικής. Στην πρώτη παράγραφο περιγράφεται η συγκεκριμένη έννοια και αναλύεται η μορφή με την οποία χρησιμοποιήθηκε από την παρούσα ερευνητική προσπάθεια. Στην επόμενη παράγραφο αναλύεται ο υπολογισμός της πιθανότητας εμφάνισης των ευπαθειών καθώς αποτελεί βασικό συστατικό στοιχείο για τον προσδιορισμό της εντροπίας. Στις επόμενες δύο παραγράφους αναλύεται η σταδιακή ανάπτυξη της μεθοδολογίας υπολογισμού των συντελεστών βαρύτητας των παραγόντων κινδύνου.

6.5.1 Εντροπία πληροφόρησης

Η έννοια της εντροπίας χρησιμοποιήθηκε κατά την δημιουργία του προτεινόμενου μοντέλου προκειμένου για τον ποσοτικό προσδιορισμό του συντελεστή βαρύτητας για κάθε παράγοντα τεχνικού κινδύνου μέσα σε ένα ΠΣ. Η χρήση της συγκεκριμένης μεθοδολογίας, σε συνδυασμό με την χρήση στοχαστικών μεθόδων, έδωσε την δυνατότητα για την ποσοτική απόδοση της επίδρασης κάθε διακριτού στοιχείου ενός ΠΣ στην ασφάλεια του. Ο κύριος σκοπός της χρήσης της εντροπίας ήταν, εκτός από την ποσοτική απόδοση της ασφάλειας, η επίτευξη αντικειμενικότητας στα αποτελέσματα που επιφέρει το τελικό μοντέλο.

Ο Shannon εισήγαγε την έννοια της εντροπίας στην θεωρία πληροφοριών με σκοπό την επίτευξη μαθηματικής μοντελοποίησης της επικοινωνίας στο άρθρο του με το οποίο θεωρείται ότι δημιούργησε την θεωρεία πληροφοριών (information theory) [**113**]. Η έννοια την εντροπίας ήταν ήδη σε χρήση σε άλλους κλάδους επιστημών και ο Shannon διαπίστωσε την συσχέτιση που έχει η θερμοδυναμική εντροπία (thermodynamic entropy) με την εντροπία πληροφόρησης (informational entropy). Με την χρήση της εντροπίας γίνεται ποσοτικοποίηση του πληροφοριακού περιεχομένου που περιέχει ένα μήνυμα μέσω του οποίου επικοινωνείται η πραγμάτωση ενός γεγονότος. Η ιδιότητα του πληροφοριακού περιεχομένου στην οποία εστιάζεται το ενδιαφέρον είναι η «έκπληξη» που προκαλεί. Στην αρχική της μορφή η «έκπληξη» είναι αντιστρόφως ανάλογη με την

πιθανότητα εμφάνισης του γεγονότος που επικοινωνείται μέσω του πληροφοριακού μηνύματος που την προκαλεί. Υπολογίζοντας την μέση έκπληξη που προκαλεί ένα πλήθος γεγονότων λαμβάνουμε ένα μέτρο της αβεβαιότητας.

Συνεπώς, η εντροπία πληροφόρησης είναι ένα μέτρο είτε της αβεβαιότητας που προκαλεί η συμπεριφορά μίας τυχαίας μεταβλητής πριν από τον προσδιορισμό της, είτε της μέσης αβεβαιότητας που αφαιρείται αφού επιτευχθεί ο προσδιορισμός της. Ο ορισμός αυτός της εντροπίας[14] στην ουσία θεωρεί την έννοια της πληροφορίας ταυτόσημη με την αβεβαιότητα. Θεωρώντας X μία τυχαία μεταβλητή και p(x) την κατανομή πιθανότητας που ακολουθεί έχουμε τον ακόλουθο τύπο για την εντροπία:

$$\mathrm{H(X)} = -\sum_{\mathrm{x}} \mathrm{p(x)} \log \mathrm{p(x)} \qquad (12)$$

Καθώς ο λογάριθμος $\log p(x)$ στον τύπο 12 είναι αρνητικός και η εντροπία πρέπει εξ ορισμού να είναι θετική τοποθετείται το αρνητικό πρόσημο στην αρχή του τύπου. Η επιλογή της βάσης του λογαρίθμου δεν έχει σημασία για το μεγαλύτερο πλήθος των εφαρμογών που μπορεί να λάβει και πραγματοποιείται ανάλογα με την κατάσταση που αποσκοπεί να περιγράψει. Μία συνήθης επιλογή είναι η βάση 2, η οποία οδηγεί στην δυαδική εντροπία και τη μέτρηση της αβεβαιότητας σε δυαδικά ψηφία (bits). Συνεπώς, η ερμηνεία για το προσδιοριζόμενο μέγεθος της εντροπίας εξαρτάται από την φύση της τυχαίας μεταβλητής, την συμπεριφορά της οποίας επιχειρεί να περιγράψει.

6.5.2 Υπολογισμός πιθανότητας εμφάνισης ευπαθειών συγκεκριμένου επίπεδου επίπτωσης

Τα στοιχεία ευπαθειών που αντλήθηκαν από τις βάσεις OSVDB και NVD επικεντρώθηκαν κυρίως στους κατασκευαστές λογισμικού Microsoft και Oracle λόγω της μεγάλης υιοθέτησης των προϊόντων τους από τους οργανισμούς παγκοσμίως καθώς και των διαφορετικών προϊόντων που προσφέρουν εκ των οποίων τα περισσότερα χρησιμοποιούνται χρόνια από την αγορά και έχει ήδη

[14] Στο υπόλοιπο της παρούσας διατριβής, χάριν συντομίας, ο όρος εντροπία πληροφόρησης θα αποκαλείται απλά εντροπία.

δημιουργηθεί ένας σημαντικός αριθμός εκδόσεων. Τα δεδομένα που αντλήθηκαν, και από τις δύο βάσεις, αφορούν έναν χρονικό ορίζοντα 20 ετών.

Αρχικώς, έγινε μέτρηση του αριθμού των ευπαθειών που σωρευτικά έχει εμφανίσει κάθε προϊόν λογισμικού, για το οποίο αντλήθηκαν στοιχεία. Στην συνέχεια κάθε ευπάθεια, που καταγράφτηκε για κάθε προϊόν λογισμικού, ταξινομήθηκε με βάση το επίπεδο επίπτωσης που προσδιορίστηκε από τα στοιχεία που παρέχουν οι δύο βάσεις. Συγκεκριμένα, η OSVDB χρησιμοποιεί ποιοτική μεθοδολογία ταξινόμησης των ευπαθειών όπου η επίπτωση προσδιορίζεται μέσω μίας κλίμακας τριών επιπέδων: None, partial, complete. Η NVD χρησιμοποιεί την μεθοδολογία CVSS v2 το οποίο, όπως αναφέρθηκε προγενέστερα, χρησιμοποιείται πλέον και από την OSVDB. Καθώς η NVD χρησιμοποιεί την συγκεκριμένη μεθοδολογία από την σύστασης της, το σύνολο των δεδομένων της παρουσιάζει ομοιογένεια στην ταξινόμηση των ευπαθειών με βάση το επίπεδο επίπτωσης. Επιπλέον, η CVSS v2 είναι μία ευρέως αναγνωρισμένη και σε μεγάλο βαθμό αντικειμενική μεθοδολογία ταξινόμησης των ευπαθειών. Για τους παραπάνω λόγους τα δεδομένα επίπτωσης των ευπαθειών αντλήθηκαν κατά κύριο λόγο από την βάση NVD.

Χρησιμοποιώντας τα προαναφερόμενα δεδομένα, προσδιορίστηκε η πιθανότητα εμφάνισης ευπαθειών ενός συγκεκριμένου επιπέδου επίπτωσης με βάση τον παρακάτω τύπο [**40**]:

$$p_j = \frac{\text{Σύνολο ευπαθειών επίπτωσης επιπέδου j}}{\text{Σύνολο ευπαθειών κάθε επιπέδου επίπτωσης}} \qquad (13)$$

Με *j* ορίζεται το επίπεδο επίπτωσης μίας ευπάθειας με βάση τις ποιοτικές και ποσοτικές μεθοδολογίες που αναφέρθηκαν προγενέστερα. Το σύνολο των ευπαθειών για κάθε προσδιοριζόμενο επίπεδο επίπτωσης, δύναται να αναφέρεται σε μεμονωμένα προϊόντα λογισμικού συγκεκριμένων εκδόσεων ή στο σύνολο των προϊόντων ενός κατασκευαστή λογισμικού αναλόγως του επιπέδου ανάλυσης που επιχειρείται.

6.5.3 Αρχικός υπολογισμός του συντελεστή βαρύτητας των παραγόντων κινδύνου

Αφού προσδιορίστηκε, με βάση τα δεδομένα που αντλήθηκαν από τις προαναφερόμενες ανοικτές βάσεις δεδομένων και τον τύπο 13, η πιθανότητα εμφάνισης ευπαθειών για κάθε επίπεδο επίπτωσης, το επόμενο βήμα ήταν να προσεγγιστεί ο συντελεστής βαρύτητας που έχει κάθε

παράγοντας κινδύνου σε ένα ΠΣ. Η χρήση του συντελεστή βαρύτητας είναι αναγκαία προκειμένου για την ποιοτική αξιολόγηση κάθε ευπάθειας, και σε ευρύτερη διάσταση, την ποιοτική αξιολόγηση του συνόλου των ευπαθειών που εμφανίζει ένας παράγοντας κινδύνου. Η παράβλεψη χρήσης του συντελεστή βαρύτητας θα οδηγούσε στην θεώρηση της σημαντικότητας που διακατέχει ένας παράγοντας κινδύνου σε ένα ΠΣ με βάση τον σωρευτικό αριθμό ευπαθειών που έχει εμφανίσει. Προγράμματα λογισμικού που είτε είναι στην αγορά για ένα σχετικά μεγάλο αριθμό ετών, είτε είναι σε χρήση από μεγάλο μέρος της αγοράς ή λόγω και των δύο αυτών παραγόντων, συνήθως εμφανίζουν υψηλά μεγέθη ευπαθειών. Συνεπώς, η έλλειψη χρήσης μίας εναλλακτικής μεθοδολογίας προσέγγισης της βαρύτητας κάθε παράγοντα κινδύνου, θα οδηγούσε τεχνικούς παράγοντες με τα προαναφερόμενα χαρακτηριστικά να θεωρούνται μεγαλύτερης σπουδαιότητας αποκλειστικά λόγω του σωρευτικού αριθμού των ευπαθειών που διαχρονικά έχουν εμφανίσει.

Το αποτέλεσμα αυτής της θεώρησης θα ήταν αγνόηση σημαντικής πληροφόρησης που μας παρέχουν τα καταγεγραμμένα δεδομένα των βάσεων που χρησιμοποιήθηκαν. Σκοπός της έρευνας ήταν η δημιουργία μίας μεθοδολογίας όπου η βαρύτητα που αποδίδεται σε κάθε παράγοντα κινδύνου να λαμβάνει υπόψη, εκτός του αριθμού των ευπαθειών που εμφανίζει κάθε παράγοντας, το σχετικό επίπεδο επίπτωσης που εμφανίζουν οι επιπτώσεις αυτές. Η βαρύτητα που αποδίδεται στις ευπάθειες κάθε παράγοντα κινδύνου δύναται να προέλθει είτε:

(α) Μέσω της ποιοτικής ταξινόμησης που ακολουθεί η OSVDB και αναλύθηκε στην ενότητα 6.2.2. Η συγκεκριμένη ταξινόμηση αποδίδει τρία επίπεδα βαρύτητας για τις ευπάθειες που καταγράφει. Μπορούμε να αντιστοιχήσουμε έναν αριθμό σε κάθε ένα επίπεδο ταξινόμησης ως ακολούθως: None – 0, Partial – 3, Complete – 10 [**40**].

(β) Μέση της ποσοτικής ταξινόμησης που ακολουθεί η NVD η οποία από την έναρξη λειτουργίας της χρησιμοποιεί την μεθοδολογία ταξινόμησης CVSS v2. Η μεθοδολογία αυτή είναι ευρέως αποδεκτή από δημόσιους και ιδιωτικούς οργανισμούς σε παγκόσμιο επίπεδο. Επίσης, το γεγονός ότι αποφέρει ποσοτικά αποτελέσματα την καθιστά περισσότερο επιθυμητή, σε σχέση με την προαναφερόμενη ποιοτική ταξινόμηση, προκειμένου για την διατήρηση της αντικειμενικότητας του προτεινόμενου μοντέλου.

Προκειμένου για την επαρκή και αντικειμενική αποτύπωση της πληροφόρησης, σχετικά με την βαρύτητα επίπτωσης που χαρακτηρίζει κάθε ευπάθεια και σε συνολικό επίπεδο την βαρύτητα επίπτωσης που χαρακτήριζε κάθε παράγοντα κινδύνου, χρησιμοποιήθηκε η εντροπία όπως αναλύθηκε στην ενότητα 6.5.1. Χρησιμοποιώντας τους συντελεστές βαρύτητας, όπως αναφέρθηκαν παραπάνω, για κάθε επίπεδο επίπτωσης j καθώς και τις αντίστοιχες πιθανότητες που υπολογίζονται βάση του τύπου 13 μπορούμε να καταλήξουμε στον ακόλουθο αναθεωρημένο τύπο για τον βασικό μοντέλο της εντροπίας κατά Shannon:

$$W(X) = W(w_1, w_2, \dots w_n; p_1, p_2, \dots p_n) = -\sum_{j=1}^{n} w_j p_j \log(p_j) \qquad (14)$$

Όπου το $W(X)$ αντιπροσωπεύει τον συνολικό συντελεστή βαρύτητας για κάθε τυχαία μεταβλητή X η οποία με την σειρά της αντιπροσωπεύει το επίπεδο ασφαλείας κάθε παράγοντα κινδύνου. Ακολούθως, j είναι το επίπεδο επίπτωσης, όπως ήδη έχει οριστεί, και λαμβάνει τιμές από 1 έως n. Επίσης, w_j και p_j είναι ο συντελεστής βαρύτητας του συνόλου των ευπαθειών επιπέδου επίπτωσης j και η πιθανότητα εμφανισης του αντιστοίχως. Συνεπώς, ο συντελεστής βαρύτητας ενός παράγοντα κινδύνου ορίζεται ως η σταθμισμένη εντροπία του συνόλου των ευπαθειών που έχουν καταγραφτεί για κάθε επίπεδο επίπτωσης με στάθμιση τον συντελεστή βαρύτητας που προσδιορίζεται για κάθε επίπεδο. Ο συντελεστής βαρύτητας ενός παράγοντα κινδύνου ορίζεται ως ακολούθως:

$$c_i = -\sum_{j=1}^{n} w_j p_j \log(p_j) \qquad (15)$$

Θέτουμε ως c_i το επίπεδο του συντελεστή βαρύτητας για κάθε i παράγοντα κινδύνου. Με τον παραπάνω τύπο επιτυγχάνεται μία αμερόληπτη προσέγγιση του συντελεστή βαρύτητας λαμβάνοντας υπόψη ταυτόχρονα τις δύο βασικές παραμέτρους που προσδιορίζουν την έννοια του κινδύνου: Την συχνότητα ενός αβέβαιου δυσάρεστου γεγονότος και την επίπτωση που δύναται να επιφέρει. Στην περίπτωση των τεχνικών παραγόντων κινδύνου το δυσάρεστο γεγονός ισοδυναμεί με μία ευπάθεια για την οποία προσεγγίζεται η πιθανότητα εμφάνισης καθώς και το επίπεδο επίπτωσης που μπορεί να επιφέρει.

6.5.4 Εισαγωγή της παραμέτρου του χρόνου στους συντελεστές βαρύτητας

Ο τύπος 15, βάση του οποίου προσδιορίζεται ο συντελεστής βαρύτητας κάθε παράγοντα κινδύνου, εμπεριέχει τις παραμέτρους της πιθανότητας εμφάνισης και του επιπέδου επίπτωσης

των ευπαθειών αλλά δεν λαμβάνει υπόψη την δυναμικότητα των συγκεκριμένων παραμέτρων στον χρόνο. Δεν είναι ρεαλιστικό να υποτεθεί πως ο συντελεστής βαρύτητας ενός προϊόντος λογισμικού παραμένει στατικός στην διάρκεια του κύκλου ζωής του συγκεκριμένου προϊόντος. Ο λόγος έγκειται στο γεγονός πως το σύνολο των ευπαθειών λογισμικού υπάγεται και αυτό σε ένα συγκεκριμένο κύκλο ζωής ο οποίος περιλαμβάνει τέσσερα στάδια: (α) Στάδιο ανακάλυψης, (β) στάδιο γνωστοποίησης, (γ) στάδιο εκμετάλλευσης και (δ) στάδιο αντιμετώπισης.

Κάθε στάδιο χαρακτηρίζεται από κινδύνους διαφορετικού επιπέδου και μορφής. Το χρονικό διάστημα που μεσολαβεί από την έναρξη του σταδίου εκμετάλλευσης έως τη λήξη του σταδίου αντιμετώπισης αναφέρεται ως «παράθυρο έκθεσης» (window of exposure). Το επίπεδο της επίπτωσης που επιφέρει μία ευπάθεια, σε αυτό το χρονικό μέρος του κύκλου ύπαρξης της, είναι το μέγιστο. Αφού ολοκληρωθεί το στάδιο αντιμετώπισης, το επίπεδο επίπτωσης μίας ευπάθειας μειώνεται δραστικά. Ουσιαστικά η ταξινόμηση που πραγματοποιείται από τις βάσης καταχώρησης των ευπαθειών χρησιμοποιεί το μέγιστο επίπεδο επίπτωσης που δύναται να επιφέρει μία ευπάθεια μέσα στα χρονικά όρια του προαναφερόμενου παραθύρου έκθεσης.

Συνεπώς, κατά την μοντελοποίηση του συντελεστή βαρύτητας κάθε παράγοντα κινδύνου, πρέπει να ληφθεί υπόψη η διάρκεια ύπαρξης των ευπαθειών που εμφανίζει. Ορίζουμε με k τον αριθμό των ετών που μία ευπάθεια επιπέδου επίπτωσης j έχει ανακαλυφθεί και υφίσταται στην αγορά. Προκειμένου να αποτυπωθεί η αντιστρόφως ανάλογη σχέση που υποθέτουμε μεταξύ του χρόνο ύπαρξης μίας ευπάθειας και την επίπτωσης που δύναται να επιφέρει ο τύπος 15 τροποποιείται ως εξής:

$$c_i = -\sum_{j=1}^{n}\sum_{k=0}^{m} e^{-k} w_j p_{jk} \log(p_{jk}) \qquad (16)$$

Όπου με m ορίζεται ο αριθμός των ετών που ένα προϊόν βρίσκεται στην αγορά το οποίο συμπίπτει με τον μέγιστο χρόνο ζωής που μπορεί να έχει μία ευπάθεια σε ένα προϊόν. Ο τελεστής e^{-k} προσδιορίζει την προαναφερώμενη αντίστροφη σχέση μεταξύ του επιπέδου επίπτωσης μίας ευπάθειας και του χρόνου ύπαρξης της. Η μεταβλητή p_{jk} αναφέρεται στην πιθανότητα εμφάνισης ευπαθειών επιπέδου επίπτωσης j που έχουν εμφανιστεί στην αγορά k έτη και ορίζεται με τον ακόλουθο τύπο ο οποίος βασίζεται στον τύπο 13:

$$p_{jk} = \frac{\text{Σύνολο ευπαθειών επίπτωσης επιπέδου j με k έτη στην αγορά}}{\text{Σύνολο ευπαθειών με επίπεδο επίπτωσης j}} \qquad (17)$$

Ουσιαστικά το σύνολο των πιθανοτήτων p_{jk} αποτελούν στοιχεία μίας μήτρας της οποίας οι διαστάσεις είναι $n\,x\,m$ ήτοι ο αριθμός των επιπέδων επίπτωσης στα οποία επιμερίζονται οι ευπάθειες ενός παράγοντα κινδύνου i με τον αριθμό των ετών που βρίσκεται ο παράγοντας κινδύνου στην αγορά. Κάθε στοιχείο της μήτρας είναι η προσδιορισμένη πιθανότητα εμφάνισης ευπαθειών συγκεκριμένου επιπέδου επίπτωσης και με συγκεκριμένο χρόνο διάρκειας ύπαρξης.

Η παράμετρος του χρόνου μπορεί να ενσωματωθεί στον προσδιορισμό του συντελεστή βαρύτητας κάθε παράγοντα κινδύνου με μία ακόμα διάσταση: Το επίπεδο χρήσης ενός λογισμικού μέσα σε ένα ΠΣ στην διάρκεια ζωής του συγκεκριμένου προϊόντος. Το επίπεδο χρήσης ενός λογισμικού προϊόντος μπορεί να θεωρηθεί ως ένας κρίσιμος παράγοντας για την επίδραση που επιφέρει ως παράγων κινδύνου στον προσδιορισμό του επιπέδου ασφαλείας για το σύστημα στο οποίο ανήκει. Προσδιορίζεται ως το ποσοστό συμμετοχής που έχει ένα λογισμικό στο σύνολο ενός ΠΣ σε μία δεδομένη χρονική στιγμή. Ο προσδιορισμός του ποσοστού χρήσης εξαρτάται από δύο παραμέτρους:

(1) Τον βαθμό εμπλοκής ενός λογισμικού προϊόντος στις διαδικασίες λειτουργίας ενός οργανισμού.

(2) Ο προσδιοριζόμενος βαθμός σπουδαιότητας που έχουν οι διαδικασίες λειτουργίας του οργανισμού στις οποίες εμπλέκεται ένα προϊόν.

Η συγκεκριμένη παράμετρος αποτελεί το μοναδικό στοιχείο του μοντέλου το οποίο δεν προσδιορίζεται από αμιγώς αντικειμενικά δεδομένα. Η φύση της συγκεκριμένης παραμέτρου την καθιστά προσδιορίσιμη από την υποκειμενική κρίση των ειδικών στελεχών του τμήματος πληροφορικής ενός οργανισμού. Ορίζουμε το ποσοστό συμμετοχής ενός λογισμικού i σε ένα ΠΣ, κατά το έτος k στο παρελθόν, ως q_k. Ο τύπος 16, με την προσθήκη της συγκεκριμένης παραμέτρου, τροποποιείται ως ακολούθως:

$$c_i = -\sum_{j=1}^{n}\sum_{k=1}^{m} q_k e^{-k} w_j p_{jk} \log(p_{jk}) \qquad (18)$$

Πρέπει επίσης να αναφερθεί πως στα έτη ύπαρξης ενός προϊόντος στην αγορά, που δεν χρησιμοποιείται σε ένα σύστημα, το ποσοστό συμμετοχή ορίζεται ως μηδέν οδηγώντας το σύνολο του γινομένου για τα συγκεκριμένα έτη σε μηδενικό αποτέλεσμα και ως συνέπεια την μη επίδραση στον υπολογισμό του συντελεστή βαρύτητας.

Ως αποτέλεσμα των ανωτέρω τροποποιήσεων, ο συντελεστής βαρύτητας ενός παράγοντα κινδύνου προσδιορίζεται από τις παρακάτω παραμέτρους:

(α) Η βαρύτητα κάθε επιπέδου επίπτωσης στα οποία κατανέμονται οι ευπάθειες.

(β) Η σταθμισμένη εντροπία πληροφόρησης με συντελεστή στάθμισης την προαναφερόμενη βαρύτητα κάθε επιπέδου επίπτωσης.

(γ) Ο αριθμός των ετών που βρίσκεται στην αγορά ένας παράγοντας κινδύνου.

(δ) Η πιθανότητα εμφάνισης ευπαθειών κάθε επιπέδου επίπτωσης για κάθε ενδιάμεσο αριθμό ετών από το σύνολο της διάρκειας ύπαρξης ενός παράγοντα κινδύνου.

(ε) Το ποσοστό συμμετοχής ενός παράγοντα κινδύνου σε ένα σύστημα για κάθε ενδιάμεσο αριθμό ετών από το σύνολο της διάρκειας ύπαρξης ενός παράγοντα κινδύνου.

6.5.5 Υπολογισμός των συντελεστών βαρύτητας

Στην συγκεκριμένη παράγραφο παραθέτονται αποτελέσματα από τον υπολογισμό των συντελεστών βαρύτητας διαφόρων παραγόντων κινδύνου χρησιμοποιώντας δεδομένα από τις δύο βάσεις ανοικτού κώδικα που υιοθετήθηκαν για την παρούσα μελέτη. Τα αποτελέσματα προέρχονται από την χρήση του τύπου 18 θέτοντας την παράμετρο q_k ίση με την μονάδα για όλους τους παράγοντες κινδύνου i που αναλύθηκαν προκειμένου να εξαχθούν συγκρίσιμα στοιχεία. Η έλλειψη τοποθέτησης συγκεκριμένου ποσοστού συμμετοχής σε κάθε παράγοντα κινδύνου δεν επιρρεάζει τις ανάγκες της παρούσας μελέτης και έχει βάση όταν αναλύεται ένα συγκεκριμένο σύστημα. Στην υφιστάμενη ανάλυση το προσδοκώμενο ήταν η εμπειρική επιβεβαίωση των αποτελεσμάτων που εξάγει το μοντέλο και η σύγκριση τους μεταξύ διαφορετικών παραγόντων κινδύνου με την χρήση δεδομένων από διαφορετικές βάσεις.

Στα πλαίσια της ερευνητικής προσπάθειας έγινε ανάλυση αρκετών διαφορετικών πακέτων λογισμικού από διαφορετικούς κατασκευαστές για τα οποία υπάρχουν δεδομένα ευπαθειών στις βάσεις που χρησιμοποιήθηκαν. Σύμφωνα με στοιχεία από τις StatOwl.com [**114**] και Statcounter.com [**115**], οι οποίοι είναι διαδικτυακοί τόποι που καταγράφουν στατιστικά χρήσης λογισμικού, τα λειτουργικά συστήματα της Microsoft κατέχουν ένα μερίδιο της αγοράς που

κυμαίνεται μεταξύ 85 – 90%[15]. Η πρωτοκαθεδρία της Microsoft στην αγορά λειτουργικών συστημάτων παγκοσμίως έχει οδηγήσει αντιστοίχως τα προϊόντα λογισμικού που παράγει να παρουσιάζουν τον μεγαλύτερο αριθμό ευπαθειών. Το γεγονός αυτό υφίσταται λόγω της εκτεταμένης χρήσης και του μεγάλου αριθμού από hackers που έχουν στόχο την επίθεση σε προϊόντα της Microsoft. Συνεπώς, λόγω της εξαιρετικά μεγάλης επάρκειας δεδομένων και στις δύο βάσεις, οι υπολογισμοί που παραθέτονται στην παρούσα διατριβή αφορούν τους συντελεστές βαρύτητας προϊόντων της συγκεκριμένης εταιρίας.

Στον Πίνακα 25 παρουσιάζονται οι υπολογιζόμενοι συντελεστές βαρύτητας για προϊόντα λογισμικού της Microsoft με την χρήση δεδομένων από την βάση OSVDB. Πρέπει να αναφερθεί πως δεν γίνεται αναφορά στο λειτουργικό σύστημα Windows 7 έστω και αν πλέον το μερίδιο αγοράς του συγκεκριμένου λογισμικού πλησιάζει το 40% καθώς ακόμα δεν υπάρχουν επαρκή δεδομένα ευπαθειών προκειμένου να εξαχθούν συγκρίσιμα αποτελέσματα.

Μπορεί κανείς να παρατηρήσει τον καθοριστικό ρόλο που διαδραματίζει η βαρύτητα w_j κάθε επιπέδου επίπτωσης συγκρίνοντας τα αποτελέσματα μεταξύ των λειτουργικών συστημάτων Windows XP και Windows 2003. Συγκεκριμένα, η υπολογιζόμενη εντροπία για το πρώτο είναι μεγαλύτερη, καθώς όμως το δεύτερο έχει μεγαλύτερο πλήθος ευπαθειών με υψηλή επίπτωση, ο τελικός συντελεστής βαρύτητας είναι μεγαλύτερος για αυτό. Τα επίπεδα επίπτωσης που χρησιμοποιούνται είναι – όπως προαναφέρθηκε – αυτά που έχουν υιοθετηθεί από την OSVDB.

Στον Πίνακα 26 παρουσιάζεται ο υπολογισμός των συντελεστών βαρύτητας χρησιμοποιώντας δεδομένα από την βάση NVD κάνοντας χρήση των ιδίων προϊόντων για λόγους συγκρισιμότητας. Η βασική διαφοροποίηση του δεύτερου Πίνακα είναι η έλλειψη αναφοράς για το επίπεδο επίπτωσης. Όπως αναφέρθηκε στην ενότητα 6.2.3, η βάση NVD κάνει χρήση της CVSS για την ταξινόμηση των ευπαθειών σε επίπεδα επίπτωσης. Συνεπώς δεν είναι εφικτό να αναφερθούν όλα τα επίπεδα επίπτωσης στον Πίνακα. Επίσης, λόγω της διαφορετικής μεθόδου ποσοτικοποίησης του επιπέδου επίπτωσης για κάθε βάση, ο συντελεστής βαρύτητας, για το ίδιο πακέτο, διαφοροποιείται αρκετά.

[15] Τα στατιστικά στοιχεία αντλήθηκαν από τους συγκεκριμένους διαδικτυακούς τόπους για χρονικό διάστημα 12 μηνών μεταξύ Ιουνίου 2011 και Μαΐου 2012. Λόγω της συχνής αλλαγής εκδόσεων από τους κατασκευαστές λογισμικού ένα διάστημα λήψης δεδομένων 12 μηνών θεωρείται επαρκές.

Πίνακας 25: Υπολογισμός των συντελεστών βαρύτητας προϊόντων της Microsoft με δεδομένα ευπαθειών από την OSVDB

Κατασκευαστής	*Προϊόν*	*Σύνολο ευπαθειών*	*Επίπεδο επίπτωσης*			*Εντροπία*	*Συντελεστής Βαρύτητας*
			None	*Partial*	*Complete*		
Microsoft	Windows XP	3.836	616	1.520	1.700	2.172	0,22
Microsoft	Windows 2003	2.496	300	890	1.306	2.062	0,35
Microsoft	Office XP	210	9	90	111	2	0,13

Η διαφοροποίηση αυτή δεν έχει ιδιαίτερη σημασία καθώς αυτό που μας ενδιαφέρει είναι η σχέση μεγέθους που έχουν οι υπολογιζόμενοι συντελεστές βαρύτητας που προσδιορίζονται από τα δεδομένα κάθε βάσης. Από τον Πίνακα 25 προκύπτει πως το προϊόν με την μεγαλύτερη έκθεση σε κινδύνους παραβιάσεων ασφαλείας είναι τα Windows 2003. Το ίδιο συμπέρασμα προκύπτει κάνοντας χρήση των δεδομένων του Πίνακα 26. Το προϊόν Windows 2003 εμφανίζει και πάλι τον μεγαλύτερο συντελεστή βαρύτητας υποδηλώνοντας μεγαλύτερη έκθεση σε κινδύνους παραβιάσεων ασφαλείας σε σχέση με τα άλλα προϊόντα. Συνεπώς, η χρήση των δεδομένων από τις δύο βάσεις δεν επηρεάζει ουσιαστικά τον υπολογισμό του συντελεστή βαρύτητας και τα συμπεράσματα που προκύπτουν σχετικά με το επίπεδο επικινδυνότητας που παρουσιάζει κάθε προϊόν σε σχέση με τα άλλα προϊόντα.

Πίνακας 26: Υπολογισμός των συντελεστών βαρύτητας προϊόντων της Microsoft με δεδομένα ευπαθειών από την NVD

Κατασκευαστής	*Προϊόν*	*Σύνολο ευπαθειών*	*Συντελεστής Βαρύτητας*
Microsoft	Windows XP	638	3,072
Microsoft	Windows 2003	565	3,375
Microsoft	Office XP	110	1,201

6.6 Ανάπτυξη του μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας

6.6.1 Ενσωμάτωση του συντελεστή βαρύτητας στο μοντέλο

Στην συγκεκριμένη ενότητα αρχικώς αναλύεται η περεταίρω ανάπτυξη του μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας. Στην συνέχεια πραγματοποιείται διερεύνηση της ύπαρξης χρονικών μοτίβων στην εμφάνιση των ευπαθειών, προκειμένου για την εμπειρική επιβεβαίωση της μεθοδολογίας που ακολουθείται, καθώς και την προσέγγιση των στοχαστικών συναρτήσεων που περιγράφουν την συμπεριφορά των παραγόντων κινδύνου. Σκοπός της χρονικής ανάλυσης των ευπαθειών ήταν η προσέγγιση των κατανομών πιθανότητας που ακολουθούν οι ευπάθειες σε επίπεδο παράγοντα κινδύνου ώστε να προσεγγιστούν οι στοχαστικές συναρτήσεις που ακολουθούν.

Στην ενότητα 6.4 παρουσιάστηκε η βασική μορφή ενός μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας με την χρήση στοχαστικής ανάλυσης. Ακολούθως, στην ενότητα 6.5 παρουσιάστηκε ο υπολογισμός των συντελεστών βαρύτητας, για κάθε παράγοντα κινδύνου που επιρρεάζει ένα σύστημα. Έγινε χρήση της σταθμισμένης εντροπίας προκειμένου για την διατήρηση στο μοντέλο της επιζητούμενης αντικειμενικότητας. Το επόμενο βήμα είναι η ενσωμάτωση στο αρχικό μοντέλο του συντελεστή βαρύτητας προκειμένου το γινόμενο των στοχαστικών συναρτήσεων κάθε παράγοντα κινδύνου να σταθμίζεται κατά τον συγκεκριμένο συντελεστή. Το αποτέλεσμα είναι το στοχαστικό ολοκλήρωμα να υπολογίζει το επίπεδο κινδύνου λαμβάνοντας την σταθμισμένη συμπεριφορά των παραγόντων κινδύνου σε ένα συγκεκριμένο χρονικό διάστημα. Λαμβάνοντας υπόψη τα προαναφερόμενα το μοντέλο διαμορφώνεται ως εξής:

$$\int_0^t \prod_{i=1}^{k} f_i^{\frac{1}{c_i}}(t)\, dt \qquad (19)$$

Ο συντελεστής βαρύτητας εισάγεται στο μοντέλο ως εκθέτης διαιρούμενος από την μονάδα προκειμένου να προσδιορίζεται η αντίστροφη σχέση του επιπέδου βαρύτητας για ένα παράγοντα κινδύνου με το συνολικό επίπεδο ασφαλείας ενός συστήματος. Συνεπώς, αν για παράδειγμα έχουμε δύο παράγοντες κινδύνου με συντελεστή βαρύτητας 0,5 και 0,35, οι εκθέτες θα είναι 2 και 2,85 αντιστοίχως. Ο πρώτος παράγοντας έχει μεγαλύτερη επικινδυνότητα καθώς έχει μεγαλύτερο συντελεστή βαρύτητας. Ο υπολογιζόμενος εκθέτης, για τον ίδιο παράγοντα, είναι μικρότερος το οποίο οδηγεί σε μικρότερο επίπεδο ασφαλείας. Επομένως, αποτυπώνεται στο μοντέλο η σχέση

μεταξύ του επιπέδου επικινδυνότητας ενός παράγοντα κινδύνου και της επίδρασης που επιφέρει στο συνολικό επίπεδο ασφαλείας ενός ΠΣ.

Επίσης, όπως αποτυπώνεται στον τύπο 19, οι στοχαστικές συναρτήσεις εξαρτώνται αποκλειστικά από την ανεξάρτητη μεταβλητή t η οποία υποδηλώνει την χρονική στιγμή στην οποία υπολογίζεται το επίπεδο ασφαλείας. Η μεταβλητή t ορίζεται από τον αριθμό των ημερών που έχουν παρέλθει από την χρονική στιγμή $t = 0$ όπου ξεκινάει ο υπολογισμός του επιπέδου ασφαλείας ενός συστήματος.

Επομένως, κατά το παραπάνω μοντέλο, το επίπεδο ασφαλείας ενός συστήματος στο χρονικό διάστημα $[0, t]$ ισούται με το στοχαστικό ολοκλήρωμα, ορισμένο στα πλαίσια του χρονικού διαστήματος, του σταθμισμένου γινομένου των στοχαστικών συναρτήσεων που αντιπροσωπεύουν την συμπεριφορά των k παραγόντων κινδύνου, που περιέχει το υπό εξέταση σύστημα, με στάθμιση τον συντελεστή βαρύτητας κάθε k παράγοντα.

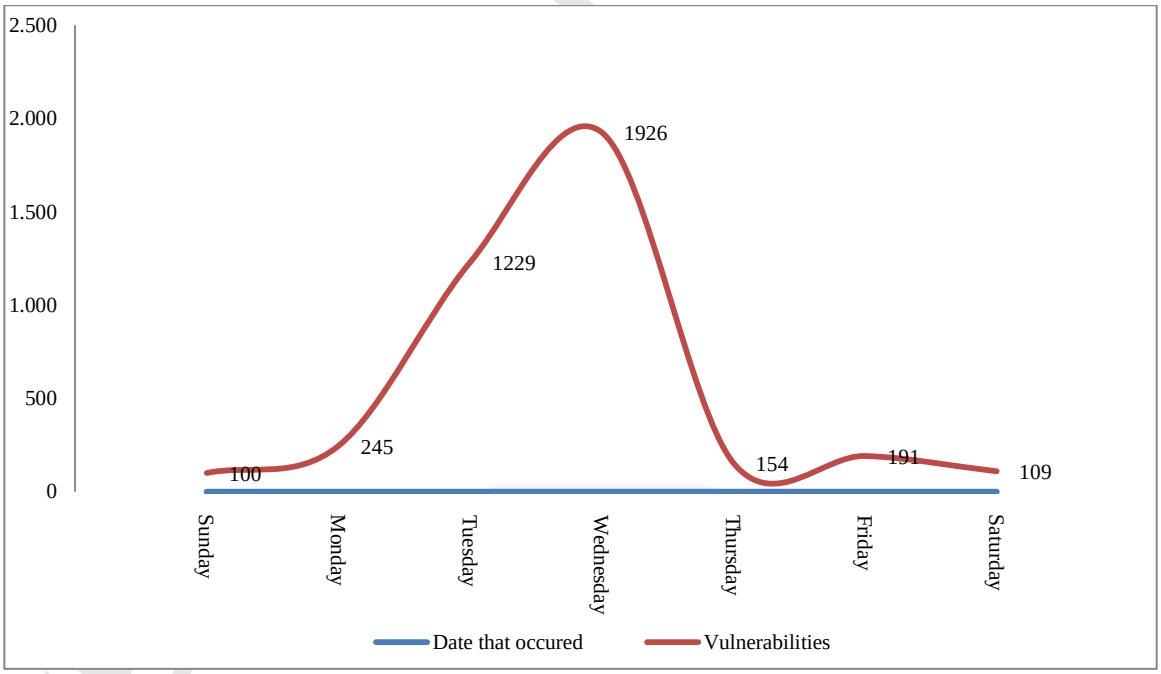
6.6.2 Ανάλυση των χρονικών μοτίβων των ευπαθειών

Στην παράγραφο αυτή εξετάζεται η πιθανή ύπαρξη μοτίβων στην χρονική κατανομή των ευπαθειών όταν οι τελευταίες αναλύονται σε επίπεδο προϊόντος λογισμικού. Στατιστική ανάλυση των ευπαθειών που παρουσιάζουν προϊόντα λογισμικού έχει επιχειρηθεί από προηγούμενες μελέτες όπως είναι η [**106**]. Οι μελέτες αυτές έχουν ως κοινό στόχο τον προσδιορισμό επαναλαμβανόμενων μοτίβων στην συμπεριφορά των ευπαθειών. Η επικέντρωση όμως, σε αυτές τις μελέτες, γίνεται στο μέγεθος του πληθυσμού των ευπαθειών και στις τάσεις ανάπτυξης που έχει. Στην παρούσα ανάλυση η βασική διαφοροποίηση έγκειται στο ότι η επικέντρωση γίνεται στην συμπεριφορά των ευπαθειών σε συγκεκριμένες χρονικές περιόδους.

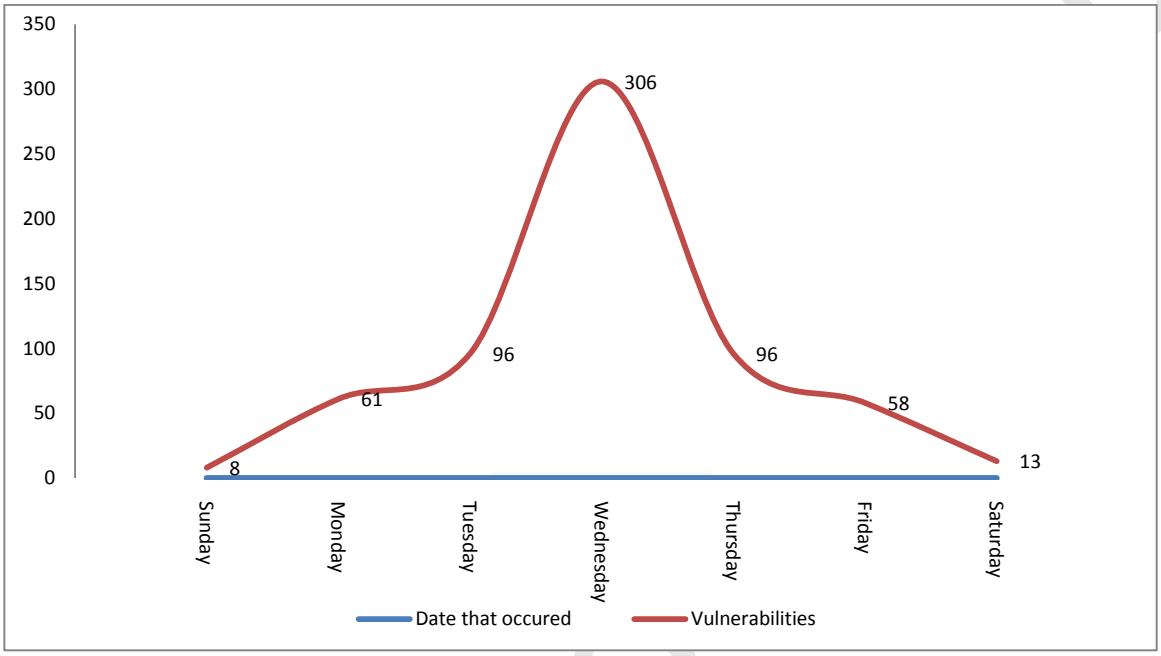
Επιχειρείται με άλλα λόγια η ανάλυση των συσσωρευμένων ευπαθειών που ιστορικά παρουσιάζει ένα πακέτο λογισμικού και η διάγνωση πιθανών επαναλαμβανόμενων μοτίβων σε συγκεκριμένα χρονικά διαστήματα. Τα διαστήματα αυτά δύναται να περιλαμβάνουν συγκεκριμένες ημέρες της εβδομάδας, το σύνολο των ημερών ενός μήνα ή ακόμα και συγκεκριμένους μήνες του έτους. Η παρούσα μελέτη υποστηρίζει πως η διάγνωση μοτίβων με αυτόν τον τρόπο έχει μεγαλύτερη σημαντικότητα για την ποσοτικοποίηση της ασφάλειας από ότι έχει η ανάλυση του όγκου των ευπαθειών στο χρόνο [**104**].

Συνεπώς, με την εμπειρική ανάλυση των δεδομένων που προέρχονται από τις βάσεις OSVDB και NVD, επιχειρείται η προσέγγιση των στοχαστικών συναρτήσεων που ακολουθούν οι παράγοντες κινδύνου μέσω της διάγνωσης επαναλαμβανόμενων μοτίβων στην κατανομή των ευπαθειών. Στο Διάγραμμα 4 και στο Διάγραμμα 5 παρουσιάζεται η κατανομή των ευπαθειών, στις ημέρες της εβδομάδας, για το λειτουργικό σύστημα Windows XP χρησιμοποιώντας τα δεδομένα των βάσεων OSVDB και NVD αντίστοιχα. Οι κατανομές παρουσιάζουν κοινά χαρακτηριστικά με κυριότερο την κορύφωση στην ίδια ημέρα η οποία είναι η Τετάρτη. Η σχηματική απεικόνιση των κατανομών προσεγγίζει το σχήμα καμπάνας το οποίο αποτελεί σημαντική διαπίστωση για την εμπειρική προσέγγιση των στοχαστικών συναρτήσεων των παραγόντων κινδύνου. Παρατηρούμε επίσης ότι είναι η δεύτερη φορά που τα δεδομένα που αντλούνται από τις δύο βάσεις οδηγούν στα ίδια συμπεράσματα σχετικά με το αντικείμενο ανάλυσης που επιχειρείται.

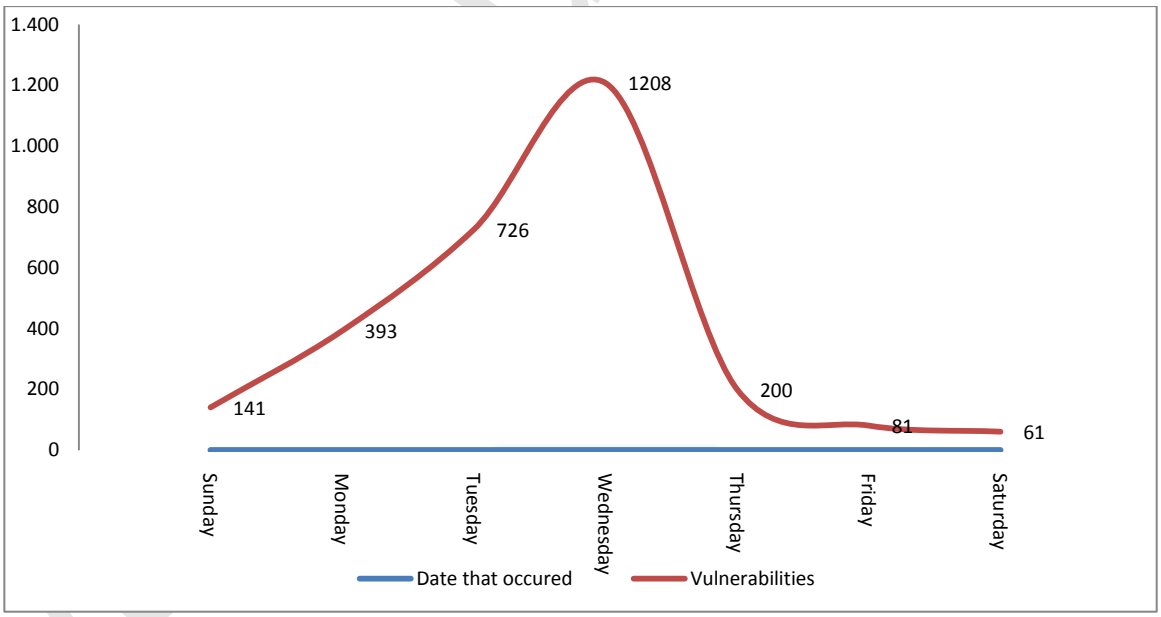
Διάγραμμα 4: Κατανομή ευπαθειών των Windows XP ανά ημέρα της εβδομάδας με την χρήση της OSVDB



Διάγραμμα 5: Κατανομή ευπαθειών των Windows XP ανά ημέρα της εβδομάδας με την χρήση της OSVDB



Διάγραμμα 6: Κατανομή ευπαθειών των Windows 2000 ανά ημέρα της εβδομάδας με την χρήση της OSVDB

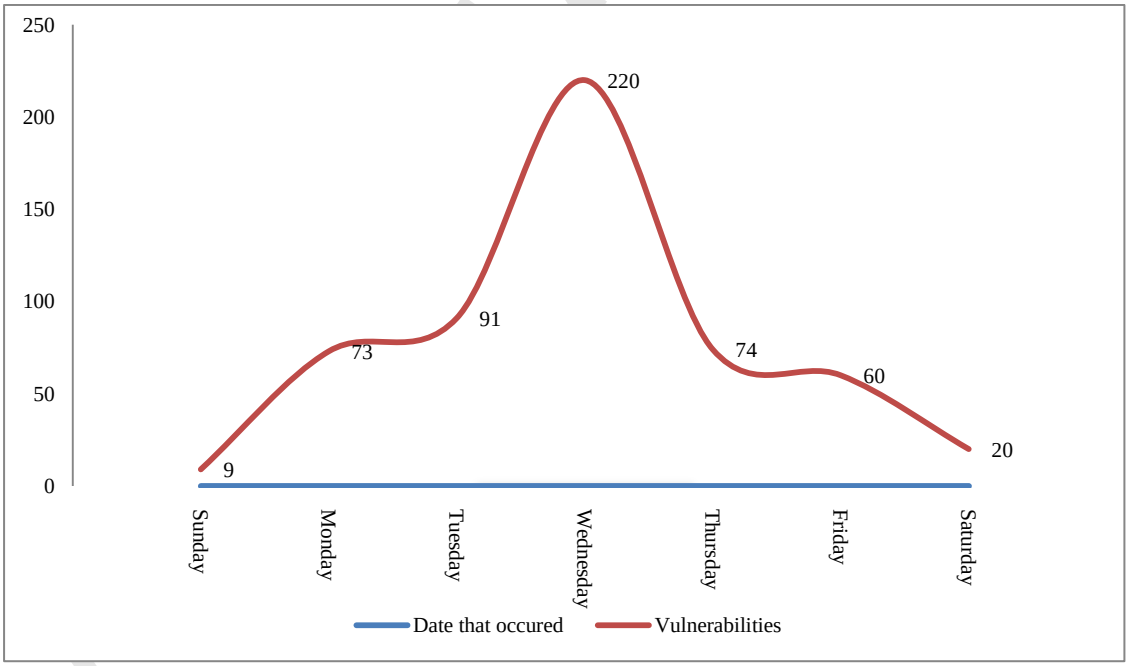


Το επόμενο προϊόν λογισμικού, στο οποίο αναλύθηκε η χρονική κατανομή των ευπαθειών του, ήταν το λειτουργικό σύστημα Windows 2000 που, λόγω του μεγάλου διαστήματος που βρίσκεται στην αγορά, υπήρχε μεγάλος αριθμός δεδομένων και στις δύο βάσεις. Στο Διάγραμμα 6 και στο

Διάγραμμα 7 παρουσιάζονται οι κατανομές για το συγκεκριμένο λειτουργικό με την χρήση δεδομένων από τις βάσεις OSVDB και NVD αντιστοίχως.

Οι κατανομές έχουν πάλι κοινά χαρακτηριστικά με βασικότερο στοιχείο το σημείο κορύφωσης που είναι και πάλι η ημέρα Τετάρτη. Επιπλέον, η απεικόνιση και των δύο κατανομών προσεγγίζει το σχήμα καμπάνας. Τα συμπεράσματα που εξάγονται από την ανάλυση της κατανομής των ευπαθειών που αφορούν το λογισμικό Windows 2000 είναι κοινά με αυτά που αφορούν το λογισμικό Windows XP. Αυτό είναι χωρίς αμφιβολία απόδειξη για την ύπαρξη συγκεκριμένων χρονικών μοτίβων στην συμπεριφορά των ευπαθειών ανεξάρτητα από τον παράγοντα κινδύνου που εξετάζεται. Συνεπώς οι ενδείξεις που παρουσιάζει η συγκεκριμένη εμπειρική ανάλυση, υποδεικνύουν ότι η προσέγγιση της συμπεριφοράς των παραγόντων κινδύνου με μία στοχαστική συνάρτηση η οποία να έχει κοινά χαρακτηριστικά είναι εφικτή. Πριν επιχειρηθεί όμως αυτό παραθέτεται η εμπειρική ανάλυση που έγινε σε άλλα προϊόντα λογισμικού προκειμένου για την περαιτέρω εμπειρική επιβεβαίωση των προαναφερόμενων χρονικών μοτίβων.

Διάγραμμα 7: Κατανομή ευπαθειών των Windows 2000 ανά ημέρα της εβδομάδας με την χρήση της NVD

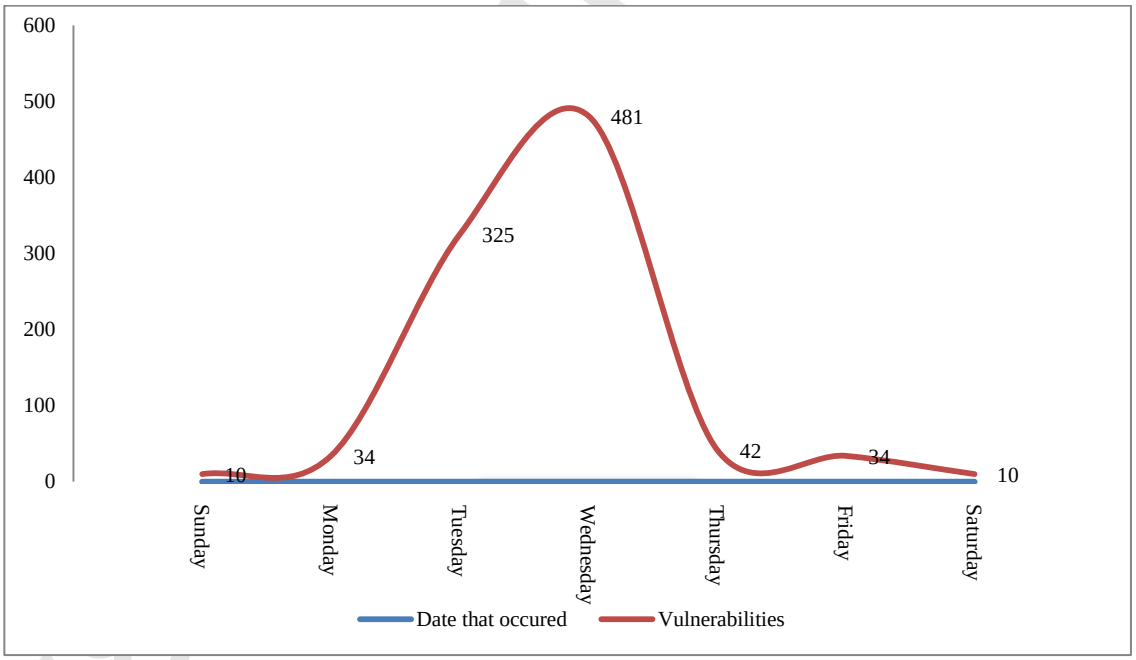


Πραγματοποιήθηκε ανάλυση σε ένα ακόμα προϊόν λογισμικού της Microsoft το οποίο είναι το λειτουργικό σύστημα Windows Vista. Επιλέχθηκε το συγκεκριμένο προϊόν καθώς έχει αρκετά

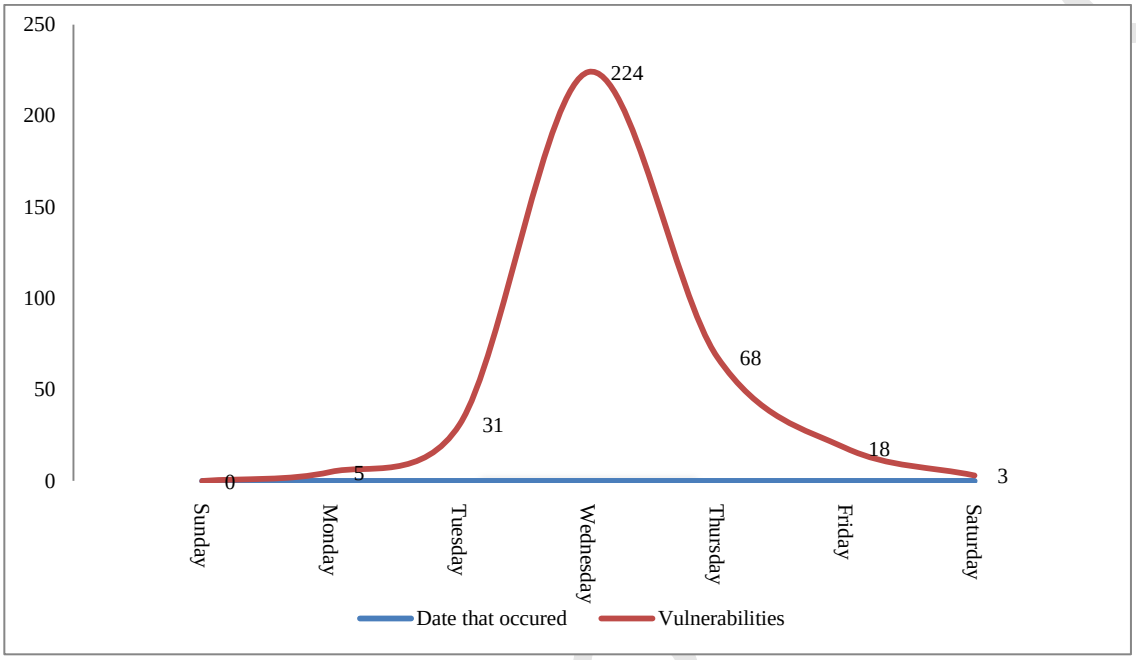
λιγότερο αριθμό ευπαθειών λόγω του μικρότερου χρόνου που είναι στην αγορά και μικρή σχετικά ανταπόκριση από το αγοραστικό κοινό. Είναι ενδεικτικό πως πρόσφατες στατιστικές μετρήσεις τοποθετούν το μερίδιο αγοράς του συγκεκριμένου λογισμικού μεταξύ 10 – 14%. Το γεγονός αυτό προσδίδει ενδιαφέρον στην εμπειρική επιβεβαίωση ότι ένας παράγοντας κινδύνου με λιγότερο χρόνο στην αγορά και μικρότερη χρήση έχει την ίδια κατανομή ευπαθειών με τους δύο προαναφερόμενους.

Στο Διάγραμμα 8 και στο Διάγραμμα 9 παρουσιάζεται η κατανομή των ευπαθειών για το λογισμικό αυτό με την χρήση των δεδομένων από τις δύο βάσεις. Η σχηματική απεικόνιση των κατανομών παρουσιάζει και πάλι κοινά χαρακτηριστικά με την κορύφωση να είναι κοινή και να παραπέμπει για άλλη μία φορά στην ημέρα Τετάρτη. Επίσης, πάλι έχουμε κατανομές με σχήμα καμπάνας επιβεβαιώνοντας εμπειρικά την ύπαρξη συγκεκριμένης κατανομής πιθανότητας για το σύνολο των προϊόντων που αναλύθηκαν.

Διάγραμμα 8: Κατανομή ευπαθειών των Windows Vista ανά ημέρα της εβδομάδας με την χρήση της OSVDB



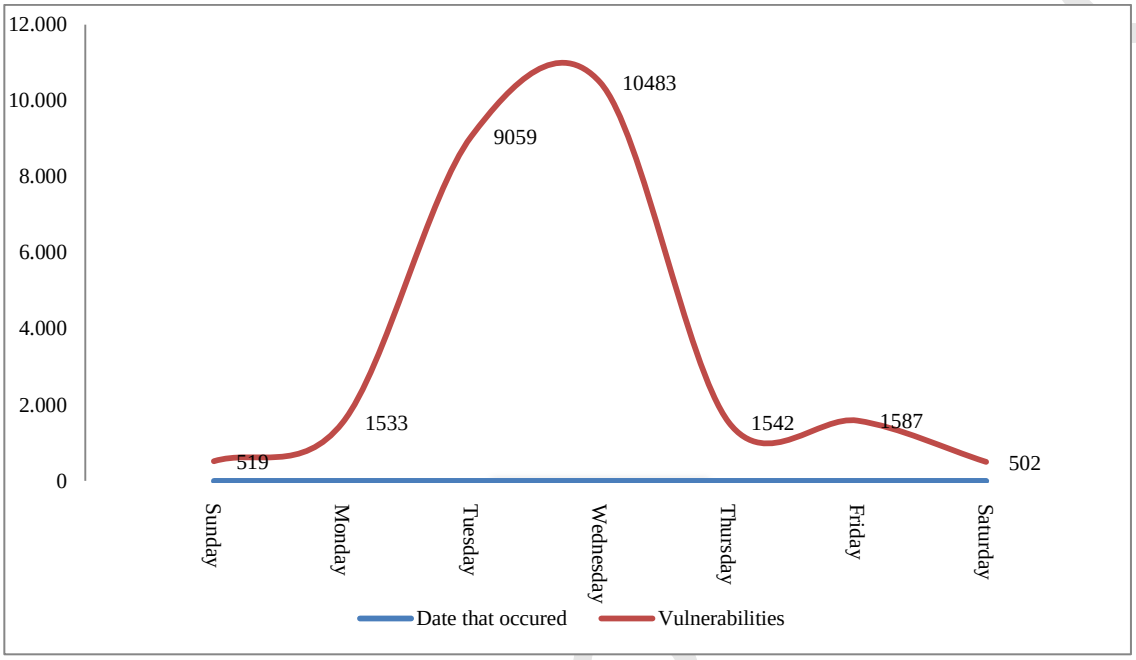
Διάγραμμα 9: Κατανομή ευπαθειών των Windows Vista ανά ημέρα της εβδομάδας με την χρήση της NVD



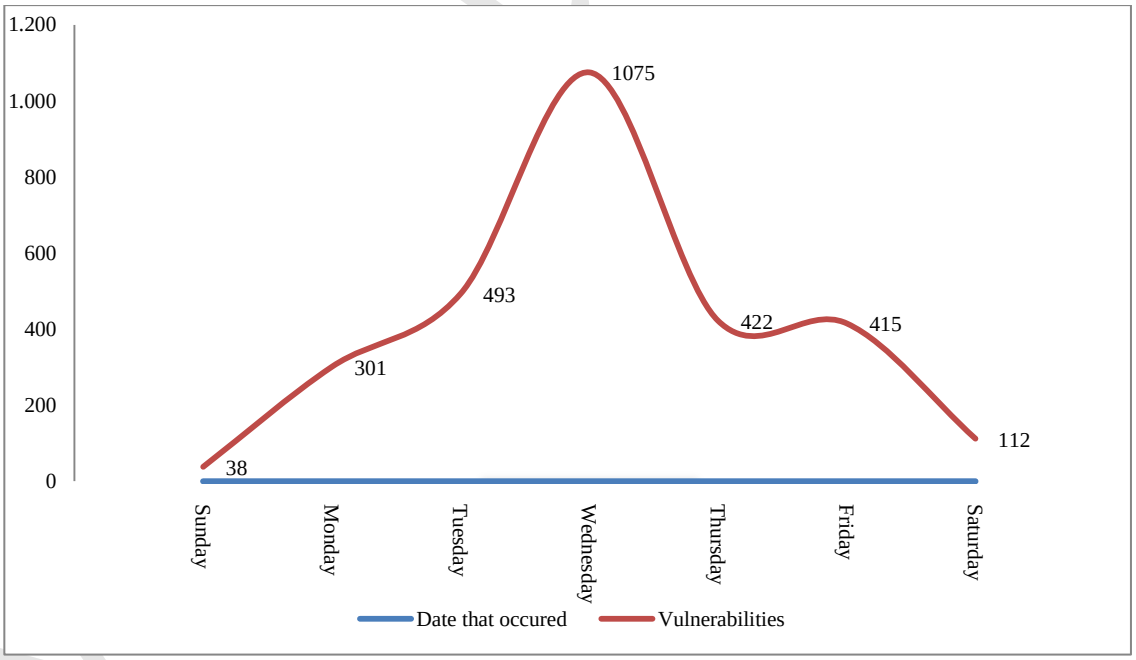
Προκειμένου να επεκτείνουμε την παραπάνω εμπειρική ανάλυση και να ερευνήσουμε κάποια περεταίρω χαρακτηριστικά στην χρονική κατανομή των ευπαθειών, πραγματοποιήθηκε ανάλυση στο σύνολο της Microsoft ως κατασκευαστή λογισμικού. Στο Διάγραμμα 10 και στο Διάγραμμα 11 απεικονίζονται οι κατανομές των ευπαθειών που παρουσιάζουν στο σύνολο τους τα προϊόντα λογισμικού της Microsoft για τα οποία υπάρχουν δεδομένα στις βάσεις που χρησιμοποιήθηκαν. Το σχήμα των κατανομών είναι κοινό με τις αντίστοιχες κατανομές των μεμονωμένων προϊόντων λογισμικού του συγκεκριμένου κατασκευαστή. Είναι πολύ σημαντικό ότι η χρονική κορύφωση των κατανομών αυτών παραμένει η ημέρα Τετάρτη σε συμφωνία με το χρονικό μοτίβο των προηγούμενων κατανομών.

Η διαπίστωση αυτή, πέρα από την εμπειρική επιβεβαίωση της κοινής κατανομής που ακολουθούν το σύνολο των παραγόντων κινδύνου που αναλύθηκαν, επιβεβαιώνει επίσης εμπειρικά την στρατηγική που ακολουθείται από την Microsoft στην διόρθωση (patching) των ευπαθειών η οποία χαρακτηριστικά ονομάζεται “Patch Tuesday” και είναι ευρέως γνωστή ανάμεσα στους ειδικούς ασφαλείας και στους διαχειριστές δικτύων.

Διάγραμμα 10: Κατανομή ευπαθειών ανά ημέρα της εβδομάδας στο σύνολο των προϊόντων της Microsoft με την χρήση της OSVDB



Διάγραμμα 11: Κατανομή ευπαθειών ανά ημέρα της εβδομάδας στο σύνολο των προϊόντων της Microsoft με την χρήση της NVD



Αναλυτικότερα, η Microsoft την δεύτερη Τρίτη κάθε μήνα εκδίδει διορθώσεις για νέες διαγνωσμένες ευπάθειες. Από την έκδοση του λειτουργικού συστήματος Windows 98, ένα νέο

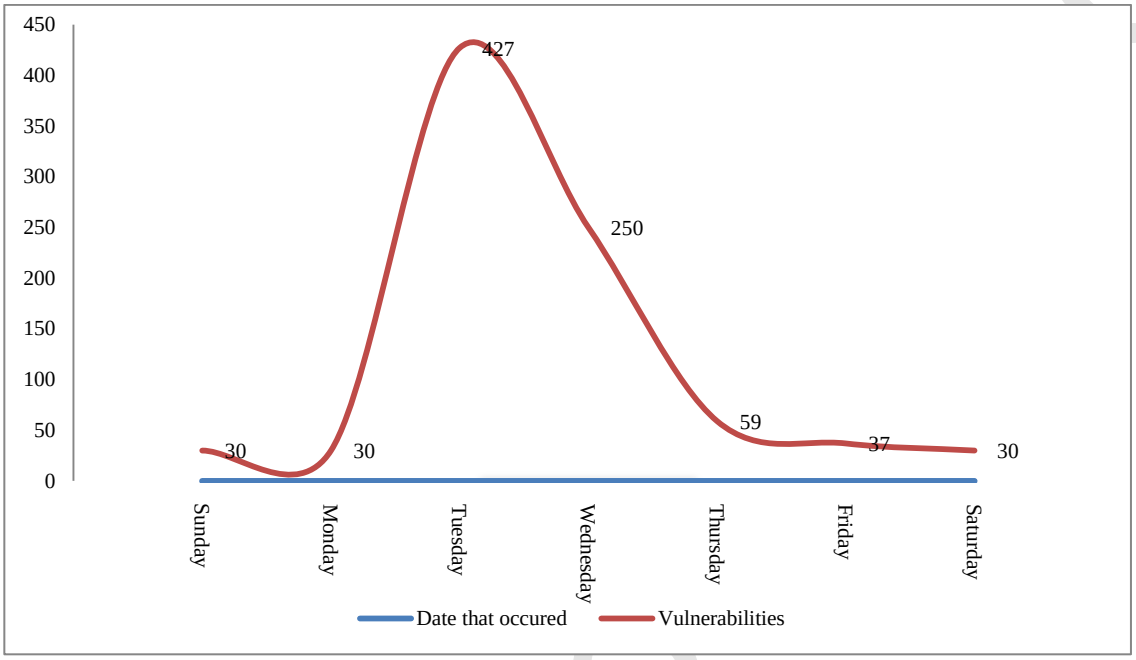
εργαλείο ενσωματώθηκε το οποίο ονομάστηκε “Windows Update”. Το εργαλείο αυτό όταν είναι ενεργοποιημένο ελέγχει αυτόματα, σε περιοδικά διαστήματα, στο διαδίκτυο για εκδόσεις διορθώσεων της Microsoft για το σύνολο των πακέτων λογισμικού των οποίων διατηρεί την υποστήριξη.

Επομένως, το γενικό συμπέρασμα που προκύπτει από το σύνολο της παραπάνω ανάλυσης είναι πως η κατανομή των ευπαθειών για το σύνολο των προϊόντων λογισμικού της συγκεκριμένης εταιρίας κορυφώνεται μία ημέρα μετά από αυτήν που συνήθως εκδίδονται οι διορθώσεις λογισμικού. Αυτό προφανώς υφίσταται λόγω της χρονικής καθυστέρησης εγκατάστασης των διορθώσεων ευπαθειών από το σύνολο των χρηστών και η σταδιακή αποκατάσταση των ενημερώσεων, οδηγεί στην σταδιακή αποκλιμάκωση της κατανομής των ευπαθειών στις ημέρες της εβδομάδας που ακολουθούν.

Η έρευνα συνεχίστηκε με την ανάλυση της κατανομής των ευπαθειών για ένα προϊόν λογισμικού με ευρεία αποδοχή και αναγνώριση στην αγορά ενός διαφορετικού κατασκευαστή. Πρόκειται για το Database 10g της Oracle το οποίο βρίσκεται στην αγορά αρκετά χρόνια ώστε να υπάρχουν αρκετά δεδομένα ευπαθειών τουλάχιστον στην βάση OSVDB. Η κατανομή που αφορά τα δεδομένα ευπαθειών, του συγκεκριμένου λογισμικού, από την NVD δεν παραθέτεται καθώς τα στοιχεία που περιλαμβάνει δεν θεωρήθηκαν επαρκή.

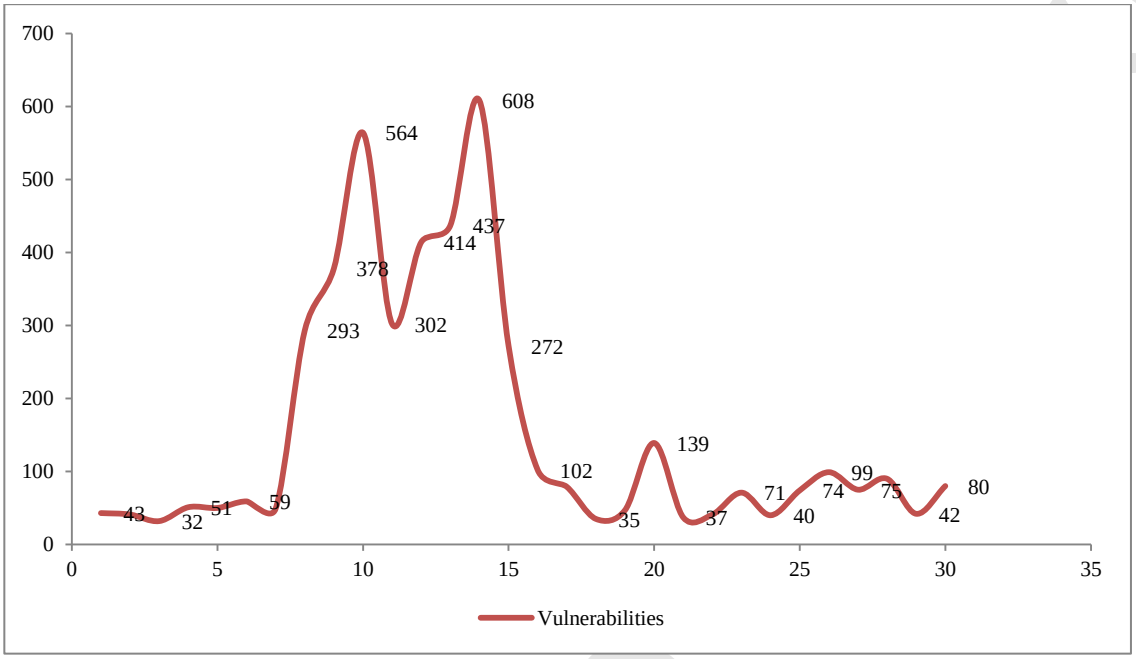
Η συγκεκριμένη ανάλυση έγινε προκειμένου να διαπιστωθεί ότι τα μοτίβα που διαγνώστηκαν στην κατανομή των ευπαθειών για τον κατασκευαστή λογισμικού Microsoft δεν εξατομικεύονται σε αυτόν. Όπως προκύπτει από το Διάγραμμα 12 η κατανομή των ευπαθειών για το συγκεκριμένο προϊόν έχει σχήμα καμπάνας και κορύφωση σε συγκεκριμένη ημέρα της εβδομάδας. Αυτό που για την Microsoft είναι κορύφωση των ευπαθειών την ημέρα Τετάρτη, είναι για την Oracle η ημέρα Τρίτη.

Διάγραμμα 12: Κατανομή ευπαθειών της Oracle Database 10g ανά ημέρα της εβδομάδας με την χρήση της OSVDB

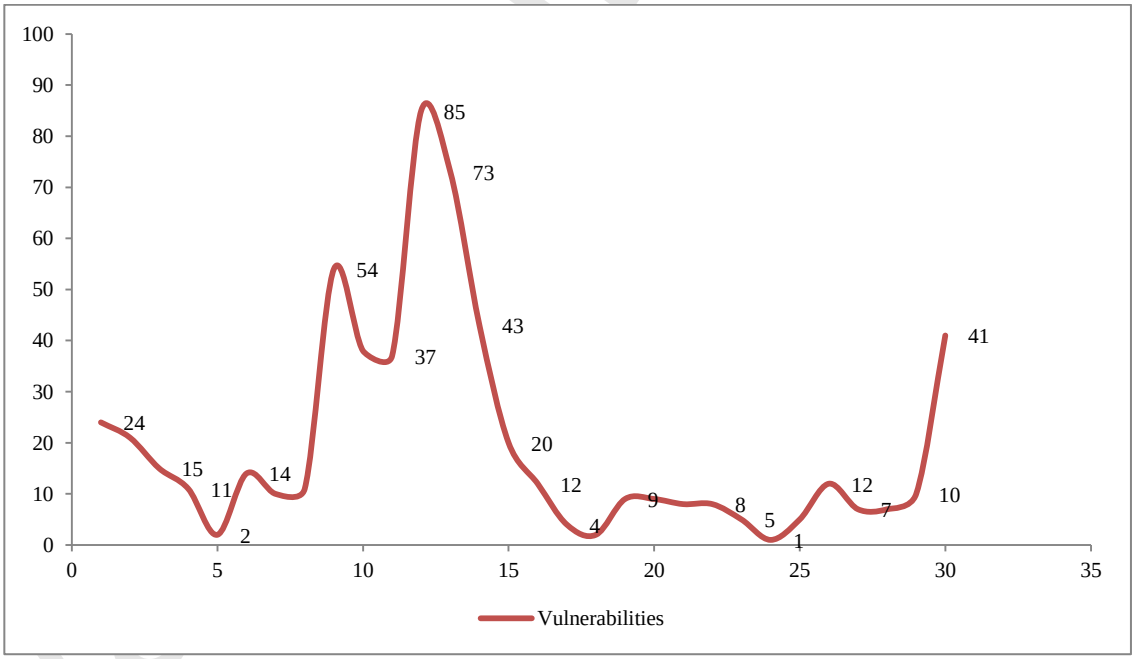


Στην συνέχεια παραθέτονται τα αποτελέσματα της εμπειρικής ανάλυσης χρησιμοποιώντας πλέον ένα ευρύτερο χρονικό πλαίσιο. Το πλαίσιο που επιλέχθηκε είναι ο μήνας με την ανάλυση σε επίπεδο ημέρας. Η επιλογή αυτή έγινε προκειμένου να επιβεβαιωθούν και ενισχυθούν τα συμπεράσματα που εξήχθησαν από την εμπειρική ανάλυση σε επίπεδο εβδομάδας. Στο Διάγραμμα 13 και στο Διάγραμμα 14 απεικονίζονται οι κατανομές ευπαθειών του λογισμικού Windows XP με τα δεδομένα των δύο βάσεων. Η σχηματική απεικόνιση των δύο κατανομών έχει κοινά χαρακτηριστικά με κύριο στοιχείο την κοινή κορύφωση την 15^{η} ημέρα του μήνα και την προσομοίωση του σχήματος καμπάνας.

Διάγραμμα 13: Κατανομή ευπαθειών των Windows XP ανά ημέρα του μήνα με την χρήση της OSVDB



Διάγραμμα 14: Κατανομή ευπαθειών των Windows XP ανά ημέρα του μήνα με την χρήση της NVD

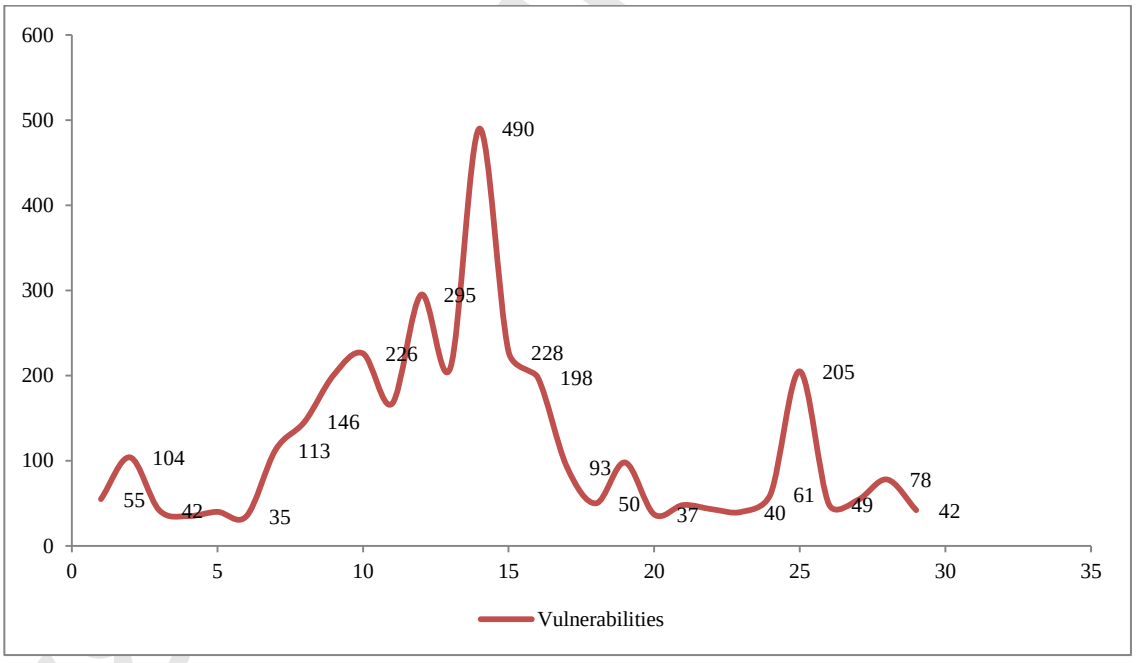


Ακολούθως, στο Διάγραμμα 15 απεικονίζεται η κατανομή των ευπαθειών για το λειτουργικό σύστημα Windows 2000 με την χρήση δεδομένων από την βάση OSVDB. Η κατανομή έχει κοινή σχηματική απεικόνιση με την αντίστοιχη κατανομή για το λειτουργικό σύστημα Windows XP. Οι

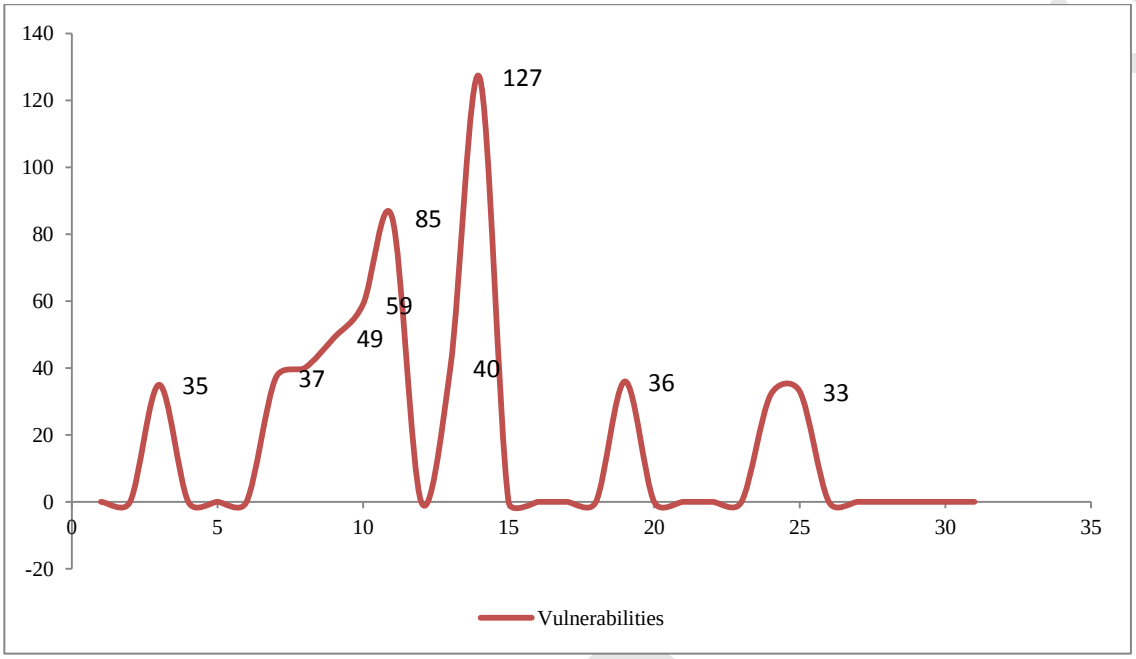
ευπάθειες κορυφώνονται την 15η ημέρα του μήνα και η κατανομή προσεγγίζει το σχήμα καμπάνας. Δεν παραθέτεται η κατανομή για το συγκεκριμένο λογισμικό χρησιμοποιώντας τα δεδομένα της βάσης NVD καθώς το σύνολο των δεδομένων δεν θεωρήθηκε επαρκές προκειμένου για την πλήρη στατιστική απεικόνιση των ευπαθειών σε διάστημα μήνα.

Στο Διάγραμμα 16 απεικονίζεται η κατανομή των ευπαθειών του Office XP με διάστημα ανάλυσης μηνός χρησιμοποιώντας δεδομένα από την βάση OSVDB. Το μοτίβο που ακολουθείται είναι αρκετά κοινό με το αντίστοιχο που παρατηρήθηκε στην ανάλυση των λοιπών προϊόντων λογισμικού του συγκεκριμένου κατασκευαστή. Τέλος, στο Διάγραμμα 17 και στο Διάγραμμα 18 παραθέτεται η κατανομή, σε διάστημα ανάλυσης μηνός για το σύνολο των προϊόντων λογισμικού της Microsoft με την χρήση δεδομένων και από τις δύο βάσεις. Οι κατανομές παρουσιάζουν κοινό μοτίβο με τις κατανομές των μεμονωμένων προϊόντων και η κορύφωση είναι πάλι γύρω από την 15η ημέρα του μήνα.

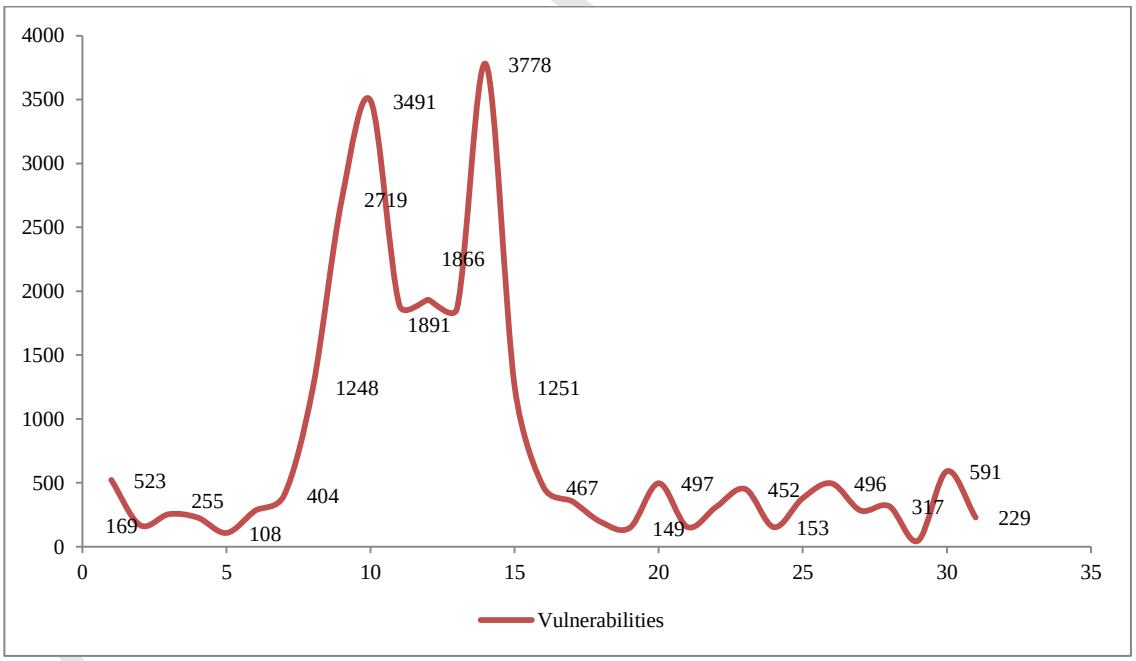
Διάγραμμα 15: Κατανομή ευπαθειών των Windows 2000 ανά ημέρα του μήνα με την χρήση της OSVDB



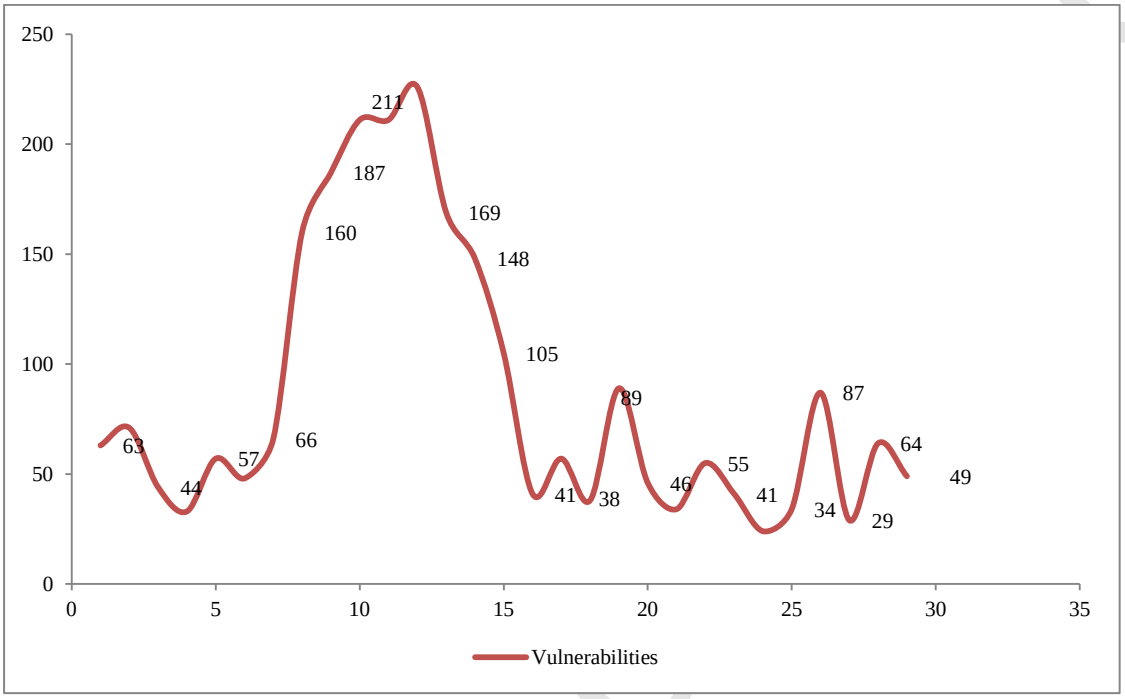
Διάγραμμα 16: Κατανομή ευπαθειών του Office XP ανά ημέρα του μήνα με την χρήση της OSVDB



Διάγραμμα 17: Κατανομή ευπαθειών ανά ημέρα του μήνα στο σύνολο των προϊόντων της Microsoft με την χρήση της OSVDB



Διάγραμμα 18: Κατανομή ευπαθειών ανά ημέρα του μήνα στο σύνολο των προϊόντων της Microsoft με την χρήση της NVD



Το σύνολο της εμπειρικής ανάλυσης, σχετικά με την κατανομή των ευπαθειών, μπορεί να οδηγήσει στην προσέγγιση των στοχαστικών συναρτήσεων που ακολουθούν οι παράγοντες κινδύνου και κατά επέκταση στην ακριβή ποσοτικοποίηση του επιπέδου ασφαλείας ενός συστήματος σε μία δεδομένη χρονική στιγμή.

Επιπλέον, η ανάλυση των χρονικών μοτίβων των ευπαθειών μπορεί να βοηθήσει τα στελέχη ενός οργανισμού, που ασχολούνται με την ασφάλεια των ΠΣ, να επιτύχουν την κατάλληλη κατανομή των διαθέσιμων πόρων την κατάλληλη χρονική στιγμή προκειμένου να πετύχουν την μέγιστη αποδοτικότητα στην αντιμετώπιση των παραβιάσεων ασφαλείας.

6.6.3 Τελικό μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας ενός συστήματος

Η προαναφερόμενη ανάλυση των χρονικών μοτίβων, που ακολουθούν οι ευπάθειες σε επίπεδο προϊόντος και κατασκευαστή λογισμικού, καταδεικνύει την ύπαρξη κοινής συμπεριφοράς στην κατανομές που ακολουθούν. Όπως αναφέρθηκε στις επί μέρους αναλύσεις των κατανομών, η

σχηματική απεικόνιση τους έχει κοινά χαρακτηριστικά τα οποία παραπέμπουν στην ακόλουθη Gaussian συνάρτηση:

$$f(t) = ae^{-\frac{(t-b)^2}{2c^2}} \qquad (20)$$

Η σταθερά a ορίζει την τιμή κορύφωσης του σχήματος καμπάνας που ακολουθεί η κατανομή της συνάρτησης. Η σταθερά b ορίζει την θέση στην οποία κορυφώνεται η κατανομή και με την σταθερά c ορίζεται το πλάτος της καμπάνας που ακολουθεί το σχήμα της κατανομής. Όπως αναφέρθηκε αρχικώς στην ενότητα 6.6.1, οι στοχαστικές συναρτήσεις που περιγράφουν την συμπεριφορά των παραμέτρων κινδύνου, εξαρτώνται από μία ανεξάρτητη μεταβλητή την t. Η μεταβλητή αυτή προσδιορίζεται από το εκάστοτε χρονικό σημείο στο οποίο υπολογίζεται το τρέχον επίπεδο ασφαλείας ενός παράγοντα κινδύνου και σε συνολικό επίπεδο ενός συστήματος.

Συνεπώς, προκειμένου να υπολογιστεί το επίπεδο ασφαλείας ενός συστήματος, πρέπει να προσεγγιστούν οι μεταβλητές a, b, c για κάθε παράγοντα κινδύνου. Η προσέγγιση, όπως καταδεικνύει η ανάλυση της συγκεκριμένης ενότητας, των συγκεκριμένων μεταβλητών μπορεί να πραγματοποιηθεί με αντικειμενικό τρόπο αξιοποιώντας τα δεδομένα που παρέχονται από τις βάσεις καταχώρησης ευπαθειών. Οι ευπάθειες, όταν αναλύονται σε επίπεδο παράγοντα κινδύνου και σε συγκεκριμένα χρονικά πλαίσια, ακολουθούν συγκεκριμένες κατανομές οι οποίες μπορούν να προσεγγιστούν με μεγάλη ακρίβεια και αντικειμενικότητα.

Συνολικά το προτεινόμενο μοντέλο, της μεθοδολογίας που αναλύθηκε στο παρόν κεφάλαιο, είναι ως εξής:

$$\text{Sec\_status}_t = \int_0^t \prod_{i=1}^{k} f_i^{\frac{1}{c_i}}(t)\, dt$$

$$\text{όπου } f_i(t) = ae^{-\frac{(t-b)^2}{2c^2}}$$

$$\text{και } c_i = -\sum_{j=1}^{n}\sum_{k=1}^{m} q_k e^{-k} w_j p_{jk} \log(p_{jk}) \quad (21)$$

Το επίπεδο ασφαλείας ενός συστήματος σε ένα συγκεκριμένο χρονικό σημείο ορίζεται από το σταθμισμένο γινόμενο των στοχαστικών συναρτήσεων του συνόλου των παραγόντων κινδύνου οι οποίες ακολουθούν της Gaussian συνάρτηση με ανεξάρτητη μεταβλητή τον χρόνο. Η στάθμιση

των στοχαστικών συναρτήσεων πραγματοποιείται μέσω των συντελεστών βαρύτητας που προσεγγίζονται από την σταθμισμένη εντροπία κάθε παράγοντα κινδύνου λαμβάνοντας υπόψη την πιθανότητα εμφάνισης ευπαθειών κάθε κατηγορίας επίπτωσης, το επίπεδο κάθε κατηγορίας επίπτωσης, τον χρόνο που υφίσταται ένα προϊόν στην αγορά, τον χρόνο που υφίσταται μία ευπάθεια και τέλος από το ποσοστό συμμετοχής διαχρονικά κάθε παράγοντα κινδύνου στο υπό ανάλυση σύστημα.

6.7 Συμπεράσματα

Στο κεφάλαιο αυτό αναλύθηκε ένα μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας ενός συστήματος με τρεις βασικές διαφοροποιήσεις σε σχέση με τις υφιστάμενες αντίστοιχες μεθοδολογίες. Η πρώτη αφορά την δυναμικότητα του μοντέλου καθώς το τελευταίο δεν είναι στατικό και ο παράγοντας χρόνος λαμβάνεται ως μεταβλητή και όχι ως σταθερά. Προς αυτή την κατεύθυνση οι στοχαστικές συναρτήσεις, που αντιπροσωπεύουν τους παράγοντες κινδύνου, εξαρτώνται αποκλειστικά από την ανεξάρτητη μεταβλητή που αντιπροσωπεύει τον παράγοντα του χρόνου. Η δεύτερη διαφοροποίηση αφορά την χρήση της στοχαστικής ανάλυσης στην ποσοτικοποίηση της ασφάλειας. Όπως προαναφέρθηκε, τα στοχαστικά εργαλεία έχουν εφαρμοστεί ευρέως σε άλλες επιστήμες όπως η Χρηματοοικονομική και μέχρι σήμερα καμία μεθοδολογία δεν εφαρμόζει την χρήση τους στην ασφάλεια των ΠΣ και στην διαχείριση των κινδύνων ΠΣ. Η τρίτη διαφοροποίηση αφορά το επίπεδο ανάλυσης ενός ΠΣ που υιοθετείται. Σε αντίθεση με τις υφιστάμενες μεθοδολογίες, οι οποίες επιμερίζονται στην ανάλυση σε επίπεδο ευπαθειών και στην ανάλυση σε κατηγορίες ευπαθειών, η προτεινόμενη μεθοδολογία λαμβάνει ένα ΠΣ ως ένα χαρτοφυλάκιο παραγόντων κινδύνου και εφαρμόζει την ανάλυση σε αυτό το επίπεδο.

Η χρήση πραγματικών δεδομένων ευπαθειών προκειμένου για τον υπολογισμό του επιπέδου επίπτωσης και της πιθανότητας εμφάνισης των ευπαθειών καθώς και η υιοθέτηση της μεθοδολογίας της εντροπίας οδήγησε στον αντικειμενικό υπολογισμό του συντελεστή βαρύτητας που έχει κάθε παράγοντας κινδύνου σε ένα σύστημα. Επίσης, η χρήση πραγματικών δεδομένων επέτρεψε στην παρούσα ερευνητική προσπάθεια την ανάλυση επαναλαμβανόμενων χρονικών μοτίβων με κοινά χαρακτηριστικά που δύναται να ακολουθούν οι παράγοντες κινδύνου που απαρτίζουν ένα σύστημα. Το σύνολο της ανάλυσης απέδωσε χρήσιμα συμπεράσματα σχετικά με

τις κατανομές πιθανοτήτων των παραγόντων κινδύνου παρέχοντας εμπειρική επιβεβαίωση στις παραδοχές του προτεινόμενου μοντέλου.

Η σχηματική απεικόνιση των προαναφερόμενων κατανομών ακολουθεί κοινά επαναλαμβανόμενα μοτίβα τα οποία προσεγγίζουν την Gaussian συνάρτηση. Η υιοθέτηση της συγκεκριμένης συνάρτησης, ορισμένης στην μεταβλητή του χρόνου, τροποποίησε καταλλήλως το προτεινόμενο μοντέλο το οποίο κατέληξε στην τελική του μορφή. Η αξιοποίηση της συγκεκριμένης μεθοδολογίας ποσοτικοποίησης της ασφάλειας στον προσδιορισμό των κινδύνων παραβιάσεων ασφαλείας αναλύεται στο κεφάλαιο 7 ενώ προτάσεις για την μελλοντική τροποποίηση του προτεινόμενου μοντέλου και την χαλάρωση των παραδοχών που θέτονται παραθέτονται στο κεφάλαιο 8.

7 Ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας

7.1 Εισαγωγή

Στο παρόν κεφάλαιο πραγματοποιείται σύνθεση των θεματικών ενοτήτων που ερευνήθηκαν στο σύνολο της διατριβής και των ερευνητικών αποτελεσμάτων που προέκυψαν με κύριο στόχο την δημιουργία ενός μοντέλου ποσοτικοποίησης των κινδύνων που προέρχονται από παραβιάσεις ασφαλείας. Τα συστατικά στοιχεία του προτεινόμενου μοντέλου, προέρχονται από το μεθοδολογικό πλαίσιο που τέθηκε στα κεφάλαια 5 και 6 σχετικά με την ανάλυση των ασυνήθη αποδόσεων και την ποσοτικοποίηση του επιπέδου ασφαλείας αντιστοίχως ενώ το σύνολο της ανάλυσης βασίζεται στο θεωρητικό υπόβαθρο σχετικά με τους κινδύνους ΠΣ, που αναλύθηκε στα κεφάλαια 2 και 3. Το υπόβαθρο αυτό συνδέθηκε με το αντίστοιχο θεωρητικό πλαίσιο των παραβιάσεων ασφαλείας, που περιγράφτηκε στην ενότητα 4.2, προκειμένου για την περαιτέρω ανάπτυξη της έννοιας των κινδύνων παραβιάσεων ασφαλείας.

Επίσης, αναλύεται το βασικό πλαίσιο της μεθοδολογίας VaR που χρησιμοποιείται κατά κύριο λόγο από τον χρηματοπιστωτικό τομέα για τον υπολογισμό των οικονομικών κινδύνων. Λαμβάνοντας υπόψη την επιτυχημένη χρήση της συγκεκριμένη μεθοδολογίας σε αυτούς τους τύπους εταιριών και υπάρχουσες προτάσεις της ακαδημαϊκής κοινότητας, ερευνήθηκε ο τρόπος εφαρμογής του στην ανάλυση των κινδύνων παραβιάσεων ασφαλείας. Η συγκεκριμένη προσπάθεια στηρίχθηκε στα ερευνητικά ευρήματα εκ του συνόλου της διατριβής και κατά κύριο λόγο στο μοντέλο ποσοτικοποίησης των κινδύνων παραβιάσεων ασφαλείας που αναλύεται στο παρόν κεφάλαιο.

Στην επόμενη ενότητα αναπτύσσεται η έννοια των κινδύνων παραβιάσεων ασφαλείας με την ανάλυση να στηρίζεται στο σύνολο της ερευνητικής προσπάθειας. Ο κύριος στόχος είναι η λεπτομερής περιγραφή των στοιχείων που συνθέτουν αυτούς τους κινδύνους και της σχέσης που έχουν μεταξύ τους. Στην τρίτη ενότητα αναπτύσσεται ένα μεθοδολογικό πλαίσιο για τον υπολογισμό της πιθανότητας πραγμάτωσης παραβιάσεων ασφαλείας. Το πλαίσιο βασίζεται σε δύο κύριες μεθοδολογικές περιοχές: Το μοντέλο των Gordon-Loeb για τον υπολογισμό του βέλτιστου επιπέδου επένδυσης στην ασφάλεια και το μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας που αναπτύχθηκε στο κεφάλαιο 6. Στην τέταρτη ενότητα αναπτύσσεται το αντίστοιχο μεθοδολογικό

πλαίσιο για τον υπολογισμό της επίπτωσης που προκαλείται από παραβιάσεις ασφαλείας το οποίο βασίζεται στα ερευνητικά ευρήματα που περιγράφτηκαν στα κεφάλαια 4 και 5. Στην επόμενη ενότητα πραγματοποιείται σύνθεση όλων των προαναφερομένων και αναπτύσσεται το μοντέλο ποσοτικοποίησης των κινδύνων παραβιάσεων ασφαλείας που προτείνεται από την παρούσα διατριβή. Στην πέμπτη ενότητα γίνεται εφαρμογή της μεθοδολογίας VaR η οποία στηρίζεται στο συγκεκριμένο μοντέλο ενώ στην τελευταία ενότητα αναφέρονται κάποιες συμπερασματικές παρατηρήσεις.

7.2 Τα στοιχεία που συνθέτουν τους κινδύνους παραβιάσεων ασφαλείας

Στην ενότητα αυτή αναλύεται η σχέση μεταξύ των στοιχείων που συνθέτουν τους κινδύνους από παραβιάσεις ασφαλείας. Η ανάλυση γίνεται με βασικό στόχο τον προσδιορισμό των μεταβλητών που επηρεάζουν τις δύο βασικές παραμέτρους του κινδύνου: (α) Πιθανότητα πραγμάτωσης ενός γεγονότος και (β) επίπτωση από την πραγμάτωση ενός γεγονότος. Τα στοιχεία που συνθέτουν τους κινδύνους ΠΣ είναι τα εξής:

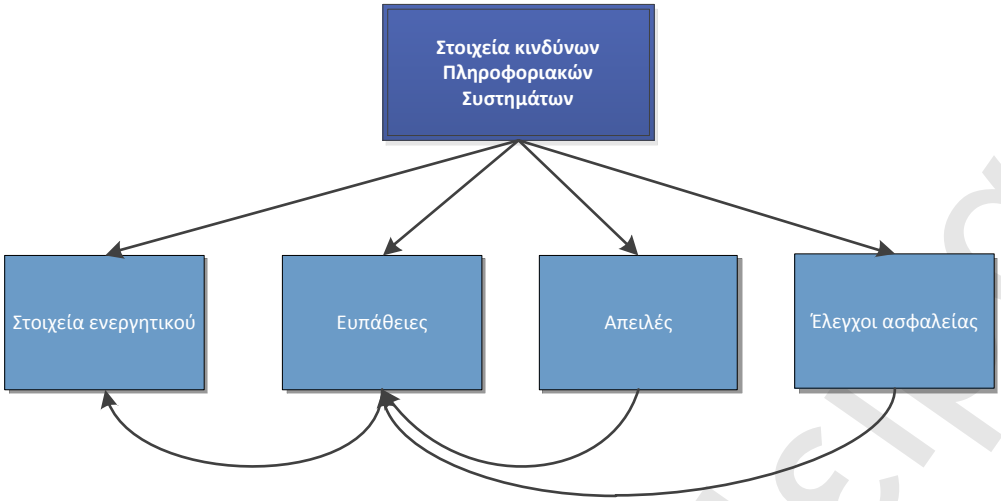
(α) Οι ευπάθειες που έχει ένα ΠΣ

(β) Οι πηγές απειλής για την ασφάλεια ενός ΠΣ

(γ) Τα μέτρα ασφαλείας ενός ΠΣ

(δ) Τα στοιχεία ενεργητικού που αποτελούν ένα ΠΣ

Γενική περιγραφή των παραπάνω στοιχείων πραγματοποιήθηκε στην ενότητα 2.4.2. Μία αρχική απεικόνιση της σχέσης των δομικών στοιχείων των κινδύνων ΠΣ γίνεται στην Εικόνα 15. Όπως φαίνεται οι ευπάθειες αφορούν τα στοιχεία ενεργητικού που συνθέτουν τα ΠΣ ενός οργανισμού. Ουσιαστικά αποτελούν μέρος της οντότητας των στοιχείων ενεργητικού και η ύπαρξη τους είναι ανεξάρτητη από τις πηγές απειλής. Όπως επίσης αποτυπώνεται, οι πηγές απειλής επιχειρούν να εκμεταλλευθούν τις υπάρχουσες ευπάθειες προκειμένου να παραβιάσουν την ασφάλεια των στοιχείων ενεργητικού. Τέλος, οι έλεγχοι ασφαλείας εστιάζουν στις ευπάθειες που έχουν τα στοιχεία ενεργητικού των ΠΣ προκειμένου για την προστασία των τελευταίων από τις πηγές απειλής.



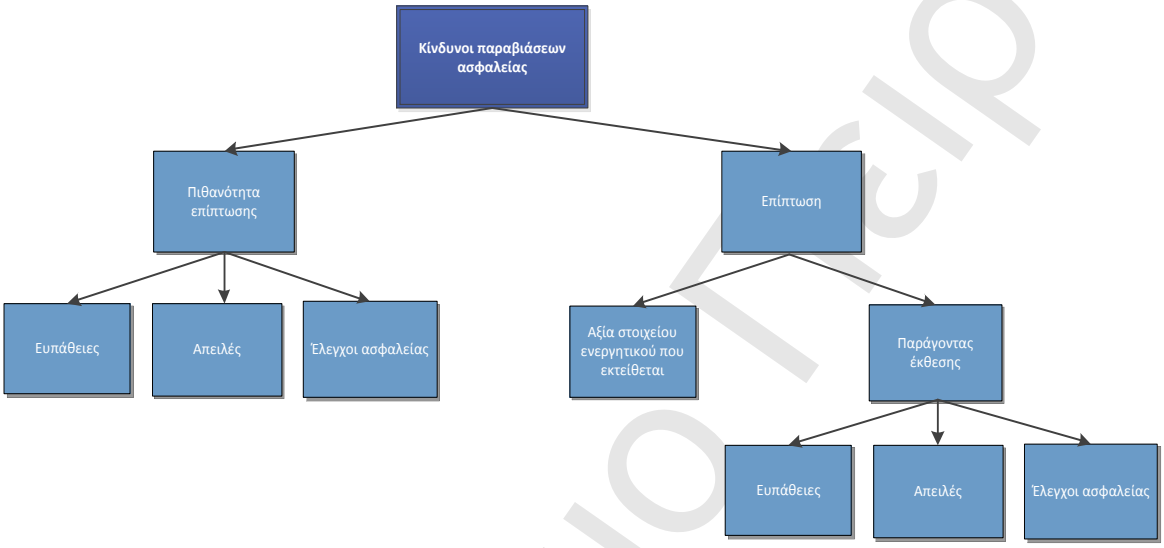
Εικόνα 15: Στοιχεία κινδύνων πληροφοριακών συστημάτων

Στην παρούσα ενότητα η ανάλυση της υπόστασης και συσχέτισης των παραπάνω στοιχείων γίνεται με επικέντρωση στους κινδύνους παραβιάσεων ασφαλείας. Όπως αναλύθηκε στην ενότητα 2.2, οι δύο βασικές παράμετροι που προσδιορίζουν κάθε εταιρικό κίνδυνο είναι η πιθανότητα πραγμάτωσης ενός ανεπιθύμητου συμβάντος και η επίπτωση του ανεπιθύμητου συμβάντος στα στοιχεία ενεργητικού που εκτίθενται. Οι δύο προαναφερόμενες παράμετροι προσδιορίζουν επίσης τους κινδύνους παραβιάσεων ασφαλείας με το ανεπιθύμητο συμβάν να είναι η παραβίαση ασφαλείας ενός ΠΣ.

Συνεπώς, από την μέχρι τώρα ανάλυση προκύπτει πως η υπόσταση των κινδύνων παραβιάσεων ασφαλείας μπορεί να λάβει δύο θεωρήσεις οι οποίες συνδέονται μεταξύ τους: (α) Γενική θεώρηση η οποία βασίζεται στις δύο βασικές παραμέτρους που καθορίζουν κάθε εταιρικό κίνδυνο. (β) Ειδική θεώρηση η οποία βασίζεται στα δομικά στοιχεία που συνθέτουν τους κινδύνους ΠΣ.

Προκειμένου να κατανοηθεί η υπόσταση κάθε μίας εκ των δύο βασικών παραμέτρων της γενικής θεώρησης προσδιορισμού των κινδύνων παραβιάσεων ασφαλείας, επιχειρήθηκε η σύνδεση τους με τα στοιχεία που συνθέτουν την ειδική θεώρηση των κινδύνων ΠΣ. Η ανάλυση που ακολουθεί αποτελεί επέκταση της εξέτασης των παραμέτρων κινδύνων ΠΣ που πραγματοποιήθηκε στην ενότητα 3.2.2, στα πλαίσια της περιγραφής του σταδίου εκτίμησης των κινδύνων ΠΣ του γενικότερου πλαισίου διαδικασιών ΔΚΠΣ. Η ανάλυση στο παρόν κεφάλαιο επικεντρώνεται στους κινδύνους παραβιάσεων ασφαλείας επιχειρώντας την εξειδίκευση των

βασικών θεωρητικών δομών, που έχουν τεθεί στην διατριβή σχετικά με τους εταιρικούς κινδύνους και τους κινδύνους ΠΣ, με γνώμονα τους κινδύνους παραβιάσεων ασφαλείας. Προς αυτή την κατεύθυνση η Εικόνα 7 την ενότητας 3.2.2 προσαρμόστηκε καταλλήλως όπως φαίνεται στην Εικόνα 16 προκειμένου να εξυπηρετήσει την ανάλυση και κατανόηση της υπόστασης των κινδύνων παραβιάσεων ασφαλείας.



Εικόνα 16: Κίνδυνοι παραβιάσεων ασφαλείας

7.2.1 Ανάλυση της πιθανότητας επίπτωσης

Όπως φαίνεται στην Εικόνα 16, η παράμετρος της πιθανότητας επίπτωσης εξαρτάται από τρία εκ των βασικών στοιχείων που συνθέτουν τους κινδύνους παραβιάσεων ασφαλείας: Από τις ευπάθειες, τις απειλές και τα μέτρα ασφαλείας. Ο αριθμός των ευπαθειών που έχουν τα ΠΣ ενός οργανισμού αποτελεί σημαντικό προσδιοριστικό παράγοντα της πιθανότητας πραγμάτωσης μίας παραβίασης ασφαλείας. Ο αριθμός των απειλών για τα ΠΣ ενός οργανισμού, που έχουν το κίνητρο και την ικανότητα επίθεσης, αποτελεί επίσης έναν σημαντικό παράγοντα προσδιορισμού της πιθανότητας παραβιάσεων ασφαλείας. Όπως έχει ήδη αναλυθεί στην ενότητα 2.4.2, η ύπαρξη μόνο ενός εκ των δύο προαναφερόμενων στοιχείων δεν συνεπάγεται κίνδυνο. Η πιθανότητα παραβίασης ασφαλείας εξαρτάται από τον συνδυασμό και των δύο αυτών στοιχείων. Επιπλέον, η πιθανότητα εξαρτάται από την αποτελεσματικότητα και πληρότητα των ελέγχων ασφαλείας που έχει εφαρμόσει ένας οργανισμός προκειμένου για την προστασία των ΠΣ του.

Η πιθανότητα πραγμάτωσης ενός αβέβαιου γεγονότος, που προκαλεί έναν συγκεκριμένο κίνδυνο, αναφέρεται σε συγκεκριμένο χρονικό ορίζοντα το μέγεθος του οποίου εξαρτάται από την φύση εκάστοτε κινδύνου. Στην περίπτωση των κινδύνων που προκαλούνται από παραβιάσεις ασφαλείας, ο χρονικός ορίζοντας στον οποίο υπολογίζεται η πιθανότητα πραγμάτωσης των γεγονότων παραβίασης ασφαλείας θέτεται ως ένα έτος. Οι δύο βασικοί λόγοι που οδηγούν σε αυτήν την επιλογή είναι πρώτον η συχνότητα που γενικώς παρουσιάζουν ως φαινόμενο οι παραβιάσεις ασφαλείας σε έναν οργανισμό και δεύτερον η χαμηλή μεταβλητότητα της αξίας των στοιχείων ενεργητικού ενός ΠΣ. Η χαμηλή συχνότητα που έχουν από την φύση τους τα γεγονότα παραβίασης ασφαλείας, σε σχέση με άλλα γεγονότα που προκαλούν λοιπούς εταιρικούς κινδύνους, οδηγεί στην επιλογή ετήσιας βάσης για τον προσδιορισμό της πιθανότητας τους προκειμένου να καθίσταται δυνατή η δημιουργία επαρκούς συνόλου δεδομένων για την στατιστική ανάλυση. Επίσης, η επιλογή του συγκεκριμένου χρονικού ορίζοντα δικαιολογείται και από την μικρή μεταβλητότητα στο χρόνο που παρουσιάζει η αξία των στοιχείων ενεργητικού που προσβάλλονται από τις παραβιάσεις ασφαλείας με συνέπεια η παραδοχή, ότι οι αξίες αυτές παραμένουν σταθερές σε ένα ετήσιο διάστημα ανάλυσης, να θεωρείται ως βάσιμη.

Η πιθανότητα επίπτωσης που αποσκοπούμε να προσδιορίσουμε αφορά την πιθανότητα ένας αριθμός παραβιάσεων ασφαλείας να πραγματοποιηθεί στα ΠΣ ενός οργανισμού μέσα σε διάστημα ενός έτους. Συνεπώς, δεν μας ενδιαφέρει ο υπολογισμός της πιθανότητας μίας απώλειας (single-loss expectancy) σε ένα έτος αλλά ο υπολογισμός της πιθανότητας του αναμενόμενου ή μέσου αριθμού απωλειών μέσα σε ένα έτος.

7.2.2 Ανάλυση της επίπτωσης

Η παράμετρος που αφορά την επίπτωση που επιφέρει ένα περιστατικό παραβίασης ασφαλείας εξαρτάται από δύο βασικά στοιχεία όπως φαίνεται στην Εικόνα 16: Την αξία του στοιχείου ενεργητικού ενός ΠΣ που εκτίθεται σε ένα περιστατικό και του επιπέδου στο οποίο ανέρχεται ο παράγοντας έκθεσης. Η ανάλυση των επιπτώσεων που προκαλούνται από περιστατικά παραβιάσεων ασφαλείας αποκαλείται επίσης Ανάλυση Εταιρικής Επίπτωσης (Business Impact Analysis) και εξαρτάται από τις παραμέτρους που καθορίζουν την κρισιμότητα των στοιχείων ενεργητικού που εκτίθενται καθώς και το μέγεθος του παράγοντα έκθεσης. Το μέγεθος της επίπτωσης μίας παραβίασης ασφαλείας ουσιαστικά είναι ο βαθμός εξασθένισης της δυνατότητας

ενός οργανισμού προκειμένου να επιτελέσει την εταιρική αποστολή. Κατά κύριο λόγο το επίπεδο διατάραξης της ομαλής λειτουργίας ενός ο οργανισμού εξαρτάται από την κρισιμότητα και ευαισθησία των ΠΣ και των δεδομένων που διαχειρίζονται.

Η αξία του στοιχείου ενεργητικού, που αναμένεται να δεχθεί μία επίθεση παραβίασης ασφαλείας, αποτελεί καθοριστικό παράγοντα για τον προσδιορισμό της αναμενόμενης επίπτωσης. Αν η αξία του εκτιθέμενου στοιχείου είναι ιδιαίτερα χαμηλή τότε ο κίνδυνος θα είναι επίσης χαμηλός ακόμα και αν ο παράγοντας έκθεσης και η πιθανότητα πραγμάτωσης είναι σε υψηλά επίπεδα. Όπως αναφέρθηκε στην παράγραφο 3.2.1, η κατάταξη των στοιχείων ενεργητικού, που απαρτίζουν τα ΠΣ ενός οργανισμού, αποτελεί βασικό παράγοντα κατά τον προσδιορισμό των κινδύνων ΠΣ. Κατά αναλογία, στην περίπτωση των κινδύνων παραβιάσεων ασφαλείας, τα στοιχεία ενεργητικού με την μεγαλύτερη αξία είναι αυτά που δύναται να παρουσιάσουν το μεγαλύτερο επίπεδο κινδύνου.

Ο παράγοντας έκθεσης αποτελεί την δεύτερη παράμετρο που προσδιορίζει την επίπτωση και υπολογίζεται ως το ποσοστό από την αξία ενός στοιχείου που αναμένεται να απολεσθεί από την πραγμάτωση μίας παραβίασης ασφαλείας. Το επίπεδο του παράγοντα έκθεσης εξαρτάται από τα ίδια στοιχεία που προσδιορίζουν την πιθανότητα επίπτωσης.

Αναλυτικότερα, η φύση των ευπαθειών που παρουσιάζει ένα ΠΣ διαδραματίζει σημαντικό ρόλο στον προσδιορισμό της έκθεσης σε κίνδυνο που δύναται να επιφέρουν σε έναν οργανισμό. Ευπάθειες που εκθέτουν στοιχεία ενός ΠΣ, τα οποία χαρακτηρίζονται ως κρίσιμης σημασίας, μπορούν να οδηγήσουν σε υψηλή έκθεση κινδύνων παραβιάσεων ασφαλείας. Όπως αναφέρθηκε στην ανάλυση της πιθανότητας επίπτωσης, οι ευπάθειες πρέπει να συνδυαστούν με πηγές απειλών προκειμένου να προκαλέσουν κινδύνους. Πηγές απειλών με μεγάλη ικανότητα παραβίασης των αντίμετρων ασφαλείας και με ισχυρά κίνητρα έχουν την δυναμική, εφόσον συνδυαστούν με τις κατάλληλες ευπάθειες, να προκαλέσουν υψηλή έκθεση σε κίνδυνο.

Οι έλεγχοι ή αντίμετρα ασφαλείας αποτελούν το τρίτο στοιχείο που προσδιορίζει το επίπεδο του παράγοντα έκθεσης. Ένας έλεγχος ασφαλείας, έστω και αν δεν αποτρέψει μία παραβίαση ασφαλείας, μπορεί να περιορίσει την διαρροή ευαίσθητων πληροφοριών σε τρίτους οδηγώντας συνεπώς σε περιορισμό του παράγοντα έκθεσης. Με άλλα λόγια ένας έλεγχος ασφαλείας, μειώνοντας τον αριθμό των εγγραφών που εκτίθενται από μία παραβίαση ασφαλείας, περιορίζει

το μέγεθος της οικονομικής επίπτωσης που επέρχεται. Η μείωση της οικονομικής επίπτωσης είναι ταυτόχρονα μείωση της έκθεσης στον κίνδυνο.

7.3 Υπολογισμός της πιθανότητας πραγμάτωσης παραβιάσεων ασφάλειας

Όπως αναλύθηκε στην προηγούμενη ενότητα η πιθανότητα παραβίασης ασφαλείας αποτελεί μία εκ των σημαντικών παραμέτρων που ορίζουν τους κινδύνους που προέρχονται από παραβιάσεις ασφαλείας. Αποτελεί επίσης την δυσκολότερη παράμετρο προκειμένου για την ακριβή και αντικειμενική εκτίμηση της. Όπως έχει ήδη εκτενώς αναλυθεί, η πιθανότητα παραβίασης ασφαλείας εξαρτάται από τρεις μεταβλητές οι οποίες προσδιορίζονται από την κατάσταση που εμφανίζουν, σε ένα συγκεκριμένο σύστημα, οι ευπάθειες, οι απειλές και τα αντίμετρα ασφαλείας σε μία δεδομένη χρονική στιγμή. Συνεπώς, η επιχείρηση μοντελοποίησης της πιθανότητας παραβίασης ασφαλείας πρέπει να λάβει υπόψη τις τρεις προαναφερόμενες μεταβλητές.

Η παρούσα ανάλυση βασίζεται στην μεθοδολογία που περιγράφτηκε στο κεφάλαιο 6, σχετικά με την ποσοτικοποίηση του επιπέδου ασφαλείας ενός συστήματος, σε συνδυασμό με την μεθοδολογία των Gordon & Loeb σχετικά με την μοντελοποίηση του βέλτιστου επιπέδου επένδυσης για την ασφάλεια [**116**]. Οι συγκεκριμένοι μελετητές προσδιόρισαν την πιθανότητα παραβίασης ασφαλείας ως συνάρτηση δύο τυχαίων μεταβλητών: Η πρώτη αφορά το επίπεδο επένδυσης σε αντίμετρα ασφαλείας και η δεύτερη την πιθανότητα μία απειλή να προκαλέσει μία επιτυχημένη επίθεση. Όρισαν δύο γενικές ομάδες συναρτήσεων για τον προσδιορισμό της πιθανότητας με τις δύο προαναφερόμενες μεταβλητές ως ανεξάρτητες μεταβλητές και θέτοντας έναν αριθμό σταθερών παραμέτρων οι οποίες προσδιορίζουν την παραγωγικότητα των αντίμετρων ασφαλείας που έχουν εγκατασταθεί σε ένα σύστημα. Οι σταθερές αυτές ουσιαστικά προσδιορίζουν την αποτελεσματικότητα των επενδύσεων σε μέτρα ασφαλείας στην μείωση της πιθανότητας παραβιάσεων ασφαλείας.

Σύμφωνα με μεταγενέστερες μελέτες, οι οποίες έχουν επιχειρήσει να επεκτείνουν και επαληθεύσουν εμπειρικά το μοντέλο των Gordon & Loeb όπως η [**117**], καμία ομάδα συναρτήσεων προσδιορισμού της πιθανότητας παραβιάσεων ασφαλείας δεν έχει επαρκώς επαληθευθεί εμπειρικά. Συνεπώς στην παρούσα μελέτη, ενώ επιχειρείται η επέκταση του

συγκεκριμένου μοντέλου, δεν υιοθετείται κάποια συγκεκριμένη εκ των προαναφερομένων συναρτήσεων. Θέτονται οι αναγκαίες παραδοχές και καθορίζονται οι σχέσεις μεταξύ των διαφόρων τυχαίων μεταβλητών που μετέχουν στον προσδιορισμό της πιθανότητας που έχει ένα σύστημα, σε μία δεδομένη στιγμή, να δεχθεί παραβίαση ασφαλείας.

Χρησιμοποιήθηκε ένα μείγμα του συμβολισμού που ακολουθήθηκε μέχρι αυτό το σημείο της διατριβής και του συμβολισμού που χρησιμοποίησαν οι Gordon & Loeb όπου στο έξης, για λόγους συντομίας, θα αναφέρονται ως GL. Θέτουμε ως $z_t > 0$ το ύψος της επένδυσης ενός οργανισμού σε μέτρα ασφαλείας σε μία δεδομένη χρονική στιγμή το οποίο μετράται σε νομισματικές μονάδες. Επίσης θέτουμε ως $u_t \in [0,1]$ την πιθανότητα μία απειλή να προκαλέσει μία πετυχημένη επίθεση. Οι GL υποδήλωσαν με $S(z,u)$ την συνάρτηση της πιθανότητας παραβίασης ασφαλείας η οποία εξαρτάται από τον βαθμό ευπάθειας ενός συστήματος με δεδομένο ένα συγκεκριμένο επίπεδο επένδυσης σε μέτρα ασφαλείας. Ο βαθμός ευπάθειας του συστήματος προσδιορίζεται από την πιθανότητα μία απειλή να προκαλέσει μία παραβίαση ασφαλείας.

Προκειμένου να υπολογιστεί η μεταβλητή u προτείνεται επέκταση του μοντέλου των GL κάνοντας χρήση της μεθοδολογίας που προτάθηκε στο κεφάλαιο 6. Συγκεκριμένα θέτουμε ότι το επίπεδο ασφαλείας ενός συστήματος σε μία δεδομένη στιγμή προσδιορίζει τον βαθμό ευπάθειας του συστήματος. Θέτοντας ως Sec_Status_t, το επίπεδο ασφαλείας ενός συστήματος μία δεδομένη στιγμή, προτείνεται ο υπολογισμός της μεταβλητής u_t με τον παρακάτω τύπο:

$$u_t = 1 - Sec\_Status_t \qquad (22)$$

Καθώς η τυχαία μεταβλητή $Sec\_Status_t \in [0,1]$, τότε και η τυχαία μεταβλητή $u_t \in [0,1]$. Η τρίτη μεταβλητή, που προσδιορίζει τη πιθανότητα παραβίασης ασφαλείας, είναι η κατάσταση των απειλών σε μία δεδομένη στιγμή. Από το σύνολο της ερευνητικής προσπάθειας προέκυψε το συμπέρασμα πως η συγκεκριμένη μεταβλητή εξαρτάται κατά κύριο λόγο από τον οικονομικό κλάδο στον οποίο ανήκει ένας οργανισμός ενός αντιθέτως δεν διαπιστώθηκε ανάλογη σχέση για τις άλλες δύο παραμέτρους που προσδιορίζουν την πιθανότητα παραβίασης ασφαλείας.

Με βάση τα παραπάνω θέτουμε την παραδοχή ότι δεν υπάρχει σημαντική συσχέτιση μεταξύ του κλάδου δραστηριότητας ενός οργανισμού και του επιπέδου ασφαλείας, όπως αυτό έχει ήδη

προσδιορισθεί. Επίσης, θέτουμε την παραδοχή πως δεν υφίσταται σημαντική συσχέτιση μεταξύ του κλάδου δραστηριότητας ενός οργανισμού και του επιπέδου επενδύσεων για την ασφάλεια. Αντιθέτως, υποστηρίζουμε την ύπαρξη σημαντικής συσχέτισης μεταξύ κλάδου δραστηριότητας και των απειλών. Συγκεκριμένοι τύποι οργανισμών δημιουργούν μεγαλύτερο κίνητρο επίθεσης και επικεντρώνουν μεγαλύτερο αριθμό επιτιθέμενων με υψηλότερα επίπεδα ικανοτήτων οδηγώντας συνεπώς σε αύξηση την πιθανότητα παραβίασης ασφαλείας.

Συνεπώς, προτείνεται η χρήση της συγκεκριμένης σχέσης για τον προσδιορισμό της συγκεκριμένης μεταβλητής. Συγκεκριμένα, το ζητούμενο είναι ο προσδιορισμός της κατανομής πιθανοτήτων που έχουν οι οργανισμοί, που ανήκουν σε κάθε οικονομικό κλάδο, να δεχθούν συγκεκριμένο αριθμό επιθέσεων. Η πιθανότητα παραβίασης ασφαλείας ορίζεται ως η αναμενόμενη τιμή της κατανομής πιθανοτήτων που έχει ο αριθμός των παραβιάσεων ασφαλείας που εκτιμάται να δεχθεί ένας οργανισμός συγκεκριμένου κλάδου μέσα σε ένα διάστημα δώδεκα μηνών. Θέτουμε ως $S_y > 0$ τον αναμενόμενο αριθμό επιθέσεων παραβίασης ασφαλείας για έναν κλάδο της οικονομίας y.

Συνδυάζοντας τον προσδιορισμό που προτάθηκε για το σύνολο των τριών παραμέτρων μπορούμε να προχωρήσουμε σε μία συνολική διατύπωση της μεθοδολογίας που προτείνεται. Η πιθανότητα ένας οργανισμός να δεχθεί μία παραβίαση ασφαλείας σε μία δεδομένη χρονική στιγμή, είναι συνάρτηση του επιπέδου ασφαλείας που εμφανίζουν τα ΠΣ που χρησιμοποιεί, του επιπέδου των επενδύσεων που έχει αφιερώσει στην ασφάλεια και της παραγωγικότητας των επενδύσεων αυτών στην μείωση της πιθανότητας παραβίασης ασφαλείας. Ακολούθως, λαμβάνεται υπόψη ο αναμενόμενος αριθμός των επιθέσεων σε ετήσια βάση, που αναμένεται να δεχθεί ένας οργανισμός, με βάση την κατανομή πιθανότητας επιθέσεων που προσδιορίζεται για τον κλάδο της οικονομίας στον οποίο ανήκει. Ο συνδυασμός των παραπάνω παραμέτρων αποδίδει τον αναμενόμενο αριθμό επιθέσεων για έναν οργανισμό σταθμισμένο στην πιθανότητα που έχει κάθε παραβίαση ασφαλείας. Το τελικό μέγεθος μπορεί να συνδυαστεί με την εκτιμώμενη οικονομική επίπτωση κάθε παραβίασης ασφαλείας προκειμένου για τον προσδιορισμό των κινδύνων παραβιάσεων ασφαλείας όπως θα αναλυθεί στις επόμενες ενότητες.

7.4 Υπολογισμός της επίπτωσης παραβιάσεων ασφάλειας

Στην συγκεκριμένη ενότητα επιχειρείται ο συνδυασμός των αποτελεσμάτων, σχετικά με το μέγεθος της επίπτωσης των παραβιάσεων ασφαλείας, που προήλθαν από την ανάλυση ερευνών μελετητικών οργανισμών και της ακαδημαϊκής κοινότητας. Έρευνες μελετητικών οργανισμών, σχετικά με την ασφάλεια ΠΣ, αναλύθηκαν στην ενότητα 4.3 και παρουσιάσθηκαν μεταξύ άλλων τα αποτελέσματα που έχουν επιφέρει σχετικά με τον προσδιορισμό της οικονομικής επίπτωσης που αναμένεται να επιφέρουν οι παραβιάσεις ασφαλείας. Οι εμπειρικές μελέτες που έχουν εκπονηθεί από την ακαδημαϊκή κοινότητα, με κύριο στόχο τον προσδιορισμό των οικονομικών επιπτώσεων των παραβιάσεων ασφαλείας, αναλύθηκαν στο κεφάλαιο 5. Στο ίδιο κεφάλαιο έγινε σύγκριση των αποτελεσμάτων προηγούμενων μελετών με αντίστοιχη εμπειρική μελέτη που εκπονήθηκε στα πλαίσια της παρούσας διατριβής προκειμένου για την αποκόμιση εμπεριστατωμένων συμπερασμάτων. Στην συγκεκριμένη ενότητα το σύνολο αυτών των συμπερασμάτων θα συγκριθεί με τα συμπεράσματα που προήλθαν από τις έρευνες μελετητικών οργανισμών ώστε να καταλήξουμε σε γενικά πορίσματα σχετικά με το άμεσο, το έμμεσο και κατά επέκταση το συνολικό κόστος που επιφέρουν οι παραβιάσεις ασφαλείας.

Στην παράγραφο 4.3.3.1 αναλύθηκαν τα αποτελέσματα προσδιορισμού του οικονομικού αντίκτυπου από παραβιάσεις ασφαλείας. Από το σύνολο των συμβουλευτικών οργανισμών που εξετάστηκαν μόνο οι CSI/FBI και Ponemon Institute παρέχουν ποσοτικά δεδομένα σχετικά με το κόστος των παραβιάσεων ασφαλείας. Οι μελέτες της Ponemon Institute, αναφορικά με το κριτήριο αυτό, υπερέχουν καθώς είναι οι μοναδικές που παρέχουν ανάλυση ανάμεσα στο άμεσο και στο έμμεσο κόστος. Επίσης, είναι οι μοναδικές μελέτες που προσεγγίζουν το κόστος ανά εγγραφή δεδομένων που προσβάλλεται σε ένα περιστατικό.

7.4.1 Ανάλυση αριθμού εγγραφών σε έκθεση

Το πρώτο στοιχείο που αναλύεται είναι ο αριθμός των εγγραφών που προσβάλλονται σε ένα περιστατικό. Στο κεφάλαιο 5 εξετάστηκε η αναλογικότητα μεταξύ του κόστους ενός περιστατικού και του μεγέθους του χρησιμοποιώντας ως κριτήριο για το μέγεθος τον αριθμό των εγγραφών που προσβλήθηκαν. Σύμφωνα με τα αποτελέσματα, τα περιστατικά μεγάλου μεγέθους άνω των 100.000 εγγραφών σε έκθεση, δεν παρουσιάζουν αναλογικότητα στο συνολικό κόστος. Στις περιπτώσεις αυτές δεν μπορεί να χρησιμοποιηθεί ο αριθμός των εγγραφών, που εκτιμάται ότι

προσβλήθηκε, προκειμένου για τον προσδιορισμό του συνολικού κόστους. Από την άλλη πλευρά, στις περιπτώσεις περιστατικών κατά τα οποία εκτίθενται το ανώτερο 100.000 εγγραφές, προέκυψε πως υφίσταται αναλογικότητα μεταξύ του μεγέθους του κόστους και του αριθμού των εγγραφών. Περιστατικά μεγέθους μεταξύ 1000 – 100.000 εγγραφών αποτελούν το τυπικό μέγεθος περιστατικού με την μεγαλύτερη συχνότητα εμφάνισης.

Η παραπάνω διαπίστωση αποτελεί εμπειρική επιβεβαίωση των προαναφερόμενων μελετών από την Ponemon Institute στις οποίες υποστηρίζεται η ύπαρξη γραμμικής σχέσης ανάμεσα στο κόστος ενός τυπικού περιστατικού και του αριθμού των εγγραφών που προσβάλλονται. Από τις ίδιες μελέτες προκύπτει ένα μέσο μέγεθος περιστατικού που προσεγγίζει τις 33.000 εγγραφές με πολύ μικρές αποκλίσεις για την περίοδο 2008-2010. Το μέσο μέγεθος περιστατικού μειώθηκε το 2011 σε 28.000 εγγραφές. Το δείγμα περιστατικών παραβιάσεων ασφαλείας, που δημιουργήθηκε κατά την διάρκεια της παρούσας διατριβής, περιλαμβάνει 54 περιστατικά που εμπίπτουν στην κατηγορία μεγέθους μεταξύ 1000 – 100.000 εγγραφών και η στατιστική ανάλυσης τους παράγει συγκρίσιμα στοιχεία προς τις παραπάνω μελέτες. Συγκεκριμένα, προκύπτει πως ο μέσος αριθμός εκτεθειμένων εγγραφών για ένα τυπικό περιστατικό είναι 24.000 εγγραφές. Το μέγεθος αυτό είναι αρκετά κοντά στο προαναφερόμενο μέγεθος των 28.000 εγγραφών που προκύπτει από τις μελέτες της Ponemon Institute.

Καταλήγουμε στο τελικό συμπέρασμα πως μία εταιρία, οποιασδήποτε κατηγορίας και μεγέθους, αναμένεται στην σημερινή εποχή να δεχθεί περιστατικά παραβίασης ασφαλείας των οποίο το μέγεθος θα ανέρχεται σε παραβίαση κατά μέσο όρο 24.000 – 28.000 εγγραφών.

7.4.2 Ανάλυση κόστους ανά περιστατικό παραβίασης ασφαλείας

Το επόμενο στοιχείο που αναλύεται είναι το κόστος ανά περιστατικό σε άμεσο και έμμεσο επίπεδο. Όπως αναφέρθηκε στην ενότητα 4.3.3.1 τα στοιχεία που αποδίδουν οι μελέτες από CSI/FBI και Ponemon Institute έχουν πολύ μεγάλη απόκλιση μεταξύ τους με τα αποτελέσματα του πρώτου φορέα να τεκμηριώνεται ο χαρακτηρισμός τους ως εξαιρετικά χαμηλά. Ανάλυση των εμπειρικών μελετών, που παραθέτεται στο κεφάλαιο 5, οδήγησε στο συμπέρασμα ότι το συνολικό κόστος που προκαλείται από τις παραβιάσεις ασφαλείας μειώνεται τα τελευταία χρόνια με την τάση να σταθεροποιηθεί σε ένα συγκεκριμένο επίπεδο. Η πτωτική τάση εμφανίζεται και στα αποτελέσματα σχετικά με το κόστος των μελετών από την Ponemon.

Αναλυτικότερα, οι εμπειρικές μελέτες στο σύνολο τους υποδεικνύουν πως μέσα στην τελευταία δεκαετία το μέσο συνολικό κόστος μίας παραβίασης ασφαλείας περιορίστηκε κάτω του 1% επί της κεφαλαιακής αξίας ενός οργανισμού. Η εμπειρική μελέτη που έγινε στα πλαίσια της παρούσας διατριβής, σε συνδυασμό με άλλες πρόσφατες ανάλογες μελέτες, υποδεικνύουν περεταίρω αποκλιμάκωση στο κόστος με τάσεις σταθεροποίησης του σε ένα συγκεκριμένο επίπεδο το οποίο κυμαίνεται μεταξύ 0,33% - 0,39% επί της κεφαλαιακής αξίας. Τα ποσοστά αυτά παραπέμπουν σε ένα μέσο συνολικό κόστος ανά παραβίαση ασφαλείας το οποίο κυμαίνεται μεταξύ $57 - $68 εκατομμύρια. Τα ποσά αυτά είναι αισθητά υψηλοτέρα από το μέσο κόστος που υπολογίζεται ανά περιστατικό μέσω των μελετών της Ponemon Institute το οποίο ανέρχεται σε $6,5 εκατομμύρια.

Η μεγάλη διαφορά που προκύπτει στην προσέγγιση του κόστους των παραβιάσεων ασφαλείας, μεταξύ των μελετών της ακαδημαϊκής κοινότητας και των συμβουλευτικών οργανισμών, προέρχεται από την μεθοδολογία στην οποία βασίζονται. Οι πρώτες επιχειρούν την ποσοτικοποίηση της αντίδρασης της αγοράς στην ανακοίνωση ενός περιστατικού ενώ οι δεύτερες επεξεργάζονται τις απαντήσεις των ερωτηθέντων που επιλέγουν να μετέχουν κατά την διάρκεια της ερευνητικής διεργασίας. Είναι προφανές πως οι ακαδημαϊκές εμπειρικές μελέτες έχουν την δυνατότητα εκροής περισσότερο αντικειμενικών αποτελεσμάτων σε σχέση με τις μελέτες δημοσκόπησης των οποίων η εγκυρότητα εξαρτάται κατά κύριο λόγο στις μεθόδους και την ακρίβεια μέτρησης που εφαρμόζουν οι ερωτηθέντες. Ένα επιπλέον μειονέκτημα των δεύτερων είναι η εξάρτηση τους από την ειλικρίνεια των ερωτηθέντων. Με άλλα λόγια είναι περισσότερο πιθανό να επιτευχθεί αντικειμενικότητα στην προσέγγιση της διάστασης των οικονομικών επιπτώσεων από εμπειρικές ακαδημαϊκές μελέτες καθώς οι μετρήσεις δεν προέρχονται από εσωτερικούς παράγοντες των οργανισμών αλλά από εκτιμήσεις της ευρύτερης αγοράς.

Όπως αναφέρθηκε στην παράγραφο 4.2.3, το συνολικό κόστος μίας παραβίασης ασφαλείας επιμερίζεται σε άμεσο και έμμεσο. Το άμεσο κόστος, λόγω της φύσης του, υπολογίζεται χωρίς ιδιαίτερη δυσκολία με ακρίβεια και αντικειμενικότητα. Το γεγονός αυτό μπορεί να μας οδηγήσει στην ασφαλή παραδοχή ότι το μέρος του κόστους παραβιάσεων ασφαλείας, που αφορά άμεσες απώλειες, προσεγγίζεται με ακρίβεια και από τις εμπειρικές μελέτες και από τις μελέτες δημοσκοπήσεων. Το έμμεσο κόστος είναι αρκετά δυσκολότερο να προσεγγιστεί με ακρίβεια λόγω

της φύσης των παραμέτρων που το προσδιορίζουν και του μακροπρόθεσμου ορίζοντα που απαιτείται πολλές φορές για την πραγμάτωση του.

Με βάση τα παραπάνω μπορούμε να καταλήξουμε στο συμπέρασμα πως οι μελέτες δημοσκόπησης υποεκτιμούν το έμμεσο κόστος που επιφέρουν οι παραβιάσεις ασφαλείας. Οι οργανισμοί που μετέχουν στις συγκεκριμένες έρευνες δημοσκόπησης υποτιμούν είτε εκούσια, είτε ακούσια το μέγεθος της συνολικής επίπτωσης με την υποτίμηση προφανώς να έγκειται κατά κύριο λόγο στο έμμεσο κόστος. Μάλιστα σε μελέτη των CSI/FBI αναφέρεται η δυσκολία ακριβής προσέγγισης του έμμεσου κόστους από μελέτες δημοσκόπησης και αμφισβητείται μάλιστα η ακρίβεια των εκτιμήσεων άλλων οργανισμών όπως του Ponemon Institute [**10**].

Επομένως, συνδυάζοντας τα παραπάνω συμπεράσματα, μπορούμε να προσεγγίσουμε το άμεσο κόστος των παραβιάσεων ασφαλείας κάνοντας χρήση των μελετών δημοσκοπήσεων και στην συνέχεια να επιτύχουμε προσέγγιση του έμμεσου κόστους υπολογίζοντας το συγκρίνοντας το άμεσο με το συνολικό κόστος. Το συνολικό κόστος εκτιμάται μέσω των εμπειρικών μελετών οι οποίες, όπως προκύπτει από το σύνολο της ερευνητικής προσπάθειας, αποδίδουν τις περισσότερο αντικειμενικές και ακριβείς εκτιμήσεις.

Η βάση ανάλυσης και καταχώρησης περιστατικών παραβίασης ασφαλείας DatalossDB, που χρησιμοποιήθηκε στην εμπειρική μελέτη του κεφαλαίου 5, χρησιμοποιεί τα στοιχεία που προέρχονται από τις μελέτες της Ponemon Institute για την προσέγγιση του άμεσου κόστους. Όπως προέκυψε από την εξέταση των δεδομένων της συγκεκριμένης βάσης, το μέσο άμεσο κόστος που χρησιμοποιείται για την κοστολόγηση περιστατικών, που έχουν συμβεί μέσα στην τελευταία τετραετία, είναι $60 ανά εκτιθέμενη εγγραφή. Σύμφωνα με τον Πίνακα 2 στο κεφάλαιο 4, όπου παρουσιάζονται τα στοιχεία κόστους παραβιάσεων ασφαλείας από την Ponemon Institute, το μέσο άμεσο κόστος ανά έγγραφη κατά το χρονικό διάστημα 2008 – 2011 ανέρχεται σε $61. Το ποσό αυτό σχεδόν ταυτίζεται με το αντίστοιχο που χρησιμοποιείται από το DatalossDB.

Είναι αξιοσημείωτο πως η προαναφερόμενη βάση ανάλυσης περιστατικών ασφαλείας δεν επιχειρεί προσέγγιση του έμμεσου κόστους χρησιμοποιώντας τα αντίστοιχα δεδομένα από τις μελέτες της Ponemon Institute ή κάποιου άλλου ανάλογου οργανισμού. Λαμβάνοντας υπόψη την σοβαρότητα και εγκυρότητα του φορέα που διαχειρίζεται την DatalossDB, η προαναφερόμενη παρατήρηση επιβεβαιώνει την άποψη της συγκεκριμένης διατριβής πως οι μελέτες

δημοσκοπήσεων δεν αποτελούν αξιόπιστες πηγές για την προσέγγιση του έμμεσου κόστους που προέρχεται από τις παραβιάσεις ασφαλείας.

Συνεπώς, το μέσο άμεσο κόστος μίας παραβίασης ασφαλείας για έναν οργανισμό ανεξαρτήτου μεγέθους και τύπου μπορεί να υπολογιστεί χρησιμοποιώντας τα εξής δεδομένα: Το μέσο άμεσο κόστος ανά εκτιθέμενη εγγραφή θέτεται στο επίπεδο των $61 όπως αναφέρθηκε παραπάνω. Το αναμενόμενο μέγεθος μίας παραβίασης ασφαλείας θέτεται στις 26.000 εγγραφές ως η μέση τιμή του διαστήματος των 24.000 – 28.000 εγγραφών το οποίο προσδιορίσθηκε στην ανάλυση της προηγούμενης παραγράφου. Λαμβάνοντας το γινόμενο μεταξύ του άμεσου κόστους ανά εκτιθέμενη εγγραφή και του συνόλου των εκτιθέμενων εγγραφών, προκύπτει το μέσο συνολικό κόστος το οποίο ανέρχεται σε περίπου $1,6 εκατομμύρια.

Επομένως, λαμβάνοντας υπόψη τα αποτελέσματα των πρόσφατων εμπειρικών μελετών, τα οποία αναφέρθηκαν και παραπάνω, καθώς και των αποτελεσμάτων για την εκτίμηση του άμεσου κόστους, μπορούμε πλέον να εκτιμήσουμε το έμμεσο κόστος. Καθώς οι εμπειρικές μελέτες θέτουν το κόστος μεταξύ $57 – $68 εκατομμύρια, αφαιρώντας το άμεσο κόστος, προκύπτει ότι το έμμεσο κόστος κυμαίνεται μεταξύ $55,4 – $66,4. Καθώς το αναμενόμενο μέγεθος ενός περιστατικού αναμένεται σε 26.000 εγγραφές, προκύπτει πως το έμμεσο κόστος ανά εκτιθέμενη εγγραφή αναμένεται μεταξύ $2.131 – $2.554 ή λαμβάνοντας την μέση τιμή αναμένεται ένα έμμεσο κόστος ύψους $2.340 περίπου ανά εγγραφή.

Όπως υποδεικνύεται από τις μελέτες συμβουλευτικών οργανισμών και επιβεβαιώνεται εμπειρικά από την ακαδημαϊκή κοινότητα, η οικονομική επίπτωση των παραβιάσεων ασφαλείας διαφοροποιείται σημαντικά ανάλογα με τον κλάδο δραστηριότητας ενός οργανισμού. Η συγκεκριμένη πρόταση αναλύθηκε διεξοδικά στο κεφάλαιο 5 και αποδείχθηκε η ύπαρξη στατιστικά σημαντικής διαφοροποίησης των οικονομικών επιπτώσεων, που προκαλούνται από τις παραβιάσεις ασφαλείας, ανάμεσα στους τεχνολογικούς και μη τεχνολογικούς οργανισμούς. Το συμπέρασμα στο οποίο καταλήγουμε είναι πως μία σημαντική μεταβλητή, που διαμορφώνει το επίπεδο της επίπτωσης των κινδύνων παραβιάσεων ασφαλείας, είναι ο κλάδος δραστηριότητας ενός οργανισμού. Παρατηρούμε επίσης πως η συγκεκριμένη μεταβλητή είναι κοινή και για τον προσδιορισμό της πιθανότητας πραγμάτωσης των κινδύνων όπως ήδη αναλύθηκε στην ενότητα 7.3.

Κάνοντας χρήση των αποτελεσμάτων που προέκυψαν από την εμπειρική μελέτη του κεφαλαίου 5, προκύπτει πως η συνολική οικονομική επίπτωση για έναν οργανισμό τεχνολογίας από μία παραβίαση ασφαλείας ανέρχεται κατά μέσο όρο σε $73 εκατομμύρια[16]. Η οικονομική επίπτωση των παραβιάσεων ασφαλείας προς τους λοιπούς οργανισμούς υπολογίζεται μεταξύ $59 - $66 εκατομμύρια. Τα μεγέθη αυτά υποδεικνύουν μία διαφοροποίηση στην οικονομική επίπτωση, ανάμεσα στις δύο κατηγορίες οργανισμών, που κυμαίνεται μεταξύ $7 - $14 εκατομμύρια.

Από την έρευνα που πραγματοποιήθηκε, στις μελέτες επαγγελματικών οργανισμών και της ακαδημαϊκής κοινότητας, δεν προέκυψαν σαφείς ενδείξεις ότι η προαναφερόμενη διαφοροποίηση προέρχεται, έστω κατά ένα ποσοστό, από το άμεσο κόστος. Διατυπώνοντας το διαφορετικά, το επίπεδο του άμεσου κόστους ανά εγγραφή, που θα προκληθεί από μία παραβίαση ασφαλείας, αναμένεται να είναι σταθερό ανεξάρτητα από το είδος του οργανισμού που προσβάλλεται. Συνεπώς, το επίπεδο του άμεσου κόστους διαμορφώνεται από παράγοντες που είναι κοινοί για το σύνολο των οργανισμών. Το πόρισμα αυτό οδηγεί στο συμπέρασμα πως η διαφοροποίηση της επίπτωσης προέρχεται αποκλειστικά από την διαφοροποίηση που επέρχεται στο επίπεδο του έμμεσου κόστους λόγω του είδους του οργανισμού που προσβάλλεται.

Με βάση τα παραπάνω, το έμμεσο κόστος που αναμένεται να προκληθεί σε οργανισμούς τεχνολογίας από παραβιάσεις ασφαλείας, υπολογίζεται ότι ανέρχεται σε $71,4 εκατομμύρια. Αντιστοίχως το έμμεσο κόστος, που αφορά οργανισμούς εκτός του τεχνολογικού τομέα, αναμένεται μεταξύ $57,4 – $64,4 εκατομμύρια. Μετατρέποντας τα αποτελέσματα σε όρους αριθμού παραβιασμένων εγγραφών, προκύπτει ότι το έμμεσο κόστος ανά εγγραφή προς τους οργανισμούς τεχνολογίας αναμένεται σε $2.746. Το έμμεσο κόστος ανά εγγραφή αντίστοιχα, προς τους λοιπούς οργανισμούς αναμένεται σε $2.208 - $2.477.

Από το σύνολο της παραπάνω ανάλυσης προκύπτει πως η συντριπτική πλειοψηφία της οικονομικής επίπτωσης, που αναμένεται να προκαλέσει μία παραβίαση ασφαλείας, προέρχεται από το έμμεσο κόστος. Η αναλογία άμεσου / έμμεσου κόστους προκύπτει επίσης υπέρ του δεύτερου και από τις μελέτες των συμβουλευτικών οργανισμών αλλά χωρίς να αποτυπώνεται η πραγματική διάσταση του έμμεσου κόστους το οποίο υποεκτιμάται σε πολύ μεγάλο βαθμό.

[16] Χρησιμοποιούνται αποκλειστικά τα αποτελέσματα που προέκυψαν από την χρήση του μοντέλου τριών μεταβλητών των Fama-French για λόγους συγκρισιμότητας με την ανάλυση που έγινε για το σύνολο των εταιριών.

Επίσης, προκύπτει σαφής διαφοροποίηση του έμμεσου κόστους με κριτήριο το είδος του οργανισμούς που προσβάλλεται.

Τέλος, πρέπει να διευκρινιστεί πως τα παραπάνω αποτελέσματα σχετικά με το έμμεσο κόστος ανά εκτιθέμενη εγγραφή έχουν αξιοπιστία για περιστατικά τυπικού μεγέθους που δεν υπερβαίνουν τις 100.000 εγγραφές. Στις περιπτώσεις περιστατικών μεγάλου και εξαιρετικά μεγάλου μεγέθους το έμμεσο κόστος δεν αναμένεται να είναι αναλογικό και οι επιπτώσεις πολλές φορές είναι καταστροφικές για έναν οργανισμό. Όπως αναφέρθηκε στο κεφάλαιο 5, υπάρχουν περιστατικά των οποίων η οικονομική επίπτωση έχει φτάσει σε πολλαπλάσιο επίπεδο της κεφαλαιοποίησης του οργανισμού που προσβλήθηκε. Επίσης, σοβαρά περιστατικά έχουν οδηγήσει οργανισμούς ακόμα και στην χρεοκοπία. Οι επιπτώσεις αυτών των περιστατικών δεν μπορούν να συστηματοποιηθούν και αποτελούν μικρό ποσοστό του συνόλου των περιπτώσεων παραβίασης ασφαλείας.

7.5 Μοντέλο ποσοτικοποίησης των κινδύνων παραβιάσεων ασφάλειας

Στην συγκεκριμένη ενότητα επιχειρείται η σύνθεση των θεωρητικών και εμπειρικών συμπερασμάτων των προηγούμενων ενοτήτων του παρόντος κεφαλαίου με στόχο την αποτύπωση ενός μοντέλου προσδιορισμού των κινδύνων παραβιάσεων ασφαλείας. Προς αυτή την κατεύθυνση γίνεται χρήση του μεθοδολογικού πλαισίου που τέθηκε σχετικά με τους παράγοντες προσδιορισμού της πιθανότητας πραγμάτωσης περιστατικών ασφαλείας καθώς και των θεωρητικών – εμπειρικών συμπερασμάτων που προέκυψαν από την ανάλυση των επιπτώσεων. Το αρχικό μοντέλο μπορεί να προσδιορισθεί ως εξής:

$$\mathrm{SBR_{ct}} = \mathrm{S_{yt}}\ \mathrm{P(z_{ct}, Sec\_status_{ct})}\ \mathrm{C_{yt}} \qquad (23)$$

Όπου με SBR_{ct} ορίζεται το επίπεδο των κινδύνων παραβιάσεων ασφαλείας για έναν συγκεκριμένο οργανισμό c σε ένα συγκεκριμένο χρονικό σημείο t. Καθώς δεν προσδιορίζουμε συγκεκριμένο μέγεθος μέτρησης για το σύνολο των μεταβλητών που προσδιορίζουν την πιθανότητα προσβολής, η μεταβλητή SBR_{ct} θα μετράται σύμφωνα με την διάσταση που ορίζεται για την μεταβλητή που προσδιορίζει την επίπτωση. Ορίζουμε ως C_{yt} το επίπεδο της επίπτωσης από μία παραβίαση ασφαλείας που αναμένεται να δεχθεί ένας οργανισμός που ανήκει στο κλάδο

της οικονομίας y την συγκεκριμένη χρονική στιγμή t. Οι υπόλοιπες μεταβλητές του παραπάνω μοντέλου έχουν ήδη οριστεί από την ενότητα 7.3.

Ένα πρόβλημα του μοντέλου είναι πως οι μεταβλητές S_{yt} και Sec_status_{ct} δεν μπορούν να θεωρηθούν ως ανεξάρτητες μεταξύ τους. Η μεταβολή του αναμενώμενου αριθμού παραβιάσεων σε έναν κλάδο μπορεί να οδηγηθεί από παράγοντες που μπορούν να διαφοροποιήσουν από κοινού τους τεχνικούς παράγοντες κινδύνου που λαμβάνονται υπόψη για τον προσδιορισμό του επιπέδου ασφαλείας. Επιπρόσθετα, δύναται να συμβεί το αντίστροφο καθώς η μεταβολή των ποιοτικών χαρακτηριστικών ενός μεγάλου μέρους τεχνικών παραγόντων κινδύνου μπορεί να οδηγήσει σε διαφοροποίηση της μεταβλητής S_{yt} για μέρος ή το σύνολο των κλάδων της οικονομίας. Ο εμπειρικός προσδιορισμός της S_{yt} προϋποθέτει την υιοθέτηση ενός μέσου επιπέδου ασφαλείας για το σύνολο των οργανισμών ενός κλάδου το οποίο είναι σταθερό για όλη την περίοδο εκτίμησης. Ο τρόπος υπολογισμού συνεπώς της συγκεκριμένης μεταβλητής οδηγεί στην συσχέτιση της με την μεταβλητή που αφορά το επίπεδο ασφαλείας. Καθώς δεν μπορούμε να λάβουμε την παραδοχή ότι όλοι οι οργανισμοί ενός κλάδου βρίσκονται σε ένα μέσο επίπεδο ασφαλείας, κατά την στιγμή προσδιορισμού της μεταβλητής S_{yt}, πρέπει να ληφθεί υπόψη στο μοντέλο η σχέση του επιπέδου ασφαλείας ενός οργανισμού με το μέσο επίπεδο ασφαλείας. Συμπεριλαμβάνοντας τη σχέση αυτή στο μοντέλο αναμένεται να αποδυναμωθεί η συσχέτιση των δύο μεταβλητών.

Προκειμένου να λυθεί το ζήτημα αυτό αποφασίστηκε να εισαχθεί ένας δείκτης ο οποίος να προσδιορίζεται από τη σχέση του επιπέδου ασφαλείας μίας εταιρίας και του επιπέδου ασφαλείας ενός αντιπροσωπευτικού ΠΣ (benchmark IS) [**118**]. Ως αντιπροσωπευτικό ΠΣ ορίζεται μία σύνθεση στοιχείων λογισμικού η οποία κατά μέσο όρο χρησιμοποιείται από τους οργανισμούς ανεξαρτήτως του είδους και του μεγέθους τους. Σε διαφορετική διατύπωση, σύμφωνα με την μεθοδολογία που έχει ήδη αναπτυχθεί, το αντιπροσωπευτικό ΠΣ προσδιορίζεται από την σύνθεση τεχνικών παραγόντων κινδύνου που χρησιμοποιείται κατά μέσο όρο στην αγορά.

Ο υπολογισμός του αντιπροσωπευτικού ΠΣ μπορεί να επιτευχθεί μέσω της χρήσης στατιστικών δεδομένων χρήσης στοιχείων λογισμικού τα οποία παρέχονται από διαδικτυακές εταιρίες ανάλυσης δεδομένων. Παραδείγματα εταιριών αυτού του είδους αποτελούν οι StatOwl και Statcounter οι οποίες έχουν ήδη αναφερθεί στην ενότητα 6.5.5 κατά τον υπολογισμό των συντελεστών βαρύτητας των τεχνικών παραγόντων κινδύνου. Με βάση τα προαναφερόμενα

στατιστικά δεδομένα, μπορεί να προσδιορισθεί μία κατάταξη των στοιχείων λογισμικού με κριτήριο το επίπεδο χρήσης. Στην συνέχεια, μεταξύ των στοιχείων λογισμικού που βρίσκονται υψηλότερα στην κατάταξη αυτή, κατασκευάζονται όλοι οι δυνατοί συνδυασμοί συστημάτων. Για κάθε διαφορετικό συνδυασμό υπολογίζεται το επίπεδο ασφαλείας με βάση την μεθοδολογία που έχει ήδη αναπτυχθεί. Ακολούθως, προσδιορίζεται η πιθανότητα εφαρμογής κάθε υποθετικού συστήματος, η οποία υπολογίζεται μέσω του γινομένου της σχετικής συχνότητας χρήσης κάθε στοιχείου λογισμικού που περιέχει. Τελικώς, το αντιπροσωπευτικό επίπεδο ασφαλείας μπορεί να εκτιμηθεί από τον ακόλουθο τύπο:

$$\mathrm{Sec\_status_{bt}} = \sum_{q=1}^{n} \mathrm{p(CF_v)Sec\_status_{vt}} \quad (24)$$

Θέτουμε ως Sec_status_{bt} το επίπεδο ασφαλείας ενός αντιπροσωπευτικού συστήματος το οποίο υπολογίζεται σε δεδομένο χρόνο t. Επίσης, ορίζουμε ως CF_v κάθε δυνατή σύνθεση στοιχείων λογισμικού, που προσδιορίζει ένα ΠΣ, από το σύνολο n συνθέσεων που έχουν προσδιορισθεί, $p(CF_v)$ ως η πιθανότητα εφαρμογής κάθε δυνατής σύνθεσης CF_v. Τέλος, θέτουμε ως Sec_status_{vt} το επίπεδο ασφαλείας κάθε συστήματος v στην δεδομένη στιγμή t που γίνεται η ανάλυση. Λαμβάνοντας υπόψη τα παραπάνω το αρχικό μοντέλο μπορεί να τροποποιηθεί ως εξής:

$$\mathrm{SBR_{ct}} = \mathrm{S_{yt}} \frac{\mathrm{Sec\_status_{bt}}}{\mathrm{Sec\_status_{ct}}} \mathrm{P(z_{ct}, Sec\_status_{ct})\ C_{yt}} \quad (25)$$

Ο λόγος μεταξύ του επιπέδου ασφαλείας του αντιπροσωπευτικού ΠΣ και του επιπέδου ασφαλείας των ΠΣ ενός οργανισμού, αποτυπώνει το σχετικό επίπεδο ασφαλείας που ένα συγκεκριμένο ΠΣ παρουσιάζει και χρησιμοποιείται προκειμένου για την προσαρμογή της μεταβλητής S_{yt}. Ο συνδιασμός της προσαρμοσμένης μεταβλητής S_{yt} με το επίπεδο της πιθανότητας μία απειλή να προκαλέσει μία πετυχημένη επίθεση σε ένα σύστημα προσδιορίζουν το αναμενόμενο ετήσιο επίπεδο εμφάνισης ευπαθειών για έναν οργανισμό c σε μία δεδομένη στιγμή t.

Στο παραπάνω μοντέλο το μέγεθος της επίπτωσης, που αναμένεται να επιφέρει κάθε περιστατικό παραβίασης ασφαλείας, εξαρτάται από τον κλάδο της οικονομίας y στον οποίο βρίσκεται ένας οργανισμός c. Η συγκεκριμένη σχέση υποστηρίχθηκε στην ενότητα 7.4 βασιζόμενη στα ερευνητικά αποτελέσματα που αναλύθηκαν στο κεφάλαιο 5. Τα εμπειρικά

αποτελέσματα υποδεικνύουν ότι είναι εφικτός ο προσδιορισμός της έμμεσης επίπτωσης από παραβιάσεις ασφαλείας για κάθε κλάδο ή τομέα της οικονομίας. Κατηγορίες οργανισμών που παρουσιάζουν κοινά χαρακτηριστικά, τα οποία οδηγούν σε κοινά μεγέθη επιπτώσεων, μπορούν να ενοποιηθούν σε μία ενιαία κατηγορίας κόστους. Χαρακτηριστικό παράδειγμα αποτελεί ο τομέας τεχνολογίας που περιλαμβάνει κλάδους όπως αυτών της κατασκευής λογισμικού, κατασκευής υπολογιστών και παροχής υπηρεσιών τηλεπικοινωνίας. Στο κεφάλαιο 5 ερευνήθηκε εμπειρικά και αποδείχθηκε ότι οι εταιρίες τεχνολογίας επωμίζονται μεγαλύτερη επίπτωση από τις παραβιάσεις ασφαλείας σε σχέση με τις εταιρίες εκτός του τεχνολογικού τομέα.

Επιπλέον, οι μελέτες συμβουλευτικών οργανισμών που αναλύθηκαν στο κεφάλαιο 4 υποδεικνύουν ότι οι χρηματοπιστωτικοί και φαρμακευτικοί τομείς της οικονομίας συγκαταλέγονται στους πλέον ευαίσθητους προς τις παραβιάσεις ασφαλείας. Από την έρευνα που πραγματοποιήθηκε προκύπτει πως, οι προαναφερόμενες μελέτες, μπορούν να αποτελέσουν αξιόπιστο οδηγό για την κατάταξη και ομαδοποίηση των οργανισμών με κριτήριο την ευαισθησία που εμφανίζουν προς τις παραβιάσεις ασφαλείας. Κατά συνέπεια, η μεταβλητή y μπορεί να διαφοροποιηθεί ώστε να αντιπροσωπεύει σύνολα από κλάδους οργανισμών τα οποία ταξινομήθηκαν και ομαδοποιήθηκαν σύμφωνα με τα προαναφερθέντα. Ακολούθως, μέσω εμπειρικής ανάλυσης, όπως αναλύθηκε στο κεφάλαιο 5, μπορεί να προσεγγιστεί η συνολική επίπτωση C_{yt} που αναμένεται να επωμιστεί κάθε σύνολο οργανισμών y. Βέβαια, πρέπει να διευκρινισθεί πως το πραγματικό ζητούμενο είναι η εκτίμηση της έμμεσης επίπτωσης για κάθε y. Όπως υποστηρίχθηκε πρωτύτερα, το άμεσο κόστος, που προκαλείται από παραβιάσεις ασφαλείας, δεν επιδέχεται σημαντικής διαφοροποίησης με κριτήριο το είδος του οργανισμού.

Ουσιαστικά, η ανάλυση της επίπτωσης αποσκοπεί στην ταξινόμηση και ομαδοποίηση των οικονομικών κλάδων που παρουσιάζουν κοινά χαρακτηριστικά στο έμμεσο κόστος. Ακολούθως, επιχειρείται η εμπειρική εκτίμηση του κοινού έμμεσου κόστους των οργανισμών που ανήκουν σε κάθε ομάδα από την κατηγοριοποίηση που θεσπίστηκε. Η προσέγγιση αυτή αποτελεί αντιπροσωπευτικό μέτρο για τα στοιχεία που επηρεάζουν την επίπτωση όπως αναφέρθηκαν στην ενότητα 7.2.2. Το πρώτο στοιχείο – ο παράγοντας έκθεσης – αντιπροσωπεύεται από την εκτίμηση του μέσου επιπέδου αρνητικών ασυνήθη αποδόσεων για έναν οργανισμό όταν αντιμετωπίζει ένα περιστατικό ασφαλείας. Ο παράγων έκθεσης μπορεί συνεπώς να προσεγγιστεί ως το μέσο ποσοστό επί της κεφαλαιακής αξίας ενός οργανισμού που μπορεί να πληγεί από ένα περιστατικό.

Ο δεύτερο παράγοντας, που προσδιορίζει το επίπεδο της επίπτωσης, είναι η αξία του στοιχείου ενεργητικού που εκτίθεται. Το στοιχείο αυτό είναι ο ίδιος ο οργανισμός με την αξία του να προσδιορίζεται από το επίπεδο της αξίας των μετοχών σε μία δεδομένη στιγμή. Όπως αναλύθηκε στο κεφάλαιο 2, οι κίνδυνοι ΠΣ πλέον μπορούν να προσβάλουν την ίδια την υπόσταση ενός οργανισμού καθώς τα ΠΣ είναι απαραίτητα για την επίτευξη των εταιρικών στόχων. Επομένως, είναι εύλογο να αναμένουμε ένα περιστατικό ασφαλείας να προκαλέσει αρνητικές ασυνήθεις αποδόσεις σε έναν οργανισμό οι οποίες αντιπροσωπεύουν, κατά κύριο λόγο, το έμμεσο κόστος που εκτιμά η αγορά ότι θα επωμιστεί ο οργανισμός από το περιστατικό.

Η εκτίμηση της επίπτωσης πραγματοποιείται σε νομισματικούς όρους το οποίο οδηγεί στον υπολογισμό των κινδύνων παραβιάσεων ασφαλείας, μέσω του προτεινόμενου μοντέλου, σε νομισματικούς όρους επίσης. Η προσέγγιση αυτή αποδίδει αποτελέσματα άμεσα κατανοητά από την διοίκηση ενός οργανισμού εγχείρημα το οποίο αποτελούσε έναν από τους κύριους στόχους της παρούσας διατριβής. Επίσης, δημιουργεί το υπόβαθρο επέκτασης μέσω της χρήσης μεθοδολογιών που έχουν εφαρμοστεί κατά κύριο λόγο στον υπολογισμό των οικονομικών κινδύνων όπως αναλύεται στην επόμενη ενότητα.

7.6 Η μεθοδολογία Value at Risk και η εφαρμογή της στους κινδύνους παραβιάσεων ασφάλειας

7.6.1 Εισαγωγικά

Στην συγκεκριμένη ενότητα αναλύεται η δυνατότητα χρήσης της μεθοδολογίας Value at Risk (VaR) στην ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας. Η συγκεκριμένη μεθοδολογία αναπτύχθηκε από την επαγγελματική και ακαδημαϊκή κοινότητα που ασχολείται με τους κινδύνους που αντιμετωπίζουν οι χρηματοπιστωτικοί οργανισμοί. Οι κίνδυνοι που αρχικά υπολογίστηκαν μέσω του VaR ήταν οι κίνδυνοι αγοράς που αποτελούν μέρος των οικονομικών κινδύνων που αντιμετωπίζει ένα χαρτοφυλάκιο επενδύσεων. Σταδιακά, καθώς αναγνωρίστηκε η αξία της διαχείρισης κινδύνων σε ενιαίο ολιστικό επίπεδο, η μεθοδολογία επεκτάθηκε στον υπολογισμό του συνόλου των οικονομικών κινδύνων συμπεριλαμβάνοντας και τους πιστωτικούς κινδύνους. Στην συνέχεια, επιχειρήθηκε η εφαρμογή παραλλαγών της μεθοδολογίας, όπως Cash Flow at Risk (CfaR) και Earnings at Risk (EaR), σε οργανισμούς εκτός του χρηματοπιστωτικού τομέα. Οι μεθοδολογίες αυτές λαμβάνουν ολιστική θεώρηση των εταιρικών κινδύνων και

επιχειρούν την εκτίμηση της επίπτωσης του συνόλου των κινδύνων στις αναμενόμενες χρηματοροές ή στα αναμενόμενα κέρδη ενός οργανισμού.

Με έναυσμα την επιτυχημένη εφαρμογή της συγκεκριμένης μεθοδολογίας στην εκτίμηση διαφόρων πτυχών των εταιρικών κινδύνων, αναλύθηκε στα πλαίσια της παρούσας διατριβής, η δυνατότητα χρήσης της στην ποσοτικοποίηση των κινδύνων ΠΣ με επικέντρωση στους κινδύνους παραβιάσεων ασφαλείας. Ένα μέρος ερευνητών έχει ήδη προτείνει μεθοδολογικά πλαίσια εφαρμογής της VaR στην ανάλυση της ασφάλειας ΠΣ [**119**], [**120**]. Η συγκεκριμένη ανάλυση βασίστηκε στις υπάρχουσες προτάσεις της ακαδημαϊκής κοινότητας και στα ερευνητικά ευρήματα εκ του συνόλου της διατριβής προκειμένου για την πρόταση ενός μεθοδολογικού πλαισίου εφαρμογής της VaR στους κινδύνους ΠΣ. Κατά κύριο λόγο έγινε χρήση του μοντέλου ποσοτικοποίησης των κινδύνων παραβιάσεων ασφαλείας που περιγράφτηκε στις προηγούμενες ενότητες του παρόντος κεφαλαίου. Αρχικώς, αναλύονται οι βασικές αρχές και παραδοχές που θέτονται από την συγκεκριμένη μεθοδολογία. Στην συνέχεια αναλύονται οι μεθοδολογικές τροποποιήσεις που προτείνονται προκειμένου η μεθοδολογία αυτή να μπορεί να εφαρμοστεί στους κινδύνους παραβιάσεων ασφαλείας.

7.6.2 Η μεθοδολογία Value at Risk

Μέσω της μεθοδολογίας VaR συνοψίζεται η μέγιστη δυνατή απώλεια για ένα χαρτοφυλάκιο αξιών σε ένα συγκεκριμένο χρονικό ορίζοντα με συγκεκριμένο διάστημα εμπιστοσύνης. Η VaR περιγράφει το επίπεδο απωλειών, που αντιστοιχεί σε συγκεκριμένο μόριο της κατανομής πιθανότητας, με βάση συγκεκριμένο διάστημα εμπιστοσύνης ή επίπεδο στατιστικής σημαντικότητας. Ο συγκεκριμένος ορισμός περιέχει δύο βασικές ποσοτικές παραμέτρους. Η πρώτη αφορά το μέγεθος του χρονικού ορίζοντα κατά τον οποίο υπολογίζεται το μέγεθος της VaR. Η δεύτερη αφορά το επίπεδο εμπιστοσύνης βάση του οποίου προσδιορίζεται το μέρος της κατανομής που αντιστοιχεί στη VaR. Δεν υφίσταται βέλτιστος συνδυασμός για τις δύο αυτές παραμέτρους και το επίπεδο τους θέτεται με κριτήριο τον λόγο για τον οποίο χρησιμοποιείται η μεθοδολογία [**22**].

Μπορούμε να διακρίνουμε δύο τρόπους υπολογισμού της VaR. Ο πρώτος τρόπος οδηγεί σε σχετικό υπολογισμό και ονομάζεται σχετική VaR καθώς λαμβάνεται υπόψη η εκτιμώμενη απώλεια σε σχέση με την μέση απόδοση. Λαμβάνεται υπόψη στον υπολογισμό το κόστος

ευκαιρίας το οποίο αντιπροσωπεύεται από το επίπεδο των θετικών αποδόσεων που θα είχαν επιτευχθεί στην απουσία έλευσης του κινδύνου. Ο δεύτερος τρόπος δεν λαμβάνει υπόψη την αναμενόμενη μέση απόδοση και οδηγεί στον υπολογισμό της απόλυτης VaR. Η πρώτη προσέγγιση οδηγεί συνήθως σε μεγαλύτερα μεγέθη VaR και για αυτό το λόγο θεωρείται περισσότερο συντηρητική. Το μειονέκτημα που έχει είναι η δυσκολία που υφίσταται σε πολλές περιπτώσεις στην ακριβή εκτίμηση της μέσης απόδοσης.

Κάθε ένας εκ των δύο προαναφερόμενων τρόπων υπολογισμού της VaR, μπορεί να διαχωριστεί περεταίρω με βάση την μεθοδολογική προσέγγιση που ακολουθείται για τον προσδιορισμό της κατανομής πιθανότητας των αποδόσεων. Διακρίνονται δύο διαφορετικοί τρόποι με τον πρώτο να χρησιμοποιεί γενικές κατανομές και τον δεύτερο παραμετρικές κατανομές. Η επιλογή εξαρτάται από την μορφή της κατανομής των αποδόσεων του χαρτοφυλακίου για το οποίο επιθυμείται ο υπολογισμός της VaR. Αν η κατανομή προσεγγίζει κάποια γνωστή κατανομή όπως είναι η κανονική, τότε ο υπολογισμός της VaR μπορεί να επιτευχθεί με την εκτίμηση των παραμέτρων της κατανομής όπως είναι η διακύμανση και η τυπική απόκλιση. Στην εναλλακτική περίπτωση, ο υπολογισμός της VaR πραγματοποιείται με την χρήση της γενικής κατανομής που ακολουθούν οι υπό εξέταση αποδόσεις. Η παραμετρική προσέγγιση είναι περισσότερο επιθυμητή καθώς αποδίδει μετρήσεις με μεγαλύτερη ακρίβεια αρκεί να τηρείται η παραδοχή της κανονικότητας για την κατανομή.

Προκειμένου να αποδοθούν σε μαθηματικούς όρους τα παραπάνω, θέτουμε τα εξής[17]: Το διάστημα εμπιστοσύνης ορίζεται ως c, η αρχική αξία του χαρτοφυλακίου ορίζεται ως V_0, ο χρονικός ορίζοντας κατά τον οποίο υπολογίζεται η VaR ορίζεται ως Δt και με z ορίζεται η τυποποιημένη τυχαία μεταβλητή η οποία αντιπροσωπεύει την απόκλιση με βάση το επίπεδο σημαντικότητας $1-c$. Επίσης, με μ και σ ορίζονται η μέση τιμή και η τυπική απόκλιση αντιστοίχως της κατανομής που ακολουθούν οι αποδόσεις του χαρτοφυλακίου. Η σχετική παραμετρική VaR ορίζεται ως Var_r και υπολογίζεται ως ακολούθως:

[17] Στην παρούσα ενότητα δεν αναπτύσσεται ο υπολογισμός της VaR μέσω μη παραμετρικών κατανομών καθώς η παρούσα μελέτη βασίζεται στην μεθοδολογία υπολογισμού της παραμετρικής VaR.

$$\mathrm{Var_r} = \mathrm{V_0}\, z\sigma\sqrt{\Delta t} \qquad (26)$$

Η $\mathrm{Var_r}$ υπολογίζεται από το γινόμενο της αρχικής αξίας του χαρτοφυλακίου, με το επίπεδο της τυπικής απόκλισης της κατανομής προσαρμοσμένο με βάση το μέγεθος του χρονικού ορίζοντα και τον αριθμό των αποκλίσεων που αντιστοιχεί στο επίπεδο σημαντικότητας που έχει τεθεί. Η απόλυτη παραμετρική VaR ορίζεται ως Var_a και υπολογίζεται ως εξής:

$$\mathrm{Var_a} = \mathrm{V_0}(\, z\sigma\sqrt{\Delta t} - \mu\Delta t) \qquad (27)$$

Η $\mathrm{Var_a}$ υπολογίζεται από το γινόμενο της αρχικής αξίας του χαρτοφυλακίου με την διαφορά της σταθμισμένης στο χρονικό ορίζοντα μέσης απόδοσης από το γινόμενο της τυπικής απόκλισης και του αριθμού των αποκλίσεων, που ορίζεται από το επίπεδο σημαντικότητας, σταθμισμένο στην ρίζα του χρονικού ορίζοντα.

7.6.3 Εφαρμογή της μεθοδολογίας Value at Risk στους κινδύνους παραβιάσεων ασφαλείας

Αφού περιγράφτηκε το βασικό θεωρητικό περίγραμμα της μεθοδολογίας VaR, στην παρούσα ενότητα περιγράφεται ο τρόπος που μπορεί να εφαρμοστεί στην ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας. Το κυριότερο μέρος της μεθοδολογίας είναι η επιλογή της φύσης των δεδομένων στα οποία θα βασιστεί ο υπολογισμός της κατανομής πιθανότητας. Όταν η VaR υπολογίζεται για ένα χαρτοφυλάκιο χρηματοοικονομικών αξιών, τα δεδομένα που αναλύονται αφορούν ημερήσιες αποδόσεις και η κατανομή πιθανοτήτων υπολογίζεται με βάση την συχνότητα των ημερήσιων αποδόσεων. Στην περίπτωση των κινδύνων παραβιάσεων ασφαλείας, το χαρτοφυλάκιο που μας ενδιαφέρει είναι η αξία του οργανισμού. Μία παραβίαση ασφαλείας, καθώς αποτελεί κίνδυνο για την δυνατότητα ενός οργανισμού στην εκπλήρωση των εταιρικών σκοπών του, μπορεί να προκαλέσει απώλειες στις μελλοντικές χρηματοροές οδηγώντας στην μείωση της αξίας του οργανισμού. Η μείωση της αξίας αποτελεί το σύνολο του πραγματικού κόστους που επιφέρει το περιστατικό στον οργανισμό.

Σε αυτή τη θεώρηση βασίζεται η εφαρμογή της μεθοδολογίας ανάλυσης γεγονότων στην εκτίμηση του κόστους παραβιάσεων ασφαλείας. Μέσω της συγκεκριμένης μεθοδολογίας, αναλύοντας ιστορικά δεδομένα προερχόμενα από πραγματικά περιστατικά, υπολογίζουμε τις

ασυνήθεις αποδόσεις που επιφέρουν τα περιστατικά αυτά στην αξία των οργανισμών που προσβλήθηκαν. Όπως υποστηρίχθηκε στο κεφάλαιο 5, όταν το σύνολο των δεδομένων αποτελούμενο από ασυνήθεις αποδόσεις είναι επαρκώς μεγάλο, μπορούμε να υποθέσουμε ότι ακολουθεί την κανονική κατανομή. Στο παρόν κεφάλαιο έγινε συνθετική ανάλυση του συνόλου των δεδομένων που δημιουργήθηκαν, κατά την διάρκεια της ερευνητικής προσπάθειας, σχετικά με το μέγεθος των επιπτώσεων από παραβιάσεις ασφαλείας. Με βάση την ανάλυση αυτή υποστηρίχθηκε η πρόταση ότι ο κύριος παράγοντας διαμόρφωσης του επιπέδου επιπτώσεων είναι ο κλάδος δραστηριότητας ενός οργανισμού.

Με βάση τα παραπάνω, καταλήγουμε στον υπολογισμό της VaR με την χρήση των ασυνήθη αποδόσεων και την κατανομή πιθανότητας που ακολουθούν για την οποία λαμβάνουμε την παραδοχή της κανονικότητας. Προκειμένου για την επιλογή των δύο βασικών ποσοτικών παραμέτρων, όπως προαναφέρθηκε, το βασικό κριτήριο είναι η χρήση για την οποία προορίζεται το VaR. Λαμβάνουμε την ενορατική παραδοχή πως η χρήση της VaR στην ασφάλεια ΠΣ θα γίνεται αποκλειστικά ως μέτρο πιθανής απώλειας. Ως συνέπεια αυτής της παραδοχής ο χρονικός ορίζοντας θέτεται με βάση τον βαθμό μεταβολής ή ρευστοποίησης που έχει το χαρτοφυλάκιο υπό ανάλυση. Στην παρούσα περίπτωση το χαρτοφυλάκιο είναι ο ίδιος ο οργανισμός και θεωρούμε εύλογο να θέσουμε ως χρονικό ορίζοντα το διάστημα ενός έτους. Ο Hulthen [**120**] για τον υπολογισμό της VaR λαμβάνει ο χρονικό ορίζοντα επίσης το ένα έτος. Πρέπει βέβαια να αναφερθεί πως σε περιπτώσεις εταιριών υψηλής τεχνολογίας, που έχουν σχετικά υψηλή ευαισθησία στους κινδύνους ΠΣ, ο χρονικός ορίζοντας είναι πολύ πιθανό να τροποποιηθεί σε χαμηλότερα επίπεδα ανάλογα με τις ιδιαίτερες ανάγκες του εκάστοτε οργανισμού.

Θεωρούμε πως και η δεύτερη ποσοτική παράμετρος, που αφορά το επίπεδο σημαντικότητας, εξαρτάται επίσης από τις ιδιαίτερες ανάγκες ενός οργανισμού οι οποίες προσδιορίζονται από την φύση του και την ευαισθησία που παρουσιάζει στους κινδύνους ΠΣ. Συνεπώς, καθώς χαμηλότερα επίπεδα σημαντικότητας οδηγούν σε υψηλότερες εκτιμήσεις του VaR, το επίπεδο σημαντικότητας θα είναι ανάλογο με το εκτιμώμενο επίπεδο ευαισθησίας ενός οργανισμού προς τους κινδύνους ΠΣ.

Μία επιπλέον παραδοχή που πρέπει να ληφθεί, κατά την εφαρμογή της μεθοδολογίας, αφορά την ανεξαρτησία των περιστατικών που λαμβάνονται στην ανάλυση και κατά επέκταση την ανεξαρτησία των ασυνήθη αποδόσεων που προκαλούνται από αυτά. Στην μεθοδολογική

προσέγγιση από τον Hulthen λαμβάνεται αυτή η παραδοχή και αναφέρεται το πρόβλημα που δύναται να προκληθεί από την συμπερίληψη στην ανάλυση επιθέσεων που προκαλούν πολλαπλά περιστατικά. Η βασική κατηγορία τέτοιου είδους επιθέσεων πηγάζει από ιούς. Όπως υποστηρίχθηκε στο κεφάλαιο 5, τα περιστατικά που προκαλούνται από ιούς δεν μπορούν να συμπεριληφθούν σε μία ανάλυση γεγονότων καθώς δημιουργούν προβλήματα στις παραδοχές που θέτει η συγκεκριμένη μεθοδολογία. Κατά αναλογία τα συγκεκριμένα περιστατικά προκαλούν προβλήματα στις παραδοχές της μεθοδολογίας VaR και πρέπει να εξαιρούνται.

Στην προσέγγιση του Hulthen προτείνεται η χρήση δεδομένων προερχομένων από το εσωτερικό ενός οργανισμού για τον υπολογισμό της συχνότητας επιτυχημένων παραβιάσεων ασφαλείας και των επιπτώσεων που επιφέρουν. Όπως έχει ήδη αναφερθεί ένα μέρος μόνο εκ του πραγματικού συνόλου των παραβιάσεων ασφαλείας, που δέχεται ένας οργανισμός, πραγματικά διαπιστώνεται. Στην περίπτωση που το μέρος των περιπτώσεων που δεν διαπιστώνονται είναι μεγάλο τότε η εκτίμηση της συχνότητας μπορεί να έχει σοβαρές αποκλίσεις από τα πραγματικά επίπεδα. Επιπλέον, τα δεδομένα κόστους που προέρχονται από το εσωτερικό ενός οργανισμού, είναι υποκειμενικές εκτιμήσεις η ποιότητα των οποίων βασίζεται στις ιδιαίτερες ικανότητες των αναλυτών. Όπως διαπιστώθηκε από την εξέταση των αποτελεσμάτων μελετών ασφαλείας επαγγελματικών οργανισμών, οι εκτιμήσεις κόστους από το εσωτερικό οργανισμών έχουν πολύ χαμηλά επίπεδα αξιοπιστίας.

Αντιθέτως, στην προσέγγιση που αποτυπώνεται από την παρούσα διατριβή, προτείνεται η χρήση δεδομένων που προέρχονται από το εξωτερικό περιβάλλον ενός οργανισμού. Οι ασυνήθεις αποδόσεις, που αντιπροσωπεύουν τις οικονομικές επιπτώσεις των παραβιάσεων ασφαλείας, υπολογίζονται από δεδομένα προερχόμενα από την ίδια την αγορά και ως εκ τούτου αποτελούν αντικειμενικά δεδομένα για την ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας.

Με βάση το σύνολο της προηγούμενης ανάλυσης, αυτό που πρέπει να προσδιορισθεί είναι οι κατανομές πιθανοτήτων που ακολουθούν οι επιπτώσεις παραβιάσεων ασφαλείας με κριτήριο την ομαδοποίηση των οικονομικών κλάδων όπως περιγράφτηκε στην ενότητα 7.5. Κάνοντας χρήση του μοντέλου, που προτάθηκε στην ίδια ενότητα, μπορούμε να καταλήξουμε σε μία προσαρμοσμένη κατανομή λαμβάνοντας υπόψη τον παράγοντα $P(z_{ct}, Sec\_status_{ct})$. Ο συγκεκριμένος παράγοντας, που αφορά την πιθανότητα πρόκλησης μίας επιτυχημένης επίθεσης από μία απειλή σε έναν οργανισμό, χρησιμοποιείται για την προσαρμογή των πιθανοτήτων των

επιπτώσεων. Με αυτόν τον τρόπο η κατανομή των επιπτώσεων, που είναι επικεντρωμένη στον κλάδο που ανήκει ένας οργανισμός, προσαρμόζεται με βάση τα ιδιαίτερα χαρακτηριστικά του οργανισμού. Η παράμετρος $S_{yt}\ \frac{Sec\_status_{bt}}{Sec\_status_{ct}}$ δεν λαμβάνεται υπόψη καθώς στον υπολογισμό της VaR αυτό που ενδιαφέρει είναι η εκτίμηση υπό συγκεκριμένες συνθήκες της μέγιστης δυνατής απώλειας από ένα μεμονωμένο συμβάν. Συνεπώς, η παραπάνω προσαρμοσμένη κατανομή των ασυνήθη αποδόσεων οδηγεί σε ένα μέτρο των κινδύνων που προκαλούνται από την πιθανότητα εμφάνισης ενός μόνο περιστατικού παραβίασης ασφαλείας σε ένα συγκεκριμένο χρονικό ορίζοντα.

Χρησιμοποιώντας της κατανομή που προτάθηκε παραπάνω μπορεί να γίνει ο υπολογισμός της VaR είτε σε σχετικό είτε σε απόλυτο επίπεδο. Η κατανομή που χρησιμοποιείται περιλαμβάνει αναμενόμενες απώλειες καθώς οι ασυνήθης αποδόσεις, που προκαλούνται από παραβιάσεις ασφαλείας, αναμένονται να είναι αρνητικές. Αυτό οδηγεί την σχετική VaR να είναι μικρότερη της απόλυτης VaR. Η σχέση αυτή είναι αντίστροφη από αυτήν που περιγράφτηκε στην προηγούμενη ενότητα και είναι απόρροια των αναγκαίων τροποποιήσεων που πραγματοποιήθηκαν προκειμένου για την εφαρμογή της μεθοδολογίας VaR στους κινδύνους παραβιάσεων ασφαλείας. Η μεθοδολογική αξία της σχετικής VaR, όταν υπολογίζεται σε μία κατανομή αναμενόμενων απωλειών, εξαλείφεται και συνεπώς προτείνεται η χρήση της απόλυτης VaR.

Συνεπώς, χρησιμοποιώντας της εξίσωση 27 μπορούμε να υπολογίσουμε την Var_a θέτοντας τις παραμέτρους που περιλαμβάνει ως εξής: Ως V_0 ορίζεται η μέση κεφαλαιακή αξία ενός οργανισμού κατά τον χρονικό ορίζοντα υπολογισμού. Οι παράμετροι της προσαρμοσμένης κατανομής πιθανότητας των επιπτώσεων μ και σ είναι η αναμενόμενη απώλεια και η τυπική της απόκλιση αντιστοίχως. Το Δt ορίζεται ίσο με την μονάδα καθώς ο χρονικός ορίζοντας μετράται σε έτη. Τέλος, το z ορίζεται με βάση το επίπεδο σημαντικότητας που έχει επιλεχθεί. Το αποτέλεσμα που προκύπτει μπορεί να συμπληρώσει τα αντίστοιχα αποτελέσματα από την εφαρμογή του μοντέλου ποσοτικοποίησης των κινδύνων παρέχοντας στην διοίκηση ενός οργανισμού πληρέστερη εικόνα για το επίπεδο των κινδύνων παραβιάσεων ασφαλείας που αντιμετωπίζει.

7.7 Συμπεράσματα

Στο κεφάλαιο αυτό προτάθηκε ένα μοντέλο ποσοτικοποίησης των κινδύνων που προέρχονται από τις παραβιάσεις ασφαλείας. Το μεθοδολογικό πλαίσιο στο οποίο βασίσθηκε το συγκεκριμένο μοντέλο προέρχεται από ερευνητικά ευρήματα εκ του συνόλου της διατριβής. Επιπλέον, προτάθηκε η εφαρμογή της μεθοδολογίας VaR στους κινδύνους παραβιάσεων ασφαλείας μέσω της χρήσης του προτεινόμενου μοντέλου. Διαπιστώθηκε πως είναι εφικτή η τροποποίηση της συγκεκριμένης μεθοδολογίας προκειμένου να αξιοποιηθεί στην διαχείριση των κινδύνων παραβιάσεων ασφαλείας. Η χρήση αντικειμενικών ποσοτικών δεδομένων μπορεί να αποδώσει αντικειμενικά αποτελέσματα όπως αναλύθηκε. Μέσω της χρήσης δεδομένων της αγοράς και επεξεργασίας τους με μεθόδους όπως είναι η ανάλυση γεγονότων και την χρήση της μεθοδολογίας ποσοτικοποίησης του επιπέδου ασφαλείας, η οποία επίσης βασίζεται σε αντικειμενικά δεδομένα, μπορεί να επιτευχθεί η παραπάνω προϋπόθεση.

Οι επιπτώσεις που προκαλούνται από παραβιάσεις ασφαλείας κατέστη εφικτό να υπολογιστούν με ακρίβεια μέσω της σύνδεσης των μεθόδων που χρησιμοποιούνται από τις εμπειρικές μελέτες ανάλυσης γεγονότων και τις μελέτες συμβουλευτικών επαγγελματικών οργανισμών. Αποδείχθηκε πως η εκμετάλλευση των συγκριτικών πλεονεκτημάτων που έχουν δύο διαφορετικές προσεγγίσεις μεταξύ τους μπορεί να αποδώσει ολοκληρωμένη θεώρηση για ένα μέγεθος με αποτέλεσμα την αντικειμενική και ακριβή ποσοτικοποίηση του.

Η σύνδεση του μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας, μέσω της χρήσης στοχαστικών μεθόδων και των μεθοδολογικών προσεγγίσεων που ακολουθούνται από τους Gordon-Loeb σχετικά με την πιθανότητα παραβίασης, οδήγησε σε μία ολοκληρωμένη μεθοδολογική θεώρηση της πιθανότητας πραγμάτωσης των παραβιάσεων ασφαλείας. Θέτοντας ένα νέο μέγεθος το οποίο αφορά το αντιπροσωπευτικό επίπεδο ασφαλείας, δημιουργήθηκε ένας λόγος ο οποίος αποδίδει το σχετικό επίπεδο ασφαλείας που έχει ένας οργανισμός. Ο συγκεκριμένος τελεστής έδωσε την δυνατότητα εξάλειψης του προβλήματος συσχέτισης μεταξύ του μεγέθους που αντιπροσωπεύει τον αναμενόμενο αριθμό παραβιάσεων ασφαλείας που εμφανίζει ένας κλάδος και του μέσου επιπέδου ασφαλείας των εταιριών που ανήκουν στον συγκεκριμένο κλάδο.

Η σύνδεση των μεθοδολογικών ευρημάτων σχετικά με τις αναμενόμενες επιπτώσεις από περιστατικά παραβίασης ασφαλείας και της πιθανότητας εμφάνισης τους οδήγησε στην δημιουργία ενός ολοκληρωμένου μοντέλου ποσοτικοποίησης που επιπέδου των κινδύνων παραβιάσεων ασφαλείας σε νομισματικούς όρους. Ένα σύνηθες πρόβλημα που επιχειρεί να επιλύσει το προτεινόμενο μοντέλο είναι η μονόπλευρη ανάλυση των κινδύνων κατά την οποία είτε η πιθανότητα πραγμάτωσης, είτε το μέγεθος των επιπτώσεων αγνοούνται. Στην περίπτωση αυτή, ένα παράγων κινδύνου δύναται να θεωρηθεί ως υπερβολικά επικίνδυνος λόγω της υψηλής εκτίμησης μίας από τις παραμέτρους που προσδιορίζουν τον κίνδυνο. Η δομή του μοντέλου αποσκοπεί στην απόδοση βαρύτητας στο σύνολο των παραμέτρων που καθορίζουν το επίπεδο των κινδύνων ώστε να αποφθεχθεί η επικέντρωση σε μία συγκεκριμένη ή να αγνοηθεί κάποια.

Η απόδοση των κινδύνων αυτών σε κατανοητά μεγέθη και ο παράλληλος υπολογισμός του VaR που τους αντιπροσωπεύει, βελτιώνει το επικοινωνιακό υπόβαθρο μεταξύ των ειδικών για την ασφάλεια και την διοίκηση ενός οργανισμού. Η μεθοδολογία αυτή δημιουργεί μία κοινή γλώσσα επικοινωνίας μεταξύ των υπευθύνων για τα ΠΣ ενός οργανισμού και των στελεχών που αποφασίζουν για τα μεγέθη επένδυσης σε τεχνολογικές υποδομές και υποδομές ασφαλείας. Η δυνατότητα έκδοσης αντικειμενικών αποτελεσμάτων για τους κινδύνους, εκφρασμένων σε νομισματικούς όρους, οδηγεί σε ακριβέστερη προσέγγιση του επιπέδου επένδυσης σε ελέγχους ασφαλείας και στην αποδοτικότερη χρήση των περιορισμένων πόρων ενός οργανισμού.

8 Σύνοψη διατριβής

8.1 Συμπεράσματα

Οι παραβιάσεις ασφαλείας αποτελούν τους κυριότερους κινδύνους ΠΣ που αντιμετωπίζουν οργανισμοί ανεξάρτητα από τον τύπο τους και το μέγεθος τους. Κατά την διάρκεια των τελευταίων ετών οι συγκεκριμένοι κίνδυνοι αυξήθηκαν σημαντικά σε συχνότητα και επίπεδο επιπτώσεων οδηγώντας τις διοικήσεις των οργανισμών να τους θεωρούν πλέον ως το σημαντικότερο πρόβλημα που καλούνται να αντιμετωπίσουν. Η σημαντικότητα αυτή είναι απόρροια κατά κύριο λόγο δύο παραγόντων: (α) Της αυξανόμενης εξάρτησης της επιχειρησιακής λειτουργίας από την εύρυθμη λειτουργία και απόδοση των τεχνολογικών υποδομών. (β) Της αυξανόμενης πολυπλοκότητας των απειλών που καλούνται να αντιμετωπίσουν οι οργανισμοί καθώς τα κίνητρα και οι μέθοδοι επίθεσης διαρκώς διαφοροποιούνται και εξελίσσονται.

Προκειμένου για την αποδοτική αντιμετώπιση των κινδύνων παραβιάσεων ασφαλείας απαιτούνται μεθοδολογικά πλαίσια εκτίμησης τα οποία επιφέρουν αντικειμενικά και ποσοτικά αποτελέσματα με την μέγιστη δυνατή ακρίβεια. Η διοίκηση ενός οργανισμού πρέπει να έχει στην διάθεση της αξιόπιστα και κατανοητά μεγέθη, εκφρασμένα σε νομισματικούς όρους, προκειμένου να αξιολογήσει με ακρίβεια το μέγεθος των κινδύνων που αντιμετωπίζει και να λάβει σημαντικές αποφάσεις σχετικά με το βέλτιστο επίπεδο επένδυσης σε μέτρα ασφαλείας για την αντιμετώπιση τους.

Ερευνήθηκε η θέση των κινδύνων ΠΣ και η σχέση τους με τους λοιπούς κινδύνους που συνθέτουν τον γαλαξία κινδύνων που αντιμετωπίζει ένας οργανισμός χωρίς την εξατομίκευση του πλαισίου που τέθηκε σε σχέση με το μέγεθος ή τον τύπο του οργανισμού. Επίσης, μελετήθηκε το πλαίσιο της διαδικασίας Διαχείρισης Κινδύνων Πληροφοριακών Συστημάτων όπως έχει διαμορφωθεί σήμερα προκειμένου να αξιολογηθεί και να προταθούν μεθοδολογικές επεμβάσεις. Σημαντικό συμπέρασμα, που προήλθε από την συγκεκριμένη ανάλυση, είναι η σημαντικότητα που έχει το στάδιο Εκτίμησης Κινδύνων σε σχέση με τα υπόλοιπα στάδια της διαδικασίας. Επιπλέον, κατέστη σαφές πως πλέον είναι απαραίτητη η χρήση ποσοτικών μεθόδων, για την εκτίμηση των κινδύνων ΠΣ, λόγω της αυξανόμενης σημαντικότητας τους μέσα στο σύνολο των κινδύνων που αντιμετωπίζει ένας οργανισμός.

Διαπιστώθηκαν ελλείψεις στην υπάρχουσα βιβλιογραφία σχετικά με την θεωρητική τεκμηρίωση των παραβιάσεων ασφαλείας ΠΣ. Με βάση τα αποτελέσματα της έρευνας, αναφορικά με την θέση των κινδύνων ΠΣ σε σχέση με το σύνολο των εταιρικών κινδύνων, έγινε περαιτέρω εμβάθυνση στους κινδύνους παραβιάσεων ασφαλείας. Προσδιορίσθηκε η θέση των κινδύνων παραβιάσεων ασφαλείας σε πρώτο επίπεδο αναφορικά με τους κινδύνους ΠΣ και σε δεύτερο επίπεδο σε σχέση με το σύνολο του εταιρικού γαλαξία κινδύνων. Προέκυψε ότι οι παραβιάσεις ασφαλείας μπορούν να κατηγοριοποιηθούν με βάση δύο κριτήρια προκειμένου για την αποδοτικότερη ανάλυση τους: Το πρώτο κριτήριο αφορά το τύπο παραβίασης ασφαλείας ενώ το δεύτερο αφορά την μορφή του κόστους που επιφέρει ένα περιστατικό. Η κατηγοριοποίηση αυτή αποτέλεσε την βάση ενός μεγάλου μέρους της ερευνητικής προσπάθειας. Επίσης, με βάση την ανάλυση του μεθοδολογικού πλαισίου της διαδικασίας ΔΚΠΣ, προτάθηκε ένα αντίστοιχο πλαίσιο εξειδικευμένο στην διαδικασία αντιμετώπισης των κινδύνων παραβιάσεων ασφαλείας.

Από το σύνολο της έρευνας προέκυψε πως το σύνολο των πηγών δεδομένων, για τα περιστατικά παραβίασης ασφαλείας, μπορεί να διαχωριστεί σε τρεις γενικές κατηγορίες. Στην πρώτη κατηγορία συμπεριλήφθησαν οι έρευνες μελετητικών οργανισμών σχετικά με την ασφάλεια. Οι διαδικτυακοί οργανισμοί καταγραφής και ανάλυσης περιστατικών ασφαλείας, έχουν εξελιχθεί τα τελευταία χρόνια σε μία από τις κύριες πηγές αυτής της κατηγορίας περιστατικών και για αυτόν τον λόγο επιλέχθηκε να αποτελέσουν μία ξεχωριστή κατηγορία. Η εμπειρική μελέτη που πραγματοποιήθηκε στα πλαίσια της παρούσας διατριβής σχετικά με τις επιπτώσεις των παραβιάσεων ασφαλείας βασίστηκε κατά κύριο λόγο σε πηγές αυτού του τύπου. Στην τρίτη κατηγορία εντάχθηκαν οι ακαδημαϊκές μελέτες σχετικά με τις παραβιάσεις ασφαλείας. Την τελευταία δεκαετία έχει αναπτυχθεί ένα σημαντικό ερευνητικό ρεύμα το οποίο έχει αυξήσει σημαντικά το γνωστικό πεδίο πάνω στις παραβιάσεις ασφαλείας και κυρίως πάνω στις οικονομικές επιπτώσεις που προκαλούν. Η αύξηση του ερευνητικού ενδιαφέροντος μπορούμε να συμπεράνουμε ότι προέρχεται κυρίως από την εξέλιξη του προβλήματος των παραβιάσεων ασφαλείας ως φαινόμενο με παγκόσμια πλέον επιρροή.

8.1.1 Προσδιορισμός των επιπτώσεων παραβιάσεων ασφαλείας

Το σύνολο της προαναφερόμενης ανάλυσης απέδωσε σημαντικά αποτελέσματα για τους συσχετιζόμενους κινδύνους με τους κινδύνους παραβιάσεων ασφαλείας, οι οποίοι δημιουργούν το

έμμεσο κόστος των περιστατικών. Η έρευνα που πραγματοποιήθηκε, σε μελέτες της επαγγελματικής και ακαδημαϊκής κοινότητας, κατέληξε στο συμπέρασμα πως το έμμεσο κόστους αποτελεί σχεδόν το σύνολο του κόστους που προκαλείται από ένα περιστατικό παραβίασης ασφαλείας. Το άμεσο κόστος, ενός τυπικού περιστατικού, είναι συγκριτικά πολύ χαμηλότερο, μετρήσιμο και δεν προκαλεί ιδιαίτερα προβλήματα στους οργανισμούς.

Αντίθετα, το έμμεσο κόστος έχει μεγάλη δυσκολία ακριβούς προσέγγισης κυρίως λόγω ότι προκαλείται από την συσχέτιση των κινδύνων παραβιάσεων ασφαλείας με λοιπούς εταιρικούς κινδύνους όπως είναι οι νομικοί κίνδυνοι και οι κίνδυνοι φήμης. Μελέτες της επαγγελματικής κοινότητας, προερχόμενες κυρίως από δημοσκοπήσεις, ενώ αποδίδουν μετρήσεις με μεγάλη ακρίβεια για το άμεσο κόστος, είναι μεθοδολογικά ανεπαρκείς για τον ακριβή υπολογισμό του έμμεσου κόστους. Οι ιδιαιτερότητες που απορρέουν από την φύση του έμμεσου κόστους, οδηγούν στην δυσκολία ακριβούς προσέγγισης του. Διαπιστώθηκε πως μελέτες, που βασίζονται σε εκτιμήσεις προερχόμενες από το εσωτερικό οργανισμών, καταλήγουν σε αποτελέσματα τα οποία υποεκτιμούν την πραγματική υπόσταση του έμμεσου κόστους.

Το πρόβλημα αυτό επιλύθηκε με τον συνδυασμό των αποτελεσμάτων που προέρχονται από τις μελέτες της ακαδημαϊκής κοινότητας αξιοποιώντας την μέθοδο ανάλυσης γεγονότων, η οποία χρησιμοποιεί δεδομένα που προέρχονται από το εξωτερικό περιβάλλον των οργανισμών. Η συγκεκριμένη μέθοδος αναλύθηκε διεξοδικά σχετικά με την εφαρμογή της στην ανάλυση περιστατικών παραβιάσεων ασφαλείας. Τα συμπεράσματα που προκύπτουν, από το σύνολο των μελετών αυτών, υποδεικνύουν ότι υφίσταται σημαντικές οικονομικές επιπτώσεις οι οποίες διαφοροποιούνται κυρίως σε σχέση με το είδος του οργανισμού και τον τύπο την παραβίασης ασφαλείας. Διαπιστώθηκε η ύπαρξη ανάμικτων αποτελεσμάτων μεταξύ των μελετών και διερευνήθηκαν τα κυριότερα αίτια πρόκλησης τους τα οποία είναι ως εξής:

(1) Η συμπερίληψη περιστατικών που προκλήθηκαν από ιούς τα οποία, όπως προέκυψε από την έρευνα που διεξήχθη και τεκμηριώθηκε στο κεφάλαιο 5, προκαλούν προβλήματα στις παραδοχές που λαμβάνονται στην εφαρμογή της μεθόδου ανάλυσης γεγονότων.

(2) Ποικίλα μεγέθη δειγμάτων και διαφορετικά μεγέθη ορίζοντα ανάλυσης ήταν επίσης ένας σημαντικός λόγος για την ύπαρξη ανάμικτων αποτελεσμάτων. Πλήθος μελετών

ανέλυσε δείγματα τα οποία δεν υπερέβαιναν τις 30 παρατηρήσεις το οποίο προκαλεί ερωτήματα για την στατιστική εγκυρότητα των αποτελεσμάτων τους και την δυνατότητα σύγκρισης τους με μελέτες που χρησιμοποίησαν σύνολα δεδομένων με επαρκέστερο μέγεθος.

(3) Η χρήση διαφορετικών δεικτών για την αντιπροσώπευση του αγοραίου χαρτοφυλακίου στα μοντέλα αποτίμησης επενδυτικών κεφαλαίων που χρησιμοποιήθηκαν από τις μελέτες ανάλυσης γεγονότων.

(4) Η μέθοδος δειγματοληψίας που υιοθετήθηκε καθώς μέρος των ερευνητών χρησιμοποίησαν, ως πηγές άντλησης δεδομένων, αποκλειστικά μέσα ενημέρωσης με εκτενή απήχηση στο κοινό ενώ μέρος των ερευνητών χρησιμοποίησαν και επιπρόσθετες πηγές λιγότερο γνωστές στο σύνολο της αγοράς. Καταλήξαμε ότι η χρήση ενός μείγματος πηγών με διαφορετική δημοτικότητα μπορεί να οδηγήσει στην δημιουργία ενός δείγματος με μικρότερο επίπεδο μεροληπτικής επιλογής και κατά συνέπεια στην συμπερίληψη περιστατικών που αφορούν οργανισμούς από κάθε επίπεδο κεφαλαιοποίησης.

(5) Η ανεπάρκεια στην εφαρμογή της μεθόδου ανάλυσης γεγονότων μέσω της χρήσης του CAPM. Παράλληλα με το συγκεκριμένο μοντέλο, χρησιμοποιήθηκε το μοντέλο τριών μεταβλητών των Fama-French προκειμένου να εξεταστεί αν το τελευταίο παράγει περισσότερο αξιόπιστα αποτελέσματα. Η διαφοροποίηση των αποτελεσμάτων μεταξύ των δύο μοντέλων είναι μεγάλη και συνεπώς μπορούμε να συμπεράνουμε πως ο σημαντικότερος παράγοντας για την ύπαρξη ανάμικτων αποτελεσμάτων μεταξύ των μελετών είναι οι μεθοδολογικές ανεπάρκειες που παρουσιάζει το CAPM.

Από το σύνολο της στατιστικής ανάλυσης που περιγράφτηκε στο κεφάλαιο 5, διαπιστώθηκε πως το μοντέλο των Fama-French αποδίδει αποτελέσματα τα οποία είναι σύμφωνα με την θεωρεία και για το σύνολο σχεδόν των συμπερασμάτων, σχετικά με το επίπεδο των οικονομικών επιπτώσεων, χρησιμοποιήθηκαν τα αποτελέσματα αυτού του μοντέλου σε σχέση με το CAPM. Τα σημαντικότερα αποτελέσματα που προέκυψαν είναι τα εξής:

(1) Από την εξέταση διαφορετικών παραθύρων ανάλυσης προέκυψαν σαφής ενδείξεις για την ύπαρξη διαρροής εσωτερικής πληροφόρησης σχετικά με τα περιστατικά

παραβίασης ασφαλείας. Αυτό συνεπάγεται πως μέρος της αγοράς πληροφορείται για τα περιστατικά αυτά πριν την επίσημη ανακοίνωση τους στο σύνολο της αγοράς. Επομένως, θεωρούμε πως η χρήση παραθύρων ανάλυσης που να περιλαμβάνουν την προηγούμενη ημέρα από την ημέρα γεγονότος κρίνεται σκόπιμη σε μία ανάλυση περιστατικών αυτού του τύπου.

(2) Αντιθέτως, προέκυψε πως η προσθήκη επόμενων ημερών από την ημέρα γεγονότος στα παράθυρα ανάλυσης δεν αποδίδει πρόσθετη πληροφόρηση αλλά απεναντίας μπορεί να συμπεριλάβει την επίδραση άλλων τυχαίων γεγονότων οδηγώντας στην εξασθένιση της εγκυρότητας των αποτελεσμάτων. Η παρατήρηση αυτή οδηγεί στο επιπρόσθετο συμπέρασμα ότι οι αγορές προοδευτικά οδηγούνται σε μεγαλύτερη αποτελεσματικότητα πληροφόρησης σε σχέση με τα περιστατικά ασφαλείας και συνεπώς η παραδοχή που τέθηκε για αποτελεσματικότητα πληροφόρησης στις αγορές ημι-ισχυρού τύπου είναι βάσιμη.

(3) Λαμβάνοντας υπόψη τα αποτελέσματα του συνόλου των εμπειρικών μελετών που αναλύθηκαν στο κεφάλαιο 5 και της αντίστοιχης μελέτης που έγινε στην παρούσα διατριβή, προκύπτει ότι οι οικονομικές επιπτώσεις που προκαλούνται από τις παραβιάσεις ασφαλείας είναι αρνητικές, έχουν στατιστική σημαντικότητα και σταδιακά μειώνονται με τάσεις σταθεροποίησης σε ένα συγκεκριμένο επίπεδο. Το συγκεκριμένο αποτέλεσμα είναι μία ακόμα σαφής ένδειξη σχετικά με την σταδιακή ωρίμανση των αγορών στην αντιμετώπιση της πληροφόρησης που προέρχεται από περιστατικά ασφαλείας.

(4) Η στατιστική ανάλυση των περιστατικών παραβιάσεων ασφαλείας, με κριτήριο το μέγεθος του περιστατικού, απέφερε σημαντικά αποτελέσματα αναφορικά με την σχέση που υφίσταται ανάμεσα στο κόστος και τον αριθμό των εγγραφών δεδομένων που εκτίθενται. Περιστατικά ενός τυπικού μεγέθους, που δεν υπερβαίνουν τις 100.000 εγγραφές σε έκθεση, παρουσιάζουν μία αναλογική σχέση μεταξύ του συνολικού κόστους που επιφέρουν και του αριθμού των εγγραφών. Αντιθέτως ασυνήθη περιστατικά, που αφορούν την προσβολή πολύ μεγάλου αριθμού εγγραφών, δεν παρουσιάζουν τέτοιου είδους συμπεριφορά στο κόστος. Το φαινόμενο αυτό προέρχεται αποκλειστικά από το έμμεσο κόστος, που προκαλείται από περιστατικά

αυτού του μεγέθους, το οποίο έχει μεγάλο εύρος διακύμανσης από ασήμαντα επίπεδα μέχρι καταστροφικά που μπορούν να απειλήσουν ακόμα και την ίδια την υπόσταση ενός οργανισμού. Τα αποτελέσματα αυτά ήταν πολύ σημαντικά στην συνολική διερεύνηση του κόστους που επιφέρουν οι κίνδυνοι παραβιάσεων ασφαλείας.

(5) Οι επιπτώσεις που προκαλούνται από τους κινδύνους παραβιάσεων ασφαλείας δύναται να διαφοροποιούνται σημαντικά από το είδος του οργανισμού που προσβάλλεται. Υφιστάμενες μελέτες, καθώς και η μελέτη που έγινε στην παρούσα διατριβή, εξέτασαν την συγκεκριμένη πρόταση σε γενικευμένο επίπεδο κατηγοριοποίησης όπως π.χ. εταιρίες τεχνολογίας και εταιρίες εκτός τεχνολογικού τομέα. Τα αποτελέσματα υπέδειξαν την ύπαρξη στατιστικά σημαντικής διαφοροποίησης στις επιπτώσεις με τις τελευταίες να είναι μεγαλύτερες για τις εταιρίες τεχνολογίας. Τα συμπεράσματα αυτά, όπως αυτά που αναλύθηκαν στην προηγούμενη παράγραφο, ήταν ιδιαιτέρως χρήσιμα στην ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας.

8.1.2 Προσδιορισμός του επιπέδου ασφαλείας Πληροφοριακών Συστημάτων

Ερευνήθηκε η ακριβέστερη ποσοτικοποίηση του επιπέδου ασφαλείας ενός ΠΣ προκειμένου να χρησιμοποιηθεί στην μοντελοποίηση της εκτίμησης των κινδύνων παραβιάσεων ασφαλείας. Η έρευνα, που περιγράφτηκε στο κεφάλαιο 6, εστίασε στην χρήση στοχαστικών μεθόδων και στην σταθμισμένη εντροπία πληροφόρησης καταλήγοντας σε ένα μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας το οποίο παράγει κατανοητά και αντικειμενικά αποτελέσματα. Τα αποτελέσματα αυτά μπορούν να χρησιμοποιηθούν από στελέχη ενός οργανισμού που δεν σχετίζονται με την ασφάλεια, όπως είναι η ανώτερη διοίκηση, και λαμβάνουν κρίσιμες αποφάσεις για το επίπεδο των επενδύσεων σε ελέγχους ασφαλείας.

Η δημιουργία του συγκεκριμένου μοντέλου κατέστη δυνατή με την υιοθέτηση του τεχνικού παράγοντα κινδύνου ως βάση για την ανάλυση του επιπέδου ασφαλείας ενός ΠΣ. Η έρευνα κατέληξε στο συμπέρασμα πως, η χρήση αυτού του παράγοντα, παράγει αντικειμενικότερα και αποδοτικότερα αποτελέσματα σε σχέση με υπάρχοντα μοντέλα που επιχειρούν την ποσοτικοποίηση της ασφάλειας σε επίπεδο ευπάθειας ή κατηγορίας ευπαθειών.

Η χρήση της εντροπίας πληροφόρησης, από το προαναφερόμενο μοντέλο, έδωσε την δυνατότητα αντικειμενικής προσέγγισης της βαρύτητας που έχει κάθε παράγοντας κινδύνου σε

ένα σύστημα. Χρησιμοποιήθηκαν δεδομένα ευπαθειών από τις δύο μεγαλύτερες βάσεις ανοικτού κώδικα προκειμένου για την πληρέστερη ανάλυση της συμπεριφοράς των ευπαθειών και για τον υπολογισμό των συντελεστών βαρύτητας. Προέκυψε πως η κατάλληλη χρήση των συγκεκριμένων βάσεων μπορεί να αποδώσει αποτελέσματα με μεγάλη ερευνητική αξία.

Τα σημαντικότερα αποτελέσματα προήλθαν από την ανάλυση των χρονικών μοτίβων που ακολουθούν οι ευπάθειες που εμφάνισαν διαφορετικά προϊόντα λογισμικού και το σύνολο προϊόντων διαφορετικών κατασκευαστών λογισμικού. Από το σύνολο της ανάλυσης προέκυψε πως οι κατανομές των ευπαθειών ακολουθούν κοινά επαναλαμβανόμενα μοτίβα τα οποία προσεγγίζουν την Gaussian συνάρτηση. Το αποτέλεσμα ήταν κοινό για τα δεδομένα που μελετήθηκαν από τις δύο βάσεις και για το σύνολο των προϊόντων και κατασκευαστών λογισμικού.

Το σύνολο των παραπάνω αποτελεσμάτων έδωσε την δυνατότητα σύνθεσης ενός μοντέλου ποσοτικοποίησης του επιπέδου ασφαλείας που παρουσιάζει ένα σύστημα σε μία δεδομένη χρονική στιγμή. Η προσέγγιση του συνόλου των παραμέτρων του μοντέλου έγινε με αντικειμενικές μεθόδους και την χρήση πραγματικών δεδομένων ευπαθειών.

8.1.3 Προσδιορισμός των κινδύνων παραβιάσεων ασφαλείας

Το σύνολο των ερευνητικών ευρημάτων της διατριβής χρησιμοποιήθηκε για την σύνθεση ενός μοντέλου ποσοτικοποίησης των κινδύνων παραβιάσεων ασφαλείας και την μεθοδολογική στήριξη του όπως περιγράφτηκε στο κεφάλαιο 7. Η υλοποίηση του συγκεκριμένου εγχειρήματος χωρίστηκε σε δύο μέρη όπου το πρώτο αφορούσε την εκτίμηση της πιθανότητας πραγμάτωσης ενώ το δεύτερο την εκτίμηση των επιπτώσεων. Καταλήξαμε στο συμπέρασμα πως η παράμετρος της πιθανότητας εξαρτάται από τους εξής παράγοντες:

(α) Το επίπεδο ασφαλείας των ΠΣ ενός οργανισμού όπως υπολογίζεται από το μοντέλο που προτάθηκε στο κεφάλαιο 6.

(β) Το επίπεδο επένδυσης σε ελέγχους ασφαλείας και τον βαθμό παραγωγικότητας τους. Η μεθοδολογική προσέγγιση της συγκεκριμένης παραμέτρου βασίστηκε στο μοντέλο των Gordon-Loeb.

(γ) Την συχνότητα παραβιάσεων ασφαλείας ανάλογα με το είδος ενός οργανισμού

(δ) Την σχέση του επιπέδου ασφαλείας των ΠΣ ενός οργανισμού και του επιπέδου ασφαλείας ενός αντιπροσωπευτικού συστήματος. Εισήχθη η έννοια του αντιπροσωπευτικού συστήματος και προτάθηκε ο τρόπος υπολογισμού του προκειμένου για την εξάλειψη του προβλήματος που δημιουργείται από την συσχέτιση μεταξύ της συχνότητας περιστατικών ανά κατηγορία εταιριών και του μέσου επιπέδου ασφαλείας των οργανισμών που ανήκουν σε μία συγκεκριμένη κατηγορία.

Προκειμένου για την σφαιρική προσέγγιση της παραμέτρου των επιπτώσεων έγινε συνθετική ανάλυση των ερευνητικών ευρημάτων προερχομένων από μελέτες της ακαδημαϊκής και επαγγελματικής κοινότητας. Η συγκεκριμένη προσέγγιση απέδωσε ακριβή αποτελέσματα σχετικά με το επίπεδο των επιπτώσεων καθώς και θεωρητικά συμπεράσματα τα οποία στο σύνολο τους στήριξαν το σύνολο της προτεινόμενης μεθοδολογίας. Προέκυψε πως το επίπεδο των επιπτώσεων εξαρτάται σε μεγάλο βαθμό από το είδος του οργανισμού που προσβάλλεται. Η μεταβλητή που αντιπροσωπεύει το είδος του οργανισμού αποτέλεσε τον βασικό προσδιοριστικό παράγοντα που επιρρεάζει το επίπεδο της επίπτωσης ανά περιστατικό.

Περαιτέρω, προέκυψε ακριβής προσέγγιση του συνολικού κόστους ανά περιστατικό και ανά εγγραφή σε έκθεση. Η ανάλυση απέδωσε αποτελέσματα για το επίπεδο του άμεσου και έμμεσου κόστους επίσης ανά περιστατικό και ανά εγγραφή σε έκθεση. Προκειμένου για την προσέγγιση του άμεσου κόστους χρησιμοποιήθηκαν τα δεδομένα που προέκυψαν από την εξέταση μελετών επαγγελματικών οργανισμών και αντίστοιχα για το έμμεσο κόστους μελέτες της ακαδημαϊκής κοινότητας.

Η σύνθεση των παραπάνω συμπερασμάτων απέδωσε ένα μεθοδολογικό πλαίσιο με ένα προτεινόμενο μοντέλο υπολογισμού των κινδύνων παραβιάσεων ασφαλείας με βασικό στόχο την απόδοση αντικειμενικών αποτελεσμάτων εκφρασμένων σε νομισματικούς όρους ώστε να είναι κατανοητό από το σύνολο της διοίκησης ενός οργανισμού. Το συγκεκριμένο μεθοδολογικό πλαίσιο επεκτάθηκε με την χρήση της μεθοδολογίας Value at Risk. Προέκυψε πως η συγκεκριμένη μεθοδολογία, εφόσον εφαρμοστεί καταλλήλως, μπορεί να αποδώσει σημαντικά αποτελέσματα προς την ενίσχυση της κατανόησης των οργανισμών σχετικά με τους κινδύνους παραβιάσεων ασφαλείας που αντιμετωπίζουν.

8.2 Προτεινόμενα πεδία περεταίρω έρευνας

Η παρούσα έρευνα διερεύνησε τις παραβιάσεις ασφαλείας και εστίασε στην ποσοτικοποίηση των κινδύνων που προκαλούν περιστατικά αυτού του είδους. Η συγκεκριμένη διατριβή πρότεινε ένα μεθοδολογικό πλαίσιο αφήνοντας ένα σύνολο από ανοικτά ερευνητικά πεδία καθώς τα θέματα στα οποία εστίασε έχουν μεγάλο επαγγελματικό και ακαδημαϊκό ενδιαφέρον και δεν είναι εφικτό να εξαντληθούν στα πλαίσια μίας διατριβής. Στην συγκεκριμένη ενότητα αναφέρονται μερικά από τα σημαντικότερα ερευνητικά πεδία τα οποία μπορούν να θεωρηθούν ως φυσική επέκταση της παρούσας εργασίας.

Το μέγεθος του δείγματος, που χρησιμοποιήθηκε στην εμπειρική μελέτη με βάση την μέθοδο ανάλυσης γεγονότων και αναλύθηκε στο κεφάλαιο 5, είναι ένα από τα μεγαλύτερα που έχουν χρησιμοποιηθεί από ανάλογη μελέτη. Οι νομοθετικές παρεμβάσεις στις οποίες έχουν προβεί τα τελευταία τέσσερα έτη οι κυβερνήσεις διαφόρων κρατών και κυρίως των ΗΠΑ, σχετικά με τις υποχρεώσεις δημόσιας ανακοίνωσης των περιστατικών, έχουν οδηγήσει στην αύξηση του ποσοστού των περιστατικών που βλέπει το φως της δημοσιότητας. Οι εξελίξεις αυτές έχουν διευρύνει την δυνατότητα σύνθεσης μεγαλύτερων και περισσότερο αντιπροσωπευτικών δειγμάτων για την εφαρμογή εμπειρικών μελετών. Συνεπώς, αναμένεται επόμενες εμπειρικές μελέτες που επιχειρούν την εκτίμηση των επιπτώσεων, που επιφέρουν περιστατικά παραβίασης ασφαλείας μέσω της μεθόδου ανάλυσης γεγονότων, να χρησιμοποιήσουν ακόμα μεγαλύτερα δείγματα. Αναμένεται παράλληλα με την αύξηση των δειγμάτων να μειωθεί και η περίοδος ανάλυσης προκειμένου για την επίτευξη της μέγιστης δυνατής συνοχής και ομοιομορφίας στα δείγματα.

Επιπρόσθετα, η αύξηση των δειγμάτων θα διευρύνει την δυνατότητα διερεύνησης στατιστικών υποθέσεων σχετικά με το μέγεθος των οικονομικών επιπτώσεων με κριτήριο το είδος του οργανισμού. Ο επιμερισμός των δειγμάτων σε επιμέρους δείγματα με κριτήριο την επιλεγμένη ομαδοποίηση των οργανισμών, εξασθενεί την στατιστική εγκυρότητα της ανάλυσης όταν τα επιμέρους δείγματα δεν ξεπερνάνε ένα ελάχιστο απαραίτητο επίπεδο. Το πρόβλημα αυτό αναμένεται να λυθεί με την χρήση μεγαλύτερων δειγμάτων τα οποία θα περιλαμβάνουν αντιπροσωπευτικό αριθμό παρατηρήσεων από κάθε κατηγορία οργανισμών που επιλέγεται προς ανάλυση. Η εξέταση ενός επαρκούς συνόλου δεδομένων μπορεί να αποφέρει ακριβέστερα αποτελέσματα σχετικά με το επίπεδο των οικονομικών επιπτώσεων ανά κλάδο δραστηριότητας. Επιπρόσθετα, προτείνεται η αφαίρεση των περιστατικών που προκαλούνται από ιούς από

μελλοντικές έρευνες καθώς - όπως τεκμηριώθηκε - τα περιστατικά αυτά μπορούν να μειώσουν την εγκυρότητα των αποτελεσμάτων μίας μελέτης ανάλυσης γεγονότων. Τα αποτελέσματα αυτά μπορούν να χρησιμοποιηθούν στο μοντέλο που προτείνεται στο κεφάλαιο 7 για την ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας.

Περαιτέρω, ένα επαρκώς αντιπροσωπευτικό δείγμα με ικανοποιητικό μέγεθος θα δώσει την δυνατότητα προσδιορισμού των οικονομικών επιπτώσεων με διαχωρισμό των οργανισμών σε μικρότερες ομάδες κλάδων δραστηριότητας. Το σύνολο των υφιστάμενων εμπειρικών μελετών και η αντίστοιχη μελέτη που έγινε στα πλαίσια της παρούσας, έχουν αναλύσει τις οικονομικές επιπτώσεις χρησιμοποιώντας διευρυμένους διαχωρισμούς των οργανισμών κυρίως λόγω των περιορισμών που προκαλούν τα μεγέθη των δειγμάτων που χρησιμοποιήθηκαν. Ανάλυση του κόστους σε μικρότερες ομάδες κατηγοριών δραστηριοποίησης των οργανισμών θα αποδώσει ακριβέστερα αποτελέσματα για το κόστος που αντιπροσωπεύει κάθε μεμονωμένο οργανισμό κατά την εφαρμογή του μοντέλου που περιγράφτηκε στο κεφάλαιο 7.

Το μοντέλο ποσοτικοποίησης του επιπέδου ασφαλείας, που αναλύθηκε στο κεφάλαιο 6, βασίστηκε στους τεχνικούς παράγοντες κινδύνου. Από το σύνολο της έρευνας προέκυψε πως οι συγκεκριμένοι παράγοντες κινδύνου αποτελούν τους σημαντικότερους στον προσδιορισμό του επιπέδου ασφαλείας ενός συστήματος. Μελλοντική έρευνα μπορεί να επιβεβαιώσει περαιτέρω τη θέση αυτή αναλύοντας την επίδραση των παραγόντων κινδύνου που σχετίζονται με το ανθρωπινό δυναμικό και τις φυσικές καταστροφές.

Ένα ενδιαφέρον ερευνητικό πεδίο θα αποτελούσε η εφαρμογή της προτεινόμενης μεθοδολογίας ποσοτικοποίησης του επιπέδου ασφαλείας μέσω ενός ολοκληρωμένου πληροφοριακού συστήματος. Μία τέτοια ερευνητική προσπάθεια παρουσιάζεται στο [**121**] όπου έχει δημιουργεί ένα εργαλείο, βασισμένο στην συγκεκριμένη μεθοδολογία, σε γλώσσα προγραμματισμού VB.net και την χρήση του εξειδικευμένου μαθηματικού πακέτου Matlab. Τα δεδομένα που χρησιμοποιούνται από το συγκεκριμένο εργαλείο προέρχονται από την NVD.

Προκειμένου για τον προσδιορισμό της πιθανότητας παραβιάσεων ασφαλείας συνδυάστηκε το μεθοδολογικό υπόβαθρο από το μοντέλο των Gordon-Loeb και το μοντέλο ποσοτικοποίησης της ασφάλειας που περιγράφτηκε στο κεφάλαιο 6. Οι Gordon-Loeb προτείνουν δύο γενικές ομάδες συναρτήσεων για την εξήγηση της σχέσης μεταξύ της πιθανότητας παραβιάσεων ασφαλείας και

της επένδυσης σε ελέγχους ασφαλείας. Η ακριβής σχέση μεταξύ των δύο αυτών μεγεθών δεν έχει ακόμα επαρκώς επιβεβαιωθεί εμπειρικά. Η ακριβέστερη εξήγηση της συγκεκριμένης σχέσης θα οδηγήσει σε περαιτέρω ανάπτυξη του μοντέλου που προτάθηκε στο κεφάλαιο 7.

Προτάθηκε ένα θεωρητικό πλαίσιο σύνδεσης της μεθοδολογίας VaR με την ποσοτικοποίηση των κινδύνων παραβιάσεων ασφαλείας. Το προτεινόμενο πλαίσιο έδωσε λύσεις σε κάποια προβλήματα της εφαρμογής της μεθοδολογίας VaR αλλά παράλληλα άνοιξε ένα πλήθος από ερευνητικά πεδία όπως είναι η χρήση μη παραμετρικών κατανομών και ο προσδιορισμός του συνδυασμού επιπέδου εμπιστοσύνης και χρονικού ορίζοντα που παράγουν τα βέλτιστα αποτελέσματα για την VaR ανά κατηγορία οργανισμού.

8.3 Επίλογος

Το θέμα των παραβιάσεων ασφαλείας είναι σήμερα ένα από τα καίρια προβλήματα που καλούνται να αντιμετωπίσουν κυβερνήσεις και ιδιωτικοί οργανισμοί παγκοσμίως. Είναι ενδεικτική η προσπάθεια που έχει ξεκινήσει τα τελευταία έτη προκειμένου να βρεθεί δίαυλος συνεργασίας ανάμεσα στα ισχυρότερα κράτη για την αποτελεσματικότερη αντιμετώπιση του κυβερνο-εγκλήματος [**122**]. Ακόμα δεν έχει υπάρξει συμφωνία στην δημιουργία μίας διεθνής συνθήκης για την καταπολέμηση του καθώς προσκρούει σε θέματα εθνικής κυριαρχίας και ανθρωπίνων δικαιωμάτων [**123**]. Όπως υποστηρίχθηκε εκτενώς, το ζήτημα της ασφάλειας ΠΣ αυξάνεται διαρκώς σε σημασία και λαμβάνει σταδιακά μεγαλύτερη προτεραιότητα στις αποφάσεις οργανισμών κάθε κατηγορίας. Περίπου το 60% των οργανισμών διεθνώς δηλώνει ότι προτίθεται να αυξήσει τον προϋπολογισμό που διαθέτει για την ασφάλεια ΠΣ με το μεγαλύτερο μέρος να αποδίδει το ενδιαφέρον στην ασφάλεια των ευαίσθητων δεδομένων από παραβιάσεις ασφαλείας [**6**].

Επομένως, σύμφωνα με τα ανωτέρω, είναι θέμα χρόνου να προωθηθεί η συνεργασία μεταξύ κρατών και επαγγελματικών οργανισμών, σε παγκόσμιο επίπεδο, προκειμένου για την προστασία των ΠΣ από τα οποία ουσιαστικά εξαρτάται η εύρυθμη λειτουργία των σύγχρονων κοινωνιών. Οι εξελίξεις αυτές αναμένεται να διευρύνουν περαιτέρω το ερευνητικό ενδιαφέρον πάνω στο ζήτημα της ασφάλειας και της διαχείρισης των κινδύνων ΠΣ. Παράλληλα, αναμένεται αύξηση του ερευνητικού ενδιαφέροντος πάνω στους κινδύνους παραβιάσεων ασφαλείας καθώς αποτελούν αδιαμφισβήτητα τους κυριότερους από την ευρύτερη κατηγορία των κινδύνων ΠΣ.

Η παρούσα διατριβή επιχείρησε την ερευνητική συνεισφορά πάνω στους κινδύνους παραβιάσεων ασφαλείας και την ποσοτικοποίηση τους. Τα ευρήματα εκ του συνόλου της έρευνας τοποθέτησαν δομές για την ακριβέστερη και αντικειμενικότερη ποσοτικοποίηση των συγκεκριμένων κινδύνων. Οι δομές αυτές αποτελούν ερευνητικά ερεθίσματα προκειμένου για την βελτίωση και περαιτέρω ανάπτυξη των προτεινόμενων μεθοδολογιών. Η σύγχρονη τεχνολογία και οι κίνδυνοι που σχετίζονται με αυτήν, χαρακτηρίζονται από ραγδαία εξέλιξη και διαφοροποίηση η οποία οδηγεί στην αναγκαιότητα συνεχούς έρευνας πάνω σε μεθοδολογίες και εργαλεία αντιμετώπισης των συγκεκριμένων κινδύνων και κυρίως των κινδύνων παραβιάσεων ασφαλείας.

ΠΑΡΑΡΤΗΜΑΤΑ

I Λεξιλόγιο όρων

Abnormal return	Οι ασυνήθεις αποδόσεις αφορούν χρηματιστηριακά προϊόντα και κυρίως μετοχές. Η θεώρηση της απόδοσης ως ασυνήθη γίνεται με βάση κάποιο μοντέλο υπολογισμού των αναμενόμενων ή απαιτούμενων αποδόσεων για μία μετοχή όπως είναι το CAPM. Στην περίπτωση που η πραγματική απόδοση έχει διαφορά από την αναμενόμενη απόδοση, η οποία δεν εξηγείται από απλή στατιστική διακύμανση, τότε θεωρείται η εμφάνιση θετικής ή αρνητικής ασυνήθης απόδοσης. Οι ασυνήθεις αποδόσεις προκαλούνται από γεγονότα που αφορούν αποκλειστικά έναν οργανισμό τα οποία δεν μπορούν να προβλεφθούν ούτε να εξηγηθούν από τις γενικές συνθήκες της αγοράς.
Advanced Persistent Threat	Εξελιγμένη επίμονη απειλή. Αφορά στοχευόμενες επιθέσεις οι οποίες επιτυγχάνονται με την χρήση υψηλών τεχνικών διείσδυσης και συνεχείς βαθμιαίες απόπειρες. Οι επιθέσεις αυτού του τύπου αποσκοπούν κατά κύριο λόγο στην κυβερνο-κατασκοπεία με κυβερνητικούς και επιχειρηματικούς στόχους.
Beta	Ο συντελεστής συνολικού κινδύνου που χρησιμοποιείται από τα μοντέλα αποτίμησης επενδυτικών κεφαλαίων είτε αυτά περιλαμβάνουν έναν παράγοντα είτε πολλούς παράγοντες. Ορίζεται επίσης και ως στατιστικός συντελεστής καθώς ο υπολογισμός του προέρχεται από την ανάλυση παλινδρόμησης των ιστορικών ή εκτιμούμενων αποδόσεων μίας μετοχής σε σχέση με έναν δείκτη που αντιπροσωπεύει τις αποδόσεις της αγοράς.
Capital-Asset Pricing Model (CAPM)	Το Μοντέλο Αποτίμησης Κεφαλαιουχικών Αγαθών είναι ένα μοντέλο αποτίμησης επενδυτικών κεφαλαίων όπου σταθμίζεται η απόδοση σε σχέση με τον κίνδυνο με σκοπό τον χαρακτηρισμό μίας χρηματιστηριακής αξίας ως υποεκτιμημένης, σε κανονική τιμή ή υπερεκτιμημένη. Δημιουργήθηκε ανεξάρτητα από τους Sharpe, Linter και Mossin. Βασίζεται στο στατιστικό στοιχείο beta καθώς και στον υπολογισμό της πρόσθετης απόδοσης (risk premium) που απαιτείται από τους επενδυτές για το αγοραίο χαρτοφυλάκιο σε σύγκριση με την απόδοση που επιφέρουν αποδόσεις μηδενικού κινδύνου.
Cloud computing	Η χρήση λογισμικού, υλικού και πληροφοριών τα οποία είναι διαθέσιμα ως μία ενιαία υπηρεσία μέσα στο διαδίκτυο. Η χρήση του τα τελευταία έτη έχει αναπτυχθεί πολύ προκειμένου να εκμεταλλευθούν οι οργανισμοί τις ευκαιρίες που παρέχει στην μείωση του λειτουργικού κόστους. Η χρήση του παράλληλα δημιουργεί απειλές καθώς αυξάνονται σημαντικά οι κίνδυνοι παραβιάσεων ασφαλείας.
Convenience sample	Τα δείγματα ευκολίας ανήκουν στην γενικότερη κατηγορία δειγμάτων που δεν επηρεάζονται από την πιθανότητα εμφάνισης μίας παρατήρησης στον πληθυσμό. Χαρακτηρίζονται ως ευκολίας καθώς προέρχονται κυρίως από ερωτηματολόγια τα οποία αποτελούν τον πλέον εύκολο και λιγότερο δαπανηρό τρόπο συλλογής δεδομένων.
Direct costs	Τα στοιχεία κόστους που αποτελούν τις άμεσες οικονομικές επιπτώσεις ενός περιστατικού παραβίασης ασφαλείας σε έναν οργανισμό. Αποτελούνται κυρίως από το κόστος παρακολούθησης των λογαριασμών προσώπων των οποίων τα στοιχεία εκτέθηκαν, το κόστος ενίσχυσης του κανονισμού ασφαλείας, της επιβολής και

	παρακολούθησης τήρησης του και το κόστος ενίσχυσης του λογισμικού ασφαλείας.
Efficient market theory	Η θεωρεία στην οποία βασίζεται η αξιολόγηση της αποτελεσματικότητας των αγορών με κριτήριο την επάρκεια και ταχύτητα διάχυσης της πληροφόρησης ώστε τα χρηματιστηριακά προϊόντα και ιδιαιτέρως οι τιμές των μετοχών να ενσωματώνουν όλες τις διαθέσιμες πληροφορίες.
Efficient market theory hypothesis	Υπόθεση ότι οι αγορές είναι αποτελεσματικές σε σχέση με την άμεση και πλήρη ενσωμάτωση των διαθέσιμων πληροφοριών στις τιμές των χρηματιστηριακών προϊόντων και κυρίως των μετοχών. Διακρίνονται τρεις τύποι για την συγκεκριμένη υπόθεση ανάλογα με τον βαθμό πληρότητας πληροφόρησης που θεωρείται ότι διακρίνει μία αγορά: (α) Ισχυρού τύπου (strong-form), (β) ημι-ισχυρού τύπου (semi-strong form) και (γ) ασθενούς τύπου (weak-form).
Enterprise Risk Management	Η Εταιρική Διαχείριση Κινδύνων αφορά στο σύνολο των διαδικασιών που επηρεάζεται από όλα τα κλιμάκια διοίκησης ενός οργανισμού, εφαρμόζεται στον καθορισμό στρατηγικών, σχεδιάζεται προκειμένου να προσδιορίζει πιθανά αρνητικά γεγονότα, με κύριο στόχο την διαχείριση των κινδύνων και την παροχή επαρκής ασφάλειας στην διαδικασία επίτευξης των εταιρικών στόχων.
Estimation period	Περίοδος εκτίμησης που χρησιμοποιείται για την ανάλυση παλινδρόμησης μεταξύ των δεδομένων αποδόσεων μίας μετοχής και των αποδόσεων που έχουν ιστορικά επιφέρει οι λοιποί παράγοντες του μοντέλου αποτίμησης που χρησιμοποιείται. Στην περίπτωση π.χ. μοντέλου μίας μεταβλητής, η δεύτερη παράμετρος είναι ένας χρηματιστηριακός δείκτης που χρησιμοποιείται ως αντιπροσώπευση (proxy) των αποδόσεων της αγοράς.
Event analysis methodology	Μεθοδολογία που βασίζεται στην υπόθεση αποτελεσματικότητας των αγορών σχετικά με την διάχυση της πληροφόρησης και άμεσης αποτύπωσης στις τιμές των μετοχών. Ένα απρόβλεπτο γεγονός θεωρείται ότι θα επιφέρει ασυνήθεις αποδόσεις σε μία μετοχή οι οποίες δεν μπορούν να δικαιολογηθούν από μακροοικονομικούς παράγοντες. Προκειμένου να ποσοτικοποιηθεί η επίπτωση σε έναν οργανισμό από ένα συγκεκριμένο γεγονός, αναλύεται η αντίδραση των αγορών την στιγμή δημοσιοποίησης του. Με αυτόν τον τρόπο υπολογίζεται έμμεσα η οικονομική επίπτωση ενός γεγονότος του οποίου η άμεση κοστολόγηση είναι δύσκολη ή αδύνατη.
Event window	Παράθυρο περιόδου ανάλυσης γεγονότος το οποίο χρησιμοποιείται από την μεθοδολογία ανάλυσης γεγονότων (event analysis). Το παράθυρο περιλαμβάνει κατά ελάχιστο την ημέρα πραγμάτωσης ενός γεγονότος και συνήθως συμπεριλαμβάνει την προηγούμενη και έναν αριθμό των ημερών που ακολουθούν. Για κάθε ημέρα υπολογίζονται οι ασυνήθεις αποδόσεις και αθροίζονται προκειμένου να ληφθεί η σωρευτική ασυνήθης απόδοση (cumulative abnormal return).
Exposure Factor	Ο παράγοντας έκθεσης είναι ένα από τα βασικά προσδιοριστικά συστατικά των κινδύνων Πληροφοριακών Συστημάτων και αφορά το επίπεδο έκθεσης ενός στοιχείου ενεργητικού σε μία πιθανή επίθεση.
Indirect costs	Τα στοιχεία κόστους που αποτελούν τις έμμεσες οικονομικές επιπτώσεις ενός περιστατικού παραβίασης ασφαλείας σε έναν οργανισμό οι οποίες εμφανίζονται κατά κύριο λόγο σε μακροπρόθεσμο ορίζοντα. Αποτελούνται κυρίως από νομικό κόστος και το κόστος προερχόμενο από την προσβολή της φήμης και πελατείας ενός οργανισμού.

Information Systems Risks	Οι κίνδυνοι Πληροφοριακών Συστημάτων ορίζονται ως η καθαρή αρνητική επίπτωση από την εκμετάλλευση μίας ευπάθειας προερχόμενη από μία συγκεκριμένη απειλή λαμβάνοντας υπόψη την πιθανότητα έκθεσης καθώς και τη διάσταση του συμβάντος η οποία εξαρτάται από την αξία του στοιχείου ενεργητικού που προσβάλλεται καθώς και τον μέγεθος της έκθεσης.
Information Security	Ασφάλεια πληροφόρησης η οποία αφορά την διαφύλαξη σε ένα Πληροφοριακό Σύστημα της εμπιστευτικότητας (confidentiality), ακεραιότητας (integrity) και διαθεσιμότητας (availability) των πληροφοριών που διαχειρίζεται καθώς και της λειτουργικότητας του.
Information Systems	Πληροφοριακά Συστήματα ορίζονται τα συστήματα που δομούνται από το ανθρώπινο στοιχείο που συλλέγει, επεξεργάζεται και αξιοποιεί την πληροφόρηση, τον σχεδιασμό, οργάνωση και λειτουργία των ροών πληροφόρησης και τα δεδομένα στα οποία οι ροές πληροφόρησης είναι κατά τέτοιο τρόπο σχεδιασμένες ώστε να ικανοποιούν τις προσδιορισμένες απαιτήσεις πληροφόρησης ενός οργανισμού. Πλέον, τα Πληροφοριακά Συστήματα είναι στην πλειοψηφία των οργανισμών σχεδόν πλήρως βασισμένα στην Τεχνολογία Πληροφόρησης.
Information Systems Risk Management	Διαχείριση Κινδύνων Πληροφοριακών Συστημάτων ορίζεται η διαδικασία η οποία έχει ως βασικό στόχο την προστασία των στοιχείων ενεργητικού ενός Πληροφοριακού Συστήματος από όλες τις απειλές, που πηγάζουν από το εσωτερικό και το εξωτερικό περιβάλλον ενός οργανισμού, ούτως ώστε το κόστος των απωλειών από την πιθανή υλοποίηση των απειλών να ελαχιστοποιείται.
Information Technology	Η Τεχνολογία Πληροφόρησης αφορά το λογισμικό, την υποδομή και τις τεχνολογίες επικοινωνιών, τα οποία συνθέτουν ένα ολοκληρωμένο υποστηριχτικό σύστημα, το οποίο αποσκοπεί στην ικανοποίηση συγκεκριμένων απαιτήσεων και αναγκών ενός οργανισμού.
Information Technology System	Ο όρος Σύστημα Τεχνολογίας Πληροφόρησης αναφέρεται σε ένα υποστηρικτικό σύστημα που περιλαμβάνει κεντρικούς υπολογιστές (mainframe computers) , υπολογιστές-πελάτες, υποδομές δικτύωσης και εφαρμογές ευρείας χρήσης των οποίων η χρήση ικανοποιεί συγκεκριμένες απαιτήσεις και καλύπτει δεδομένες ανάγκες του οργανισμού.
Informational entropy	Η εντροπία πληροφόρησης είναι ένα μέτρο είτε της αβεβαιότητας που προκαλεί η συμπεριφορά μίας τυχαίας μεταβλητής πριν από τον προσδιορισμό της, είτε της μέσης αβεβαιότητας που μπορεί να αφαιρεθεί αφού επιτευχθεί ο προσδιορισμός της. Η εντροπία αποσκοπεί στην μέτρηση του μεγέθους ή της βαρύτητας που έχει ένα μήνυμα μέσω του οποίου επικοινωνείται η πραγμάτωση ενός γεγονότος. Η ερμηνεία της προσδιοριζόμενης εντροπίας εξαρτάται από την φύση της τυχαίας μεταβλητής την αβεβαιότητα της οποίας επιχειρούμε να εξηγήσουμε.
Insider information leakage	Διαρροή εσωτερικής πληροφόρησης η οποία κατέχεται από προνομιακά άτομα όπως διευθυντικά στελέχη, μετόχους με ποσοστό συμμετοχής άνω του 10% και μόνιμο προσωπικό του οποίου η θέση επιτρέπει την πρόσβαση σε προνομιακή πληροφόρηση. Η κοινολόγηση ή εκμετάλλευση εσωτερική πληροφόρησης είναι παράνομη από το σύνολο σχεδόν των χρηματαγορών παγκοσμίως.
IT Asset	Τα στοιχεία ενεργητικού ενός οργανισμού, που αποτελούνται από δεδομένα, υλικό, λογισμικό και προσωπικό και συνθέτουν ένα σύστημα πληροφόρησης.
Judgment sample	Τα δείγματα ευκολίας ανήκουν στην γενικότερη κατηγορία δειγμάτων που δεν επηρεάζονται από την πιθανότητα εμφάνισης μίας παρατήρησης

	στον πληθυσμό. Οι παρατηρήσεις τους προέρχονται αποκλειστικά από τις απόψεις ειδικών πάνω σε ένα θέμα.
Market portfolio	Το αγοραίο χαρτοφυλάκιο το οποίο περιλαμβάνει το σύνολο των υλικών και άυλων αξιών που περιέχουν οι αγορές παγκοσμίως. Το αγοραίο χαρτοφυλάκιο χρησιμοποιείται κατά κύριο λόγο από τα μοντέλα αποτίμησης επενδυτικών κεφαλαίων και καθώς είναι αδύνατος ο άμεσος υπολογισμός των αποδόσεων όλων των αξιών παγκοσμίως, χρησιμοποιούνται δείκτες που αντιπροσωπεύουν τις αγοραίες αποδόσεις. Παραδείγματα δεικτών με ευρεία χρήση είναι ο S&P 500 και ο NYSE.
Non-systematic risk	Ο μη συστηματικός κίνδυνος που αντιμετωπίζει μία εταιρία προέρχεται από μοναδικές πηγές κινδύνου που αφορούν αποκλειστικά την συγκεκριμένη εταιρία χωρίς να επηρεάζουν άμεσα το εξωτερικό της περιβάλλον.
National Vulnerability Database	Βάση δεδομένων ανοικτού κώδικα για την λεπτομερή και ακριβή καταγραφή ευπαθειών λογισμικού η οποία σχεδιάστηκε και λειτουργεί υπό την εποπτεία και ενίσχυση του τμήματος ασφαλείας υπολογιστών του NIST και υποστηρίζεται επικουρικά από το Computer Emergency Readiness Team των ΗΠΑ Η συγκεκριμένη βάση προσφέρει έναν εξαιρετικό μηχανισμό αναζήτησης ευπαθειών από το 1997. Οι ευπάθειες που καταγράφονται αφορούν αποκλειστικά αυτές που καταχωρούνται στις λίστες του CVE.
Open source vulnerability database	Βάση δεδομένων ανοικτού κώδικα για την λεπτομερή και ακριβή καταγραφή ευπαθειών λογισμικού. Η βάση αυτή αποτελεί συλλογικό αποτέλεσμα της κοινότητας που αποτελείται από ενδιαφερόμενα φυσικά και νομικά πρόσωπα για την ασφάλεια των Πληροφοριακών Συστημάτων. Την υποστήριξη του εγχειρήματος έχει ο μη κοινωφελής οργανισμός Open Security Foundation.
Record of data	Μία εγγραφή ορίζεται ως η αυτόνομη πληροφορία που αφορά προσωπικά δεδομένα ενός φυσικού ή νομικού προσώπου ή ολοκληρωμένη περιγραφή απόρρητων εταιρικών δεδομένων. Το μέγεθος ενός περιστατικού παραβίασης ασφαλείας μπορεί να οριστεί με κριτήριο των αριθμό των εγγραφών που εκτέθηκαν.
Residuals	Υπόλοιπα ή κατάλοιπα τα οποία αντιπροσωπεύουν την μεταβλητή τυχαίας αποκλίσεως και μετατρέπουν το γραμμικό υπόδειγμα ανάλυσης παλινδρόμησης στην στοχαστική του μορφή. Στο μοντέλο αποτίμησης κεφαλαιουχικών αγαθών τα υπόλοιπα αντιπροσωπεύουν ασυνήθεις αποδόσεις προερχόμενες από απρόβλεπτα γεγονότα που επηρεάζουν αποκλειστικά έναν οργανισμό χωρίς οι συνέπειες τους να διευρύνονται στο εξωτερικό του περιβάλλον.
Security controls	Έλεγχοι ασφαλείας οι οποίοι επίσης αποκαλούνται αντίμετρα, διασφαλίσεις ή απλά έλεγχοι και περιλαμβάνουν διαδικασίες, πολιτικές, υλικό εξοπλισμό ασφαλείας, συστήματα προστασίας τα οποία στο σύνολο τους έχουν ως πρωταρχικό στόχο την μείωση ή εξάλειψη των ευπαθειών και απειλών ώστε να μετριαστεί ο κίνδυνος των Πληροφοριακών Συστημάτων.
Systematic risk	Ο συστηματικός κίνδυνος που αντιμετωπίζει μία εταιρία και προέρχεται από πηγές που έχουν να κάνουν με το γενικότερο οικονομικό περιβάλλον καθώς και την ψυχολογία των αγορών.
Threat statement	Η δήλωση απειλών ορίζεται ως η αναφορά που περιλαμβάνει την κατάσταση του συνόλου των ευπαθειών, που προσδιορίζονται στα Πληροφοριακά Συστήματα ενός οργανισμού, συνδυαζόμενων με συγκεκριμένες πηγές απειλών.

Threat-source	Ένα από τα βασικά συστατικά στοιχεία των κινδύνων Πληροφοριακών Συστημάτων είναι αυτό της απειλής το οποίο ορίζεται ως κάθε γεγονός ή μέθοδος που έχει την δυνατότητα να επιφέρει αρνητικές επιπτώσεις σε ένα στοιχείο ενεργητικού είτε ακούσια, είτε εκούσια.
Value at Risk	Η μεθοδολογία αυτή χρησιμοποιείται για τον προσδιορισμό της μέγιστης δυνατής απώλειας που μπορεί να δεχθεί ένα χαρτοφυλάκιο αξιών σε συγκεκριμένο χρονικό ορίζοντα και με συγκεκριμένο επίπεδο εμπιστοσύνης.
Vulnerability	Ευπάθεια υπολογιστικών συστημάτων χαρακτηρίζεται κάθε ελάττωμα και αδυναμία στον σχεδιασμό των συστημάτων, στην εφαρμογή τους, στις διαδικασίες ασφαλείας και στους ελέγχους ασφαλείας που προστατεύουν μία αξία από πιθανές απειλές.

ΙΙ Δείγμα γεγονότων παραβίασης ασφαλείας

Στο παράρτημα αυτό παραθέτεται ο Πίνακας 27, ο οποίος περιλαμβάνει το δείγμα που χρησιμοποιήθηκε για την εφαρμογή της μεθοδολογίας με τα κύρια χαρακτηριστικά κάθε περιστατικού παραβίασης ασφαλείας και του οργανισμού που προσβλήθηκε. Η πηγή που αναφέρεται είναι η πρωταρχική πηγή άντλησης στοιχείων για ένα συμβάν και από την οποία αντλήθηκε η ημερομηνία δημοσίευσης γεγονότος. Για κάθε συμβάν, προκειμένου για την σύνθεση του συνόλου των χαρακτηριστικών του χρησιμοποιήθηκε χρήση πολλαπλών πηγών. Η ημερομηνία δημοσίευσης προέκυψε κατόπιν έρευνας πολλαπλών πηγών για κάθε συμβάν προκειμένου να διασταυρωθεί η πρώτη επίσημη δημόσια ανακοίνωση για κάθε περιστατικό. Όπως αναφέρθηκε παραπάνω το κριτήριο επιλογής, για κάθε συμβάν, της πρωταρχικής πηγής είναι η πηγή που θεωρήθηκε ότι δημοσίευσε πρώτη επισήμως ένα συμβάν. Επίσης, η εκτίμηση των άμεσων οικονομικών επιπτώσεων έχει προέλθει από εκτιμήσεις οργανισμών όπως η Ponemon Institute και από εκτιμήσεις που έχουν ανακοινώσει οι ίδιοι οργανισμοί που προσβλήθηκαν.

Πίνακας 27: Βασικά χαρακτηριστικά γεγονότων παραβιάσεων ασφαλείας

Α/Α Γεγονότος	Οργανισμός	Πηγή	Ημέρα δημοσίευσης γεγονότος	Κατηγορία παραβίασης ασφαλείας	Εκτίμηση άμεσων οικονομικών επιπτώσεων	Αριθμός εγγραφών σε έκθεση	Χρηματιστηριακή αγορά	Τομέας δραστηριοποίησης	Κεφαλαιοποίηση (000.000)
1	CBIZ, Inc.	DATALOSSDB.ORG	28/1/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	2.127.300	35.455	NYSE	Γενικές υπηρεσίες	331.120
2	Kraft Foods Inc.	DATALOSSDB.ORG	26/2/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	1.154.760	19.246	NYSE	Καταναλωτικά αγαθά	67.150
3	DaVita Inc.	DATALOSSDB.ORG	3/3/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	528.000	8.800	NYSE	Προϊόντα υγείας	7.880
4	Advance Auto Parts Inc Advance	DATALOSSDB.ORG	31/3/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	3.360.000	56.000	NYSE	Γενικές υπηρεσίες	6.280

5	WellPoint, Inc.	DATALOSSDB.ORG	8/4/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	7.680.000	128.000	NYSE	Προϊόντα υγείας	23.090
6	Westpac Banking Corporation	DATALOSSDB.ORG	4/5/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	120.000	2.000	NYSE	Χρηματοοικονομικές υπηρεσίες	68.690
7	HSBC Holdings, plc.	DATALOSSDB.ORG	8/5/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	9.540.000	159.000	NYSE	Χρηματοοικονομικές υπηρεσίες	164.980
8	Pfizer, Inc.	DATALOSSDB.ORG	12/5/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	780.000	13.000	NYSE	Προϊόντα υγείας	162.890
9	State Street Corporation	DATALOSSDB.ORG	29/5/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	2.730.000	45.500	NYSE	Χρηματοοικονομικές υπηρεσίες	19.620
10	AT&T Inc.	DATALOSSDB.ORG	4/6/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	6.815.700	113.595	NYSE	Τεχνολογίας	183.320
11	Aon Corporation	CNET	19/6/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	3.429.600	57.160	NYSE	Χρηματοοικονομικές υπηρεσίες	15.670
12	Unilever PLC	DATALOSSDB.ORG	25/6/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	720.000	12.000	NYSE	Καταναλωτικά αγαθά	92.370
13	Baxter International Inc.	DATALOSSDB.ORG	11/7/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	414.000	6.900	NYSE	Προϊόντα υγείας	32.200
14	Pearson, Plc	DATALOSSDB.ORG	15/7/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	116.400	1.940	NYSE	Γενικές υπηρεσίες	15.280
15	Honeywell International Inc.	DATALOSSDB.ORG	16/7/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	97.020	1.617	NYSE	Βιομηχανικά αγαθά	46.580
16	Bristol-Myers Squibb Company	DATALOSSDB.ORG	17/7/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	6.321.780	105.363	NYSE	Προϊόντα υγείας	56.120
17	Visa Inc.	DATALOSSDB.ORG	28/7/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	246.000	4.100	NYSE	Γενικές υπηρεσίες	73.840
18	Bank of America Corporation	CNET	7/8/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	1.370.640	22.844	NYSE	Χρηματοοικονομικές υπηρεσίες	84.500
19	The Princeton Review, Inc.	DATALOSSDB.ORG	20/8/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	6.480.000	108.000	NasdaqCM	Γενικές υπηρεσίες	7.220

20	Target Corporation	DATALOSSDB.ORG	11/9/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	561.300	9.355	NYSE	Γενικές υπηρεσίες	35.350
21	PSS World Medical Inc.	DATALOSSDB.ORG	15/9/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	318.000	5.300	NasdaqGS	Γενικές υπηρεσίες	1.310
22	Orbitz Worldwide, Inc.	DATALOSSDB.ORG	25/9/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	96.000	1.600	NYSE	Γενικές υπηρεσίες	381
23	United Parcel Service, Inc.	DATALOSSDB.ORG	14/11/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	510.000	8.500	NYSE	Γενικές υπηρεσίες	74.230
24	Starbucks Corporation	DATALOSSDB.ORG	24/11/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	5.820.660	97.011	NasdaqGS	Γενικές υπηρεσίες	36.500
25	Luxottica Group, S.p.A.	DATALOSSDB.ORG	25/11/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	3.565.140	59.419	NYSE	Γενικές υπηρεσίες	17.590
26	Hewlett-Packard Company	DATALOSSDB.ORG	11/12/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	2.144.880	35.748	NYSE	Τεχνολογίας	58.710
27	American Express Company	DATALOSSDB.ORG	18/12/2008	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	990.000	16.500	NYSE	Χρηματοοικονομικές υπηρεσίες	63.170
28	Wyndham Worldwide Corp	DATALOSSDB.ORG	22/12/2008	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	22.800.000	480.000	NYSE	Γενικές υπηρεσίες	6.760
29	Heartland Payment Systems, Inc.	DATALOSSDB.ORG	20/1/2009	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	7.800.000.000	130.000.000	NYSE	Γενικές υπηρεσίες	1.090
30	Monster Worldwide, Inc.	DATALOSSDB.ORG	23/1/2009	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	270.000.000	4.500.000	NYSE	Γενικές υπηρεσίες	822
31	Prudential Financial, Inc.	DATALOSSDB.ORG	27/1/2009	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	98.580	1.643	NYSE	Χρηματοοικονομικές υπηρεσίες	28.500
32	Best Buy Co., Inc.	DATALOSSDB.ORG	2/2/2009	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	239.400	3.990	NYSE	Γενικές υπηρεσίες	8.620
33	United Parcel Service, Inc.	DATALOSSDB.ORG	6/3/2009	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	3.540.000	59.000	NYSE	Γενικές υπηρεσίες	74.230
34	Aetna Inc.	CNET	28/5/2009	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	65.000	NYSE	Προϊόντα υγείας	15.850

35	AT&T Inc.	DATALOSSDB.ORG	8/7/2009	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	126.000	2.100	NYSE	Τεχνολογίας	183.320
36	Williams Companies, Inc.	DATALOSSDB.ORG	31/7/2009	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	264.000	4.400	NYSE	Πρώτων υλών	17.330
37	Chart Industries, Inc.	DATALOSSDB.ORG	10/8/2009	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	96.000	1.600	NasdaqGS	Βιομηχανικά αγαθά	1.720
38	Titanium Metals Corporation	DATALOSSDB.ORG	13/8/2009	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	Άγνωστο	Άγνωστο	NYSE	Πρώτων υλών	1.960
39	Mitsubishi Corporation	DATALOSSDB.ORG	5/9/2009	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	3.120.000	52.000	Other OTC	Καταναλωτικά αγαθά	39.500
40	Cobra Electronics Corporation	DATALOSSDB.ORG	9/11/2009	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	540.000	9.000	NasdaqGS	Καταναλωτικά αγαθά	35
41	Health Net Inc.	DATALOSSDB.ORG	19/11/2009	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	90.000.000	1.500.000	NYSE	Προϊόντα υγείας	3.250
42	Lincoln National Corporation	DATALOSSDB.ORG	4/1/2010	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	72.000.000	1.200.000	NYSE	Χρηματοοικονομικές υπηρεσίες	7.610
43	Adobe Systems Incorporated	ZNET	12/1/2010	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	16.170
44	Equifax, Inc.	CNET	11/2/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	Άγνωστο	Άγνωστο	NYSE	Χρηματοοικονομικές υπηρεσίες	5.020
45	Citigroup, Inc.	DATALOSSDB.ORG	24/2/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	36.000.000	600.000	NYSE	Χρηματοοικονομικές υπηρεσίες	98.830
46	Wyndham Worldwide Corporation	DATALOSSDB.ORG	26/2/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NYSE	Γενικές υπηρεσίες	6.760
47	Arrow Electronics, Inc.	DATALOSSDB.ORG	3/3/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	240.240	4.004	NYSE	Γενικές υπηρεσίες	4.680
48	ESB Financial Corporation	ITRC	23/4/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	185.820	3.097	NasdaqGS	Χρηματοοικονομικές υπηρεσίες	175
49	J.M. Smucker Company (The) New	ITRC	29/4/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	Άγνωστο	6.000	NYSE	Καταναλωτικά αγαθά	8.470

50	UnitedHealth Group Incorporated	DATALOSSDB.ORG	10/6/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	977.880	16.291	NYSE	Προϊόντα υγείας	56.840
51	WellPoint, Inc.	DATALOSSDB.ORG	23/6/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	28.200.000	645.000	NYSE	Προϊόντα υγείας	23.090
52	AMR Corporation	CNET	2/7/2010	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	4.740.000	79.000	Other OTC	Γενικές υπηρεσίες	214
53	Humana Inc.	DATALOSSDB.ORG	18/8/2010	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	157.860	2.631	NYSE	Προϊόντα υγείας	13.940
54	Aon Corporation	CNET	30/8/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	1.358.520	22.642	NYSE	Χρηματοοικονομικές υπηρεσίες	15.670
55	McDonald's Corporation	CNET	11/12/2010	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NYSE	Γενικές υπηρεσίες	102.650
56	Honda Motor Company, Ltd.	DATALOSSDB.ORG	23/12/2010	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	294.000.000	4.900.000	NYSE	Καταναλωτικά αγαθά	67.460
57	Sina Corporation	DATALOSSDB.ORG	4/1/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	18.000.000	300.000	NasdaqGS	Τεχνολογίας	4.460
58	Telecom Corporation of New Zeal	DATALOSSDB.ORG	16/1/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	129.000.000	2.150.000	NYSE	Τεχνολογίας	3.420
59	Credit Suisse Group American De	DATALOSSDB.ORG	7/2/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	90.000	1.500	NYSE	Χρηματοοικονομικές υπηρεσίες	33.520
60	Omnicare, Inc.	CNET	8/3/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	530.700	9.000	NYSE	Γενικές υπηρεσίες	3.720
61	Health Net Inc.	CNET	14/3/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	114.000.000	2.000.000	NYSE	Προϊόντα υγείας	3.250
62	EMC Corporation	CNET	17/3/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	66.300.000	1.105.000	NYSE	Τεχνολογίας	55.520
63	Google Inc.	CNET	1/4/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	20.000.000	NasdaqGS	Τεχνολογίας	196.590
64	Verizon unications Inc.	CNET	6/4/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NYSE	Τεχνολογίας	109.000

65	Sony Corporation	DATALOSSDB.ORG	26/4/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	4.620.000.000	77.000.000	NYSE	Καταναλωτικά αγαθά	20.670
66	Sony Corporation	DATALOSSDB.ORG	2/5/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	1.476.000.000	24.600.000	NYSE	Καταναλωτικά αγαθά	20.670
67	Fidelity National Information	DATALOSSDB.ORG	3/5/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	430.200	7.170	NYSE	Γενικές υπηρεσίες	8.760
68	Honda Motor Company, Ltd.	DATALOSSDB.ORG	12/5/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	16.800.000	280.000	NYSE	Καταναλωτικά αγαθά	67.460
69	Lockheed Martin Corporation	CNET	28/5/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NYSE	Βιομηχανικά αγαθά	28.250
70	L-3 unications Holdings	CNET	31/5/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NYSE	Βιομηχανικά αγαθά	7.070
71	Northrop Grumman Corporation	CNET	31/5/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NYSE	Βιομηχανικά αγαθά	15.180
72	Google Inc.	CNET	1/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	196.590
73	Sony Corporation	DATALOSSDB.ORG	2/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	60.000.000	1.000.000	NYSE	Καταναλωτικά αγαθά	20.670
74	Pharmerica Corporation	DATALOSSDB.ORG	3/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	3.102.660	51.711	NYSE	Γενικές υπηρεσίες	383.050
75	Citigroup, Inc.	CNET	9/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	21.604.980	360.000	NYSE	Χρηματοοικονομικές υπηρεσίες	98.830
76	Automatic Data Processing, Inc.	DATALOSSDB.ORG	15/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	26.610
77	Electronic Arts	DATALOSSDB.ORG	16/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	1.080.000	18.000	NasdaqGS	Τεχνολογίας	5.790
78	Sega Sammy	DATALOSSDB.ORG	17/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	77.445.300	1.290.755	Other OTC	Τεχνολογίας	5.670
79	Gannett Co., Inc.	DATALOSSDB.ORG	27/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NYSE	Γενικές υπηρεσίες	3.560

80	Viacom Inc.	CNET	28/6/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NasdaqGS	Γενικές υπηρεσίες	29.620
81	Apple Inc.	WALL STREET JOURNAL	4/7/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υπαλλήλων	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	468.160
82	Morgan Stanley	CNET	6/7/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	34.000	NYSE	Χρηματοοικονομικές υπηρεσίες	36.920
83	Moody's Corporation	THE REGISTER	8/7/2011	Λοιπές κατηγορίες παραβιάσεων	Άγνωστο	Άγνωστο	NYSE	Γενικές υπηρεσίες	8.570
84	Toshiba Corporation	CNET	11/7/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	7.520	Other OTC	Καταναλωτικά αγαθά	18.190
85	Booz Allen Hamilton Holding	DATALOSSDB.ORG	11/7/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	5.400.000	90.000	NYSE	Γενικές υπηρεσίες	2.350
86	General Mills, Inc.	DATALOSSDB.ORG	25/7/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	12.840.000	214.000	NYSE	Καταναλωτικά αγαθά	24.720
87	News Corporation	CNET	1/8/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NasdaqGS	Γενικές υπηρεσίες	48.490
88	Research In Motion Limited	CNET	9/8/2011	Λοιπές κατηγορίες παραβιάσεων	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	7.770
89	Seiko Epson	DATALOSSDB.ORG	20/8/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	21.000.000	350.000	Other OTC	Τεχνολογίας	1.240
90	Vasco Data Security Internation	CNET	30/8/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	376
91	UBS AG	BANKINFOSECURITY	15/9/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	2.000.000.000	Άγνωστο	NYSE	Χρηματοοικονομικές υπηρεσίες	53.490
92	SAIC Inc	DATALOSSDB.ORG	28/9/2011	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	307.067.940	4.900.000	NYSE	Γενικές υπηρεσίες	4.430
93	Sony Corporation	DATALOSSDB.ORG	11/10/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	5.580.000	93.000	NYSE	Καταναλωτικά αγαθά	20.670
94	Mobile TeleSystems	DATALOSSDB.ORG	25/10/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	96.000.000	1.600.000	NYSE	Τεχνολογίας	17.640

95	Microsoft Corporation	DATALOSSDB.ORG	11/11/2011	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	2.820.000	40.000	NasdaqGS	Τεχνολογίας	255.540
96	Amazon.com, Inc.	ZNET	16/1/2012	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	24.000.000	NasdaqGS	Γενικές υπηρεσίες	81.520
97	Symantec Corporation	CNET	17/1/2012	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	13.040
98	Euronet Worldwide, Inc.	DATABREACHES.NET	23/1/2012	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NasdaqGS	Γενικές υπηρεσίες	995
99	New York State Electricity	DATALOSSDB.ORG	23/1/2012	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	108.000.000	1.800.000	Other OTC	Γενικές υπηρεσίες	3.100
100	RealNetworks, Inc.	DATABREACHES.NET	30/1/2012	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	360
101	VeriSign, Inc.	ITRC	2/2/2012	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	6.000
102	Bank of America Corporation	ITRC	9/2/2012	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών	Άγνωστο	Άγνωστο	NYSE	Χρηματοοικονομικές υπηρεσίες	84.500
103	Intel Corporation	DATABREACHES.NET	10/2/2012	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NasdaqGS	Τεχνολογίας	135.340
104	NASDAQ	CNET	15/2/2012	Λοιπές κατηγορίες παραβιάσεων	Άγνωστο	Άγνωστο	NasdaqGS	Γενικές υπηρεσίες	n/a
105	Koninklijke Philips Electronics	CNET	23/2/2012	Μη εξουσιοδοτημένη πρόσβαση σε γενικά εταιρικά δεδομένα	Άγνωστο	Άγνωστο	NYSE	Καταναλωτικά αγαθά	19.690

ΙΙΙ Παραδείγματα δημοσίευσης γεγονότων παραβίασης ασφαλείας

Στο συγκεκριμένο παράρτημα παραθέτονται παραδείγματα δημοσιεύσεων που χρησιμοποιήθηκαν κατά την διάρκεια της έρευνας. Προκειμένου να διατηρηθεί η συνοχή με το παράρτημα ΙΙ, τοποθετείται ο Α/Α γεγονότος προκειμένου για τον χαρακτηρισμό κάθε γεγονότος.

Δημοσίευση γεγονότος Α/Α 61

Πηγή: The Hartgord Courant μέσω του datalossdb.org

Τίτλος: 1.5 Million Medical Files At Risk In Health Net Data Breach

A hard drive with seven years of personal and medical information on about 1.5 million Health Net customers, including 446,000 in Connecticut, was lost six months ago and was first reported Wednesday, state and company officials said.

The insurance company informed the state attorney general's office and the Department of Insurance Wednesday of the security breach that puts personal medical records at risk in a historic lapse, the first of its kind to be publicly reported.

Δημοσίευση γεγονότος Α/Α 62

Πηγή: CNET

Τίτλος: RSA warns SecurID customers after company is hacked

IDG News Service - EMC's RSA Security division says the security of the company's two-factor SecurID tokens could be at risk following a sophisticated cyber-attack on the company. In a note published on the company's website late Thursday, RSA Executive Chairman Art Coviello said his company is "actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack," Coviello said.

Coviello's note offered few details on what happened, but it has offered some guidance for customers. The cyber-attack was "recent" and was a so-called Advanced Persistent Threat incident, Coviello said. This is the

type of attack that compromised systems at Google and as many as 100 other companies in late 2009. Hackers use e-mail-based or Web-based attacks to get a foothold in the company and then move about the company's internal networks looking for sensitive data to sneak out. In this case, the hackers found information on RSA's SecurID products -- which are used on PCs, USB devices, phones and key fobs in about 25,000 corporations to provide an extra layer of security beyond a username and password for people logging into programs or networks. Having access to RSA's internal networks and the SecurID source code might give criminals some subtle way of attacking SecurID users, but it shouldn't give them a way of completely breaking RSA's encryption, said Thorsten Holz, an assistant professor at Ruhr-University Bochum who studies computer security. "If RSA implemented everything correctly, nobody should be worried too much," he said. However, from RSA's statement, it's not clear exactly what the hackers were able to learn off the company network. According to Nate Lawson, a cryptographer and the founder of Root Labs, there's simply not enough information available to tell how bad the problem really is. "If I was a customer of theirs it makes it really hard to know what I need to do. They recommend a lot of things that people are already doing," he said. RSA representatives did not immediately return calls and e-mails seeking comment. No EMC products were affected by the attack and RSA doesn't think other RSA products are affected. Also, there's no evidence that customer or employee information was compromised, Coviello said. EMC's stock [EMC] was down 1.25 percent in after-hours trading following the news. In a regulatory filing, EMC said it "does not believe that the matter described in the letter and note will have a material impact on its financial results."

Δημοσίευση γεγονότος Α/Α 75

Πηγή: CNET

Τίτλος: Report: Hackers accessed Citigroup customer data

Citigroup said today that hackers breached the bank's network and may have gained access to the personal data of hundreds of thousands of bank card customers. Customer names, account numbers, and contact information, including e-mail addresses, were accessed during the breach, which was discovered in May during routine monitoring. However, no Social Security numbers, birth dates or security codes were accessed, Citi said. Citi said the breach affected about 1 percent of its 21 million customers. "We are contacting customers whose information was impacted," Citi spokesperson Sean Kevelighan said in a statement. "Citi has implemented enhanced procedures to prevent a recurrence of this type of event. For the security of these customers, we are not disclosing further details." The breach, which was first reported by the Financial Times, adds Citi's name to a growing list of companies that has suffered an intrusion in recent months. RSA, the company sells SecurID tokens that are used by corporations, organizations, and government agencies to allow workers to remotely access a sensitive network securely, announced in March that it was victimized by an "extremely sophisticated cyberattack" in which sensitive data related to the SecurID technology had been pilfered. In April, Sony warned 77 million customers that their personal information, including names,

addresses, e-mail addresses, birthdays, PlayStation Network and Qriocity passwords, and usernames, as well as online user handles, had been obtained illegally by an "unauthorized person" between April 17 and 19. Less than a week later, Sony announced that data of more than 24 million Sony Entertainment Online customers had also been exposed. Google revealed earlier this month that it had "detected and disrupted" a plan to break into hundreds of Gmail accounts through a series of phishing attacks. The targets of the attacks included top government officials from the U.S. and several Asian countries, along with journalists, political activists, and military personnel.

Δημοσίευση γεγονότος Α/Α 90

Πηγή: CNET

Τίτλος: DigiNotar declares bankruptcy after major security breach

The disgraced Dutch certificate authority DigiNotar, recently at the center of a hacking scandal, has declared itself bankrupt. The firm first realized it had been compromised July 19 but failed to make any public announcement until the end of August when Iranian users began to notice their Gmail accounts were using fake SSL certificates. Theses certificates are used by hackers to intercept people's login details and private information when visiting secure sites like Google's Gmail service. In the subsequent investigation that followed, DigiNotar was found to have issued over 500 fake certificates during the period of its breach, with many high profile companies compromised, including Microsoft and its Windows Update service. DigiNotar's parent company, VASCO Data Security International confirmed yesterday that the embattled company had filed for bankruptcy. A trustee for the Haarlem District Court in the Netherlands has been appointed to manage the company during this process. "Although we are saddened by this action and the circumstances that necessitated it, we would like to remind our customers and investors that the incident at DigiNotar has no impact on VASCO's core authentication technology," commented T Kendall Hunt, VASCO's chairman and CEO when making a statement regarding DigiNotar. Hunt was also very keen to point out that "The technological infrastructures of VASCO and DigiNotar remain completely separated, meaning that there is no risk for infection of VASCO's strong authentication business." He said he would cooperate fully with the Haarlem District Court during this process to conclude the matter for its customers and staff. Jan Valcke, VASCO's chief operating officer made it clear that the group had no plans to re-enter the certificate authority business any time in the near future, with the chief financial officer, Cliff Bown further pointing out that DigiNotar's demise would have a significant impact financially on the group. An Iranian hacker known only as ComodoHacker claimed responsibility for the attack using his Pastebin account. He later claimed responsibility for breaches to GlobalSign and said to have access to two more certificate authorities, but as of yet no further information has been revealed on the latter.

IV Πρόγραμμα υπολογισμών διαδικασιών ανάλυσης γεγονότων

Στο παρόν παράρτημα παραθέτεται ο κώδικας γραμμένος σε Visual Basic ο οποίος χρησιμοποιήθηκε για την αυτοματοποίηση της διαδικασίας ανάλυσης γεγονότων. Συγκεκριμένα οι διαδικασίες ανάλυσης παλινδρόμησης, υπολογισμών των σωρευτικών ασυνήθη αποδόσεων, των στατιστικών μέτρων και των τελικών αποτελεσμάτων ανάλυσης στατιστικών υποθέσεων πραγματοποιούνται από τις διαδικασίες του παρακάτω κώδικα.

```
Public Sub reg()
    Dim CompanyName As String, SheetName As String
    Dim Event_Date As Date
    Dim Event_Date_T0 As Date
    Dim Event_Date_MinusOne As Date
    Dim Event_Date_MinusTwo As Date
    Dim Event_Date_PlusOne As Date
    Dim i As Integer
    Dim Deletion As Boolean
    Dim TotalCarFormula As String
    Dim Technology As String
    Dim Rest As String
    Dim LowerBound As Long
    Dim StartRange As String
    Dim EndRange As String
    Dim CompaniesProccessed As Long
    Dim TechnologyProcessed As Long
    Dim Perform3FactorRegression As Boolean

    Application.DisplayAlerts = False

    Application.ScreenUpdating = False

Start_Over:
    For i = 1 To ActiveWorkbook.Worksheets.Count
        Select Case ActiveWorkbook.Worksheets(i).Name
            Case "Results", "Stock Data", "Russell 3000 Index", "NYSE", "Security Breaches", "Four Factors Data"

            Case Else
                ActiveWorkbook.Worksheets(i).Delete
                GoTo Start_Over
        End Select
    Next i

    Application.DisplayAlerts = True

    ActiveWorkbook.Sheets("Security Breaches").Select

    ActiveWorkbook.Worksheets("Security Breaches").ListObjects("BREACHES_DATASET").Sort.SortFields.Clear

    With ActiveWorkbook.Worksheets("Security Breaches")
        .Range("BREACHES_DATASET").Sort _
            Key1:=.Columns("E"), Order1:=xlAscending, _
            Key2:=.Columns("B"), Order2:=xlAscending, Header:=xlYes
    End With
```

```
Dim r As Range
Set r = Range("$B$1:$O$126")

LowerBound = r.Rows.Count
CompaniesProccessed = 0
TechnologyProcessed = 0

'If 3 factor regression is activated mark Perform3FactorRegression as true
If Worksheets("Results").Cells(35, 3).Value = 0 Then
   Perform3FactorRegression = True
Else
   Perform3FactorRegression = False
End If

For nrow = 2 To LowerBound
   DoEvents

   'Mark the record as not "Done"
   Worksheets("Security Breaches").Cells(nrow, 1).Value = ""

   'Intialize environment
   CompanyName = Worksheets("Security Breaches").Cells(nrow, 2).Value
   Event_Date = Worksheets("Security Breaches").Cells(nrow, 11).Value
   SheetName = CompanyName

   If Worksheets("Security Breaches").Cells(nrow, 13).Value <> "YES" Then
      GoTo End_Loop
   End If

   If Worksheets("Results").Cells(24, 3).Value <> -1 And Worksheets("Results").Cells(24, 4).Value <> -1 Then
      'if not between min and max records ignore it
      Dim NumOfRecs As Long
      NumOfRecs = IIf(Worksheets("Security Breaches").Cells(nrow, 17).Value = "UNKNOWN", 0, Worksheets("Security Breaches").Cells(nrow, 17).Value)

      If Not (NumOfRecs >= Worksheets("Results").Cells(24, 3).Value _
            And NumOfRecs <= Worksheets("Results").Cells(24, 4).Value _
           ) Or Worksheets("Security Breaches").Cells(nrow, 17).Value = "UNKNOWN" Then
         GoTo End_Loop
      End If
   End If

   'If it is activated the test mode then run only these three companies
   If Worksheets("Results").Cells(34, 3).Value = 1 Then
      If Worksheets("Security Breaches").Cells(nrow, 2).Value <> "Heartland Payment Systems, Inc." _
        And Worksheets("Security Breaches").Cells(nrow, 2).Value <> "Sony Corporation Common Stock-B" _
        And Worksheets("Security Breaches").Cells(nrow, 2).Value <> "Adobe Systems Incorporated" Then
         GoTo End_Loop
      End If
   End If

   If Len(TotalCarFormula) = 0 Then
      TotalCarFormula = """ & CompanyName & ":" & CompanyName & """
   Else
      TotalCarFormula = Split(TotalCarFormula, ":")(0) & ":" & CompanyName & """
   End If

   If Worksheets("Security Breaches").Cells(nrow, 5).Value = "Technology" Then
      TechnologyProcessed = TechnologyProcessed + 1
```

```
        If Len(Technology) = 0 Then
            Technology = """ & CompanyName & ":" & CompanyName & """
        Else
            Technology = Split(Technology, ":")(0) & ":" & CompanyName & """
        End If
    End If

    If Worksheets("Security Breaches").Cells(nrow, 5).Value <> "Technology" Then
        If Len(Rest) = 0 Then
            Rest = """ & CompanyName & ":" & CompanyName & """
        Else
            Rest = Split(Rest, ":")(0) & ":" & CompanyName & """
        End If
    End If

    CompaniesProccessed = CompaniesProccessed + 1

'for debuging reasons
'GoTo End_Loop

    'Always choose the data sheet as the active sheet
    ActiveWorkbook.Sheets("Stock Data").Select

    'Clear filters
    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=2

    'Set filters
    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=2, Criteria1 _
    :="" & CompanyName

    Dim rg As Range
    ActiveSheet.Select

    With ActiveSheet.AutoFilter.Range
        Set rg = .Offset(1, 0).Resize(.Rows.Count - 1, 1).SpecialCells(xlCellTypeVisible)
        StartRange = Replace(rg.Offset(0, 9).Address, Split(Split(rg.Offset(0, 9).Address, ":")(0), "$")(2), Split(Split(rg.Offset(0, 9).Address, ":")(0), "$")(2) + 1)
        EndRange = Replace(rg.Offset(0, 10).Address, Split(Split(rg.Offset(0, 10).Address, ":")(0), "$")(2), Split(Split(rg.Offset(0, 10).Address, ":")(0), "$")(2) + 1)
    End With


'================================================================================================
'================================================================================================
    'Calculate Event Window
'================================================================================================
'================================================================================================
    Dim j As Integer
    Dim rng As Range
    Dim Offset_MinusOne As Long
    Dim Offset_MinusTwo As Long

    On Error Resume Next

    '1. Check to see if there data for the Event date T0 till t+10
    For j = 0 To 9
        Event_Date_T0 = Event_Date + j

        'Clear Event Date filters
        ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3
```

```
    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3, Operator _
    :=xlFilterValues, Criteria2:=Array(2, Format(Event_Date_T0, "mm/dd/yyyy"))

    Set rng = ActiveSheet.AutoFilter.Range

    If rng.Columns(1).SpecialCells(xlCellTypeVisible).Count - 1 > 0 Then
      Exit For
    End If
  Next j

  '2. Check to see if there data for the Event date - 1  T-1 till t-10
  For j = 1 To 10
    Event_Date_MinusOne = Event_Date - j

    'Clear Event Date filters
    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3

    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3, Operator _
    :=xlFilterValues, Criteria2:=Array(2, Format(Event_Date_MinusOne, "mm/dd/yyyy"))

    Set rng = ActiveSheet.AutoFilter.Range

    If rng.Columns(1).SpecialCells(xlCellTypeVisible).Count - 1 > 0 Then
      Offset_MinusOne = Split(Split(rng.Columns(1).SpecialCells(xlCellTypeVisible).Offset(1, 2).Address, ",")(1), "$")(2)
      StartRange = Split(StartRange, ":")(0) & ":$J$" & Offset_MinusOne
      If Perform3FactorRegression = False Then
        EndRange = Split(EndRange, ":")(0) & ":$K$" & Offset_MinusOne
      Else
        EndRange = Split(EndRange, ":")(0) & ":$M$" & Offset_MinusOne
      End If

      Exit For
    End If
  Next j

  '3. Check to see if there data for the Event date - 2  Event_Date_MinusOne - 1 till t-10
  For j = 1 To 10
    Event_Date_MinusTwo = Event_Date_MinusOne - j

    'Clear Event Date filters
    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3

    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3, Operator _
    :=xlFilterValues, Criteria2:=Array(2, Format(Event_Date_MinusTwo, "mm/dd/yyyy"))

    Set rng = ActiveSheet.AutoFilter.Range

    If rng.Columns(1).SpecialCells(xlCellTypeVisible).Count - 1 > 0 Then
      Offset_MinusTwo = Split(Split(rng.Columns(1).SpecialCells(xlCellTypeVisible).Offset(1, 2).Address, ",")(1), "$")(2) - 1
      StartRange = Split(StartRange, ":")(0) & ":$J$" & Offset_MinusTwo
      If Perform3FactorRegression = False Then
        EndRange = Split(EndRange, ":")(0) & ":$K$" & Offset_MinusTwo
      Else
        EndRange = Split(EndRange, ":")(0) & ":$M$" & Offset_MinusTwo
      End If

      Exit For
    End If
```

```
    Next j

    '4. Check to see if there data for the Event date + 1  T0+1 till t0+10
    For j = 1 To 10
      Event_Date_PlusOne = Event_Date_T0 + j

      'Clear Event Date filters
      ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3

       ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3, Operator _
      :=xlFilterValues, Criteria2:=Array(2, Format(Event_Date_PlusOne, "mm/dd/yyyy"))

      Set rng = ActiveSheet.AutoFilter.Range

      If rng.Columns(1).SpecialCells(xlCellTypeVisible).Count - 1 > 0 Then
        Exit For
      End If
    Next j

    'Clear Event Date filters
    ActiveSheet.ListObjects("Return_Data").Range.AutoFilter Field:=3
'=============================================================================================
'=============================================================================================

    'Run Regression
    On Error GoTo My_Error

    Application.Run "ATPVBAEN.XLAM!Regress", _
      ActiveSheet.Range(StartRange), _
      ActiveSheet.Range(EndRange), _
      False, False, 95, SheetName, _
      False, False, False, True, , False

    With ActiveWorkbook.Sheets(SheetName)
      'Set company name
      .Range("D1").Select
      ActiveCell.Font.Bold = True
      ActiveCell.Font.ThemeColor = xlThemeColorLight2
      ActiveCell.Formula = CompanyName

      'Set numeric formats
      .Range("C12").Select
      Selection.NumberFormat = "0.000000000"
      .Range("D12").Select
      Selection.NumberFormat = "0.000000000"
      .Range("G17").Select
      Selection.NumberFormat = "0.000000000"
      .Range("I17").Select
      Selection.NumberFormat = "0.000000000"

      'Set titles
      .Range("E31").Select
      ActiveCell.Formula = "Event Day 1" ' .FormulaR1C1 = "test"
      .Range("E32").Select
      ActiveCell.Formula = "Event Day 2" '
      .Range("E33").Select
      ActiveCell.Formula = "Event Day 3"
      .Range("E34").Select
      ActiveCell.Formula = "Market -RF return 1"
```

```
.Range("E35").Select
ActiveCell.Formula = "Market -RF return 2"
.Range("E36").Select
ActiveCell.Formula = "Market -RF return 3"
.Range("E37").Select
ActiveCell.Formula = "Required return 1"
.Range("E38").Select
ActiveCell.Formula = "Required return 2"
.Range("E39").Select
ActiveCell.Formula = "Required return 2"
.Range("E40").Select
ActiveCell.Formula = "Stock Actual -RF Return 1"
.Range("E41").Select
ActiveCell.Formula = "Stock Actual -RF Return 2"
.Range("E42").Select
ActiveCell.Formula = "Stock Actual -RF Return 3"
.Range("E43").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "AR 1"
.Range("E44").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "AR 2"
.Range("E45").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "AR 3"
.Range("E46").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "CAR"
.Range("E47").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "Event window [-1,1] Residual Var"
.Range("E48").Select
ActiveCell.Formula = "Var AR Day 1"
.Range("E49").Select
ActiveCell.Formula = "Var AR Day 2"
.Range("E50").Select
ActiveCell.Formula = "Var AR Day 3"
.Range("E51").Select
ActiveCell.Formula = "SAR 1"
.Range("E52").Select
ActiveCell.Formula = "SAR 2"
.Range("E53").Select
ActiveCell.Formula = "SAR 3"
.Range("E54").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "CSAR"
.Range("E55").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "Event window [0,0] Residual Var"
.Range("E56").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "Event window [0,1] Residual Var"
.Range("E57").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
```

```
ActiveCell.Formula = "CAR event window [0,1]"
.Range("E58").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "CSAR event window [0,1]"
.Range("E59").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "CAR event window [-1,0]"
.Range("E60").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "CSAR event window [-1,0]"

If Perform3FactorRegression = True Then
   .Range("E61").Select
   ActiveCell.Formula = "SMB return 1"
   .Range("E62").Select
   ActiveCell.Formula = "SMB return 2"
   .Range("E63").Select
   ActiveCell.Formula = "SMB return 3"
   .Range("E64").Select
   ActiveCell.Formula = "HML return 1"
   .Range("E65").Select
   ActiveCell.Formula = "HML return 2"
   .Range("E66").Select
   ActiveCell.Formula = "HML return 3"
   .Range("E67").Select
   ActiveCell.Formula = "UMD return 1"
   .Range("E68").Select
   ActiveCell.Formula = "UMD return 2"
   .Range("E69").Select
   ActiveCell.Formula = "UMD return 3"
   .Range("E70").Select
   ActiveCell.Font.Bold = True
   ActiveCell.Font.ThemeColor = xlThemeColorLight2
   ActiveCell.Formula = "Event window [-1,0] Residual Var"
Else
  .Range("E61").Select
  ActiveCell.Font.Bold = True
   ActiveCell.Font.ThemeColor = xlThemeColorLight2
   ActiveCell.Formula = "Event window [-1,0] Residual Var"
End If

'set formulas
.Range("F31").Select
Selection.NumberFormat = "d/m/yyyy"
ActiveCell.FormulaR1C1 = Event_Date_MinusOne
.Range("F32").Select
Selection.NumberFormat = "d/m/yyyy"
ActiveCell.FormulaR1C1 = Event_Date_T0
.Range("F33").Select
Selection.NumberFormat = "d/m/yyyy"
ActiveCell.FormulaR1C1 = Event_Date_PlusOne
.Range("F34").Select
 Selection.NumberFormat = "0.0000%"
ActiveCell.FormulaR1C1 = "=VLOOKUP(R[-3]C,'Russell 3000 Index'!R2C1:R10000C9,9,FALSE )"
.Range("F35").Select
 Selection.NumberFormat = "0.0000%"
ActiveCell.FormulaR1C1 = "=VLOOKUP(R[-3]C,'Russell 3000 Index'!R2C1:R10000C9,9,FALSE )"
.Range("F36").Select
```

```
 Selection.NumberFormat = "0.0000%"
ActiveCell.FormulaR1C1 = "=VLOOKUP(R[-3]C,'Russell 3000 Index'!R2C1:R10000C9,9,FALSE )"
.Range("F37").Select
Selection.NumberFormat = "0.0000%"
If Perform3FactorRegression = False Then
    ActiveCell.FormulaR1C1 = "=R17C2+R18C2*R[-3]C"
Else
    ActiveCell.FormulaR1C1 = "=R17C2+R18C2*R[-3]C+R19C2*R[24]C+R20C2*R[27]C"
End If
.Range("F38").Select
 Selection.NumberFormat = "0.0000%"
If Perform3FactorRegression = False Then
    ActiveCell.FormulaR1C1 = "=R17C2+R18C2*R[-3]C"
Else
    ActiveCell.FormulaR1C1 = "=R17C2+R18C2*R[-3]C+R19C2*R[24]C+R20C2*R[27]C"
End If
.Range("F39").Select
 Selection.NumberFormat = "0.0000%"
If Perform3FactorRegression = False Then
    ActiveCell.FormulaR1C1 = "=R17C2+R18C2*R[-3]C"
Else
    ActiveCell.FormulaR1C1 = "=R17C2+R18C2*R[-3]C+R19C2*R[24]C+R20C2*R[27]C"
End If
.Range("F40").Select
Selection.NumberFormat = "0.00%"
ActiveCell.FormulaR1C1 = "=VLOOKUP(R1C4 & ""@""& TEXT(R[-9]C,""η/μ/εεεε""),'Stock Data'!R2C1:R25000C12,10,FALSE)"
.Range("F41").Select
Selection.NumberFormat = "0.00%"
ActiveCell.FormulaR1C1 = "=VLOOKUP(R1C4 & ""@""& TEXT(R[-9]C,""η/μ/εεεε""),'Stock Data'!R2C1:R25000C12,10,FALSE)"
.Range("F42").Select
Selection.NumberFormat = "0.00%"
ActiveCell.FormulaR1C1 = "=VLOOKUP(R1C4 & ""@""& TEXT(R[-9]C,""η/μ/εεεε""),'Stock Data'!R2C1:R25000C12,10,FALSE)"
.Range("F43").Select
Selection.NumberFormat = "0.00%"
ActiveCell.Font.Bold = True
ActiveCell.FormulaR1C1 = "=R[-3]C-R[-6]C"
.Range("F44").Select
Selection.NumberFormat = "0.00%"
ActiveCell.Font.Bold = True
ActiveCell.FormulaR1C1 = "=R[-3]C-R[-6]C"
.Range("F45").Select
Selection.NumberFormat = "0.00%"
ActiveCell.Font.Bold = True
ActiveCell.FormulaR1C1 = "=R[-3]C-R[-6]C"
.Range("F46").Select
Selection.NumberFormat = "0.00%"
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.FormulaR1C1 = "=SUM(R[-3]C:R[-1]C)"
.Range("F47").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.FormulaR1C1 = "=SUM(R48C6:R50C6)"
.Range("F48").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.Formula = "=R55C6*(1+(1/R8C2)+((R[-8]C-R30C9)^2/R30C10))"
.Range("F49").Select
Selection.NumberFormat = "0.000000000"
```

```
ActiveCell.Formula = "=R55C6*(1+(1/R8C2)+((R[-8]C-R30C9)^2/R30C10))"
.Range("F50").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.Formula = "=R55C6*(1+(1/R8C2)+((R[-8]C-R30C9)^2/R30C10))"
.Range("F51").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.Formula = "=R[-8]C/SQRT(R[-3]C)"
.Range("F52").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.Formula = "=R[-8]C/SQRT(R[-3]C)"
.Range("F53").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.Formula = "=R[-8]C/SQRT(R[-3]C)"
.Range("F54").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.Font.Bold = True
ActiveCell.Formula = "=SUM(R[-3]C:R[-1]C)/SQRT(3)"
.Range("F55").Select
ActiveCell.Font.Bold = True
Selection.NumberFormat = "0.000000000"
ActiveCell.Font.ThemeColor = xlThemeColorLight2
If Perform3FactorRegression = False Then
    ActiveCell.Formula = "=VAR.S(R25C3:R1000C3)"
Else
    ActiveCell.FormulaR1C1 = "=VAR.S(R27C3:R1000C3)"
End If
.Range("F56").Select
ActiveCell.Font.Bold = True
Selection.NumberFormat = "0.000000000"
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "=SUM(R49C6:R50C6)"
.Range("F57").Select
ActiveCell.Font.Bold = True
Selection.NumberFormat = "0.00%"
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "=SUM(R44C6:R45C6)"
.Range("F58").Select
ActiveCell.Font.Bold = True
Selection.NumberFormat = "0.000000000"
ActiveCell.Formula = "=SUM(R52C6:R53C6)/SQRT(2)"

.Range("F59").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
Selection.NumberFormat = "0.00%"
ActiveCell.Formula = "=SUM(R43C6:R44C6)"
.Range("F60").Select
ActiveCell.Font.Bold = True
Selection.NumberFormat = "0.000000000"
ActiveCell.Formula = "=SUM(R51C6:R52C6)/SQRT(2)"

If Perform3FactorRegression = True Then
    .Range("F61").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-30]C,'Russell 3000 Index'!R2C1:R10000C8,6,FALSE)"
    .Range("F62").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-30]C,'Russell 3000 Index'!R2C1:R10000C8,6,FALSE)"
    .Range("F63").Select
```

```
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-30]C,'Russell 3000 Index'!R2C1:R10000C8,6,FALSE)"
    .Range("F64").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-33]C,'Russell 3000 Index'!R2C1:R10000C8,7,FALSE)"
    .Range("F65").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-33]C,'Russell 3000 Index'!R2C1:R10000C8,7,FALSE)"
    .Range("F66").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-33]C,'Russell 3000 Index'!R2C1:R10000C8,7,FALSE)"
    .Range("F67").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-36]C,'Russell 3000 Index'!R2C1:R10000C8,8,FALSE)"
    .Range("F68").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-36]C,'Russell 3000 Index'!R2C1:R10000C8,8,FALSE)"
    .Range("F69").Select
    Selection.NumberFormat = "0.0000%"
    ActiveCell.Formula = "=VLOOKUP(R[-36]C,'Russell 3000 Index'!R2C1:R10000C8,8,FALSE)"
    .Range("F70").Select
    ActiveCell.Font.Bold = True
    ActiveCell.Font.ThemeColor = xlThemeColorLight2
    Selection.NumberFormat = "0.000000000"
    ActiveCell.Formula = "=SUM(R48C6:R49C6)"
Else
    .Range("F61").Select
    ActiveCell.Font.Bold = True
    ActiveCell.Font.ThemeColor = xlThemeColorLight2
    Selection.NumberFormat = "0.000000000"
    ActiveCell.Formula = "=SUM(R48C6:R49C6)"
End If

.Range("G31").Select
ActiveCell.Formula = "=R[1]C-R[-23]C[-5]"
.Range("G32").Select
'ActiveCell.Formula = "=MATCH(VLOOKUP(R1C4,'Security Breaches'!R1C2:R1000C16,14,FALSE),'Russell 3000 Index'!R2C1:R10000C1,0)"
ActiveCell.Formula = "=MATCH(DateValue(""" & Event_Date_MinusTwo & """),'Russell 3000 Index'!R2C1:R10000C1,0) + 1"

.Range("I30").Select
ActiveCell.Font.Bold = True
Selection.NumberFormat = "0.00000%"
ActiveCell.Formula = "=AVERAGE(R[1]C:OFFSET(R[1]C,R8C2-1,0))"
.Range("J30").Select
ActiveCell.Font.Bold = True
Selection.NumberFormat = "0.000000%"
ActiveCell.Formula = "=SUM(R[1]C:OFFSET(R[1]C,R8C2-1,0))"

For i = 0 To 200
    .Range("H" & (31 + i)).Select
    ActiveCell.Formula = i
    .Range("I" & (31 + i)).Select
    Selection.NumberFormat = "0.000000000%"
    ActiveCell.Formula = "=OFFSET(Russell_3000_Index[[#Headers],[Date]],R32C7-R8C2+RC[-1],4)"
    Selection.NumberFormat = "0.000000000%"
    .Range("J" & (31 + i)).Select
    ActiveCell.Formula = "=(RC[-1]-R30C9)^2"
Next i
```

```
        'Set numeric formats on various cells
        .Range("D12").Select
        Selection.NumberFormat = "0.000000000"
        .Range("G17").Select
        Selection.NumberFormat = "0.000000000"
        .Range("I17").Select
        Selection.NumberFormat = "0.000000000"

        'Auto fit entire worksheet
        ActiveSheet.Columns("A:P").EntireColumn.AutoFit

        .ChartObjects("Chart 1").Activate
        .ChartObjects("Chart 1").Activate
        .Shapes("Chart 1").ScaleWidth 1.2145833333, msoFalse, msoScaleFromTopLeft
        .Shapes("Chart 1").ScaleHeight 1.3374485597, msoFalse, msoScaleFromTopLeft

        If Perform3FactorRegression = True Then
          .ChartObjects("Chart 2").Activate
          .ChartObjects("Chart 2").Activate
          .Shapes("Chart 2").ScaleWidth 1.2145833333, msoFalse, msoScaleFromTopLeft
          .Shapes("Chart 2").ScaleHeight 1.3374485597, msoFalse, msoScaleFromTopLeft

          .ChartObjects("Chart 3").Activate
          .ChartObjects("Chart 3").Activate
          .Shapes("Chart 3").ScaleWidth 1.2145833333, msoFalse, msoScaleFromTopLeft
          .Shapes("Chart 3").ScaleHeight 1.3374485597, msoFalse, msoScaleFromTopLeft

          ActiveChart.ChartArea.Select
          ActiveSheet.Shapes("Chart 3").IncrementLeft 18
          ActiveSheet.Shapes("Chart 3").IncrementTop 169.5

          ActiveChart.ChartArea.Select
          ActiveSheet.Shapes("Chart 2").IncrementLeft 314.25
          ActiveSheet.Shapes("Chart 2").IncrementTop 2.25

          ActiveSheet.ChartObjects("Chart 3").Activate
          ActiveSheet.Shapes("Chart 3").IncrementLeft -18
          ActiveSheet.Shapes("Chart 3").IncrementTop -21
          ActiveSheet.Shapes("Chart 3").ScaleWidth 1.0506003431, msoFalse, msoScaleFromTopLeft

          ActiveSheet.Shapes.Range(Array("Chart 1", "Chart 3")).Select
          Selection.ShapeRange.Align msoAlignLefts, msoFalse

          ActiveSheet.Shapes.Range(Array("Chart 2", "Chart 1")).Select
          Selection.ShapeRange.Align msoAlignTops, msoFalse
        End If
      End With

      If Worksheets("Security Breaches").Cells(nrow, 13).Value = "YES" Then
        Worksheets("Security Breaches").Cells(nrow, 1).Value = "Done"
      End If

      DoEvents

    My_Error:
      If Err.Number <> 0 Then
        MsgBox " Πρόβλημα στην εκτέλεση της ανάλυσης για την εταιρία: " & CompanyName & vbCrLf & Err.Description, vbCritical
        Application.ScreenUpdating = True
        On Error Resume Next
```

```
        End If
End_Loop:
    Next nrow

    If CompaniesProccessed = 0 Then
        MsgBox "Δεν βρέθηκαν εταιρίες με τα συγκεκριμένα κριτήρια.", vbInformation
        ActiveWorkbook.Sheets("Results").Select
        Exit Sub
    End If

    'Update Results worksheet
    With ActiveWorkbook.Sheets("Results")
        .Select

        'Set titles
       .Range("B1").Select
        ActiveCell.Font.Bold = True
        ActiveCell.Formula = "Hypothesis 1"
       .Range("C1").Select
        ActiveCell.Font.Bold = True
        ActiveCell.Formula = "Event window [-1,1]"
        .Range("B2").Select
        ActiveCell.Formula = "CAR"
        .Range("B3").Select
        ActiveCell.Formula = "Event window Residual Var"
        .Range("B4").Select
        ActiveCell.Formula = "t statistic"
        .Range("B5").Select
        ActiveCell.Formula = "Average CSAR"
        .Range("B6").Select
        ActiveCell.Formula = "z statistic"


       .Range("B8").Select
        ActiveCell.Font.Bold = True
        ActiveCell.Formula = "Hypothesis 1"
       .Range("C8").Select
        ActiveCell.Font.Bold = True
        ActiveCell.Formula = "Event window [0,0]"
        .Range("B9").Select
        ActiveCell.Formula = "CAR"
        .Range("B10").Select
        ActiveCell.Formula = "Event window Residual Var"
        .Range("B11").Select
        ActiveCell.Formula = "t statistic"
        .Range("B12").Select
        ActiveCell.Formula = "Average CSAR"
        .Range("B13").Select
        ActiveCell.Formula = "z statistic"

       .Range("B15").Select
        ActiveCell.Font.Bold = True
        ActiveCell.Formula = "Hypothesis 1"
       .Range("C15").Select
        ActiveCell.Font.Bold = True
        ActiveCell.Formula = "Event window [0,1]"
        .Range("B16").Select
        ActiveCell.Formula = "CAR"
        .Range("B17").Select
```

```
ActiveCell.Formula = "Event window Residual Var"
.Range("B18").Select
ActiveCell.Formula = "t statistic"
.Range("B19").Select
ActiveCell.Formula = "Average CSAR"
.Range("B20").Select
ActiveCell.Formula = "z statistic"

.Range("B26").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "Hypothesis 1"
.Range("C26").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "Event window [-1,0]"
.Range("B27").Select
ActiveCell.Formula = "CAR"
.Range("B28").Select
ActiveCell.Formula = "Event window Residual Var"
.Range("B29").Select
ActiveCell.Formula = "t statistic"
.Range("B30").Select
ActiveCell.Formula = "Average CSAR"
.Range("B31").Select
ActiveCell.Formula = "z statistic"

.Range("B33").Select
ActiveCell.Font.Bold = True
ActiveCell.Formula = "Number of events"

.Range("C5").Select
ActiveCell.Font.Bold = True
ActiveCell.Font.ThemeColor = xlThemeColorLight2
ActiveCell.Formula = "Total Regression Sheets"

'Reset initial values
.Range("C33").Select
Selection.NumberFormat = "0"
ActiveCell.Formula = 0
.Range("D33").Select
Selection.NumberFormat = "0"
ActiveCell.Formula = 0
.Range("E33").Select
Selection.NumberFormat = "0"
ActiveCell.Formula = 0

'Set values
.Range("C2").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R46C6)"
.Range("C3").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & TotalCarFormula & "!R47C6)"
.Range("C4").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=R2C3/SQRT(R3C3)"
.Range("C5").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R54C6)"
.Range("C6").Select
```

```
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=SQRT(R33C3)*R5C3"

.Range("C9").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R44C6)"
.Range("C10").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & TotalCarFormula & "!R49C6)"
.Range("C11").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=R9C3/SQRT(R10C3)"
.Range("C12").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R52C6)"
.Range("C13").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=SQRT(R33C3)*R12C3"

.Range("C16").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R57C6)"
.Range("C17").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & TotalCarFormula & "!R56C6)"
.Range("C18").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=R16C3/SQRT(R17C3)"
.Range("C19").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R58C6)"
.Range("C20").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=SQRT(R33C3)*R19C3"

.Range("C27").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R59C6)"
.Range("C28").Select
Selection.NumberFormat = "0.000000000"
If Perform3FactorRegression = True Then
   ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & TotalCarFormula & "!R70C6)"
Else
   ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & TotalCarFormula & "!R61C6)"
End If
.Range("C29").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=R27C3/SQRT(R28C3)"
.Range("C30").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=AVERAGE(" & TotalCarFormula & "!R60C6)"
.Range("C31").Select
Selection.NumberFormat = "0.000000000"
ActiveCell.FormulaR1C1 = "=SQRT(R33C3)*R30C3"
.Range("C33").Select
Selection.NumberFormat = "0"
ActiveCell.Formula = CompaniesProccessed
.Range("I2").Select
Selection.NumberFormat = "0"
```

```
ActiveCell.Formula = "=AVERAGE(" & TotalCarFormula & "!R8C2)"
.Range("N2").Select
Selection.NumberFormat = "0"
ActiveCell.Formula = "=AVERAGE(" & TotalCarFormula & "!R8C2)"

'TECHNOLOGY EVENTS
If Len(Technology) > 0 Then
   .Range("D2").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R46C6") & ")"
   .Range("D3").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=(1/R33C4^2)*SUM(" & CreateFormula(Technology, "!R47C6") & ")"
   .Range("D4").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=R2C4/SQRT(R3C4)"
   .Range("D5").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R54C6") & ")"
   .Range("D6").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=SQRT(R33C4)*R5C4"

   .Range("D9").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R44C6") & ")"
   .Range("D10").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=(1/R33C4^2)*SUM(" & CreateFormula(Technology, "!R49C6") & ")"
   .Range("D11").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=R9C4/SQRT(R10C4)"
   .Range("D12").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R52C6") & ")"
   .Range("D13").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=SQRT(R33C4)*R12C4"

   .Range("D16").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R57C6") & ")"
   .Range("D17").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=(1/R33C4^2)*SUM(" & CreateFormula(Technology, "!R56C6") & ")"
   .Range("D18").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=R16C4/SQRT(R17C4)"
   .Range("D19").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R58C6") & ")"
   .Range("D20").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=SQRT(R33C4)*R19C4"

   .Range("D27").Select
   Selection.NumberFormat = "0.000000000"
   ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R59C6") & ")"
   .Range("D28").Select
```

```
    Selection.NumberFormat = "0.000000000"
    If Perform3FactorRegression = True Then
        ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & CreateFormula(Technology, "!R70C6") & ")"
    Else
        ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & CreateFormula(Technology, "!R61C6") & ")"
    End If
    .Range("D29").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=R27C4/SQRT(R28C4)"
    .Range("D30").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Technology, "!R60C6") & ")"
    .Range("D31").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=SQRT(R33C4)*R30C4"
    .Range("D33").Select
    Selection.NumberFormat = "0"
    ActiveCell.Formula = TechnologyProcessed
    .Range("J2").Select
    Selection.NumberFormat = "0"
    ActiveCell.Formula = "=AVERAGE(" & CreateFormula(Technology, "!R8C2") & ")"
    .Range("O2").Select
    Selection.NumberFormat = "0"
    ActiveCell.Formula = "=AVERAGE(" & CreateFormula(Technology, "!R8C2") & ")"
End If


'REST EVENTS
If Len(Rest) > 0 Then
    .Range("E2").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R46C6") & ")"
    .Range("E3").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=(1/R33C5^2)*SUM(" & CreateFormula(Rest, "!R47C6") & ")"
    .Range("E4").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=R2C5/SQRT(R3C5)"
    .Range("E5").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R54C6") & ")"
    .Range("E6").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=SQRT(R33C5)*R5C5"

    .Range("E9").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R44C6") & ")"
    .Range("E10").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=(1/R33C5^2)*SUM(" & CreateFormula(Rest, "!R49C6") & ")"
    .Range("E11").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=R9C5/SQRT(R10C5)"
    .Range("E12").Select
    Selection.NumberFormat = "0.000000000"
    ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R52C6") & ")"
    .Range("E13").Select
    Selection.NumberFormat = "0.000000000"
```

```
        ActiveCell.FormulaR1C1 = "=SQRT(R33C5)*R12C5"

        .Range("E16").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R57C6") & ")"
        .Range("E17").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=(1/R33C5^2)*SUM(" & CreateFormula(Rest, "!R56C6") & ")"
        .Range("E18").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=R16C5/SQRT(R17C5)"
        .Range("E19").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R58C6") & ")"
        .Range("E20").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=SQRT(R33C5)*R19C5"
        .Range("E27").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R59C6") & ")"
        .Range("E28").Select
        Selection.NumberFormat = "0.000000000"
        If Perform3FactorRegression = True Then
            ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & CreateFormula(Rest, "!R70C6") & ")"
        Else
            ActiveCell.FormulaR1C1 = "=(1/R33C3^2)*SUM(" & CreateFormula(Rest, "!R61C6") & ")"
        End If
        .Range("E29").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=R27C5/SQRT(R28C5)"
        .Range("E30").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=AVERAGE(" & CreateFormula(Rest, "!R60C6") & ")"
        .Range("E31").Select
        Selection.NumberFormat = "0.000000000"
        ActiveCell.FormulaR1C1 = "=SQRT(R33C5)*R30C5"
        .Range("E33").Select
        Selection.NumberFormat = "0"
        ActiveCell.Formula = CompaniesProccessed - TechnologyProcessed
        .Range("K2").Select
        Selection.NumberFormat = "0"
        ActiveCell.Formula = "=AVERAGE(" & CreateFormula(Rest, "!R8C2") & ")"
        .Range("P2").Select
        Selection.NumberFormat = "0"
        ActiveCell.Formula = "=AVERAGE(" & CreateFormula(Rest, "!R8C2") & ")"
    End If

    'Auto fit entire worksheet
    .Columns("A:X").EntireColumn.AutoFit
  End With

  Application.ScreenUpdating = True

  MsgBox "Η διαδικασία τελείωσε επιτυχώς αφού επεξεργάστηκε " & CompaniesProccessed & " εταιρίες.", vbInformation
End Sub


Function CreateFormula(InputString As String, InputFormula As String) As String
  CreateFormula = InputString & InputFormula
```

```
  'For k = 0 To UBound(Split(InputString, "@")) - 1
  '    If Split(InputString, "@")(k) <> "" Then
  '        CreateFormula = CreateFormula & """ & Split(InputString, "@")(k) & """ & InputFormula & ","
  '    End If
  'Next k

  'CreateFormula = IIf(Len(InputString) = 0, 0, Left(CreateFormula, Len(CreateFormula) - 1))
End Function
```

V Αποτελέσματα ανάλυσης του μεγέθους γεγονότος με την χρήση του CAPM

Στο συγκεκριμένο παράρτημα παραθέτονται τα αποτελέσματα ανάλυσης του δείγματος γεγονότων παραβιάσεων ασφαλείας με κριτήριο το μέγεθος περιστατικού με την χρήση του CAPM. Κάθε Πίνακας αφορά τα στατιστικά αποτελέσματα για κάθε υπό-δείγμα όπως αυτά καθορίστηκαν στην ανάλυση της συγκεκριμένης υπόθεσης στην ενότητα 5.7.3.

Πίνακας 28: CAPM - Ανάλυση συνολικού δείγματος περιστατικών προσβολής μέχρι 100.000 εγγραφών

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	48	0,0067	0,9022	0,8157
[-1,0]	48	0,0013	0,3245	0,6270
[0,0]	48	0,0014	0,5151	0,6963
[0,1]	48	0,0069	1,1448	0,8728

Πίνακας 29: CAPM - Ανάλυση συνολικού δείγματος περιστατικών προσβολής 100.000 - 1.000.000 εγγραφών

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	13	0,0031	0,1579	0,5626
[-1,0]	13	0,0077	0,6251	0,7335
[0,0]	13	0,0030	0,5605	0,7120
[0,1]	13	-0,0016	-0,0353	0,4859

Πίνακας 30: CAPM - Ανάλυση συνολικού δείγματος περιστατικών προσβολής άνω των 1.000.000 εγγραφών

Παράθυρο ανάλυσης	Μέγεθος δείγματος	Mean CAR	t statistic	P-value
[-1,1]	17	0,0020	0,5434	0,7062
[-1,0]	17	0,0020	0,5881	0,7213
[0,0]	17	0,0012	0,3298	0,6290
[0,1]	17	0,0012	0,3106	0,6217

VI Βιβλιογραφία

[1] Netcraft. (2012, June) [Online]. http://news.netcraft.com/archives/2012/

[2] Pingdom Blog. (2011, January) [Online]. http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

[3] Robert N. Charette, "Why software fails," *IEEE Spectrum*, 2006.

[4] Detica, "The cost of cyber crime," 2011.

[5] Mark Gerencser and DeAnne Aguirre, "Security concerns prominent on CEO agenda," 2002.

[6] Ernst & Young, "Into the cloud, out of the fog," Global information security survey 2011.

[7] PriceWaterHouseCoopers, "Information security breaches survey," Technical report 2012.

[8] PriceWaterHouseCoopers, "Information security breaches survey," Technical report 2010.

[9] K. D. Loch, H. H. Carr, and M. E. Warkentin, "Threats to information systems: today's reality, yesterday's understanding," vol. 16, no. 2, 1992.

[10] Richardson, Robert, "CSI Computer crime and security survey," Computer Security Insitute, Survey report 2010.

[11] Ponemon Institute, "Five countries: Cost of data breach," 2010.

[12] The Economist. (2010, July) Cyberwar: War in the fifth domain. [Online]. http://www.economist.com/node/16478792/print

[13] Verizon, "2011 Data breach investigations report," 2011.

[14] Michael Riley and John Walcott. (2011, Dec.) China-Based hacking of 760 companies shows cyber cold war. Bloomberg.

[15] McAfee, "Global Energy Cyberattacks: Night Dragon," White paper 2011.

[16] BBC. (2009, Mar.) Major cyber spy network uncovered.

[17] Shishir Nagaraja and Ross Anderson, "The snooping dragon: Social-malware surveillance of the Tibetan movement," University of Cambridge, Technical report 2009.

[18] Ariana Eunjung Cha and Ellen Nakashima. (2010, Jan.) Google China cyberattack part of vast espionage campaign, experts say. Washington Post.

[19] Kathrin Hille. (2010) Chinese media hit at 'White House's Google'. The Financial Times.

[20] Dmitri Alperovitch, "Revealed: Operation shady RAT," McAffe, White paper 2011.

[21] Holton H. A., "Defining risk," *Financial Analysts Journal*, vol. 60, no. 6, pp. 19-25, 2004.

[22] Philippe Jorion, *Value at Risk*, 2nd ed.: McGraw-Hill International Edition, 2002.

[23] British Bankers' Association, *Operational risk: The next frontier*.: The Risk Management Association, 1999.

[24] Rob Jameson, "Operational risk: Playing the name game," *Risk*, pp. 38-42, October 1998.

[25] Rob Jameson, "Operational risk: Getting the measure of the beast," *Risk*, pp. 38-41, November 1998.

[26] Basel Committee on Banking Supervision, "Other risks discussion paper," Risk Management Group, BS/00/27, 2000.

[27] Ponemon Institute, "2011 Cost of data breach study United States," Benchmark research 2011.

[28] Fred H. Cate, "Information security breaches, looking back and thinking ahead," The Centre for Information Policy Leadership, 2008.

[29] L. Willcocks, "Evaluating information technology investments: research findings and appraisal.," vol. 2, no. 3, pp. 1-26, 1992.

[30] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk management guide for information technology systems," NIST, 2001.

[31] Γ. Πάγκαλος and I. Μαυρίδης, *Ασφάλεια πληροφορικών συστημάτων και δικτύων*.: Ανικούλα, 2002.

[32] Jake Kouns and Daniel Minoli, *Information technology risk management in enterprise environments*.: John Wiley and sons Inc, 2010.

[33] Peter Tippett, "The future of information security," in *Computer Security Handbook*.: John Wiley & Sons, Inc, 2002.

[34] G. Dhillon and J. Backhouse, "Risks in the use of information technology within organizations," *International Journal of Information Management*, vol. 16, no. 1, pp. 65-74, 1996.

[35] L. Willcocks and H. Margetts, "Risk assessment and information systems," *European Journal of Information Systems*, 1994.

[36] E. E. Brown, D. S. Longstaff, and L. T. Schultz, "Responding to computer security incidents.," *Lawrence Livemore National Laboratory*, July 1990.

[37] National Vulnerability Database. [Online]. http://ndv.gov/

[38] P. Mell, K. Scarfone, and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," 2007.

[39] Forum of Incident Reports and Security Teams. [Online]. http://www.first.org/cvss

[40] Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, and Gregory Chondrokoukis, "The role of weighted entropy in security quantification," *IEEE International Conference on Information Security and Artificial Inteligence (ISAI 2010)*, Dec. 2010. Accepted for publication on the International Journal of Information and Electronics Engineering.

[41] H. O. Alhazmi, S. W. Woo, and Y. K. Malaiya, "Security vulnerability categories in major software systems".

[42] I.S. Gottfried, "When disaster strikes," *Journal of Information Systems Management*, pp. 86-90, 1989.

[43] H. H. Rainer, R. K. Snyder, and C. A. Carr, "Risk analysis for information technology," *Journal of Management Information Systems*, vol. 8, no. 1, pp. 129-147, 1991.

[44] David G.W. Birch and Neil A. McEvoy, "Risk analysis for information systems," *Journal of Information Technology*, vol. 7, pp. 44-53, 1992.

[45] Ravindranath Pandian, *Applied software risk management*., 2007.

[46] B. W. Boehm, "Software risk management: Principles and practices," *IEEE Software*, vol. 8, no. 1, January 1991.

[47] NIST, "Managing information security risk," Special Publication 800-39, 2011.

[48] IT Governance Institute, "COBIT 4.1," 2007.

[49] ISACA, "The Risk IT framework," 2009.

[50] Kakoli Bandyopadhyay, Peter P. Mykytyn, and Kathleen Mykytyn, "A framework for integrated risk

management in information technology," *Journal of Management Decision*, vol. 37, no. 5, 1999.

[51] C. Corder, *Taming your company computer*.: McGraw-Hill, 1989.

[52] COSO, "Enterprise Risk Management - Integrated framework," Executive summary framework 2004.

[53] Australian Government - Office of the Privacy Commissioner, "Guide to handling personal information security breaches," 2008.

[54] Ernst & Young, "Borderless security," Global information security survey 2010.

[55] Ponemon Institute, "2010 Annual study: U.S. Cost of a data breach," Benchmark study of companies 2010.

[56] Robert Richardson, "CSI Computer crime and security survey," Computer Security Institute, Survey report 2008.

[57] Robert Richardson, "CSI Computer crime and security survey," Computer Security Institute, Survey report 2009.

[58] Ponemon Institute, "Fourth annual US cost of data breach study," Ponemon Institute, Benchmark study of companies 2008.

[59] Ponemon Institute, "2009 Annual study: Cost of a data breach," Benchmark study of companies 2009.

[60] Verizon, "2010 Data breach investigations report," 2010.

[61] Verizon, "2012 Data breach investigations report," 2012.

[62] Verizon, "Verizon enterprise risk and incident sharing metrics framework: The Veris Framework," White paper 2012.

[63] Open Security Foundation. DatalossDB. [Online]. http://datalossdb.org

[64] Identity Theft Report Center. [Online]. http://www.idtheftcenter.org

[65] Privacy Rights Clearinghouse. [Online]. http://www.privacyrights.org/

[66] IdentityTheft. [Online]. http://www.identitytheft.info

[67] Office of Inadequate Security. Databreaches.net. [Online]. http://www.databreaches.net

[68] BANKinfoSECURITY. [Online]. http://www.bankinfosecurity.com

[69] Information security media group. DataBreachToday. [Online]. http://www.databreachtoday.com

[70] B. L. Dos Santos, K. Peffers, and D. Mauer, "The impact of information technology investment announcements on the market value of the firm," *Information systems research*, pp. 1-23, 1993.

[71] Claudio F. Loderer and David C. Mauer, "Corporate dividends and seasoned equity issues:An empirical investigation," *Journal of Finance*, vol. 47, no. 1, pp. 201-225, March 1992.

[72] M. Ettredge and V. J. Richardson, "Assessing the risk in e-commerce," in *Proceedings of the thirty-fifth Hawaii international conference on system sciences*, Los Alamitos, 2001.

[73] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," *Journal of computer security*, vol. 11, pp. 431-448, 2003.

[74] Anat Hovav and John D'Arcy, "The impact of denial-of-service attack announcements on the market value of firms," *Risk Management and Insurance Review*, vol. 6, no. 2, pp. 97-121, 2003.

[75] Anat Hovav and John D'Arcy, "The impact of virus attack announcements on the market value of firms," *Information Systems Security*, vol. 13, no. 3, pp. 32-40, 2004.

[76] A. Briney, "Got security?," *Information Security*, July 1999.

[77] Ali Alper Yayla and Qing Hu, "The impact of information security events on the stock value of firms: The effect of contigency factors," *Journal of Information Technology*, vol. 26, pp. 60-77, 2011.

[78] Ashish Garg, Jeffrey Curtis, and Hilary Halper, "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security*, vol. 11, no. 2, pp. 74-83, 2003.

[79] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, pp. 69-104, Fall 2004.

[80] Nishant Patel, "The Effect of IT Hack Announcements on the Market Value of public traded corporations," April 2010.

[81] Kevin M. Gatzlaff and Kathleen A. McCullough, "The effect of data breaches on shareholder wealth," *Risk Management and Insurance Review*, vol. 13, no. 1, pp. 61-83, 2010.

[82] Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, "The impact of information security breaches: Has

there been a downward shift in costs?," *Journal of Computer Security*, vol. 19, pp. 33-56, 2011.

[83] Eugene F. Fama, "Efficient capital markets: II," *The Journal of Finance*, vol. 46, no. 5, pp. 1575-1617, 1991.

[84] Eugene F. Fama, "Efficient capital markets: A review of theory and empirical work," *Journal of Finance*, vol. 25, no. 2, pp. 384-417, May 1970.

[85] K. S. Im, K. E. Dow, and V. Grover, "A reexamination of IT investment and the market value of the firm - An event study methodology," *Information systems research*, vol. 12, no. 1, pp. 103-117, March 2001.

[86] Mark P. Kritzman, "What practitioners need to know about event studies," *Financial Analysts Journal*, vol. 50, pp. 17-20, 1994.

[87] William F. Sharpe, "Capital asset prices: A theory of market equilibrium under conditions of risk," *Journal of Finance*, vol. 19, no. 3, pp. 425-442, September 1964.

[88] Eugene F Fama and Kenneth R French, "The cross-section of expected stock returns," *Journal of Finance*, vol. 47, no. 2, pp. 427-465, June 1992.

[89] Eugene F Fama and Kenneth R French, "Common risk factors in the returns of stocks and bonds," *Journal of Financial Economics*, vol. 33, pp. 3-56, 1993.

[90] Eugene F Fama and Kenneth R French, "Multifactor explanations of asset pricing anomalies," *Journal of Finance*, vol. 51, no. 1, pp. 55-84, March 1996.

[91] Kenneth R. French. Official site. [Online]. http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/index.html

[92] James M. Patell, "Corporate forecasts of earnings per share and stock price behavior:Empirical test," *Journal of Accounting Research*, vol. 14, no. 2, pp. 246-276, 1976.

[93] M. Subramani and E. Walden, "The impact of e-commerce announcement on the market value of firms," *Information systems research*, vol. 12, no. 2, pp. 135-154, June 2001.

[94] KPMG, "Cyber crime - A growing challenge for governments," 2011.

[95] John M Griffin, "Are the Fama and French factors global or country specific?," *The Review of Financial Studies*, vol. 15, no. 3, pp. 783-803, 2002.

[96] Stephen J. Brown and Jerold B. Warner, "Using daily stock returns: The case of event studies," *Journal*

of Financial Economics, vol. 14, pp. 3-31, 1985.

[97] Fred H. Cate, "The identity theft scare," *The Wansighton Post*, Oct. 2006.

[98] Joseph Gross, "Operation Shady rat — Unprecedented Cyber-espionage Campaign and Intellectual Property Bonanza," CNET, 8/2/2011.

[99] Steven Musil. (2012, January) Symantec says source code stolen in 2006 hack. CNET. [Online]. http://news.cnet.com/8301-1009_3-57360662-83/symantec-says-source-code-stolen-in-2006-hack/

[100] National Conference of State Legislatures. [Online]. http://www.ncsl.org/issues-research/telecom/security-breach-legislation-2010.aspx

[101] D. McCullagh. (10/13/2011) SEC Orders discolosure of 'potential' security breaches. CNET.

[102] Open Source Vulnerability Database. [Online]. http://osvdb.org/

[103] United States Computer Emergency Readiness Team (US-CERT). [Online]. http://www.us-cert.gov/

[104] Nikolaos Alexandris, Evangelos Fountas, Dimitrios Mermigas, and Sotirios Pirounias, "Using time patterns to verify the utilization of stochastic calculus in security quantification," *IEEE International Conference on Information Security and Artificial Inteligence (ISAI 2010)*, Dec. 2010. Accepted for publication on the International Journal of Information and Electronics Engineering.

[105] S. Frei, M. May, U. Fiedler, and B. Plattner, "Large-scale vulnerability analysis," *Computer engineering and networks labaratory*.

[106] H. O. Alhazmi, K. Y. Malaiya, and I. Ray, "Vulnerabilities in major operating systems," Colorado State University, 2004.

[107] J. Homer, X. Ou, and D. Schmidt, "A sound and practical approach to quantifying security risk in enterprise networks,".

[108] S. Christey and A. R. Martin, "Vulnerability type distributions in CVE," Mitre corporation,.

[109] LISA technical program, "A machine-oriented integrated vulnerability database for automated vulnerability detection and processing," in *LISA '04: Eighteenth systems administration conference*, 2004, pp. 47-58.

[110] State of Hawai, "Risk and vulnerability assessment," Multi hazard mitigation plan 2007.

[111] W. Jansen, "Directions in security metrics research," National Institute of Standards and Technology,

Interagency report 2009.

[112] Constantinos Patsakis, Dimitrios Mermigas, Sotirios Pirounias, Nikolaos Alexandris, and Evangelos Fountas, "Towards a formalistic measuring of security using stochastic calculus," in *2010 3rd IEEE International conference on computer science and information technology*, 2010.

[113] C. E. Shannon, *A mathematical theory of communication*.: Bell Syst. Tech. J., 1948.

[114] StatOwl. (2012, June) [Online]. http://www.statowl.com/index.php

[115] Statcounter GlobalStats. (2012, June) [Online]. http://gs.statcounter.com/

[116] Lawrence A. Gordon and Martin P. Loeb, "The economics of information security investment," in *ACM Transactions on Information and System Security*, 2002, pp. 438-457.

[117] Jan Willemson, "Extending the Gordon & Loeb model for information security investment," in *2010 International Conference on Availability, Reliability and Security*, 2010.

[118] Dimitrios Mermigas, Sotirios Pirounias, and Nikolaos Alexandris, "A probabilistic method for quantification of corporate losses due to security breaches," in *International Congress on Mathematics MICOM*, 2012.

[119] Jeevan Jaisingh and Jackie Rees, "Value at Risk: A methodology for Information Security Risk Assessment," 2000.

[120] Rolf Hulthen, "Communicating the economic value of security investments: Value at Security Risk," *Managing information risk and the economics of security*, 2009.

[121] Constantinos Patsakis and Dimitrios Mermigas. (2012) Sqt Project. http://sourceforge.net/projects/sqt.

[122] "UK seeks global accord on cyber threat," *FT.com*, Feb. 2011.

[123] "Global cybercrime treaty rejected at U.N.," *SC magazine*, April 2010.