ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΛΟΓΙΣΤΙΚΗ ΦΟΡΟΛΟΓΙΑ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ (ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΣΤΡΑΤΗΓΙΚΗ ΔΙΟΙΚΗΤΙΚΗ ΛΟΓΙΣΤΙΚΗ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΓΙΑ ΣΤΕΛΕΧΗ ΕΠΙΧΕΙΡΗΣΕΩΝ)

Διπλωματική Εργασία

ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΧΩΡΟΥ ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ

ΠΑΝΑΓΙΩΤΗΣ ΣΤΡΑΚΑΛΗΣ

Επιβλέπων Καθηγητής: ΕΥΣΤΡΑΤΙΟΣ ΛΙΒΑΝΗΣ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος στη Λογιστική Φορολογία και Χρηματοοικονομική Διοίκηση (Πρόγραμμα Μεταπτυχιακών Σπουδών στη Στρατηγική Διοικητική Λογιστική και Χρηματοοικονομική Διοίκηση για Στελέχη Επιχειρήσεων)

Θεσσαλονίκη 2019

Στους γονείς μου,

Νικόλαο και Αναστασία

και σε κάθε πολυμήχανο Κανένα.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον Θεό που με ευλόγησε να βρίσκομαι σε αυτή τη θέση σήμερα. Δεν θα κατάφερνα τίποτα χωρίς τη βοήθεια Του.

Θα ήθελα να ευχαριστήσω την οικογένειά μου,για την ολόψυχη αγάπη και υποστήριξη που μου προσέφεραν και σε αυτό το ταξίδι. Επιπλέον να ζητήσω ένα μεγάλο συγγνώμη για την ταλαιπωρία τους όλο αυτό το χρονικό διάστημα.

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου,Ευστράτιο Λιβάνη,που πίστεψε σε εμένα από την πρώτη στιγμή. Μου προσέφερε τα ερεθίσματα ώστε να πραγματοποιήσω αυτή την διπλωματική εργασία καθώς και την αμέριστη συμπαράστασή του όλο το χρονικό διάστημα των μεταπτυχιακών σπουδών μου.

Τέλος θα ήθελα να ευχαριστήσω όλο το διδακτικό προσωπικό του Τμήματος Λογιστικής και Χρηματοοικονομικής. Μου παρείχαν τις κατάλληλες γνώσεις οι οποίες είναι απαραίτητες στην εξέλιξη μου και στην επαγγελματική μου σταδιοδρομία.

ΠΕΡΙΛΗΨΗ

Οι τεχνολογικές εξελίξεις σηματοδοτούσαν πάντοτε καθοριστικό παράγοντα αλλαγών στην πορεία της ανθρωπότητας με πολλαπλές επιδράσεις σε μία σειρά τομέων της κοινωνίας. Σε ένα κόσμο παγκόσμιας διασύνδεσης μέσω της εξέλιξης της επικοινωνίας και της τεχνολογίας θα μπορούσαμε να φανταστούμε τον κόσμο σαν ένα σύστημα αμέτρητων πληροφοριών ή μάλλον καλύτερα δεν μπορεί να το φανταστεί ο ανθρώπινος νους,λόγω του μεγέθους των πληροφοριών. Μέσα από την ενδελεχή εξέταση ορισμένων εκ των πιο καίριων ζητημάτων που αναδύονται αποσκοπούν σε μια ολιστική περιγραφή των ανωτέρω αυτών θεμάτων,όσο το δυνατόν καλύτερη. Η ανασκόπηση της παγκόσμιας βιβλιογραφίας εξυπηρετεί ακόμα περισσότερο τον στόχο της εργασίας δίνοντας την ευκαιρία στον αναγνώστη να αποκτήσει άποψη για τις σύγχρονες εξελίξεις και τους προβληματισμούς που ελλοχεύουν.

Σκοπός της παρούσας διπλωματικής εργασίας είναι η επισκόπηση των βασικών θεμάτων:

a) της ανάλυση των κινδύνων του Κυβερνοχώρου στη σημερινή εποχή
b) κυρίως από την χρηματοοικονομική τους πλευρά
c) καθώς και των στρατηγικών διαχείρισης τους.

Για τη σοβαρότητα των κινδύνων του Κυβερνοχώρου όσο και για τους τρόπους διαχείρισης και αντιμετώπισής των κινδύνων του Κυβερνοχώρου,κυρίως από τη σκοπιά των οικονομικών επιπτώσεων και προσδιορισμού του κόστους. Αρχικά με τον καθαρισμό της έννοιας του κινδύνου με την παράθεση των ποικίλων ορισμών. Έπειτα με τις διακρίσεις των κινδύνων αυτών και τη διαχείριση τους από τους υψηλόβαθμους διοικητικούς αξιωματούχους των εταιρειών,εστιάζοντας στην ανάλυση των κινδύνων και σε μία προσπάθεια παρουσίασης των μέτρων,των μεθοδολογιών και των διαδικασιών που προτείνονται από την παγκόσμια βιβλιογραφία. Η ανάλυση των κινδύνων του κυβερνοχώρου εστιάζεται και στον κίνδυνο που προκαλείται από τη χρήση των Πληροφοριακών Συστημάτων.

Το πιο πολυσυζητημένο θέμα καθημερινά είναι η παγκόσμια οικονομική κρίση και ερχόμαστε σε επαφή με τον διαδικτυακό κίνδυνο που αφορά την οικονομία,σύνολο πολλων παραγόντων. Καθημερινά διαβάζουμε άρθρα τετελεσμένων γεγονότων επιθέσεων και οικονομικών εγκλημάτων. Στην παρούσα εργασία αναλύθηκαν δεδομένα για το κόστος των τριών τελευταίων ετών σε όλους τους τομείς και τους λόγους απώλειας σημαντικών δεδομένων από τις εταιρείες. Παρουσιάστηκε εκτενώς η ανάλυση τους στο χρηματοοικονομικό τομέα που αποτελεί αυτόν με τα μεγαλύτερα κόστη,τα οποία αυξάνονται κάθε χρόνο.

Εξετάστηκαν λεπτομερώς οι κυριότερες στρατηγικές διαχείρισης του κινδύνου και των απειλών του Κυβερνοχώρου. Έγινε επιπλέον εκτενής αναφορά σε θέματα που σχετίζονται στην κατεύθυνση αυτή όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων,θέματα κυβερνοασφάλειας και κυβερνοασφάλισης.

Καταλήγοντας ο χρηματοοικονομικός τομέας και οι εταιρείες που ανήκουν σε αυτόν πρέπει να επενδύσουν περισσότερο στην οργάνωση των τμημάτων,την ενημέρωση των εργαζομένων και την αναβάθμιση των συστημάτων. Να διδαχθούν από παρελθοντικές επιθέσεις σε άλλες εταιρείες ώστε να γνωρίσουν τα ευάλωτα σημεία τους καθώς και τις αντιδράσεις των αγορών και των πελατών σε αυτές. Στο σημείο αυτό βοηθάει και η μελέτη περίπτωσης της εταιρείας Equifax Inc,πού αποτελεί ίσως και την μεγαλύτερη γνωστή και καταγεγραμμένη εταιρική κυβερνοεπίθεση στον χρηματοοικονομικό κλάδο και μία από τις μεγαλύτερες γενικά. Η εξέλιξη και ανάπτυξη έρχονται όταν μαθαίνουμε από τα λάθη του παρελθόντος και από τη δύναμη όσες φορές και να πέσεις να σηκωθείς άλλη μία.

ABSTRACT

Technological developments have always signaled the decisive factor in the evolution of humanity with multiple effects on a number of areas of society. In a world of global interconnectedness through the evolution of communication and technology,we could imagine the world as a system of innumerable information,or rather the human mind could not imagine it because of the sheer size of information. In-depth examination of some of the most important issues that arise seeks a comprehensive description of the above issues as best as possible. An overview of the world literature further serves the purpose of the paper by giving the reader an opportunity to get an idea of the current developments and concerns.

The purpose of this thesis is to provide an overview of the key issues:

(a) the analysis of cyber risks

(b) mainly from their economic point of view

(c) and their management strategies.

On the seriousness of the risks in the Cyberspace as well as on the methods of managing and responding,mainly in terms of economic impact and cost determination. First of all by clearing up the concept of risk by referring to the various definitions. Furthermore leadership focuses on risk analysis and an effort to present the measures,methods and procedures suggested by international literature. The analysis of cyber risks also focuses on the risk caused by the use of Information Systems.

The most debated topic on a daily basis is the global financial crisis and comes in contact with the online risk associated with the economy. We read articles of assault and financial crimes daily. This paper analyzed data on the costs of the last three years in all sectors and the reasons for the loss of significant assets by companies. Their analysis of the financial sector which accounts for the largest number of expenditure by cyber attacks and has been extensively every year.

The main strategies for managing risk and threats in cyberspace were examined in detail. There was also extensive reference to issues related to this direction, such as the General Data Protection Regulation (GDPR),issues of cyber security and cyber insurance.

The consumer of the financial sector and the companies belonging to it should invest more in organizing departments,informing employees and upgrading systems. Learn from past attacks on other companies to get to know their sensitive points as well as the reactions of their markets and customers. This point helps a case study of Equifax Inc.,which is perhaps

the largest known and registered corporate cyber attack in the financial sector and one of the largest generally. Evolution and development come when we learn from the mistakes and the power of rise again after every fall.

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΦΙΕΡΩΣΕΙΣ..... II

ΕΥΧΑΡΙΣΤΙΕΣ..... III

ΠΕΡΙΛΗΨΗ..... IV

ABSTRACT..... VI

ΠΕΡΙΕΧΟΜΕΝΑ..... VIII

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ..... X

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ..... X

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ..... XI

ΚΕΦΑΛΑΙΟ 1 ΕΙΣΑΓΩΓΗ..... 1

ΚΕΦΑΛΑΙΟ 2 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ..... 2

2.1 Κοινωνία της Πληροφορικής..... 2

2.2 Διαδίκτυο..... 4

2.3 Έννοια Κυβερνοχώρου..... 5

2.4 Κυβερνοεπιθέσεις και απειλές στον Κυβερνοχώρο..... 8

2.5 Μέρη-Στόχοι Κυβερνοεπιθέσεων..... 11

2.6 Σύνδεση επιχειρήσεων και Κυβερνοχώρου..... 16

2.7 Σκοπός εργασίας - Ερευνητικά ερωτήματα..... 17

ΚΕΦΑΛΑΙΟ 3 ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΧΩΡΟΥ..... 18

3.1 Έννοια Κινδύνου..... 18

3.2 Διακρίσεις του Κινδύνου (Cyber Risks)..... 20

3.3 Διαχείριση Κινδύνων Κυβερνοχώρου και η νέα πρόκληση για τους Διευθύνοντες Συμβούλους (CEO) και Οικονομικούς Διευθυντές (CFO)..... 24

3.4 Πληροφοριακά Συστήματα και οι Κινδυνοι τους..... 29

ΚΕΦΑΛΑΙΟ 4 ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ..... 34

4.1 Οικονομικός αντίκτυπος κινδύνων Κυβερνοχώρου..... 34

4.2 Προσδιορισμός του Κόστους.....35
4.3 Λόγοι που δεν επενδύονται ποσά στην προστασία κυβερνοαπειλής.....35
4.4 Διαχείριση Οικονομικών Επιπτώσεων..... 36
4.5 Κόστος χρήσης Ασφαλιστικών προϊόντων.....37
4.6 Οικονομικό έγκλημα.....41

ΚΕΦΑΛΑΙΟ 5 ΣΤΡΑΤΗΓΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ..... 44
5.1 Διαχείριση κινδύνου-Διαχείριση των απειλών του Κυβερνοχώρου.....44
5.2 Κύριες στρατηγικές διαχείρισης του Κινδύνου..... 44
5.3 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)..... 45
5.4 Κυβερνοασφάλεια (CyberSecurity).....48
5.5 Κυβερνοασφάλιση (Cyber Insurance)..... 53

ΚΕΦΑΛΑΙΟ 6 ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΣΤΟ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΟ ΤΟΜΕΑ ΚΑΙ ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ (CASE STUDY).....56
6.1 Κυβερνοεπιθέσεις και Χρηματοοικονομικός τομέας.....56
6.2 Μελέτη Περίπτωσης της εταιρείας Equifax Inc (EFX.N)..... 60

ΚΕΦΑΛΑΙΟ 7 ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ..... 66

ΒΙΒΛΙΟΓΡΑΦΙΑ.....69
ΒΙΒΛΙΑ.....69
ΑΡΘΡΑ.....70
ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ..... 74

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

- Πίνακας 1: Διαχρονικά η ιστορική εξέλιξη των υπολογιστικών μηχανών. (Πηγή: Κοινωνία της Πληροφορίας,Μ. Παρασκευάς,Γ. Ασημακόπουλος,Β. Τριανταφύλλου,Κάλλιπος,Εθνικό Μετσόβιο Πολυτεχνείο (2015))..... 2
- Πίνακας 2: Προσέγγιση εξέτασης της δομής του Κυβερνοχώρου. (Πηγή: Διδακτορική Διατριβή του Κ. Φυσεντζίδη,Η Σημασία της Ενσωμάτωσης του Κυβερνοχώρου στις Κοινωνικοχωρικές Δομές:Η Κυβερνόπολη (Πανεπιστήμιο Θεσσαλίας,Βόλος 2012) και Βασισμένο στην Trialectics) του Lefebvre στο βιβλίο του La Production de l'Espace (1974))..... 7
- Πίνακας 3: Προσέγγιση εξέτασης της δομής του Κυβερνοχώρου. (Πηγή: Ιδία επεξεργασία,βασισμένο σε κείμενο των James Cebula,Mary Popeck και Lisa Young,A Taxonomy of Operational Cyber Security Risks Version 2,(www.sei.cmu.edu) Carnegie Mellon University (2014))..... 22
- Πίνακας 4: Χρονοδιάγραμμα των γεγονότων που περιβάλλουν την παραβίαση Δεδομένων,αμέσως μετά την ανακοίνωση από την εταιρεία. (Πηγή: Ιδία επεξεργασία).. 63

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

- Εικόνα 1: Πυξίδα Κυβερνοχώρου. (Πηγή: Η Ασφαλής πλοήγηση στο διαδίκτυο είναι υπόθεση όλων μας,3ο Συνέδριο για την Ασφαλή Πλοήγηση στο Διαδίκτυο (2014))..... 21

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

- Διάγραμμα 1: Η εξέλιξη του πλήθους των δικτυωμένων συσκευών. (Πηγή: Κοινωνία της Πληροφορίας,Μ. Παρασκευάς,Γ. Ασημακόπουλος,Β. Τριανταφύλλου,Κάλλιπος,Εθνικό Μετσόβιο Πολυτεχνείο (2015))..... 3
- Διάγραμμα 2: Τα Τρία Μορφώματα του Κυβερνοχώρου. (Πηγή: Διδακτορική Διατριβή του Κ. Φυσεντζίδη,Η Σημασία της Ενσωμάτωσης του Κυβερνοχώρου στις Κοινωνικοχωρικές Δομές:Η Κυβερνόπολη (Πανεπιστήμιο Θεσσαλίας,Βόλος 2012) και Βασισμένο στην Trialectics) του Lefebvre στο βιβλίο του La Production de l'Espace (1974))..... 7
- Διάγραμμα 3: Κατηγορίες κυβερνοεπιθέσεων ανάλογα με την επιδίωξη. (Πηγή: Ιδια επεξεργασία (Βασισμένο στο άρθρο των M. Uma and G. Padmavathi,"A Survey on Various Cyber Attacks and Their Classification",International Journal of Network Security, Vol.15, No.5, PP.390-396, Sept. 2013))..... 9
- Διάγραμμα 4: Αιτίες επικινδυνότητας των κυβερνοεπιθέσεων. (Πηγή: Ιδια επεξεργασία, βασισμένο σε κείμενο και εικόνα του TAKING CONTROL OF CYBERSECURITY: A Practical Guide for Officers and Directors (Foley's Cybersecurity Team,Foley & Lardner LLP,Milwaukee Wisconsin USA 2015))..... 10
- Διάγραμμα 5: Τα κυριότερα μέρη στόχοι των κυβερνοεπιθέσεων τον Ιούνιο του 2019. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από www.hackmageddon.com)..... 13
- Διάγραμμα 6: Τα κυριότερα κράτη προέλευσης των κυβερνοεπιθέσεων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από https://blog.f-secure.com)..... 14
- Διάγραμμα 7: Τα κυριότερα κράτη προορισμού των κυβερνοεπιθέσεων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από https://blog.f-secure.com)..... 14
- Διάγραμμα 8: Τα κυριότερα κίνητρα κυβερνοεπιθέσεων κατά το 2018. (Πηγή:Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από www.hackmageddon.com).... 15
- Διάγραμμα 9: Ορισμός του Κινδύνου. (Πηγή: Ιδια επεξεργασία)..... 19
- Διάγραμμα 10: Η ταξινόμηση των κινδύνων του Κυβερνοχώρου αποτελούμενη από έξι θεμελιώδεις πυλώνες-αρχές. (Πηγή: Livanis, Efstratios, Financial Aspects of Cyber Risks and Taxonomy for the Efficient Handling of These Risks (May 2016). Economic and Social Development (Book of Proceedings),14th International Scientific Conference on Economic and Social Development, Belgrade, Serbia (2016))..... 23

- Διάγραμμα 11: Μια μεθοδολογία των ενεργειών διαχείρισης του κινδύνο. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στο BUSINESS RISK A practical guide for board members,willis,pwc,chartis,airmic p.35 ,www.iod.com).....24
- Διάγραμμα 12: Η AIM (Align,Integrate,Measure) προσέγγιση διαχείρισης στο πλαίσιο καθορισμού των παραγόντων διαχείρισης των κινδύνων του Κυβερνοχώρου. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση της Grant Thornton,Taking AIM at cyber risk (2018)).....28
- Διάγραμμα 13: Στάδια διαχείρισης των κινδύνων. (Πηγή: Ιδια επεξεργασία, βασισμένο σε διάγραμμα του Κηρυττόπουλου Κ.,Η διαχείριση κινδύνων έργων στην κατασκευαστική βιομηχανία (2006)).....28
- Διάγραμμα 14: Πληροφοριακό σύστημα. (Πηγή: Θεόδωρος Μητάκος,Πληροφοριακά Συστήματα Διοίκησης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015)).....29
- Διάγραμμα 15: Πληροφοριακό Σύστημα ως μοντέλο πέντε τμημάτων. (Πηγή: Θεόδωρος Μητάκος,Πληροφοριακά Συστήματα Διοίκησης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015)).....31
- Διάγραμμα 16: Μια ιεραρχία τεσσάρων επιπέδων των Πληροφοριακών Συστημάτων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στο άρθρο των Laudon, K.C. και Laudon, J.P. Management Information Systems, (2nd edition), Macmillan, 1988).....32
- Διάγραμμα 18: Η εξέλιξη των δαπανων της ευρωπαϊκής αγοράς κυβερνοασφάλισης σε εκατομμύρια ευρώ (EUR) άνα έτος (2012-2016). (Πηγή: www.advisenltd.com).....40
- Διάγραμμα 19: Η εκτιμώμενη αξία των ασφαλίστρων κυβερνοασφάλισης σε δισεκατομμύρια δολάρια (USD). (Πηγή: www.statista.com).....40
- Διάγραμμα 20: Προστασία των πληροφοριών σε διάφορα επίπεδα ασφαλείας. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε άρθρο των Popescu R. C.,Popescu G.,Risks of cyber attacks on financial audit activity,Audit Financiar, XVI, Nr. 1(149) p.140-147 (2018)).....50
- Διάγραμμα 21: Ετήσιες δαπάνες σε εκατομμύρια δολάρια (USD) στην κυβερνοασφάλεια και στην κυβερνοασφάλιση. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε άρθρο των Gartner,Munich Re,Global Cyber Risk Perception Survey 2019).....53
- Διάγραμμα 22: Η κατάσταση της επιχείρησής σας σε σχέση με την κυβερνοασφάλιση. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε έρευνα των Marsh και Microsoft,Global Cyber Risk Perception Survey 2019).....54

- Διάγραμμα 23: Κόστος ανά μονάδα κλεμμένου δεδομένου σε κάθε τομέα και διαφοροποίηση μεταξύ του μέσου όρου των τελευταίων 4 ετών και του 2017,σε δολάρια (USD). (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2017))..... 57
- Διάγραμμα 24: Κυριότερες αιτίες απώλειες δεδομένων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2019))..... 58
- Διάγραμμα 25: Παραβολική καμπύλη κόστους παραβίασης,σε δολάρια (USD). (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2018))..... 58
- Διάγραμμα 26: Αλληλεπίδραση μεταξύ του συνολικού αριθμού εργαζομένων και του συνολικού κόστους παραβίασης δεδομένων,σε εκατομμύρια δολάρια (USD). (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2018))..... 59
- Διάγραμμα 27: Χρονολογική σειρά παρουσίασης των κυριών περιστατικών της παραβιάσης. (Πηγή: Ιδια επεξεργασία, βασισμένο σε άρθρο των Ping Wang, Robert Morris,Christopher Johnson,Cybersecurity Incident Handling,Issues in Information Systems,Volume 19, Issue 3, pp. 150-159 (2018))..... 62
- Διάγραμμα 28: Η τιμή της μετοχής της Equifax τις πρώτες μέρες μετά τη δημοσίευση των συμβάντων παραβιάσεων δεδομένων. (Πηγή: www.finance.yahoo.com)..... 64
- Διάγραμμα 29: Η τιμή της μετοχής της Equifax από τη δημοσίευση των συμβάντων παραβιάσεων δεδομένων σε διάστημα δύο ετών. (Πηγή: Ιδια επεξεργασία βασισμένο σε άρθρο στο www.reuters.com)..... 64

ΚΕΦΑΛΑΙΟ 1 ΕΙΣΑΓΩΓΗ

Οι κοινωνίες αλλάζουν με το χρόνο και την εξέλιξη που επέρχεται άλλοτε αργά κι άλλοτε γρηγορότερα. Η σύγχρονη κοινωνία έχει αλλάξει ριζικά στον τρόπο λειτουργίας με σημαντικότερο λόγο τη χρήση νέων τεχνολογιών και την απελευθέρωσης των αγορών και του κεφαλαίου σε παγκόσμιο επίπεδο. Οι μορφές της ανθρώπινης δραστηριότητας έχουν επηρεαστεί από την υιοθέτηση νέων τεχνολογικών εργαλείων και μέσων που προσφέρονται και οδηγούν στην επέκταση της ανθρώπινης συμπεριφοράς με νέες μορφές διάδρασης. Η σύγχρονη τεχνολογική επανάσταση της εποχής έχουν επηρεάσει την συντριπτική πλειοψηφία των ατόμων και των οντοτήτων της κοινωνίας. Πολλοί από εμάς,κυρίως μεγαλύτερης ηλικίες,δεν είχα φανταστεί ποτέ ότι θα επηρέαζε τόσο σημαντικό ρόλο στην καθημερινότητά μας η τεχνολογία. Η τεχνολογική εποχή που βιώνουμε είναι απόλυτα συνυφασμένη με τον Κυβερνοχώρο. Η εκτενής χρήση των ηλεκτρονικών υπολογιστών και της σύνδεσης στο διαδίκτυο συντελούν στην κατεύθυνση αυτή. Ο παγκόσμιος επιχειρηματικός κόσμος συνεχώς ανακατατάσσεται,μεταβάλλεται και αναπροσαρμόζεται για να ανταποκρίνεται στις απαιτήσεις του περιβάλλοντος. Η αξιοποίηση των τεχνολογιών της πληροφορικής αποτελεί καθοριστικό παράγοντα βελτίωσης. Πάντοτε μία θετική κατάσταση δημιουργίας εσωκλείει όμως και το αρνητικό όφελος. Έτσι και ο κυβερνοχώρος εσωκλείει πάντοτε τον κίνδυνο. Η ιστορία έχει δείξει ότι τα αποτελέσματα κάθε σημαντικής τεχνολογικής εξέλιξης εξαρτώνται από τον τρόπο χρήσης. Έτσι μπορεί η τεχνολογία να βελτιώσει ριζικά το επίπεδο διαβίωσης των ανθρώπων,αλλά και να οδηγήσει σε καταστροφικές εξελίξεις.

Η παρούσα εργασία εστιάζει στο ευρύτερο φάσμα μελέτης του Κυβερνοχώρου από τη σκοπιά της χρηματοοικονομικής ανάλυσης και των οικονομικών επιπτώσεων των κινδύνων του. Στοχεύει στις επιπτώσεις των κυβερνοεπιθέσεων σε χρηματοοικονομικά ιδρύματα,στα κόστη που αυτές δημιουργούν καθώς και στις στρατηγικές διαχείρισης τις οποίες πρέπει να εφαρμόσουν τα ανώτατα στελέχη διοίκησης κάθε επιχειρήσεις για την αντιμετώπιση και εξάλειψη των κινδύνων. Ώστε τα οφέλη από τη χρήση διασύνδεσης με τον Κυβερνοχώρο να παραμείνουν,όπως η δυνατότητα στις επιχειρήσεις να αυξάνουν ταχύτητα τις διενέργειας των διαδικασιών,την αποδοτικότητα και το ανταγωνιστικό τους πλεονέκτημα.

Μετά από τη σύντομη εισαγωγή είναι εμφανής η ανάγκη για περαιτέρω έρευνα, προσδιορίζοντας και αναλύοντας τις προσφερόμενες δυνατότητες με αντίποδα τον περιορισμό των σκοτεινών σημείων. Σε πρώτο βαθμό μελετώντας τους κινδύνους του Κυβερνοχώρου και στη συνέχεια αναλύοντας συγκεκριμένους τομείς του.

ΚΕΦΑΛΑΙΟ 2 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1 Κοινωνία της Πληροφορικής

Η μεγάλη ταχύτητα,που χαρακτηρίζει στην εποχή μας, με την οποία συντελούνται οι τεχνολογικές αλλαγές έχει ως αποτέλεσμα οι σύγχρονες κοινωνίες δυτικού τύπου να αλλάζουν καθημερινά την ποιότητα ζωής σε μεγάλο βαθμό. Η χρήση των νέων τεχνολογιών έχει διεισδύσει πλέον στην επαγγελματική και προσωπική ζωή των πολιτών. Οι τεχνολογικές εξελίξεις άλλοτε συναντούν την απόρριψη ή την αδιαφορία της και άλλοτε αφομοιώνονται εύκολα. Με την πρόοδο των μαθηματικών ειδικά μετά τον 17ο αιώνα έγινε προσπάθεια κατασκευής μηχανών υπολογιστών. Οι άνθρωποι επινόησαν για να διευκολύνουν τους υπολογισμούς τους από την αρχαιότητα ακόμα διάφορες συσκευές. Από τον άβακα και τον μηχανισμό των Αντικυθήρων στην αρχαιότητα εώς τη μηχανή του Pascal και τη διαφορική μηχανή του Babbage στο Μεσαίωνα φτάσαμε στους πρώτους υπολογιστές ENIAC και UNIVAC στα μέσα του 20ού αιώνα.

Πίνακας 1: Διαχρονικά η ιστορική εξέλιξη των υπολογιστικών μηχανών. (Πηγή: Κοινωνία της Πληροφορίας,Μ. Παρασκευάς,Γ. Ασημακόπουλος,Β. Τριανταφύλλου,Κάλλιπος,Εθνικό Μετσόβιο Πολυτεχνείο (2015))

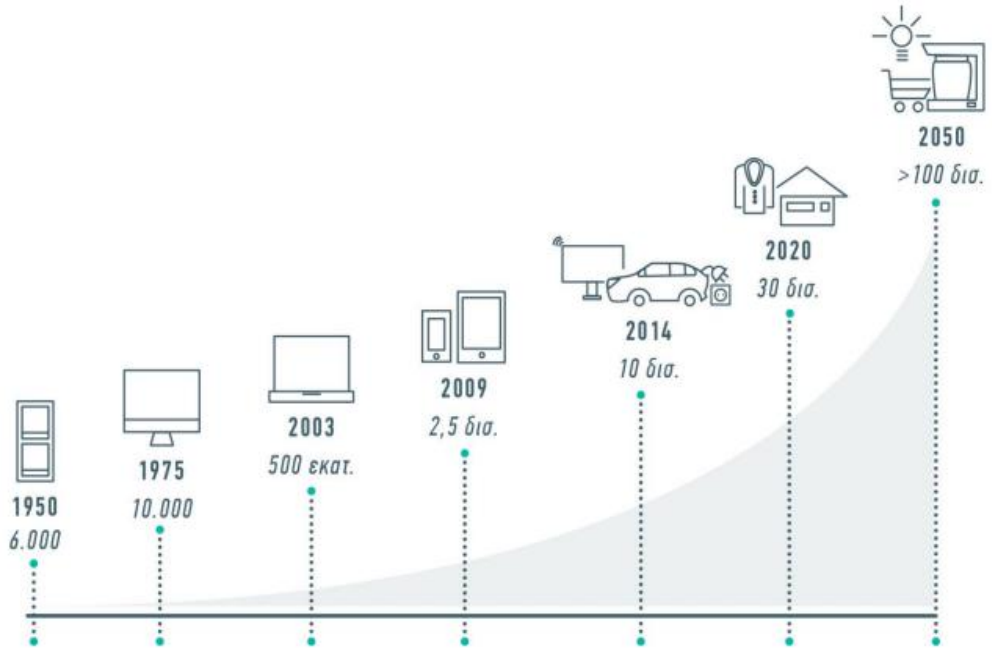
Χρονολογία	Περιγραφή
2700 π.Χ.	Ο άβακας χρησιμοποιείται για αριθμητικούς υπολογισμούς από τους Σουμέριους.
150 π.Χ.	Οι Έλληνες κατασκευάζουν τον μηχανισμό των Αντικυθήρων.
1617 μ.Χ.	Ο Napier επινοεί τους λογαριθμικούς πίνακες.
1622	Ο Oughtred επινοεί τον λογαριθμικό κανόνα.
1642	Ο Pascal κατασκευάζει την πρώτη αθροιστική μηχανή (Πασκαλίνα).
1822	Ο Babbage σχεδιάζει την πρώτη διαφορική μηχανή.
1854	Ο Boole θεμελιώνει τη Μαθηματική Λογική.
1890	Ο Hollerith επινοεί την επεξεργασία διάτρητων δελτίων, για τις ανάγκες της Εθνικής Στατιστικής Υπηρεσίας των ΗΠΑ.
1946	Οι Eckert και Mauchly κατασκευάζουν τον ENIAC.
1950	Ο Shockley εφευρίσκει το τρανζίστορ στα Bell Labs.
1951	Κατασκευάζεται στις ΗΠΑ ο UNIVAC, ο πρώτος εμπορικός Η/Υ.
1957	Κατασκευάζεται από την IBM ο πρώτος εκτυπωτής ακίδων.

Ο ηλεκτρονικός υπολογιστής[1] είναι μια ηλεκτρονική μηχανή που εκτελεί αριθμητικές

[1] Κοινωνία της Πληροφορίας,Μ. Παρασκευάς,Γ. Ασημακόπουλος,Β. Τριανταφύλλου,Κάλλιπος,Εθνικό Μετσόβιο Πολυτεχνείο (2015)

και λογικές πράξεις με μεγάλη ταχύτητα, διαχειριζόμενος συνήθως τεράστιο όγκο δεδομένων και ο όρος ΄΄πληροφορική΄΄ χρησιμοποιείται για να περιγράψει την επιστήμη που σχετίζεται με τη συλλογή,επεξεργασία,μετάδοση και αξιολόγηση κάθε λογής πληροφοριών, και υποβοηθείται στο έργο της από τους ηλεκτρονικούς υπολογιστές. Είναι δηλαδή η επιστήμη η οποία μελετά το οργανωμένο σύνολο γνώσεων που αφορούν τις αρχές, το σχεδιασμό, την κατασκευή, τη χρήση, τον προγραμματισμό και τις εφαρμογές των ηλεκτρονικών υπολογιστών χρησιμοποιώντας το ακατέργαστο υλικό της πληροφορίας. Ο μαθηματικός ορισμός της έννοιας της πληροφορίας αποδίδεται στον αμερικανό μαθηματικό C. Shannon, ο οποίος θεμελίωσε το 1948 τη μαθηματική θεωρία της πληροφορίας και διατύπωσε τις σχέσεις και τους κανόνες για τη μέτρηση της εσωτερικής οργάνωσης της πληροφορίας, αλλά και διάφορους ποσοτικούς προσδιορισμούς.

Σήμερα η μορφή της πληροφορίας έχει αλλάξει σε ψηφιακή,κάνοντας την εύκολα προσπελάσιμη χωρίς φυσική μετακίνηση και αποθήκευση. Είναι το σημαντικότερο στοιχείο του νέου μοντέλου κοινωνίας και οικονομικής οργάνωσης. Το διαδίκτυο έχει πλέον ενσωματωθεί σε πολλές καθημερινές δραστηριότητες λειτουργίας. έχουμε πλέον διασυνδεδεμένες όλες τις ηλεκτρονικές συσκευές καταγράφοντας πλήθος πληροφοριών για την καθημερινότητά μας.



Διάγραμμα 1: Η εξέλιξη του πλήθους των δικτυωμένων συσκευών. (Πηγή: Κοινωνία της Πληροφορίας,Μ. Παρασκευάς,Γ. Ασημακόπουλος,Β. Τριανταφύλλου,Κάλλιπος,Εθνικό Μετσόβιο Πολυτεχνείο (2015))

Παλιές και νέες εφαρμογές αναβαθμίζονται καταγράφοντας δεδομένα στους υπολογιστές,ακόμη και χωρίς τη συγκατάθεσή τους,αντικαθιστούν τις ικανότητες ακόμα και την κρίση των ανθρώπων. Επιπλέον κυβερνητικά και επιχειρηματικά δίκτυα κατευθύνονται σε

αυτή τη κατεύθυνση αυξάνοντας τη σύνδεση και την ανταλλαγή δεδομένων μεταξύ οντοτήτων,επιχειρήσεων,οργανισμών,κυβερνήσεων και ατόμων. Οι αποστάσεις και ο χρόνος πρόσβασης στην πληροφορία εκμηδενίζονται κάνοντας την κοινωνία της πληροφορικής το εργαλείο και το μέλλον της πραγματικής κοινωνίας αν όχι την ίδια.

2.2 Διαδίκτυο

Το Διαδίκτυο (Internet) αποτελεί σπουδαίας σημασίας έννοια και αποτελεί μία από τις λέξεις της εποχής μας που χρησιμοποιούμε καθημερινά. Διαδίκτυο εννοείται,σύμφωνα με τους Γεώργιος Πάγκαλο και Ιωάννης Μαυρίδη[2],κάθε συνένωση δύο τουλάχιστον δικτύων ίδιας ή διαφορετικής τεχνολογίας όπου επιτυγχάνεται η επικοινωνία μεταξύ τους σε λογικό επίπεδο σαν ένα δίκτυο. Εννοούμε δηλαδή το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP (Πρωτόκολλο Ελέγχου Μετάδοσης/ Πρωτόκολλο Διαδικτύου),ενώ μπορεί να βρίσκονται εγκατεστημένοι σε κάθε γωνιά του πλανήτη. Το Διαδίκτυο είναι δηλαδή ένα παγκόσμιο σύνολο δικτύων στο οποίο συνδέονται εκατοντάδες χιλιάδες άλλα δίκτυα διαφόρων μεγεθών και το οποίο επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου ηλεκτρονικού υπολογιστή. Λειτουργεί σε πολύ μεγάλο ποσοστό με κονδύλια και εξοπλισμό του ιδιωτικού τομέα και δεν έχει κεντρική διοίκηση, διεύθυνση ή διακυβέρνηση, τόσο στην χρήση τεχνολογιών όσο και στις πολιτικές πρόσβασης και χρήσης κάθε επιμέρους δικτύου. Ένα δίκτυο υλοποιείται με σκοπό την παροχή στους χρήστες του τη δυνατότητα απόκτησης διαμοιραζόμενης πρόσβασης σε δεδομένα,λογισμικό και συσκευές[3].

Αποτελεί σήμερα ένα παγκόσμιο χαμηλού κόστους ομοιογενές εργαλείο διακίνησης πληροφοριών και παροχής υπηρεσιών, στις οποίες περιλαμβάνονται και εφαρμογές που παρέχουν διακίνηση ευαίσθητων και προσωπικών δεδομένων των οποίων η ασφάλεια αποτελεί ένα από τα σημαντικότερα ζήτημα. Ο άνθρωπος χρησιμοποιεί την τεχνολογία για διάφορος σκοπούς,καλούς ή κακούς. Οι μορφές της ανθρώπινης δραστηριότητας έχουν επηρεαστεί από την υιοθέτηση των νέων τεχνολογικών εργαλείων και μέσων προσφέροντας την επέκταση της ανθρώπινης συμπεριφοράς σε νέες μορφές αλληλεπιδράσεων. Το διαδίκτυο προσφέρει έναν όγκο γνώσεων όπου σε λίγα κλάσματα των δευτερολέπτων κάποιος μπορεί να είναι ο κάτοχος. Είναι ένα πανίσχυρο εργαλείο που μπορεί να δημιουργήσει μεγάλα επιτεύγματα και μεγάλες καταστροφές,γιατί η μέγιστη ισχύς είναι η γνώση. Μία γνώση πολλών συγκοινωνούντων δοχείων.

[2] Στο βιβλίο τους Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων (Θεσσαλονίκη 2002,Εκδόσεις Ανικούλα)

[3] Στο άρθρο του Χρήστος Βεράτης, ΚΕΔΙΣΑ,Κυβερνοχώρος-Κυβερνοεπιθέσεις- Κυβερνοάμυνα-1ο Μέρος (Νοέμβριος 2015, http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe)

2.3 Έννοια Κυβερνοχώρου

Ο Κυβερνοχώρος (Cyberspace) μπορεί να θεωρηθεί σε γενικές γραμμές αντίστοιχος του Διαδικτύου αλλά δεν μπορεί να συνδεθεί απόλυτα. Δεν υπάρχει κοινά αποδεκτός ορισμός για τον Κυβερνοχώρο αλλά μόνο προσεγγίσεις του. Δεν μπορεί σαν έννοια να αποσαφηνιστεί ακριβώς. Όπως αναφέρει το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών,ορίζεται ως Κυβερνοχώρος ένα παγκόσμιο πεδίο εντός του περιβάλλοντος πληροφοριών που αποτελείται από τα αλληλοεξαρτώμενα δίκτυα υποδομών της τεχνολογίας των πληροφοριών και δεδομένων, συμπεριλαμβανομένου του Διαδικτύου,των τηλεπικοινωνιακών δικτύων,των ηλεκτρονικών υπολογιστών,των συστημάτων πληροφορικής και ενσωματωμένων επεξεργαστών και ελεγκτών[4]. Ο όρος Κυβερνοχώρος χρησιμοποιείται για να περιγράψει το πλασματικό - εικονικό περιβάλλον μέσα στο οποίο λαμβάνουν χώρα ηλεκτρονικές επικοινωνίες, όπως το διαδίκτυο και η ανταλλαγή ηλεκτρονικών μηνυμάτων.[5] Δεν έχει τοποθεσία και μεταβλητό μέγεθος,με τα όρια του αυξάνονται συνεχώς. Η αύξηση του μεγέθους του οφείλεται στην εξέλιξη της ψηφιακής τεχνολογίας μέσω της ανάπτυξης και της ανακάλυψης νέων τεχνολογιών,καθώς και την εξέλιξη των δικτύων και της ταχύτητας του Διαδικτύου μέσα από την εξέλιξη της νανοτεχνολογίας[6]. Η εξέλιξη του Κυβερνοχώρου ποσοτικά όσο και ποιοτικά ακολουθεί σχεδόν πιστά την πορεία του Διαδικτύου και της τεχνολογίας των δικτύων και των υπολογιστών. Είναι ένας σύνθετος κόσμος σχηματισμένος από τη παράθεση δεδομένων σε ένα πολυδιάστατο χώρο τον οποίο οι χρήστες μπορούν να αλληλεπιδράσουν. Υπάρχει,πηγαίνουμε εκεί αλλά δεν έχει τοποθεσία. Αποτελεί ένα ανθρώπινο κατασκεύασμα,μία εφεύρεση με δικούς του όρους,που αποτελεί ένα εικονικό μέσο χωρίς ομοιότητες με τους υπόλοιπους χώρους. Μια πραγματικότητα δομημένη από δεδομένα και δεν αποτελεί απλώς ως ένα τεχνολογικό συνονθύλευμα. Οι Richard Clarke και Robert Knake[7] δίνουν ως ορισμό ότι ο κυβερνοχώρος είναι όλα τα δίκτυα των ηλεκτρονικών υπολογιστών σε παγκόσμιο επίπεδο καθώς και οτιδήποτε συνδέεται και ελέγχεται από αυτά. Δεν είναι απλώς το ίντερνετ αλλά περιλαμβάνει και τα δίκτυα των υπολογιστών που έχουν πρόσβαση σε αυτόν.

Όπως παρουσιάζεται παρακάτω, η υπόσταση του Κυβερνοχώρου δεν είναι αμιγώς υλική και γεωγραφική,με το σημαντικότερο τμήμα του να είναι άυλο. Η φύση του έχει

[4] Στο άρθρο Joint Publication 1-02 ,Department of Defense Dictionary of Military and Associated Terms(8 November 2010,As Amended Through 15 February 2016) p. 58

[5] Στο άρθρο του Ryan Patterson, Silencing the Call to Arms: A Shift Away from Cyber Attacks as Warfare (Los Angeles,2015)

[6] Στο άρθρο του Kabay, M. E, PhD, CISSP Director of Education "Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy Paper" presented at the Annual Conference of the European Institute for Computer Anti-virus

[7] Στο βιβλίο τους Cyber War: The Next Threat to National Security and What to Do About It(1st Edition HarperCollins Publishers,New York 2010) p.70

εξεταστεί με διάφορα μοντέλα που εφαρμόζονται στην έρευνα των λειτουργιών και δομών του.

Ένας τρόπος ώστε να αποσαφηνίσουν τα βασικά χαρακτηριστικά και να παρουστεί καλύτερα ο Κυβερνοχώρο είναι το σύστημα των τριών επιπέδων.

Σύμφωνα με τον καθηγητή Martin Libicki [8]προτείνει ώστε να γίνει καλύτερα κατανοητός ο κυβερνοχώρος στην θεώρηση τριών επιπέδων ως προς τη λειτουργία του των Συστημάτων Πληροφορικής (IT Systems).:

- Φυσικό επίπεδο, αναφέρεται στο υλικό. Αποτελείται από το σύνολο των μέσων ενός πληροφοριακού συστήματος όπως είναι οι τα μηχανήματα (όπως κουτιά Η/Υ, τα έξυπνα κινητά και εκτυπωτες), ηλεκτρικά (όπως καλώδια) και ηλεκτρονικά (όπως μικροκυκλώματα και ολοκληρωμένα κυκλώματα). Σε περίπτωση απουσίας του φυσικού επιπέδου εξαφανίζεται και το σύστημα πληροφορικής.
- Συντακτικό επίπεδο περιλαμβάνει τις οδηγίες του κατασκευαστή και του χρήστη που δίνεται στη μηχανή καθώς και στα Πρωτόκολλα μέσω των οποίων επικοινωνούν. Θα πρέπει να σημειωθεί ότι οι δικτυοπειρατές δραστηριοποιούνται σε αυτό το επίπεδο καθώς επεμβαίνουν στο λογισμικό χωρίς κατάλληλη εξουσιοδότηση και επιτυγχάνοντας κυριότητα έναντι των σχεδιαστών και των χρηστών.
- Σημασιολογικό επίπεδο περιλαμβάνει το σύνολο των πληροφοριών που έχει μία μηχανή όπως είναι τα δεδομένα και τις ψηφιακές πληροφορίες. Σε αυτό το επίπεδο εξετάζεται η ορθότητα μιας οδηγίας,η οποία μπορεί συντακτικά να είναι ορθή ωστόσο σημασιολογικά να είναι λανθασμένη. Αν κάποιος καταφέρει μία μετατροπή στην σημασιολογική ερμηνεία ενός συστήματος πληροφορικής,καταφέρνει και τη χειραγώγηση του. Είναι εφικτό να πραγματοποιηθεί μία επίθεση μόνο σε αυτό το επίπεδο, τροφοδοτώντας το σύστημα με λανθασμένες πληροφορίες δημιουργώντας υπερχειλίσεις φορτίου ή ακόμα εμπεριέχοντας κακόβουλο κώδικα σε ιστοσελίδες.

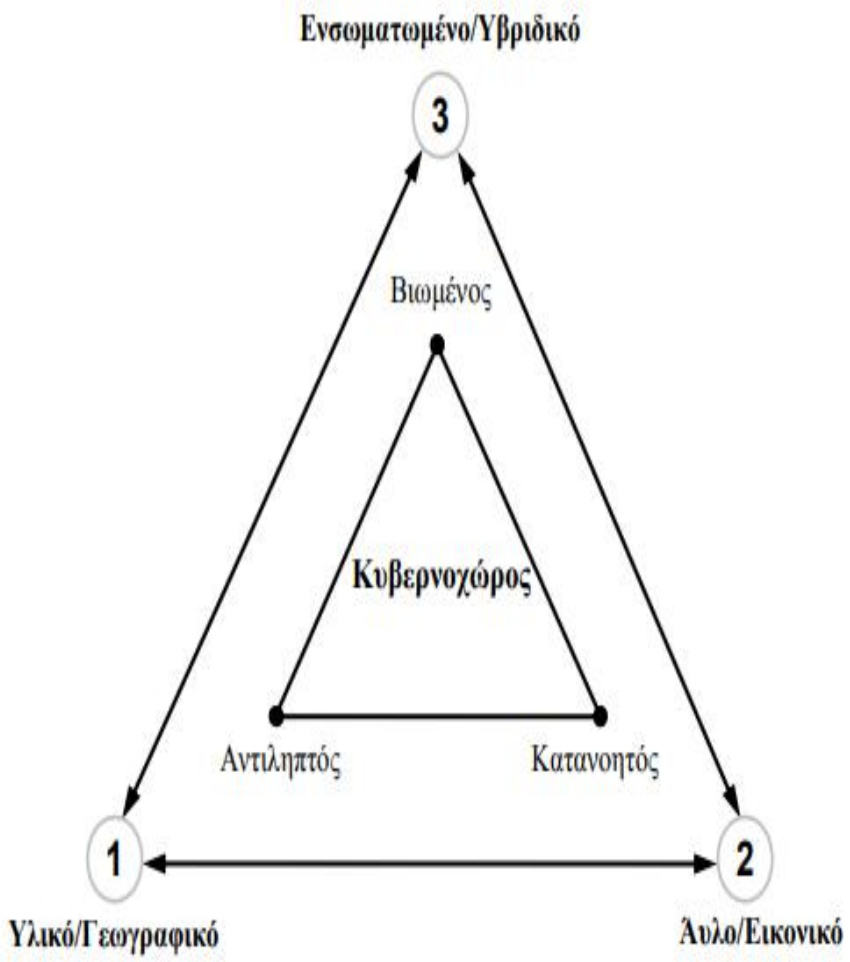
Επιπρόσθετα ένα παρόμοιο μοντέλο τριαδικής ανάλυσης των δομών και λειτουργιών του Κυβερνοχώρου η Trialectics του Lefebvre [9] όπως την αναφέρει και ο Δρ. Κώστα Φυσεντζίδη[10],όπου ο Κυβερνοχώρος παρουσιάζεται να αποτελείται από τρία βασικά μορφώματα,όπως παρουσιάζεται παρακάτω. Οι τρεις βασικές δομές βρίσκονται σε συνεχή

[8] Στο βιβλίο του Cyberdeterrence and Cyberwar (USA RAND Project Air Force 2009) p12-15

[9] Στο βιβλίο του La Production de l'Espace (4e édition,Ethno-sociologie 1974)

[10] Στη Διδακτορική Διατριβή του,Η Σημασία της Ενσωμάτωσης του Κυβερνοχώρου στις Κοινωνικοχωρικές Δομές:Η Κυβερνόπολη (Πανεπιστήμιο Θεσσαλίας,Βόλος 2012)

αλληλεπίδραση δημιουργίας αναπαραστάσεων κάνοντας έτσι κατανοητή την δομή του Κυβερνοχώρου.



Διάγραμμα 2: Τα Τρία Μορφώματα του Κυβερνοχώρου. (Πηγή: Διδακτορική Διατριβή του Κ. Φυσεντζίδη,Η Σημασία της Ενσωμάτωσης του Κυβερνοχώρου στις Κοινωνικοχωρικές Δομές:Η Κυβερνόπολη (Πανεπιστήμιο Θεσσαλίας,Βόλος 2012) και Βασισμένο στην Trialectics) του Lefebvre στο βιβλίο του La Production de l'Espace (1974))

Πίνακας 2: Προσέγγιση εξέτασης της δομής του Κυβερνοχώρου. (Πηγή: Διδακτορική Διατριβή του Κ. Φυσεντζίδη,Η Σημασία της Ενσωμάτωσης του Κυβερνοχώρου στις Κοινωνικοχωρικές Δομές:Η Κυβερνόπολη (Πανεπιστήμιο Θεσσαλίας,Βόλος 2012) και Βασισμένο στην Trialectics) του Lefebvre στο βιβλίο του La Production de l'Espace (1974))

Χώρος	**Κυβερνοχώρος**	**Παραδείγματα**
① Φυσικός/Αντιληπτός	Υλικός/Γεωγραφικός	Η/Υ,καλώδια και έξυπνα κινητά τηλέφωνα
② Νοητικός/Κατανοητός	Άυλος/Εικονικός	Δεδομένα και ψηφιακές πληροφορίες
③ Κοινωνικός/Βιωμένος	Ενσωματωμένος/Υβριδικός	Μικροκύματα ασύρματης επικοινωνίας

2.4 Κυβερνοεπιθέσεις και απειλές στον Κυβερνοχώρο

Ο ορισμός της Κυβερνοεπίθεσης (Cyber-attack) είναι ένα εξαιρετικά δύσκολο εγχείρημα. Σύμφωνα με τον καθηγητή Matthew Waxman[11] Κυβερνοεπίθεση είναι το σύνολο των ενεργειών με στόχο τη μεταβολή, διακοπή ή καταστροφή υπολογιστικών συστημάτων,δικτύων,πληροφοριών ή προγραμμάτων τους. Σύμφωνα με το Practical Law Company,Whitepaper on Cyber Attacks, Κυβερνοεπίθεση ορίζεται ως μία επίθεση που από έναν υπολογιστή εναντίον ενός ιστότοπου,ενός υπολογιστικού συστήματος ή μεμονωμένο υπολογιστή με σκοπό να εκτεθεί η αξιοπιστία,η εχεμύθεια και η δυνατότητα του στόχου και των πληροφοριών αποθήκευσης του. Ο ορισμός έχει τρία διακριτά μέρη:

a) επίθεση ή μία παράνομη προσπάθεια που
b) κερδίζει κάτι
c) από ένα υπολογιστικό σύστημα.

Το κυβερνοέγκλημα αποτελεί εξέλιξη του ηλεκτρονικού εγκλήματος στο Διαδίκτυο.

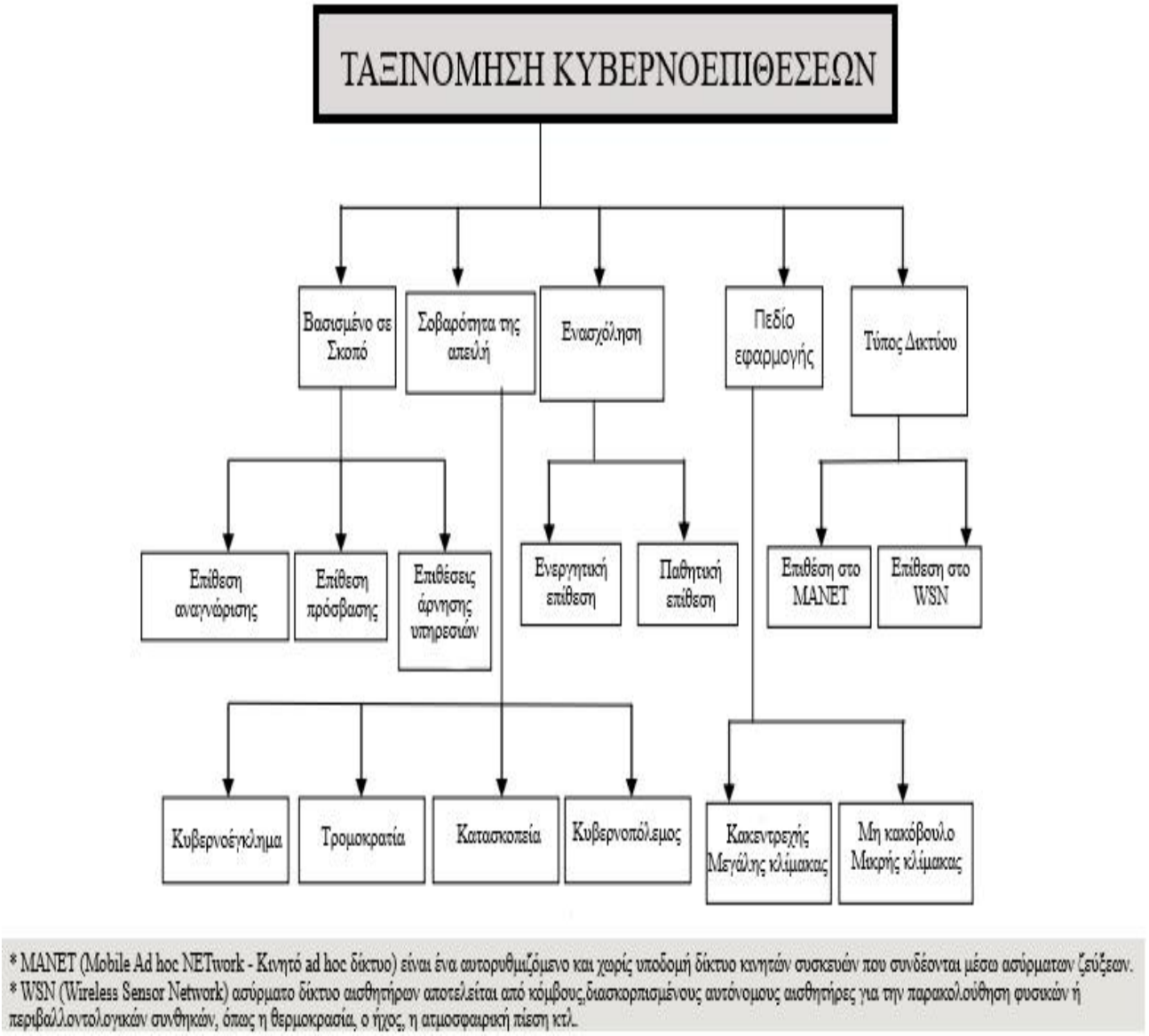
Οι Richard Clarke και Robert Knake[12] κατατάσσουν τις Κυβερνοεπιθέσεις ανάλογα με τη σοβαρότητα της απειλής που αποτελούν ξεκινώντας από εκείνες με υψηλή σοβαρότητα σε εκείνες με χαμηλότερη.

- Κυβερνοπόλεμος
- Κυβερνοκατασκοπεία
- Βίαιες Επιθέσεις
- Έγκλημα
- Ενόχληση

Επίσης μπορούν να χωριστούν ανάλογα με την επιδίωξη. Την οικονομικό εκμετάλλευση ή την στόχευση επιθέσεις σε συγκεκριμένο στόχο και διαφορετικό κίνητρα. Μία πιο ενδελεχής ταξινόμηση παρουσιάζεται στο παρακάτω διάγραμμα.

[11] Στο άρθρο του Cyber-Attacks and the Use of Force: Back to the Future (Article 2(4)' (2011) 36 Yale J. Int'l L. 421, 422.)

[12] Στο βιβλίο τους Cyber War: The Next Threat to National Security and What to Do About It (1st Edition HarperCollins Publishers,New York 2010) p.92

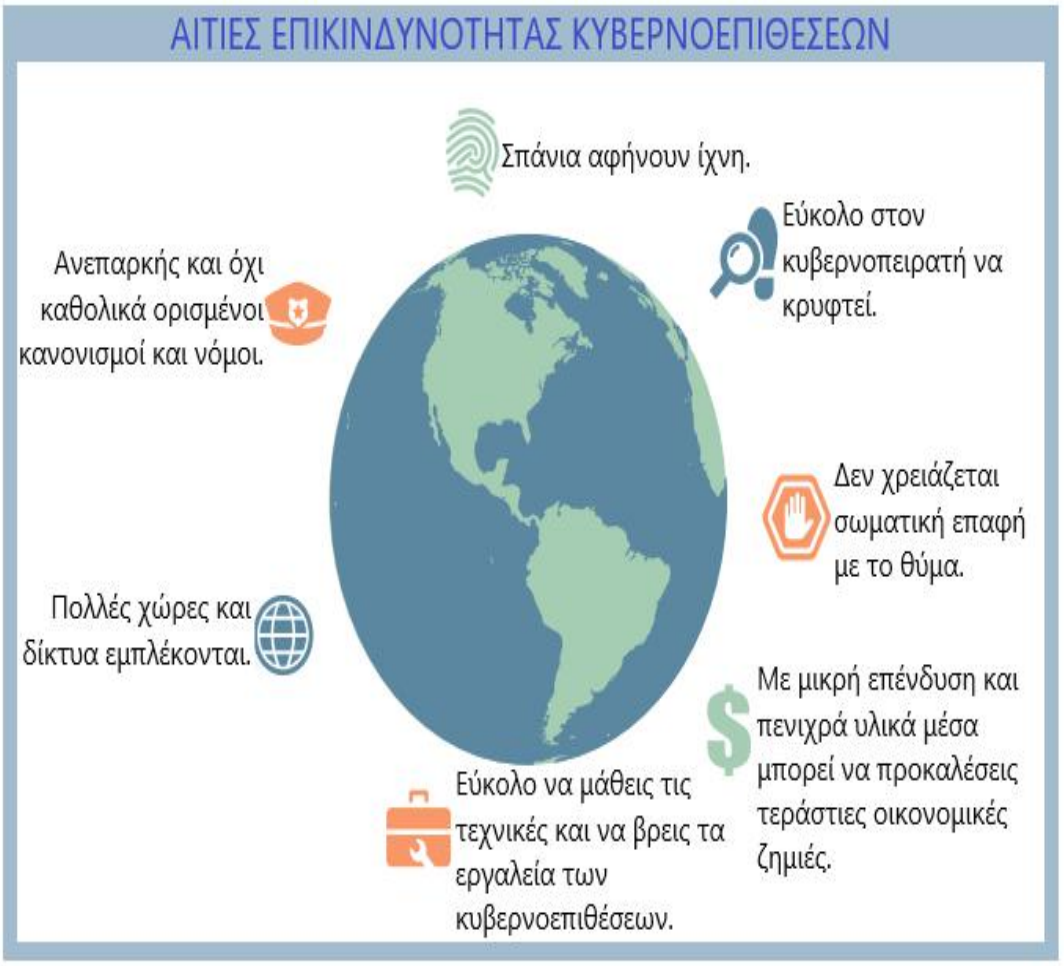


Διάγραμμα 3: Κατηγορίες κυβερνοεπιθέσεων ανάλογα με την επιδίωξη. (Πηγή: Ιδια επεξεργασία (Βασισμένο στο άρθρο των M. Uma and G. Padmavathi,"A Survey on Various Cyber Attacks and Their Classification",International Journal of Network Security, Vol.15, No.5, PP.390-396, Sept. 2013))

Είναι λογικό πως όταν ο Κυβερνοχώρος δεν έχει γεωγραφικό χώρο και δεν μπορεί να εκπροσωπείται δημιουργούνται προβλήματα επιβολής κυριαρχίας και οριοθέτησης, αποτελώντας πηγή απειλών για την κυριαρχία μέσω των Κυβερνοεπιθέσεων[13]. Στο θέμα της σοβαρότητας της απειλής ο καθηγητή Martin Libicki[14] υποστηρίζει ότι ο κυβερνοπόλεμος χρησιμοποιείται περισσότερο για την ενόχληση ενός αντιπάλου,εκνευρίζοντας ή ενοχλώντας τον,παρά την συντριβή του. Δεδομένου ότι οι μόνιμες επιδράσεις είναι παροδικές ενώ η απειλή της τιμωρίας δεν έχει κάνει αρκετά για την πρόληψη των κυβερνοεπιθέσεων σε

[13] Στο βιβλίο των David Betz, Tim Stevens,Cyberspace and the state toward a strategy for cyber-power (iiss , November 2011, p. 58- 60)
[14] Στο βιβλίο του Cyberdeterrence and Cyberwar (USA RAND Project Air Force 2009) p20

στρατιωτικά και μη δίκτυα. Οι στοιχειώδεις δεξιότητες κυβερνοπειρατείας (hacking) μπορούν να φτάσουν σε οπουδήποτε. Οι σκληρές τιμωρίες τείνουν να χάσουν την αξιοπιστία τους ως μηχανισμούς επιβολής του νόμου γιατί οι εγκληματίες σπάνια εντοπίζονται. Ακόμη και αν ο επιτιθέμενος εντοπιστεί,ενδέχεται στη χώρα του να μην ασκούνται συγκεκριμένοι νόμοι για το έγκλημα στον κυβερνοχώρο ή να μην υπάρχουν δικαιοδοσίες από το κράτος όπου έχει γίνει η επίθεση προς το κράτος διαμονής του. Οποιοσδήποτε με φορητό υπολογιστή, σύνδεση στο Διαδίκτυο και στοιχειώδεις δεξιότητες κυβερνοπειρατείας μπορεί να φτάσει οπουδήποτε στον κόσμο προκαλώντας δραματική βλάβη,διακόπτοντας λειτουργίες και υποκλέπτοντας δεδομένα. Η ανικανότητα επιβολής δικαιοσύνης και στοιχειοθέτησης της κατηγορίας συναινούν στη ταχεία αύξηση του αριθμού των επιθέσεων,των κυβερνοεπιθέσεων. Οι σημαντικότερες αιτίες κυβερνοεπιθέσεων παρουσιάζονται αναλυτικότερα παρακάτω.



Διάγραμμα 4: Αιτίες επικινδυνότητας των κυβερνοεπιθέσεων. (Πηγή: Ιδια επεξεργασία, βασισμένο σε κείμενο και εικόνα του TAKING CONTROL OF CYBERSECURITY: A Practical Guide for Officers and Directors (Foley's Cybersecurity Team,Foley & Lardner LLP,Milwaukee Wisconsin USA 2015))

2.5 Μέρη-Στόχοι Κυβερνοεπιθέσεων

Τα κυριότερα μέρη στόχοι κυβερνοεπιθέσεων όπου σε ετήσια βάση,με μεταβολή μόνο της ιεράρχησης μεταξύ τους ,βρίσκονται στις προτιμήσεις είναι:

- **Χρηματοπιστωτικά ιδρύματα**

Οι σημαντικές πληροφορίες των στοιχείων των πελατών οικονομικών και τραπεζικών υπηρεσιών,των αριθμών τηλεφώνων,των διευθύνσεων,των στοιχείων πιστωτικών καρτών,των τραπεζικών και επενδυτικών κινήσεων τους είναι ένα σύνολο αρχείων όπου αποτελεί πολύτιμο στόχο κυβερνοεπιθέσεων. Η κίνηση των τραπεζικών συναλλαγών μέσω διαδικτύου και έξυπνων τηλεφώνων αυξάνουν την απειλή. Επιπλέον θα πρέπει να σημειωθεί ότι ένα σημαντικό ποσοστό αυτών των επιθέσεων στα χρηματοπιστωτικά ιδρύματα γίνεται για ιδεολογικούς σκοπούς.

- **Δημόσιας διοίκησης,Εθνικής Άμυνας και Ασφάλειας**

Ο χώρο της Δημόσιας διοίκησης, Εθνικής Άμυνας και Ασφάλειας αποτελεί έναν από τους κύριους στόχους επιθέσεων που φτάνουν ακόμα και τους κυβερνοπολέμους. Τα στοιχεία των Ενόπλων Δυνάμεων και τα κομβικά Υπουργεία σε πρώτο βαθμό και κατά δεύτερον στις υπομονάδες και στις υπο-υπηρεσίες αυτών. Το σύνολο των εμπιστευτικών πληροφοριών και δεδομένων που κατέχουν αποτελούν το στόχο. Τέλος οι επιθέσεις των στόχων αυτών διακατέχονται από πολλά κίνητρα και η επιτυχία αυτών έχει ανυπολόγιστες καταστροφές από οικονομικές ως και απώλεια εθνικής κυριαρχίας.

- **Εκπαίδευση**

Ο χώρο της εκπαίδευσης αποτελεί έναν από τους κύριους στόχους επιθέσεων. Τα ανώτερα και ανώτατα εκπαιδευτικά ιδρύματα καθώς και αρκετά ιδρύματα και ινστιτούτα τριτοβάθμιας εκπαίδευσης, συλλέγουν συνήθως ένα μεγάλο σύνολο εμπιστευτικών και προσωπικών δεδομένων. Η αποθήκευση των δεδομένων γίνεται κυρίως σε φορητές συσκευές που ανήκουν στο προσωπικό και τους σπουδαστές,όπου αποτελούν μία ευκολότερη λεία και μία ακόμα πιθανότητα ώστε να χαθούν. Τέλος τα απομακρυσμένης πρόσβασης δίκτυα και μέσα διαχείρισης ακαδημαϊκών πληροφοριών σε συνδυασμό με τα χαμηλού επιπέδου ασφαλείας δίχτυα των ιδρυμάτων επιβαρύνουν την έκθεση στον κίνδυνο.

- **Φορείς Υγεία**

Οι πάροχοι υπηρεσιών υγείας και παροχής υγειονομικών υπηρεσιών. και τα νοσοκομεία αποτελούν κύριο στόχο παραβιάσεις ιδιωτικών και ιατρικών δεδομένων. Η ψηφιακή διαχείριση του ιατρονοσηλευτικού προσωπικού,των ιατρικών εξετάσεων,των υγειονομικών,του ιατροτεχνολογικού εξοπλισμού και των υπολοίπων αναλωσίμων αναπτυγμένων κυρίως χώρων που διαθέτουν ψηφιακά μητρώα,συστήματα και εφαρμογές,εύκολα μπορούν να υποκλαπούν και να χρησιμοποιηθούν σε οποιοδήποτε μέρος του κόσμου για οποιοδήποτε σκοπό.

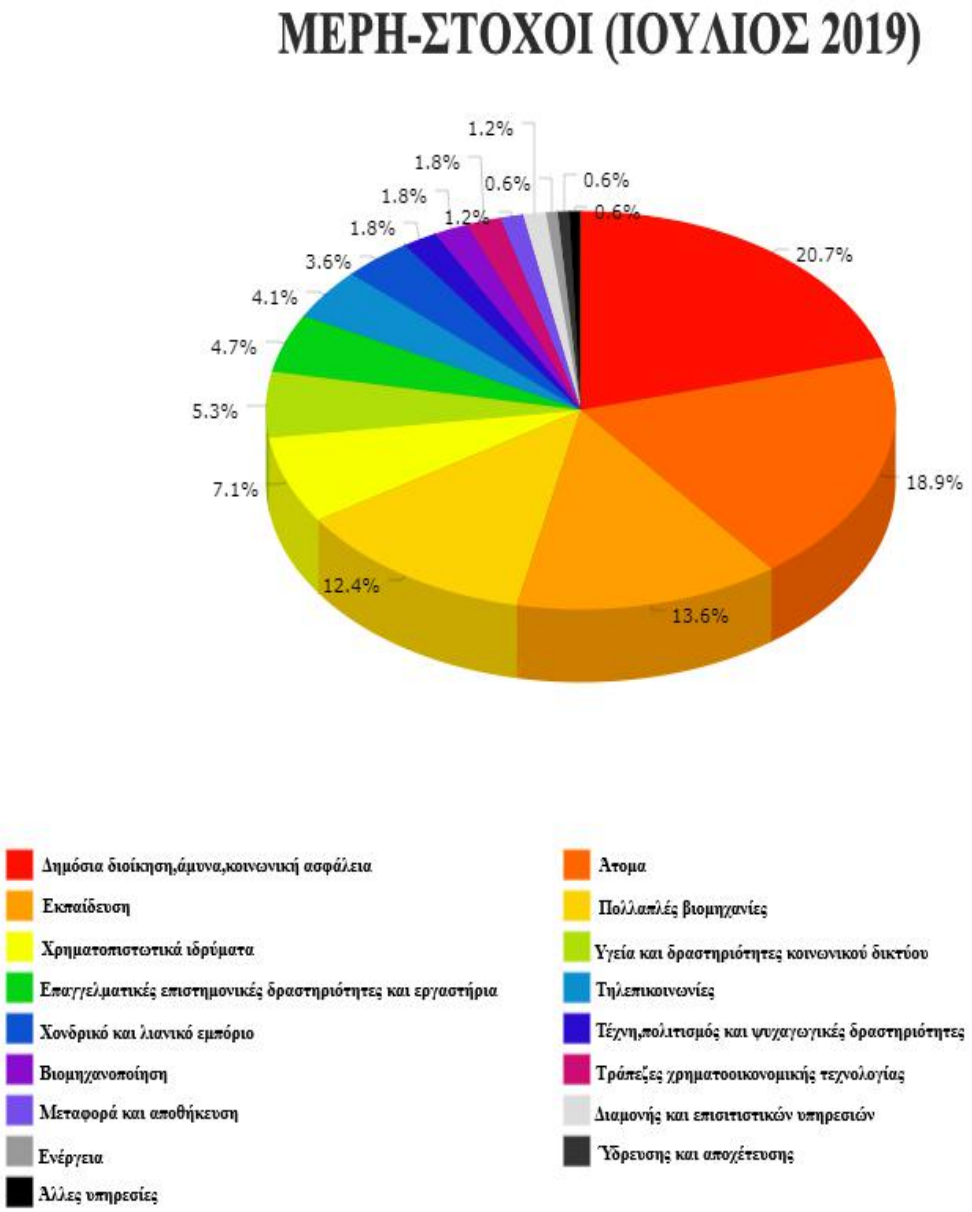
- **Επιχειρήσεις χονδρικής και λιανικής πώλησης**

Το σύνολο των επιχειρήσεων διαθέτουν πλέον πληθώρα προσωπικών δεδομένων των πελατών τους καθώς και τραπεζικών στοιχείων τους λόγω των ηλεκτρονικών πληρωμών και των πληρωμών με χρήση καρτών (χρεωστικών και πιστωτικών). Εξάλλου βρισκόμαστε σε μία περίοδο όπου πλέον ηλεκτρονικές διαδικτυακές συναλλαγές σε παγκόσμιο επίπεδο έχουν αλματώδη άνοδο ως προς τα έσοδα και τον αριθμό πωλήσεων.

- **Τηλεπικοινωνίες,Δίκτυα Επικοινωνιών και Πληροφορικής**

Οι εταιρείες Τηλεπικοινωνιών,δημοσίων και ιδιωτικών**,**διαχειρίζονται έναν τεράστιο όγκο προσωπικών δεδομένων είτε αφορά τα στοιχεία των πελατών τους είτε τις διαβιβαζόμενες πληροφορίες. Πλέον οι περισσότερες συναλλαγές,και σε αυτόν το χώρο,γίνονται είτε με χρήση καρτών είτε ηλεκτρονικά,με αποτέλεσμα μια επιτυχημένη επίθεση να έχει ως συνέπεια την υποκλοπή των δεδομένων. Σε αρκετές περιπτώσεις ακόμα και τη διακοπή λειτουργίας του παρόχου με κοινό παρονομαστή την τεράστια απώλεια εσόδων.

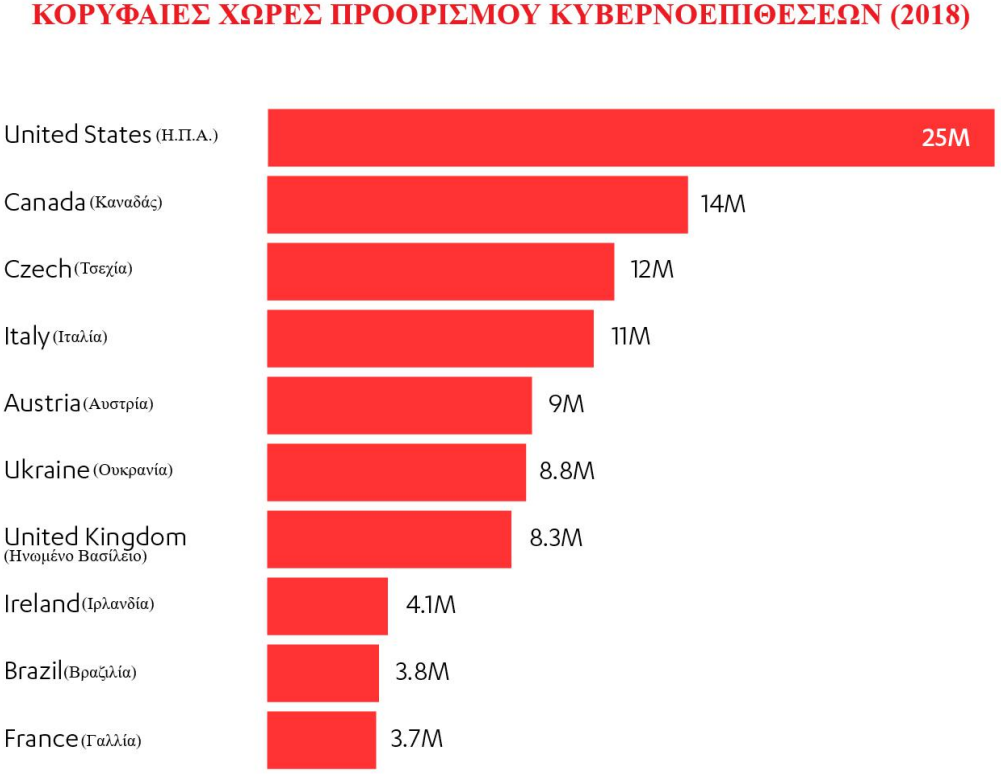
Ένα ενδεικτικό διάγραμμα αποτελεί το παρακάτω,όπου παρουσιάζει τα κυριότερα μέρη στόχους των κυβερνοεπιθέσεων τον Ιούνιο του 2019. Σημαντικό είναι να παρατηρήσουμε ότι οι κυριότεροι στόχοι κυβερνοεπιθέσεων παραμένουν ίδιοι τα τελευταία έτη με τον Ιούλιο του 2019 με μικρές μόνο μεταβολές μεταξύ τους.



Διάγραμμα 5: Τα κυριότερα μέρη στόχοι των κυβερνοεπιθέσεων τον Ιούνιο του 2019. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από www.hackmageddon.com)

Σύμφωνα με έκθεση που συνέταξε πρόσφατα η εταιρεία κυβερνοασφάλειας Kaspersky Lab, οι επιθέσεις στοχεύουν κινητά τηλέφωνα και εστιάζουν κυρίως σε πλούσιες χώρες με αναπτυγμένες αγορές και στις οποίες χρησιμοποιούνται ευρέως οι υποδομές ηλεκτρονικών πληρωμών μέσω smartphone. Βάσει της ετήσιας έκθεσης της εταιρείας για την περίοδο 2016-2017, οι παραπάνω συνθήκες είναι ελκυστικές για τους κυβερνοεγκληματίες αφού τους επιτρέπουν να μεταφέρουν τα λύτρα με σχετική ευκολία. Στα παρακάτω γραφήματα παρουσιάζονται οι κυριότερες χώρες προέλευσης και προορισμού κυβερνοεπιθέσεων.

Διάγραμμα 6: Τα κυριότερα κράτη προέλευσης των κυβερνοεπιθέσεων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από https://blog.f-secure.com)



Διάγραμμα 7: Τα κυριότερα κράτη προορισμού των κυβερνοεπιθέσεων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από https://blog.f-secure.com)

Κατά την περίοδο 2015-2016, η Γερμανία ήταν η χώρα που δέχτηκε τις περισσότερες επιθέσεις, ενώ ακολουθούν ο Καναδάς, η Βρετανία και οι ΗΠΑ. Ωστόσο, το σκηνικό αυτό άλλαξε σημαντικά, αφού την περίοδο 2016-2017,2017-2018 και 2018-2019 οι ΗΠΑ έγιναν ο κύριος στόχος των κυβερνοεγκληματιών,με τον Καναδά να καταλαμβάνει την επόμενη θέση. Αυτές οι γεωγραφικές αλλαγές στο τοπίο των κυβερνοεπιθέσεων θα μπορούσαν να αποτελούν ένα σημάδι της τάσης εξάπλωσης των επιθέσεων σε πλούσιες, απροετοίμαστες, ευάλωτες ή ακόμα και απρόσιτες περιοχές,σημειώνει ο Roman Unuchek ειδικός ασφαλείας της Kaspersky. Αυτό προφανώς σημαίνει ότι οι χρήστες, ειδικά σε αυτές τις χώρες, θα πρέπει να είναι εξαιρετικά προσεκτικοί κατά του Threats & Research και απρόσιτες περιοχές και οι χρήστες ειδικά στις χώρες κυβερνοεπιθέσεων θα πρέπει να είναι εξαιρετικά προσεκτικοί.

Τα μέρη-στόχοι μπορούν να εξεταστούν από τρεις σκοπιές: ως προς το κράτος, ως προς την κατηγορία στόχου και ως προς το κίνητρο της επίθεσης. Ο κάθε παράγοντας δεν είναι ανεξάρτητος από τους άλλους με το μέρος-στόχος να αποτελεί το σημείο τομής και των τριών. Το πόσο ευάλωτη θα είναι μία κατηγορία στόχου ή ακόμα και η ιεράρχηση της ως προς το πλήθος των επιθέσεων εξαρτάται και από την χώρα όπου λαμβάνει χώρο. Επιπλέον το κίνητρο της επίθεσης επηρεάζεται και από τις πολιτικές των κρατών που ακολουθούν σε όλα τα επίπεδα διακυβέρνησης. Αυτό μας βοηθάει στο να προετοιμαστούμε και να κάνουμε κάποιες εκτιμήσεις ως προς τους πιθανούς στόχους.

Διάγραμμα 8: Τα κυριότερα κίνητρα κυβερνοεπιθέσεων κατά το 2018. (Πηγή:Ιδια επεξεργασία και μετάφραση, βασισμένο σε στοιχεία από www.hackmageddon.com)

Τέλος για να μπορέσουμε να προσδιορίσουμε τα μέρη στόχους θα πρέπει να προσδιορίσουμε το κίνητρο της επίθεσης. Η σοβαρότητα της απειλής όπως το κυβερνοέγκλημα,η κυβερνοκατασκοπεία,η κυβερνοτρομοκρατία και ο κυβερνοπόλεμος,είναι αμφιμονοσημαντα συνυφασμένη με το κινητό και τα ανάλογα οφέλη των επιθέσεων που κυρίως είναι οικονομικά,ιδεολογικα,εθνικά ακόμη και θρησκευτικά. Μεταβολή των επιθυμητών ωφελειών συνεπάγεται και μεταβολή το στόχων.

2.6 Σύνδεση επιχειρήσεων και Κυβερνοχώρου

Η τεχνολογία εξελίσσεται ταχέως σε έναν κόσμο που κατευθύνεται από τα κοινωνικά δίκτυα, τις ηλεκτρονικές συναλλαγές, των πρακτικών δικτύων απομακρυσμένων διακομιστών,των αυτοματοποιημένων διαδικασιών,πληροφοριών αποθήκευσης ή διαχείρισης μέσω διαδικτύου και αυτοματοποιημένες διαδικασίες που εκτελούνται. Οι χρηματοοικονομικές συναλλαγές στο Διαδίκτυο έχουν αυξηθεί σημαντικά,ταχύτερα από την ποσότητα της απάτης. Οι επιχειρήσεις έχουν άμεση εξάρτησή από τα σύγχρονα πληροφοριακά συστήματα,τα τηλεπικοινωνιακά συστήματα,τα ηλεκτρονικά μέσα και το διαδίκτυο τα τελευταία χρόνια με ραγδαία αύξηση και εξάρτηση στη λειτουργία και στην βιωσιμότητά της. Κάθε εταιρεία σήμερα δεν είναι απολύτως ασφαλής σε κυβερνοεπιθέσεις ανεξάρτητα από το ποσό εξελιγμένα συστήματα,τεχνικές και εφαρμογές έχει,με σημαντικότερο μειονέκτημα ο προσδιορισμός του πότε θα γίνει μία κυβερνοεπίθεση και όχι αν θα γίνει. Ως αποτέλεσμα οι κυβερνοεπιθέσεις αναδεικνύονται σε ένα συστημικό πρόβλημα για όλες τις επιχειρήσεις όλων των κλάδων και των κρατών.

Το εύρος των οικονομικών ωφελειών που αυτόματα θα επιφέρουν ως φυσική συνέπεια της αξιοποιήσεις των δυνατοτήτων που προσφέρουν η χρήση και η σύνδεση των επιχειρήσεων με τον κυβερνοχώρο, έρχεται σε αντίθεση με την έντονα δραματοποιημένη απαισιοδοξία για τις αρνητικές συνέπειες που πιθανόν να συνεπάγονται από τη χρήση του. Η ψηφιοποίηση της οικονομίας και η χρήση όλων των τεχνολογικών επιτευγμάτων έχει μόνο έναν αρνητικό. Το αρνητικό αυτό αποτελεί η ενδεχόμενη απώλεια δεδομένων μέσω των κυβερνοεπιθέσεων. Η εκμηδένιση αυτού του κινδύνου θα είχε ως αποτέλεσμα μόνο οφέλη από την διασύνδεση αυτή. Ακολουθώντας τις νέες τεχνολογικές εξελίξεις η διασύνδεση όλων των επιχειρήσεων με τον κυβερνοχώρο είναι αναμφισβήτητη μονόδρομος στη σύγχρονη κοινωνία,αλλά με χρήση μεθόδων και εργαλείων διαχείρισης έναντι των κινδύνων του κυβερνοχώρου.

2.7 Σκοπός εργασίας - Ερευνητικά ερωτήματα

Η παρούσα εργασία εντάσσεται στο ευρύτερο φάσμα της μελέτης του κυβερνοχώρου και της ψηφιοποίησης της οικονομίας. Πρόκειται για ένα νεοσύστατο σημείο τομή των επιστημών της οικονομίας και της πληροφορικής με πληθώρα νέων εννοιών όπου σε αυτή την εργασία θα στοχεύουμε να αναλύσουμε στην παρούσα εργασία. Η ανάλυση σχετικών όρων σε συνδυασμό με την αναφορά αντίστοιχων περιστατικών ώστε να γίνει καλύτερα κατανοητή η χρηματοοικονομική ανάλυση και οι στρατηγικές διαχείρισης των κινδύνων όπου η εργασία επικεντρώνεται. Ο κύριος σκοπός αυτής της εργασίας είναι να τονιστούν οι οικονομικές πτυχές του Κυβερνοχώρου καθώς και την διαχείριση των κινδύνων σε αυτόν. Στα πλαίσια της παγκοσμιοποίησης και άμεσης εξάρτησης της επιχειρηματικότητας από τον κυβερνοχώρο οι σύγχρονοι διευθύνοντες σύμβουλοι και οικονομικοί διευθυντές βρίσκονται αντιμέτωποι με νέες προκλήσεις στη διαχείριση και αντιμετώπιση των κινδύνων αυτών.

Ερευνητικά ερωτήματα που τέθηκαν στην παρούσα εργασία:

- Ποιό το αντίκτυπο των κυβερνοεπιθέσεων στο χρηματοοικονομικό τομέα;
- Ποιές εταιρείες και χώρες αντιμετωπίζουν μεγαλύτερο κίνδυνο και είναι περισσότερο ευάλωτες ;
- Τι πρέπει να προσέχουν οι σύγχρονοι διευθύνοντες σύμβουλοι και οικονομικοί διευθυντές;
- Ποιοι οι κίνδυνοι που διατρέχουν όλες οι οικονομικά ενέργειας οντότητες;
- Ποιές οι στρατηγικές διαχείρισης των κινδύνων του κυβερνοχώρου;
- Ποιός ο οικονομικός αντίκτυπος,τα κόστη απώλειας δεδομένων και τα κόστη αντιμετώπισης των κινδύνων;

ΚΕΦΑΛΑΙΟ 3 ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΧΩΡΟΥ

3.1 Έννοια Κινδύνου

Βρισκόμαστε σε μία εποχή όπου η παγκοσμιοποίηση του επιχειρηματικού πνεύματος και των ταχέων βελτιώσεων της τεχνολογίας πληροφοριών και επικοινωνιών αναδύει στην επιφάνεια νέους κινδύνους και νέες προκλήσεις ως προς την διαχείριση και την εξάλειψη από τους αξιωματούχους των επιχειρήσεων.

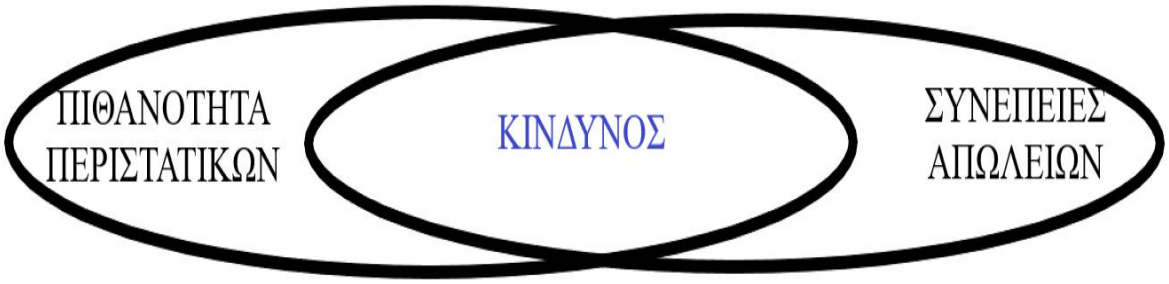
Η ισορροπία μεταξύ κινδύνου και ανταμοιβής είναι η ίδια η ουσία της επιχείρησης.χωρίς την ανάληψη κινδύνων η εταιρεία δεν μπορεί να επιφέρει κέρδη. Σε ένα κόσμο γεμάτο κινδύνους μεγαλύτερο ρόλο και βέλτιστη λύση είναι όχι να εκμηδενίσει στον κίνδυνο αλλά να τον αποτρέψεις. Σύμφωνα με τον Dan Borge η διαχείριση κινδύνου είναι δυνατόν να μας βοηθήσει να αρπάξουμε μία ευκαιρία και όχι μόνο να αποφύγουμε έναν κίνδυνο. Οι κίνδυνοι από τη μία όπου έχω αντιμετωπιστεί με προνοητικότητα και προσεκτική κρίση έρχονται στον αντίποδα των κινδύνων που έχουν ληφθεί απρόσεκτα και άθελα. Το σημείο εκκίνησης των διοικητικών συμβουλίων είναι να εποπτεύουν τον κίνδυνο σε σχέση με τον οργανισμό τους μέσα από την διαχείριση και τις στρατηγικές ευρύτερης προσέγγισης και ευθυγράμμισης, σε ένα κόσμο αυξημένης πολυπλοκότητας,αβεβαιότητας και συνεχών αλλαγών. το μεγαλύτερο λάθος συνήθως είναι η υποτίμηση του αντιπάλου και υποτίμηση του κινδύνου παραμένοντας τυφλοί[15]. Με τον όρο κίνδυνο υποθέτουμε ότι ο αρμόδιος λήψης απόφασης γνωρίζει προγενέστερα τις πιθανές καταστάσεις προσδιορισμού της φύσης ενός αποτελέσματος κάθε εναλλακτικής και διαθέσιμης λύσης. Οι πιθανότητες αυτές είναι συνήθως αντικειμενικές όταν ο υπολογισμός στηρίζεται σε αντικειμενικά κριτήρια ή υποκειμενικές στην περίπτωση που ο υπολογισμός τους βασίζεται στην υποκειμενική κρίση, τη διαίσθηση και την πείρα αυτού που αποφασίζει[16].

Σύμφωνα με τον καθηγητή Ιορδάνη Ελευθεριάδη ως κίνδυνος υφίσταται όταν ένα τυχαίο γεγονός επιδρά αρνητικά στην πιθανότητα πραγματοποίησης ενός εφικτού στόχου,ενώ μαθηματικά ο κίνδυνος μπορεί να εκφραστεί ως το προϊόν της πιθανότητας των περιστατικών

[15]Στο BUSINESS RISK A practical guide for board members,willis,pwc,chartis,airmic(Editor, Director Publications Ltd: Lysanne Currie Consultant Editor: Tom Nash) Published for the Institute of Directors, Airmic Ltd, Chartis Europe Ltd, PricewaterhouseCoopers LLP and Willis UK Ltd by Director Publications Ltd, 116 Pall Mall, London SW1Y 5ED 020 7766 8910 www.iod.com (2012)

[16] Στο βιβλίο του Ε. Καρασαββίδου – Χατζηγρηγορίου: Λήψη επιχειρηματικών αποφάσεων: προσέγγιση με την επιχειρησιακή έρευνα. University Studio Press, (1986)

και των συνεπειών της απώλειας που προκλήθηκε από τον κίνδυνο[17]. Επίσης κατά τον Ελευθεριάδη σημαντικό είναι η αβεβαιότητα του κινδύνου όπου προκύπτει από την ύπαρξη αποζημιώσεις της κατανομής πιθανότητας στο σύνολο των μελλοντικών εκβάσεων και γεγονότων που πιθανώς θα πραγματοποιηθούν. Με σημαντικές μεταβλητές το αν θα συμβεί,που θα συμβεί καθώς και τη χρονική περίοδο που θα συμβεί μελλοντικά[18].



Διάγραμμα 9: Ορισμός του Κινδύνου. (Πηγή: Ιδια επεξεργασία)

Υπάρχουν δύο τρόποι προσδιορισμού του κινδύνου σε γενικές γραμμές:

- Ως μέτρο της αβεβαιότητας και του μη προβλέψιμου.
- Ως μέτρο της διατήρησης μια απώλεια και των συνεπειών.

Οι συχνότερα εμφανιζόμενοι χρηματοοικονομικοί κίνδυνοι είναι κυρίως ο πιστωτικός κίνδυνος,ο κίνδυνος αγοράς,ο λειτουργικός κίνδυνος,ο επιχειρηματικός κίνδυνος,ο κίνδυνος ρευστότητας ο νομικός κίνδυνος καθώς και νέες μορφές κινδύνων όπως ο συναλλαγματικός κίνδυνος,ο επιτοκιακός κίνδυνος,ο πολιτικός κίνδυνος και ο κίνδυνος φήμης. Τα τελευταία χρόνια νέες μορφές κινδύνων έχουν εμφανιστεί μεταξύ των πιο επικίνδυνων να αποτελούν τους κινδύνους του Κυβερνοχώρου. Ηλεκτρονικός κίνδυνος ορίζεται ως η πιθανότητα ενός συμβάντος, του οποίου η εμφάνιση προκαλεί απώλεια της επιχείρηση και ως κίνδυνος κυβερνοχώρου ορίζεται ο κίνδυνος που σχετίζεται με κακόβουλες ηλεκτρονικές πράξεις που

[17] Πληροφορίες αντλήθηκαν από Ι. Ελευθεριάδη,Διοίκηση Εταιρικών Κινδύνων. Πανεπιστημιακές Σημειώσεις Πανεπιστήμιο Μακεδονίας,p.2 (2018) (https://docplayer.gr/23848931-Analysi-epiheirimatikon-kindynon.html)

[18] Πληροφορίες αντλήθηκαν από Ι. Ελευθεριάδη,Διοίκηση Εταιρικών Κινδύνων. Πανεπιστημιακές Σημειώσεις Πανεπιστήμιο Μακεδονίας),p.3(2018) (https://docplayer.gr/23848931-Analysi-epiheirimatikon-kindynon.html)

προκαλούν διαταραχές στις επιχειρήσεις, καθώς και οικονομικές απώλειες[19]. Οι παράγοντες κινδύνου Κυβερνοχώρου σύμφωνα με τους καθηγητές Mukhopadhyay A.,Saha, D.,Chakrabarti, B.,Mahanti, A. και Podder A. εξαρτάται κυρίως από την ευπάθεια της ηλεκτρονικής συναλλαγής(αριθμό ωρών ηλεκτρονικής συναλλαγής,την ευκολία με την οποία μπορεί να χρεωθεί ο ιστότοπος και το κόστος επισκευής του καθώς και την ευπάθεια του εξοπλισμού χρηστών),από τον κίνδυνο προσβολής από ιούς,την αποτυχίας λογισμικού ή υλικού,τη διακίνηση του διακομιστή και τους ιστοτόπους πρόσβασης του χρήστη. Το σύνολο των οντοτήτων προσπαθούν να οργανώσουν την αντιμετώπιση,τη διαχείριση και την εύρεση εναλλακτικών στην αντιμετώπιση της αβεβαιότητας ασφάλεια του Κυβερνοχώρου. Κάθε επιχειρηματική δραστηριότητα θα πρέπει να προσδιορίζει τον κίνδυνο υλοποίησης και να βρίσκει αντισταθμιστικά μέτρα αποτελεσματικής διαχείρισης του. Οι Böhme και Kataria, αναφέρουν ότι κίνδυνοι είναι υπαίτιοι για τα προβλήματα στα πληροφοριακά συστήματα προσδιορίζοντας τους έτσι μέσω των συνεπειών και των αποτελεσμάτων που επιφέρουν[20]. Τέλος σύμφωνα με την Επιτροπή Βασιλείας οι λειτουργικοί κίνδυνοι ορίζονται ως οι κινδυνοι που απορρέουν από ανεπαρκείς εσωτερικές διαδικασίες ή παραβιάσεις των διαδικασιών αυτών, ανθρώπινη συμπεριφορά, συστήματα ή από εξωτερικούς παράγοντες. Ειδικότερα οι κίνδυνοι Κυβερνοχώρου αναφέρονται στην ενδεχόμενη ζημία που μπορεί να προκύψει από μη εξουσιοδοτημένη πρόσβαση,χρήση, διαρροή, δυσλειτουργία, τροποποίηση ή καταστροφή δεδομένων,πληροφοριακών συστημάτων και επικοινωνιών μιας επιχείρησης[21].

3.2 Διακρίσεις του Κινδύνου (Cyber Risks)

Στην σχετική έκθεση περί κινδύνων του Κυβερνοχώρου της Grant Thornton αναφέρεται ότι σε σχέση με άλλες μορφές επιχειρηματικών κινδύνων, οι κίνδυνοι αυτοί παρουσιάζουν αρκετές προκλήσεις. Οι κίνδυνοι του Κυβερνοχώρου αποτελούν μία συνεχόμενη,αδιάκοπη,απροσδιόριστη και δύσκολο στην ποσοτικοποίηση της απειλής και σε αντίθεση με τους υπόλοιπους κινδύνους εκθέτουν τον οργανισμό σε πολύπλευρους τομείς χωρίς να οριοθετηθούν[22]. Πριν την ανάπτυξη και την εφαρμογή ενός ολοκληρωμένου πλαισίου διαχείρισης θα πρέπει να εξεταστούν τα χαρακτηριστικά αυτών των κινδύνων και τη σχέση που έχουν με τον ίδιο τον οργανισμό. Για καλύτερη κατανόηση και διαχείριση αυτών

[19] Στο άρθρο των Mukhopadhyay A., Saha, D.,Chakrabarti, B., Mahanti, A. and Podder, A., Insurance for Cyber-risk: A Utility Model, (*Decision*, 32 (1) , pp. 1-19 (2005))

[20] Στο άρθρο των Böhme, R. και Kataria, G., Models and measures for correlation in cyber-insurance, Workshop on Economics of Information Security (WEIS) (2006)

[21] Στο άρθρο των Basel Committee on Banking Supervision, Operational Risk: Supporting Document to the New Basel Capital Accord Document, Bank for International Settlements (2001)

[22] Στην έκθεση της Grant Thornton,Taking AIM at cyber risk (2018)

των κινδύνων είναι απαραίτητο η διάκριση και ταξινόμηση τους. Αποτελεί την πυξίδα προκειμένου να βοηθηθεί η διαδικασία διαχείρισης των κινδύνων .

Εικόνα 1: Πυξίδα Κυβερνοχώρου. (Πηγή: Η Ασφαλής πλοήγηση στο διαδίκτυο είναι υπόθεση όλων μας,3ο Συνέδριο για την Ασφαλή Πλοήγηση στο Διαδίκτυο (2014))

Η εταιρεία RSA Security,κατατάσσει τους κινδύνους του Κυβερνοχώρου, βάσει της πηγής προέλευσής τους και του σκοπού τους. Κατηγοριοποιούνται και εντοπίζονται οι εξής μορφές κινδύνων:

- Εσωτερικοί Κακόβουλοι (Internal Malicious): Σχετίζονται με εσκεμμένες πράξεις σαμποτάζ, κλοπής ή άλλων κακόβουλων δράσεων που διαπράττονται από υπαλλήλους του οργανισμού σε έμπιστα συνδεδεμένα μέρη του.
- Εσωτερικοί Ακούσιοι (Internal Unintentional): Αφορούν πράξεις που οδηγούν σε ζημιές ή απώλειες δεδομένων από τα πληροφοριακά συστήματα του οργανισμού, που οφείλονται σε ανθρώπινο λάθος των εργαζομένων και άλλων έμπιστων συνεργατών.
- Εξωτερικοί Κακόβουλοι (External Malicious): Πρόκειται για την πιο δημοφιλή μορφή κινδύνων στον κυβερνοχώρο. Αποτελούν οργανωμένες επιθέσεις,μη συνδεδεμένων με την εταιρεία,κυρίως εγκληματικών οργανώσεων και κυβερνοπειρατών.
- Εξωτερικοί Ακούσιοι (External Unintentional): Είναι κίνδυνοι παρόμοιοι με τους εσωτερικούς ακούσιους και προκαλούν απώλεια ή βλάβη στην επιχείρηση μη σκόπιμα[23].

Σύμφωνα με τους ερευνητές James Cebula,Mary Popeck και Lisa Young η ταξινόμηση των κινδύνων του Κυβερνοχώρου είναι δομημένη γύρω από την ιεραρχία τεσσάρων κύριων κατηγοριών-κλάσεων. Στην πρώτη κατηγορία εντάσσονται οι δράσεις των ατόμων ή έλλειψη δράσης και επηρεάζουν την ασφάλεια στον Κυβερνοχώρο. Στην δεύτερη κατηγορία περιλαμβάνονται οι τεχνολογικές αποτυχίες. Ακολουθούν οι αποτυχίες εσωτερικών διαδικασιών που επηρεάζουν την ικανότητα εφαρμογής,ελέγχου,διαχείρισης και

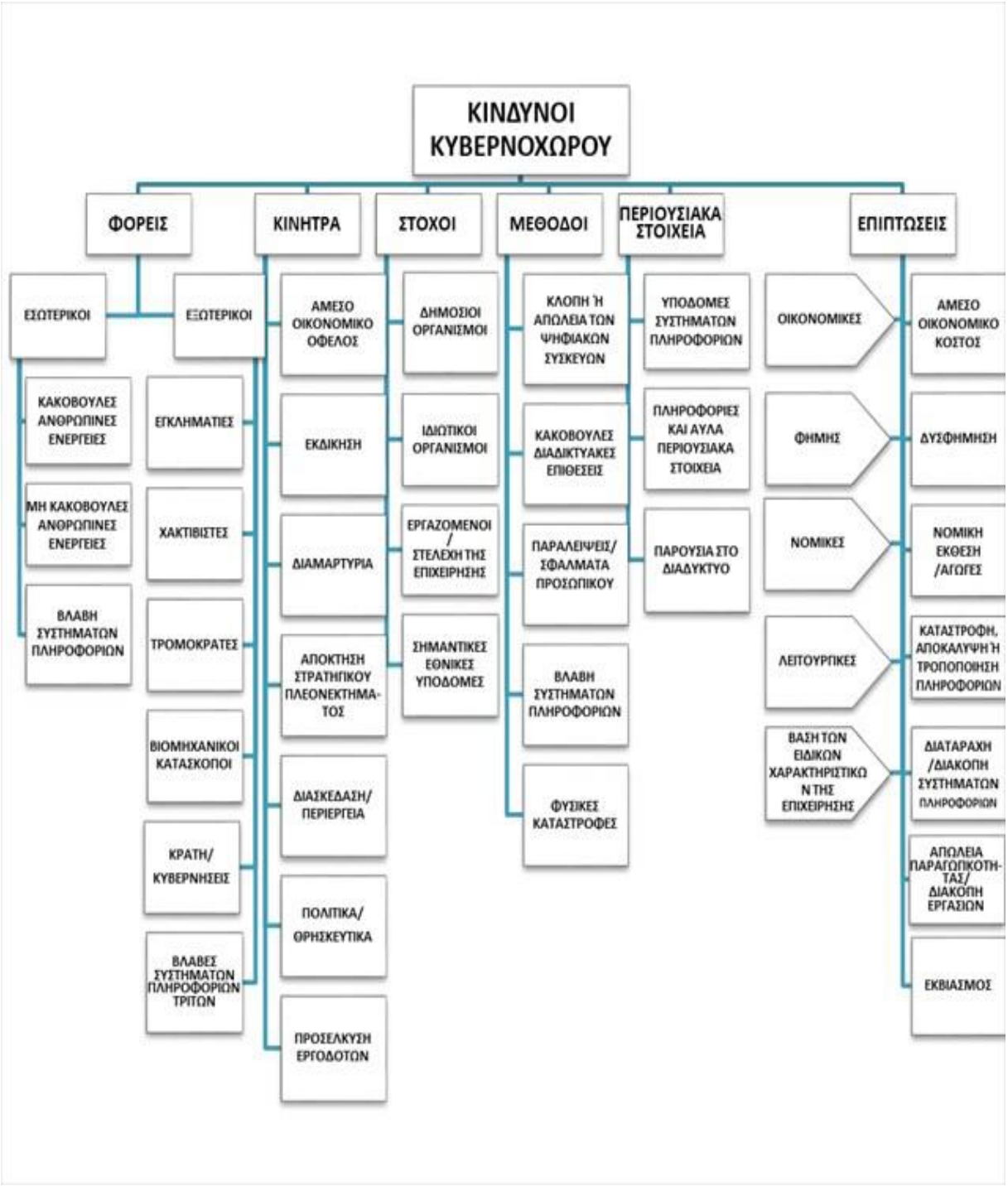
[23] Πληροφορίες αντλήθηκαν από την ιστοσελίδα της πολυεθνικής εταιρείας (www.rsa.com),που σχετίζεται σε θέματα διαχείρισης κινδύνου και κυβερνοασφάλειας

διατήρησης της ασφάλειας. Τέλος εντάσσονται τα εξωτερικά γεγονότα εκτός ελέγχου του οργανισμού. Κάθε μία από αυτές τις τέσσερις κλάσεις αποσυντίθεται περαιτέρω σε υποκατηγορίες και κάθε υποκατηγορία περιγράφεται από τα στοιχεία του. Η ταξινόμηση περιγράφεται ως εξής[24]:

Πίνακας 3: Προσέγγιση εξέτασης της δομής του Κυβερνοχώρου. (Πηγή: Ιδία επεξεργασία,βασισμένο σε κείμενο των James Cebula,Mary Popeck και Lisa Young,A Taxonomy of Operational Cyber Security Risks Version 2,(www.sei.cmu.edu) Carnegie Mellon University (2014))

Δράσεις Ατόμων	**Συστημάτων και Τεχνολογικών Αποτυχιών**	**Αποτυχημένων Εσωτερικών Διεργασιών**	**Εξωτερικά Γεγονότα**
Αθέλητα ▪ Λάθη ▪ Σφάλματα ▪ Παραλείψεις	**Υλικού** ▪ Χωρητικότητας ▪ Απόδοσης ▪ Συντήρησης ▪ Απαρχαίωσης	**Σχεδιασμός διαδικασίας/εκτέλεση** ▪ Ροής διεργασιών ▪ Διαδικασία τεκμηρίωσης ▪ Ρόλοι και ευθύνες ▪ Ειδοποιήσεις και προειδοποιήσεις ▪ Ροή πληροφοριών ▪ Εξέλιξη των θεμάτων ▪ Επίπεδο εξυπηρέτησης συμφωνιών ▪ Χειρισμός εργασιών	**Καταστροφές** ▪ Καιρικές συνθήκες ▪ Πυρκαγιά ▪ Πλημμύρες ▪ Σεισμός ▪ Κοινωνικοπολιτικές Αναταραχές ▪ Πανδημία
Σκόπιμα ▪ Απάτη ▪ Σαμποτάζ ▪ Κλοπή ▪ Βανδαλισμός	**Λογισμικού** ▪ Συμβατότητας ▪ Διαμόρφωσης διαχείρισης ▪ Ελέγχου αλλαγής ▪ Ρυθμίσεων ασφαλείας ▪ Πρακτικών κωδικοποίησης ▪ Δοκιμών	**Έλεγχοι διεργασιών** ▪ Παρακολούθηση καταστάσεων ▪ Μετρήσεις ▪ Περιοδική αναθεώρηση ▪ Ιδιοκτησία διαδικασίας	**Νομικά ζητήματα** ▪ Νομοθεσία ▪ Συμμόρφωση Κανονισμών ▪ Δικαστικές υποθέσεις
Αδράνειας ▪ Δεξιοτήτων ▪ Γνώσεων ▪ Καθοδήγησης ▪ Διαθεσιμότητας	**Συστημάτων** ▪ Σχεδιασμού ▪ Προδιαγραφών ▪ Ολοκλήρωσης ▪ Πολυπλοκότητας	**Υποστηρικτικές διαδικασίες** ▪ Προσωπικό ▪ Χρηματοδότηση ▪ Κατάρτιση και ανάπτυξη ▪ Προμήθειες	**Επιχειρηματικά ζητήματα** ▪ Αποτυχία προμηθευτή ▪ Συνθήκες αγοράς ▪ Οικονομικές συνθήκες
			Υπηρεσία εξαρτήσεις ▪ Βοηθητικά προγράμματα ▪ Υπηρεσίες Έκτακτης Ανάγκης ▪ Καύσιμα ▪ Μεταφορές

[24] Στο άρθρο των James Cebula,Mary Popeck και Lisa Young,A Taxonomy of Operational Cyber Security Risks Version 2,(www.sei.cmu.edu) Carnegie Mellon University (2014)



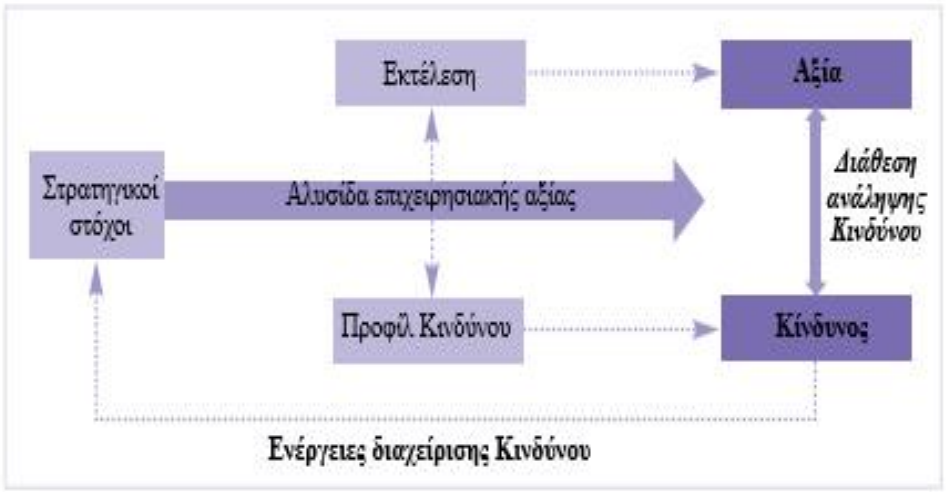
Διάγραμμα 10: Η ταξινόμηση των κινδύνων του Κυβερνοχώρου αποτελούμενη από έξι θεμελιώδεις πυλώνες-αρχές. (Πηγή: Livanis, Efstratios, Financial Aspects of Cyber Risks and Taxonomy for the Efficient Handling of These Risks (May 2016). Economic and Social Development (Book of Proceedings),14th International Scientific Conference on Economic and Social Development, Belgrade, Serbia (2016))

Σε μια παρόμοια,αλλά εκτενέστερη ανάλυση των κινδύνων,από τον καθηγητή Ευστράτιο Λιβάνη (2016) η ταξινόμηση των κινδύνων του Κυβερνοχώρου αποτελείται από έξι θεμελιώδεις αρχές. Ο πρώτος πυλώνας αναφέρεται στους φορείς των κινδύνων κυβερνοχώρου. Ο δεύτερος πυλώνας περιλαμβάνει τα ποικίλα και πολύπλευρα κίνητρα. Ο τρίτος πυλώνας αναφέρεται στους στόχους. Ο τέταρτος πυλώνας αφορά τους τρόπους με τους

οποίους θα μπορούσε να συμβεί ένα περιστατικό παραβίασης. Ο πέμπτος πυλώνας περιγράφει τα περιουσιακά στοιχεία που κινδυνεύουν. Ο έκτος πυλώνας περιλαμβάνει τις βασικές επιπτώσεις των κινδύνων κυβερνοχώρου. Η ανάλυση αυτών των πυλώνων περιγράφεται στο παρακάτω διάγραμμα.

3.3 Διαχείριση Κινδύνων Κυβερνοχώρου και η νέα πρόκληση για τους Διευθύνοντες Συμβούλους (CEO) και Οικονομικούς Διευθυντές (CFO)

Η σύγχρονη νοοτροπία διαχείρισης κινδύνου έχει ως σκοπό την αντιμετώπιση, την μέτρηση και την ανάλυση του κινδύνου που αντιμετωπίζει κάθε σύγχρονη επιχείρηση σε πρώτο βαθμό καθώς την οριοθέτηση το συνεπειών για τη βιωσιμότητα και την εξέλιξη οποιασδήποτε επιχείρησης. αφορά την ελεγχόμενη λήψη αποφάσεων και όχι την αποφυγή του κινδύνου μέσω της εξισορρόπησης του κινδύνου και της ανταμοιβής. Ο χαρακτηρισμός της θέσης που βρισκόμαστε καθορίζει την λήψη κάθε απόφασης. Αρχικά θα πρέπει να ορίσουμε τον τελικό στόχο στο συγκεκριμένο χρόνο καθώς και τις συνέπειες των ενεργειών που έχουν πραγματοποιηθεί θετικές ή αρνητικές. Πρέπει να μην ξεχνάμε ότι ο διαθέσιμος χρόνος για τη λήψη μιας απόφασης είναι περιορισμένο. Ο κίνδυνος και η αβεβαιότητα είναι οι κύριες διαστάσεις της επιχειρηματικότητας και τα επιτεύγματα τα οποία κατορθώνει κάθε επιχείρηση εξαρτώνται πάντοτε από τη διαχείριση των κρίσιμων καταστάσεων από τους αξιωματούχους. Στις επιχειρήσεις όπως και στον πόλεμο το βασικό δεν είναι μόνο να αποκρούσεις τα χτυπήματα αλλά να βρίσκει και από που προέρχονται. Να προλαμβάνεις και όχι να διαπιστώνεις.



Διάγραμμα 11: Μια μεθοδολογία των ενεργειών διαχείρισης του κινδύνο. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στο BUSINESS RISK A practical guide for board members,willis,pwc,chartis,airmic p.35 ,www.iod.com)

Μία απλή επαγωγική μέθοδος κάνοντας βήματα αντιμετώπισης κινδύνου γίνεται αρχικά με τον προσδιορισμό της μορφής και του κινήτρου,την μέτρηση του κινδύνου,τον προσδιορισμό των στόχων,των φορέων κινδύνου και τέλος την παρακολούθηση των αποτελεσμάτων διαχείρισης μέσω της διάθεσης ανάληψης κινδύνου και ανταμοιβής. Μία μεθοδολογία διαχείριση κινδύνου περιγράφεται στο παραπάνω διάγραμμα. Τελικός στόχος είναι η μείωση του κινδύνου και αύξηση της αξίας μέσω της επιχειρησιακής αλυσίδας και των στρατηγικών στόχων που τίθενται εξαρχής. Πρέπει να σημειωθεί μεταξύ άλλων το κενό που υπάρχει μεταξύ της ανησυχίας για τις απειλές στον κυβερνοχώρο και της προσέγγισής τους. Η έλλειψη χρόνου των ανώτερων στελεχών στο να επικεντρωθούν στους κινδύνους του Κυβερνοχώρου δημιουργεί ανησυχία, την ίδια στιγμή που οι απειλές στον κυβερνοχώρο βρίσκονται στο υψηλότερο σημείο όλων των εποχών και η εμπιστοσύνη στην ικανότητα ενός οργανισμού να τις διαχειρίζεται έχει μειωθεί. Σύμφωνα με την έρευνα των εταιρειών Marsh και Microsoft, σχεδόν το (80%) των οργανισμών κατατάσσει τον κίνδυνο στον κυβερνοχώρο ως μία από τις 5 σημαντικότερες ανησυχίες τους, σε σύγκριση με το (62%) το 2017,ενώ μόνο το (11%) εξέφρασε υψηλό βαθμό εμπιστοσύνης στην ικανότητά εκτίμησης και αποτροπής των επιθέσεων στον Κυβερνοχώρο αποτελεσματικά. Τα δύο τρίτα των ερωτηθέντων οργανισμών (65%) προσδιόρισαν ανώτατο στέλεχος ή το διοικητικό συμβούλιο ως κύριο υπεύθυνο της διαχείρισης κινδύνων στον κυβερνοχώρο.Σημαντικότερο συμπέρασμα αποτελεί ότι μόνο το (17%) των στελεχών και των μελών του διοικητικού συμβουλίου δήλωσε ότι πέρασε περισσότερες από μερικές ημέρες κατά το προηγούμενο έτος εστιάζοντας στο θέμα της διαχείρισης των κινδύνων του κυβερνοχώρου ενώ περισσότερο από τους μισούς (51%) πέρασαν αρκετές ώρες ή λιγότερο[25]. Επομένως φαίνεται ότι οι ανώτατοι αξιωματούχοι και το διοικητικό συμβούλιο δεν εστιάζουν και δεν αφιερώνουν χρόνο στην αντιμετώπιση και στην πρόληψη των κινδύνων του κυβερνοχώρου.

Σήμερα ένα μέρος της αγοράς αλλά και της ακαδημαϊκής κοινότητας θεωρεί ότι η διαχείριση του κινδύνου αποτελεί υπόθεση του τμήματος πληροφορικής μιας επιχείρησης,του Διευθυντή Τεχνολογίας (CTO) και του Διευθυντή Πληροφοριών (CIO)[26],και σύμφωνα με τους καθηγητές Κωνσταντίνο Ζοπουνίδη και Ευστράτιο Λιβάνη (2018) σταδιακά διαφαίνεται ο καθοριστικός ρόλος των και των υπολοίπων αξιωματούχων στην ολιστική αντιμετώπιση αυτού του κινδύνου. Η εμπλοκή αυτών των υψηλόβαθμων στελεχών,του Διευθύνοντα Συμβούλου (CEO) και του Οικονομικού Διευθυντή (CFO),γίνεται ακόμα πιο επιβεβλημένη με την εφαρμογή πλέον του νέου ευρωπαϊκού κανονισμού περί προστασίας δεδομένων

[25] Στην έρευνα των Marsh και Microsoft,Global Cyber Risk Perception Survey (2019)

[26] Στο άρθρο τους Διαχείριση Κινδύνων Κυβερνοχώρου : Η νέα πρόκληση για τους Διευθύνοντες Συμβούλους και Οικονομικούς Διευθυντές (www.naftemporiki.gr/printStory/1363646)

προσωπικού χαρακτήρα (GDPR) καθώς η λανθασμένη διαχείριση κινδύνου Κυβερνοχώρου που μπορεί να θέσει σε κίνδυνο προσωπικά δεδομένα τα οποία διατηρεί μία επιχείρηση θα επιφέρει σημαντικές οικονομικές και όχι μόνο επιπτώσεις. Το Διοικητικό Συμβούλιο αν και διαδραματίζει βασικό ρόλο στην εποπτεία και στις δραστηριότητες διαχείρισης των κινδύνων οι περισσότερες δραστηριότητες διαχείρισης κινδύνου θα έπρεπε να αναλαμβάνονται από τον Διευθύνοντα Σύμβουλο όπου πρέπει να συντονίσει τους μεμονωμένους διευθυντές γραμμών και κατα συνεπεια τον εξειδικευμένο έλεγχο των τμημάτων, δεδομένου ότι το Διοικητικό Συμβούλιο έχει σχετικά περιορισμένους πόρους. Έτσι μετά από μία απλή και πρακτική ταξινόμηση τον κίνδυνο κυβερνοχώρου, σύμφωνα με πρόσφατες έρευνες και περιστατικά παραβίασης δεδομένων, προκύπτει η ενίσχυση της ικανότητας των οργανώσεων να αποσαφηνίσουν και να αντιμετωπίσουν αυτούς τους κινδύνους.

Στην έκθεση της Deloitte, σχετικά με την ορθή εκτίμηση και την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου, παρουσιάζονται δέκα καίριες ερωτήσεις όπου παρουσιάζονται παρακάτω έχοντας σχεδιαστεί για τον εντοπισμό των τρωτών σημείων και τις δυνατότητες βελτίωσης, τις οποίες καλούνται να απαντήσουν οι διοικούντες των οργανισμών προκειμένου να αξιολογήσουν τον βαθμό της ετοιμότητας των υπαλλήλων της επιχείρησής τους απέναντι στους κινδύνους του Κυβερνοχώρου και κεντρικός άξονας είναι η εκτίμηση κατά πόσον η επιχείρηση[27]:

- Είναι ασφαλής.
- Βρίσκεται σε συνεχή επαγρύπνηση.
- Διαθέτει ανθεκτικές δομές.

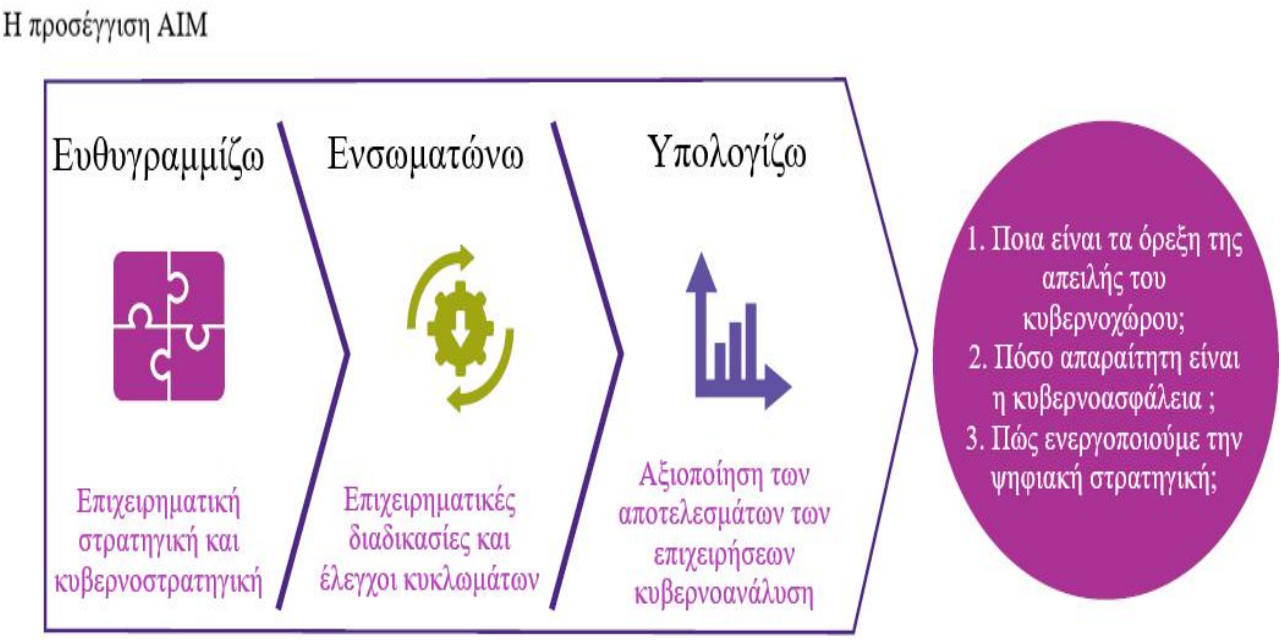
1.Αποδεικνύουμε τη δέουσα επιμέλεια ως προς την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου;
2.Έχουμε το σωστό ηγέτη και οργανωτικό ταλέντο,διαθέτει τις απαιτούμενες γνώσεις και την αντίστοιχη διορατικότητα προκειμένου να διαχειριστεί σωστά αυτούς τους κινδύνους;
3.Έχουμε καθιερώσει ένα κατάλληλο πλαίσιο κλιμάκωσης και προσδιορισμού των κινδύνων του Κυβερνοχώρου που συμπεριλαμβάνει αναλόγως του αντικτύπου τους για τον οργανισμό την όρεξη για ανάληψη κινδύνου αλλά και τα κατώτατα όρια υποβολής εκθέσεων;
4.Επικεντρωνόμαστε και επενδύουμε στα σωστά πράγματα και πώς θα το κάνουμε;

[27] Στην έκθεση της Deloitte.,Assessing Cyber Risk.Critical questions for the board and the C-suite (2016)

5.Ευθυγραμμίζεται το εταιρικό πρόγραμμα διαχείρισης και οι επιμέρους δυνατότητές μας με τα βιομηχανικά πρότυπα και τις αντίστοιχες επιχειρήσεις του ίδιου κλάδου;
6.Έχουμε μια εταιρική νοοτροπία προσανατολισμένη και ευαισθητοποιημένη έναντι των κινδύνων του κυβερνοχώρου;
7.Τι έχουμε πράξει για να προστατέψουμε τον οργανισμό από τους κινδύνους του κυβερνοχώρου από τρίτους;
8.Μπορούμε να περιορίσουμε γρήγορα τις ζημιές και να κινητοποιήσουμε τους πόρους απόκρισης όταν συμβαίνει μια επίθεση κατά των πληροφοριακών μας συστημάτων;
9.Πώς αξιολογούμε την αποτελεσματικότητα του προγράμματος διαχείρισης των κινδύνων του κυβερνοχώρου του οργανισμού μας;
10.Έχουμε μια ισχυρή και ασφαλή διασύνδεση στα ιδιαίτερα συνδεδεμένα οικοσυστήματα στα οποία λειτουργούμε;

Η Grant Thornton LLP έχει αναπτύξει ένα πλαίσιο για να βοηθήσει στον καθορισμό των παραγόντων διαχείρισης του κινδύνου στον κυβερνοχώρο,στοιχείων ενός προγράμματος και των αναμενόμενων αποτελεσμάτων,ώστε να αναλυθούν στο πλαίσιο της βιομηχανίας και των επιχειρήσεων του οργανισμού. Η ιεράρχηση των προτεραιοτήτων που παρουσιάζει η Grant Thornton LLP από ένα ισορροπημένο συντονισμό καλύπτει οι σημαντικότερες επείγουσες ανάγκες προσεγγίζοντας της διαχείρισης του κυβερνοχώρου επιτρέποντας στη διοίκηση την τοποθέτηση των κινδύνων του κυβερνοχώρου σε ένα στρατηγικό πλαίσιο και συνδέει έπειτα με την ανάπτυξη και την απόδοση των στρατηγικών διαχείρισης καθώς και με τον εξορθολογισμό κρατικών και δαπανών δίνοντας τη δυνατότητα στη διοίκηση να προχωρήσει πέρα από τις συγκεκριμένες λύσεις και να τις συνδέσει με τους στρατηγικούς στόχους και τη στάθμιση τους. Η AIM (Align,Integrate,Measure) προσέγγιση διαχείρισης στο πλαίσιο επιχειρησιακών και οικονομικών στόχων των κινδύνων του κυβερνοχώρου αναπτύσσεται γύρω από τρεις πυλώνες(μέτρο,ευθυγράμμιση και ενσωμάτωση). Η μέτρηση και αντιμετώπιση με οργανωμένο τρόπο των αποτελεσμάτων του κόστους και των αποδόσεων επιτρέποντας στη διοίκηση τον προσδιορισμό των απαιτούμενων πόρων. Η ευθυγράμμιση της διαχείρισης των κινδύνων με την επιχειρηματική στρατηγική εξασφαλίζοντας ότι η οργάνωση δέχεται μόνο κινδύνους που υποστηρίζουν τους στόχους των επιχειρήσεων και των επιδόσεων διευρύνοντας την ανάλυση αποφάσεων και στρατηγικών. Τέλος η ενσωμάτωση των ελέγχων στον κυβερνοχώρο έρχεται μέσω της ευθυγράμμισης με

τις επιχειρηματικές διαδικασίες επιτρέποντας εξασφαλίζοντας συγκεκριμένες λύσεις προσδιορίζοντας μετρήσεις συνεχής ευθυγράμμισης και αποτελεσματικότητας[28].



Διάγραμμα 12: Η AIM (Align,Integrate,Measure) προσέγγιση διαχείρισης στο πλαίσιο καθορισμού των παραγόντων διαχείρισης των κινδύνων του Κυβερνοχώρου. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση της Grant Thornton,Taking AIM at cyber risk (2018))

Διάγραμμα 13: Στάδια διαχείρισης των κινδύνων. (Πηγή: Ιδια επεξεργασία, βασισμένο σε διάγραμμα του Κηρυττόπουλου Κ.,Η διαχείριση κινδύνων έργων στην κατασκευαστική βιομηχανία (2006))

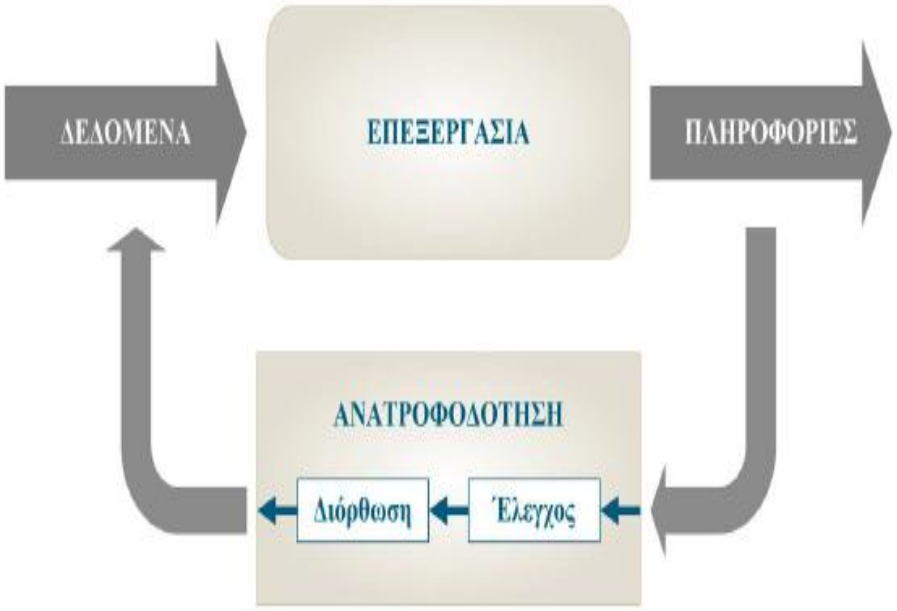
Από τη στιγμή που θα κατανοηθούν τα χαρακτηριστικά των κινδύνων Κυβερνοχώρου ο Διευθύνων Σύμβουλος(CEO) θα πρέπει να συντονίσει όλα τα τμήματα της επιχείρησης για την ανάπτυξη ενός ολοκληρωμένου πλαισίου διαχείρισης αυτών των κινδύνων ενώ από την

[28] Στην έκθεση της Grant Thornton,Taking AIM at cyber risk (2018)

άλλη ο Οικονομικός Διευθυντής(CFO) πρέπει να εστιάσει στη χρηματοοικονομική ανάλυση των κινδύνων Κυβερνοχώρου προσδιορίζοντας τις χρηματοοικονομικές επιπτώσεις τους, αξιολογώντας επενδύσεις σε όλους τους τομείς διαχείρισης και αντιμετώπισης (λογισμικό,υλικό,εξειδικευμένο ανθρώπινο δυναμικό σε θέματα ασφάλειας,πληροφοριακά και τηλεπικοινωνιακά συστήματα). Η ταξινόμηση,η αξιολόγηση των κινδύνων και η ανάπτυξη ενός στρατηγικού σχεδίου αποτελεσματικής διαχείρισης μπορεί να διευρύνει περαιτέρω την βέλτιστη σχετική δαπάνη για κάθε συνέπεια παραβίασης των δεδομένων, μειώνοντας τα κόστη και τις χρηματοοικονομικές επιπτώσεις για τον οργανισμό.

3.4 Πληροφοριακά Συστήματα και οι Κινδυνοι τους

Οι κίνδυνοι στον κυβερνοχώρο αντιπροσωπεύουν μια συνεχώς αυξανόμενη απειλή για τα δημόσια και ιδιωτικά ιδρύματα εξαιτίας των δυνητικά καταστροφικών επιπτώσεων στα οργανωτικά συστήματα πληροφόρησης και πληροφοριακών συστημάτων καθώς και του κινδύνου φήμης και πιθανής απώλειας εμπιστοσύνης καταναλωτών και εμπλεκομένων. Οι κίνδυνοι του Κυβερνοχώρου δεν πρέπει να ξεχνάμε ότι δεν αποτελούν πρόβλημα πληροφορικής αλλά επιχειρηματικό. Για αυτό και τα Πληροφοριακά Συστήματα αποτελούν ζωτικό σημείο των κινδύνων του κυβερνοχώρου διότι προέκυψαν ως γέφυρα μεταξύ των πρακτικών εφαρμογών της επιστήμης υπολογιστών και των επιχειρηματικών προκλήσεων.



Διάγραμμα 14: Πληροφοριακό σύστημα. (Πηγή: Θεόδωρος Μητάκος,Πληροφοριακά Συστήματα Διοίκησης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015))

Σύμφωνα με τον Δρ. Θεόδωρο Μητάκο ένα Πληροφοριακό Σύστημα είναι ένα σύστημα το οποίο δέχεται δεδομένα στις εισόδους του όπου επεξεργάζεται και παράγει πληροφορίες στις εξόδους του, με κάποιες από τις εξόδους του να ανατροφοδοτούνται ως είσοδοι[29]. Η διαδικασία αυτή παρουσιάζεται στο παρακάτω διάγραμμα.

Σύμφωνα με τον καθηγητή Robert Lucas Jr. Πληροφοριακό Σύστημα είναι ένα σύνολο οργανωμένων διαδικασιών που όταν εφαρμοστεί παρέχει πληροφορίες για υποστήριξη της λήψης αποφάσεων και του ελέγχου του οργανισμού[30]. Τα συστήματα πληροφοριών αποτελούν κοινωνικοτεχνικά και οργανωτικά συστήματα σχεδιασμένα να συλλέγουν,να επεξεργάζονται,να αποθηκεύουν και να διανέμουν πληροφορίες[31]. Οι επιχειρήσεις πλέον χρησιμοποιούν τα πληροφοριακά συστήματα για να παρακολουθούν τις διαδικασίες για να διασφαλίζουν την αποτελεσματικότητα και αποδοτικότητα τους. Τα συστήματα πληροφοριών απαρτίζονται από τέσσερα στοιχεία Εργασία,Άνθρωποι,Δομή και Τεχνολογία[32]:

Σύμφωνα με το μοντέλο των πέντε τμημάτων ένα πληροφοριακό σύστημα απαρτίζεται από[33]:

- Υλικό(hardware),αναφέρεται στην τεχνολογική υποδομή η οποία έχει φυσική υπόσταση.
- Λογισμικό(software),εννοούμε τα προγράμματα του υπολογιστή και τις εντολές πραγματοποίησης χρήσιμων εργασιών
- Άνθρωποι,οποίος άνθρωπος αλληλεπιδρά με το πληροφοριακό σύστημα είναι μέρος του
- Δεδομένα,αποτελούν τα πρωταρχικά στοιχεία από τα οποία παράγονται πληροφορίες έπειτα από επεξεργασία
- Διαδικασίες,το σύνολο των τρόπων με τους οποίους διεκπεραιώνονται οι λειτουργίας που εκτελεί το πληροφορικό σύστημα

* Μερικοί θεωρούν το δίκτυο ως ένα επιπλέον ξεχωριστό τμήμα των πληροφοριακών συστημάτων το οποίο πλαισιώνει τα υπόλοιπα τμήματα.

---

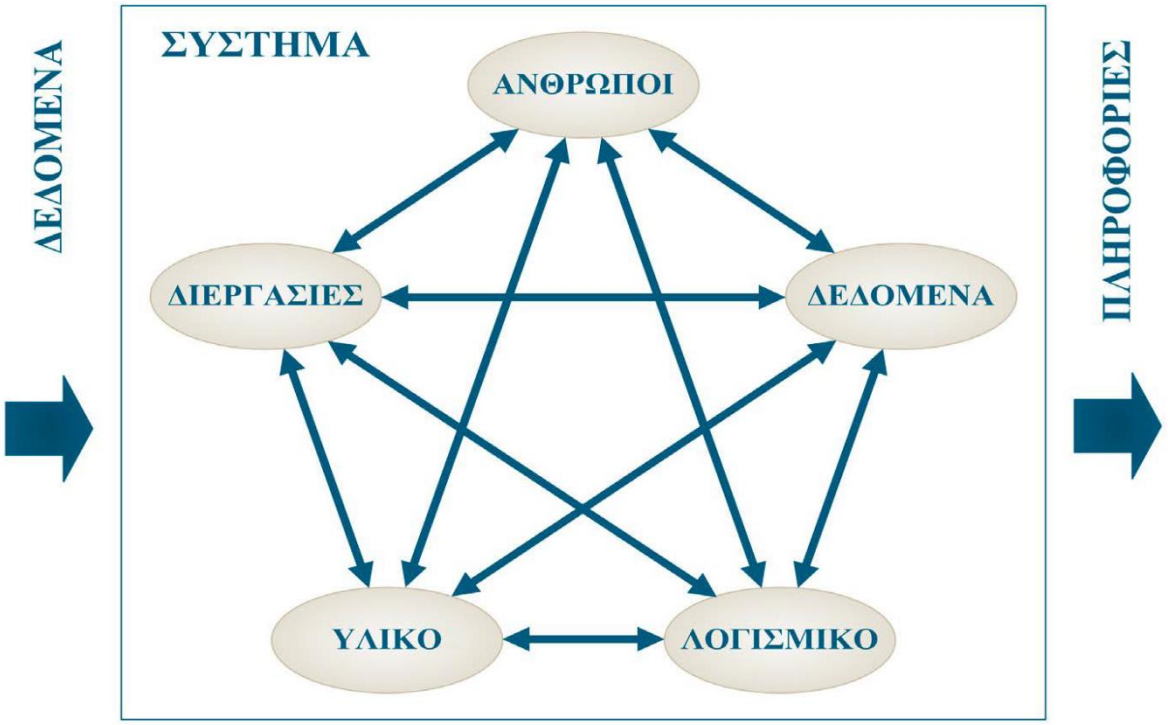
[29] Στο βιβλίο του Θεόδωρος Μητάκος,Πληροφοριακά Συστήματα Διοίκησης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015) p.27

[30] Στο άρθρο του Lucas, R.E. Jr.,Making a miracle,Econometrica, Vol. 61, No. 2, pp. 251-272(1993)

[31] Στο άρθρο των Piccoli Gabriele και Pigni Federico,Information systems for managers: with case Louisiana State University,Grenoble School of Management,Prospect Press (2018)

[32] Στο άρθρο των O'Hara Margaret; Watson Richard,Cavan Bruce,Managing the three levels of change,Information Systems Management. 16 (3) (1999)

[33] Στο βιβλίο του Θεόδωρος Μητάκος,Πληροφοριακά Συστήματα Διοίκησης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015) p.37-39



Διάγραμμα 15: Πληροφοριακό Σύστημα ως μοντέλο πέντε τμημάτων. (Πηγή: Θεόδωρος Μητάκος,Πληροφοριακά Συστήματα Διοίκησης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015))

Σύμφωνα με τους καθηγητές Δημήτριο Γκίνογλου,Παναγιώτη Ταχυνάκη και Νικολάου Πρωτόγερο τα Πληροφοριακά Συστήματα μπορούν να ταξινομηθούν με διάφορους τρόπους. Με βάση τον τρόπο επεξεργασίας[34]:

- Συστήματα επεξεργασίας κατά δεσμίδες (batch),οι συναλλαγές συγκεντρώνονται και η επεξεργασία τους γίνεται σε δεσμίδες περιοδικά.
- Συστήματα επεξεργασίας κατά δεσμίδες σε απευθείας σύνδεση (on line batch),οι πληροφορίες των συναλλαγών συλλέγονται σε απευθείας σύνδεση, αλλά υποβάλλονται σε επεξεργασία περιοδικά, κατά δεσμίδες.
- Συστήματα σε απευθείας σύνδεση πραγματικού χρόνου (on line real time),η συλλογή και η επεξεργασία των δεδομένων των συναλλαγών γίνονται σε πραγματικό χρόνο.

Με βάση το στόχο[35]:

- Συστήματα επεξεργασίας συναλλαγών (Transaction Processing Systems- TPS),στόχος αποτελεί η επεξεργασία των συναλλαγών προκειμένου να ενημερωθούν τα αρχεία της επιχείρησης.

[34] Στο βιβλίο των Γκίνογλου Δημήτριος,Ταχυνάκης Παναγιώτης, Πρωτόγερος Νικόλαος,Λογιστικά Πληροφοριακά Συστήματα Μηχανογραφημένη Λογιστική, Εκδόσεις Rosili (2004)

[35] Στο βιβλίο των Γκίνογλου Δημήτριος,Ταχυνάκης Παναγιώτης, Πρωτόγερος Νικόλαος,Λογιστικά Πληροφοριακά Συστήματα Μηχανογραφημένη Λογιστική, Εκδόσεις Rosili (2004)

- Συστήματα στήριξης αποφάσεων (Decision Support Systems-DSS),στόχος είναι η υποστήριξη των διευθυντικών αποφάσεων και στηρίζονται κυρίως σε μοντέλα λήψης αποφάσεων διοικητικής και τη χρηματοοικονομικής στρατηγικής .
- Εμπειρογνώμονα συστήματα (Expert Systems),αποτελούν την υποστήριξη των διευθυντικών στελεχών στη διάγνωση και επίλυση προβλημάτων ενσωματώνοντας την πείρα στον οικονομικό τομέα.

Τα Πληροφοριακά Συστήματα σχετίζονται με τα συστήματα διαχείρισης βάσης δεδομένων και με τα συστήματα δραστηριότητας από την άλλη. Αποτελούν μορφή συστήματος επικοινωνίας όπου τα δεδομένα αντιπροσωπεύουν και επεξεργάζονται ως μορφή κοινωνικής μνήμης και μπορούν να θεωρηθούν επίσης ημι-τυπική γλώσσα που υποστηρίζει στη λήψη αποφάσεων αποτελώντας το κύριο αντικείμενο μελέτης για την οργανωτική πληροφορική[36].

Διάγραμμα 16: Μια ιεραρχία τεσσάρων επιπέδων των Πληροφοριακών Συστημάτων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στο άρθρο των Laudon, K.C. και Laudon, J.P. Management Information Systems, (2nd edition), Macmillan, 1988)

Οι κυριότεροι τύποι πληροφοριακών συστημάτων,που χρησιμοποιούνται σήμερα από τις επιχειρήσεις,είναι:

[36] Στο άρθρο του Beynon-Davies P.,Business Information Systems,Palgrave Basingstoke (2009)

- Συστήματα Επεξεργασίας Συναλλαγών(TPS)
- Πληροφοριακά Συστήματα Διοίκησης(MIS)
- Συστήματα Υποστήριξης Αποφάσεων(DSS)
- Συστήματα Υποστήριξης(ESS)
- Γεωγραφικά Πληροφοριακά Συστήματα(GIS)
- Επιχειρησιακά Συστήματα Σχεδιασμού Ενδοεπιχειρησιακών Πόρων(ERP)

Η χρήση της τεχνολογίας και των συστημάτων στη σύγχρονη επιχειρηματική πραγματικότητα εκτός από τα τεράστια πλεονεκτήματα εγκυμονεί και ένα σύνολο κινδύνων που απειλούν τη λειτουργία και τη βιωσιμότητα της. Ασφάλεια Πληροφοριακών Συστημάτων είναι το οργανωμένο πλαίσιο εννοιών,αντιλήψεων,αρχών,πολιτικών,διαδικασιών,τεχνικών και μέτρων που απαιτούνται για να προστατευθούν τα στοιχεία και το σύστημα ολόκληρο από κάθε σκόπιμη ή τυχαία απειλή[37]. Οι κρισιμότεροι παράγοντες κινδύνου είναι:

- Ανθρώπινη συμπεριφορά.
- Δυσλειτουργία Πληροφοριακών Συστημάτων εξοπλισμού.
- Απόκλιση από τους κανόνες λειτουργίας.
- Ανεπαρκής στρατηγικός σχεδιασμός εξωτερικών επιδράσεων.
- Μη αποδοτική αξιοποίηση πόρων της επιχείρησης,υλικών και άυλων.

Μπορούμε να κατηγοριοποιήσουμε τους κινδύνους στις ακόλουθες κατηγορίες:
- Επιχειρησιακούς (business risks)
- Ελεγκτικούς (audit risks)
- Ασφαλείας (security risks)
- Συνέχειας (continuity risks)

[37] Στο βιβλίο του Ευάγγελος Κιουντούζης: Μεθοδολογίες Ανάλυσης & Σχεδιασμού Πληροφοριακών Συστημάτων, Εκδόσεις Ε. Μπένου, Γ΄Έκδοση (2009)

ΚΕΦΑΛΑΙΟ 4 ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ

4.1 Οικονομικός αντίκτυπος κινδύνων Κυβερνοχώρου

Ο κίνδυνος επιθέσεων στον Κυβερνοχώρο αυξάνεται τακτικά στη συχνότητα και τον κίνδυνο. Κάθε μέρα, φαίνεται ότι υπάρχει και ένα άλλο ειδησεογραφικό άρθρο σχετικά με την επόμενη επίθεση, η οποία προκαλεί μεγάλη ανησυχία σε μεγάλους και μικρούς οικονομικούς οργανισμούς. Ωστόσο, η ασφάλεια στον κυβερνοχώρο συνολικά εξακολουθεί να υπολείπεται από πολλές οργανώσεις. Οι απειλές στον Κυβερνοχώρο είναι μια μεγάλη υπόθεση. Οι επιθέσεις στον κυβερνοχώρο μπορούν να προκαλέσουν ηλεκτρικές διακοπές,αποτυχία του στρατιωτικού εξοπλισμού μέχρι και παραβιάσεις μυστικών εθνικής ασφάλειας. Μπορούν να οδηγήσουν στην κλοπή πολύτιμων,ευαίσθητων δεδομένων,όπως τα ιατρικά αρχεία. Μπορούν να διαταράξουν τα δίκτυα τηλεφώνου και υπολογιστών ή να παραλύσουν τα συστήματα, καθιστώντας τα δεδομένα μη διαθέσιμα. Δεν είναι υπερβολή να πούμε ότι οι απειλές στον κυβερνοχώρο μπορεί να επηρεάσουν τη λειτουργία της ζωής όπως την ξέρουμε[38].

Οι περισσότερες εταιρείες που χρησιμοποιούν τα Πληροφοριακά Συστήματα και η επιμέρους οργάνωση τους έχει να κάνει με τον Κυβερνοχώρο και την απειλή της παραβίασης των δεδομένων τους που αφορούν,τα προσωπικά στοιχεία των πελατών και των εργαζομένων τους. Οι καταστάσεις αυτές,γίνονται ολοένα και πιο συχνές,με αποτέλεσμα οι εταιρείες να πρέπει να υποστούν μεγάλες δαπάνες. Πολλές φορές τα περιστατικά παραβίασης των δεδομένων επηρεάζουν αρνητικά την κερδοφορία της επιχείρησης. Το άμεσο κόστος που θα προκύψει στην επιχείρηση λόγω της ελλιπούς ασφάλειας των δεδομένων της,σχετίζεται με αποζημιώσεις λόγω της διαρροής των δεδομένων και με έμμεσες οικονομικές απώλειες όπως για παράδειγμα την μείωση των πωλήσεων και επαγωγικά την μείωση του μεριδίου της αγοράς. Επιπρόσθετες έμμεσες δαπάνες μπορούν να χαρακτηριστούν η δυσφήμιση της επιχείρησης από την απώλεια της εμπιστοσύνης των πελατών της για την διασφάλιση των προσωπικών τους δεδομένων,η αύξηση του κόστους λειτουργίας για την υιοθέτηση νέων συστημάτων ασφαλείας αλλά και να βρίσκονται σε θέση να τα εφαρμόσουν με συνέπεια με ότι κόστος αυτό συνεπάγεται και να μετριάσουν τον αντίκτυπο των επιθέσεων που πραγματοποιούνται στον Κυβερνοχώρο. Από όλα τα παραπάνω

[38]Πληροφορίες αντλήθηκαν από την ιστοσελίδα https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

μπορούμε εύκολα να συμπεράνουμε ότι οι ηλεκτρονικοί και διαδικτυακοί κίνδυνοι έχουν αρνητική επίδραση σε σχέση με την αγορά και τη διαμόρφωση της χρηματιστηριακής αξίας της μετοχής στην επιχείρηση που πλήττεται. Επίσης, σύμφωνα με έρευνα που έχει πραγματοποιηθεί προκύπτει ότι οι παραβιάσεις στον Κυβερνοχώρο είναι μεγαλύτερες από τις παραβιάσεις που προκαλούνται από τη δυσλειτουργία του συστήματος και τους ανθρώπινους παράγοντες.

4.2 Προσδιορισμός του Κόστους

Εκτίμηση του κόστους ενός διαδικτυακού κινδύνου σχετίζεται με τον ακριβή προσδιορισμό των μεταβλητών που συνθέτουν την εξίσωση του κινδύνου ώστε να παρέχει μια σταθερή βάση για την καθοδήγηση όλων των αποφάσεων για τη διαχείριση αυτού του κινδύνου.
Το οικονομικό κόστος μίας κυβερνοεπίθεσης αναλογεί στις οικονομικές απώλειες μιας μεγάλης φυσικής καταστροφής και το κόστος αυτό μπορεί να φτάσει στο ποσό των 53δις δολαρίων σύμφωνα με μία έκθεση της Lloyd'sofLondon. Η έρευνα αυτή εξετάζει τις δυνητικές οικονομικές ζημιές από την υποθετική επίθεση χάκερς σε έναν πάροχο υπηρεσιών could και τις κυβερνοεπιθέσεις σε λειτουργικά συστήματα που διαθέτουν παγκόσμιοι κολοσσοί. Το οικονομικό κόστος μιας υποθετικής επίθεσης σε πάροχο υπηρεσιών cloud ξεπερνά κατά πολύ τα 8 δισ. δολάρια που κόστισε παγκοσμίως η επίθεση «wannacry» τον περασμένο Μάιο, η οποία επηρέασε πάνω από 100 χώρες, σύμφωνα με την Cyence. Το οικονομικό κόστος συνήθως αφορά στη διακοπή των δραστηριοτήτων και στην επιδιόρθωση βλαβών στους υπολογιστές.«Επειδή οτιδήποτε σχετίζεται με το διαδίκτυο είναι εικονικό, είναι πολύ δύσκολο να κατανοήσουμε τι ακριβώς θα γίνει σε ένα μεγάλο συμβάν», δήλωσε στο Reuters η διευθύνουσα σύμβουλος της Lloyd'sofLondon, IngaBeale[39].
Παρακάτω παρουσιάζονται τρεις από τους λόγους που μοιράζονται και εξηγούν γιατί οι υπεύθυνοι λήψης αποφάσεων εντός των οργανισμών συχνά δεν λαμβάνουν σοβαρά την ασφάλεια στον Κυβερνοχώρο.

4.3 Λόγοι που δεν επενδύονται ποσά στην προστασία κυβερνοαπειλής

Κάποια στελέχη θεωρούν ότι η ασφάλεια στον Κυβερνοχώρο είναι ένα είδος διαδικασίας οχύρωσης στην οποία ισχυρά τείχη προστασίας και έξυπνοι τρόποι αντιμετώπισης θα τους επιτρέψουν να δουν απειλές από μακριά. Επίσης,υποθέτουν ότι η συμμόρφωση με ένα πλαίσιο ασφαλείας όπως το NIST ή το FISMA είναι επαρκής ασφάλεια. Ένας ακόμα λόγος

[39] Πληροφορίες αντλήθηκαν από την ιστοσελίδα http://insuranceinnovation.gr/forum/lloyds-sta-53-dis-to-kostos-mias-pagkosmias-kyvernoepithesis/ | Insurance Innovation

είναι ότι οι επιχειρήσεις αυτές δεν έχουν πρόσφατα παραβιάσει την ασφάλεια, οπότε αυτό που δεν φαίνεται να σπάει δεν χρειάζεται να διορθωθεί. Σύμφωνα με τον Blau, το πρόβλημα με αυτά τα νοητικά μοντέλα είναι ότι αντιμετωπίζουν την ασφάλεια στον Κυβερνοχώρο ως πεπερασμένο πρόβλημα που μπορεί να λυθεί παρά ως η συνεχιζόμενη διαδικασία που συμβαίνει. Για όλους τους παραπάνω λόγους προτείνεται ότι οι προσπάθειες στον τομέα της ασφάλειας στον Κυβερνοχώρο πρέπει να επικεντρωθούν στη διαχείριση κινδύνου αντί για τον μετριασμό του. Κάθε οργανισμός χρειάζεται ένα συνεχιζόμενο σχέδιο για να προστατεύσει από την πιθανότητα επιθέσεων στον κυβερνοχώρο,οι οποίες μπορεί να κοστίζουν εκατομμύρια και ακόμη να σταματήσουν τη λειτουργία της επιχείρησης[40].

4.4 Διαχείριση Οικονομικών Επιπτώσεων

Οι απειλές γίνονται όλο και πιο σοβαρές. Ο Gartner εξηγεί πως οι κίνδυνοι στον κυβερνοχώρο διασκορπίζονται σε κάθε οργανισμό και δεν είναι πάντοτε υπό τον άμεσο έλεγχο της πληροφορικής. Οι ηγέτες των επιχειρήσεων προχωρούν με τις ψηφιακές επιχειρηματικές πρωτοβουλίες τους και οι ηγέτες αυτοί κάνουν καθημερινά επιλογές κινδύνου που σχετίζονται με την τεχνολογία. Ο αυξημένος κίνδυνος στον κυβερνοχώρο είναι πραγματικός - αλλά και οι λύσεις ασφάλειας δεδομένων.

Συμφώνα με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και των Πληροφοριών (ENISA ,European Union Agency for Network and Information Security), το κόστος της εγκληματικότητας στον κυβερνοχώρο μπορεί να φτάσει ετησίως τα 15 εκατομμύρια ευρώ ανά επιχείρηση. Πιο αναλυτικά το Ηνωμένο Βασίλειο ήταν η πιο μελετημένη χώρα στην ΕΕ. Σύμφωνα με μία μελέτη, οι απώλειες των επιχειρήσεων του Ηνωμένου Βασιλείου φτάνουν τα 37 δισεκατομμύρια ευρώ ετησίως (27 δισεκατομμύρια λίρες Αγγλίας). Συγκριτικά, αυτό ήταν περίπου η επένδυση της Ευρωπαϊκής Επιτροπής στην καινοτομία, την έρευνα και την ανάπτυξη κατά τη διάρκεια μιας τριετούς περιόδου για το σύνολο του προγράμματος H2020. Μια άλλη μελέτη υπογραμμίζει ότι ο οικονομικός αντίκτυπος μπορεί να κυμαίνεται μεταξύ 1,01 και 26,19 εκατομμύρια ευρώ ετήσιο κόστος ανά εταιρεία. Επίσης, αναφέρεται το κόστος από 104.000 ευρώ σε 4,35 εκατομμύρια ευρώ ανά επηρεαζόμενη εταιρεία. Η Γερμανία βρίσκεται επίσης στο επίκεντρο μιας από τις μελέτες με απώλειες που κυμαίνονται από 425.000 έως 20 εκατομμύρια ευρώ ανά εταιρεία ετησίως. Η Γαλλία πλήττεται επίσης από ζημίες από οικονομικές επιπτώσεις από 445.000 έως 18,9 εκατομμύρια ευρώ ανά εταιρεία ετησίως[41].

[40]Πληροφορίες αντλήθηκαν από την ιστοσελίδα https://innovationatwork.ieee.org/cyber-security-cyber-attack/

[41]Στην ENISA, (2016), The cost of incidents affecting CIIs Systematic review of studies concerning the economic impact of cyber-security incidents

4.5 Κόστος χρήσης Ασφαλιστικών προϊόντων

Πολλές επιχειρήσεις, ιδίως μικρομεσαίες, δεν έχουν συναίσθηση της έκθεσής τους στον κυβερνοκίνδυνο, παρότι όλες σχεδόν οι εταιρείες, ανεξαρτήτως μεγέθους και κλάδου, ανεξάρτητα από το είδος των δεδομένων που αποθηκεύουν, είναι ευάλωτες τόσο σε κακόβουλες επιθέσεις όσο και σε δυσλειτουργίες των συστημάτων τους. Ακόμη και οι εταιρείες που έχουν συναίσθηση της απειλής δεν θεωρούν τη θωράκισή τους έναντι του κυβερνοκινδύνου προτεραιότητα, ώστε να εξετάσουν το ενδεχόμενο μεταβίβασης του ρίσκου μέσω της ασφάλισης.

Οι ασφαλιστικές ενώσεις σε πολλές χώρες της Ευρωπαϊκής ‘Ενωσης συνεργάζονται στενά με τις κυβερνήσεις τους για να ευαισθητοποιήσουν τις επιχειρήσεις απέναντι στον κυβερνοκίνδυνο. ΄Ενα παράδειγμα αποτελεί η Ένωση Βρετανικών Ασφαλιστικών Εταιρειών, η οποία εξέδωσε πρόσφατα δωρεάν οδηγό, για να βοηθήσει τις μικρομεσαίες επιχειρήσεις να αξιολογήσουν τις ανάγκες τους αναφορικά με την προστασία τους έναντι του κυβερνοκινδύνου. Η αύξηση των προγραμμάτων κυβερνοασφάλισης, εξάλλου, είναι ιδιαίτερα σημαντική για συγκεκριμένους κλάδους, που αφορούν ζωτικής σημασίας υποδομές και παρουσιάζονται ιδιαίτερα ευάλωτοι στις κυβερνοεπιθέσεις.

Οι ασφαλιστικές εταιρείες μπορούν να βοηθήσουν τους πελάτες τους να επιτύχουν το υψηλότερο δυνατό επίπεδο κυβερνοανθεκτικότητας,όχι μόνο προσφέροντας πολύτιμα εργαλεία μεταβίβασης του σχετικού κινδύνου μέσω των σχετικών καλύψεων,αλλά και αξιοποιώντας την τεράστια εμπειρία τους στη διαχείριση κινδύνων για να βοηθήσουν τους πελάτες τους μέσω ελέγχων ασφαλείας ή της χρήσης πιστοποιήσεων από τρίτα μέρη[42].

Μια κυβερνοεπίθεση μπορεί να δημιουργήσει περιορισμούς πρόσβασης σε διαδικτυακές υπηρεσίες μιας εταιρείας ακόμα και ολική έλλειψη διαθεσιμότητάς τους ή και απώλεια εμπιστευτικών πληροφοριών. Οι ασφαλιστικές εταιρείες για την προστασία των εταιρειών στην διαφύλαξη των ευαίσθητων δεδομένων προσφέρουν πακέτα υπηρεσιών που καλύπτουν τα έξοδα διαχείρισης της κρίσης που προκαλεί μία παραβίαση του Κυβερνοχώρου. Εξαιτίας της ευρείας γκάμας και της πολυπλοκότητας των κυβερνοκινδύνων, δεν υπάρχει κάποιο τυποποιημένο ασφαλιστικό προϊόν για τις απώλειες που προκύπτουν από κυβερνοεπιθέσεις. Τα έξοδα αυτά μπορούν να αφορούν έξοδα για την πρόσληψη εξειδικευμένων ερευνητών ασφαλείας,έξοδα για την ενημέρωση πελατών,έξοδα δημοσίων σχέσεων και διαχείρισης κρίσης,νομικά έξοδα για τη διαχείριση των κανονιστικών απαιτήσεων,έξοδα νομικών

on critical information infrastructures (CII).

[42] Πληροφορίες αντλήθηκαν από την ιστοσελίδα https://insuranceworld.gr/38069/eidiseis/asfalistikes-eidiseis/psifiopiisi-digitalization-ke-asfalistiki-agora/

συμβουλών. Τα ασφαλιστικά πακέτα κάλυψης αφορούν και την αστική ευθύνη του ασφαλισμένου στην περίπτωση που ασκηθεί αγωγή κατά του ασφαλισμένου για ζημία που μπορούν να υποστούν οι πελάτες του λόγω περιστατικών παραβιάσεων ηλεκτρονικών συστημάτων και διαρροής προσωπικών τους δεδομένων και την απώλεια κερδών.

Η ευρωπαϊκή προσέγγιση της συγκεκριμένης αγοράς είναι περισσότερο συνδεδεμένη με την απώλεια κερδών μιας επιχείρησης σε περίπτωση διακοπής εργασιών λόγω στοχευμένων επιθέσεων άρνησης υπηρεσίας (ddos). Αρχικά, τα πρώτα ασφαλιστικά προϊόντα που δημιουργήθηκαν κάλυπταν μόνο τις χρηματοοικονομικές ανάγκες των εταιριών σε περίπτωση παραβίασης συστημάτων και διαρροής δεδομένων. Στην συνέχεια, λαμβάνοντας υπόψη τις ανάγκες των εταιριών πελατών δημιουργήθηκαν νέα ασφαλιστικά καινοτόμα προϊόντα τα οποία ενσωμάτωσαν υπηρεσίες διαχείρισης συμβάντων σε συνεργασία με πάροχους υπηρεσιών ψηφιακής εγκληματολογίας,νομικούς, επικοινωνιολόγους με σκοπό την αποτελεσματικότερη διαχείριση των συμβάντων και την μείωση των συνεπειών στην εταιρική φήμη. Το κόστος των ασφαλιστικών προϊόντων αποτελεί μία συνάρτηση διάφορων παραγόντων:

- Η δραστηριότητα της εταιρείας.
- Το μέγεθος των εσόδων της εταιρείας.
- Ο όγκος και ο τύπος των δεδομένων.
- Η εξάπλωση της εταιρείας διεθνώς.
- Η προηγούμενη εμπειρία σε περιπτώσεις παραβιάσεων.
- Ο ανταγωνισμός.
- Ο ασφαλισμένος κίνδυνος και η αξιολόγηση του από τις ασφαλιστικές εταιρείες.
- Το ύψος των ασφαλιστικών κεφαλαίων.
- Τα μέτρα προστασίας που έχουν ληφθεί.

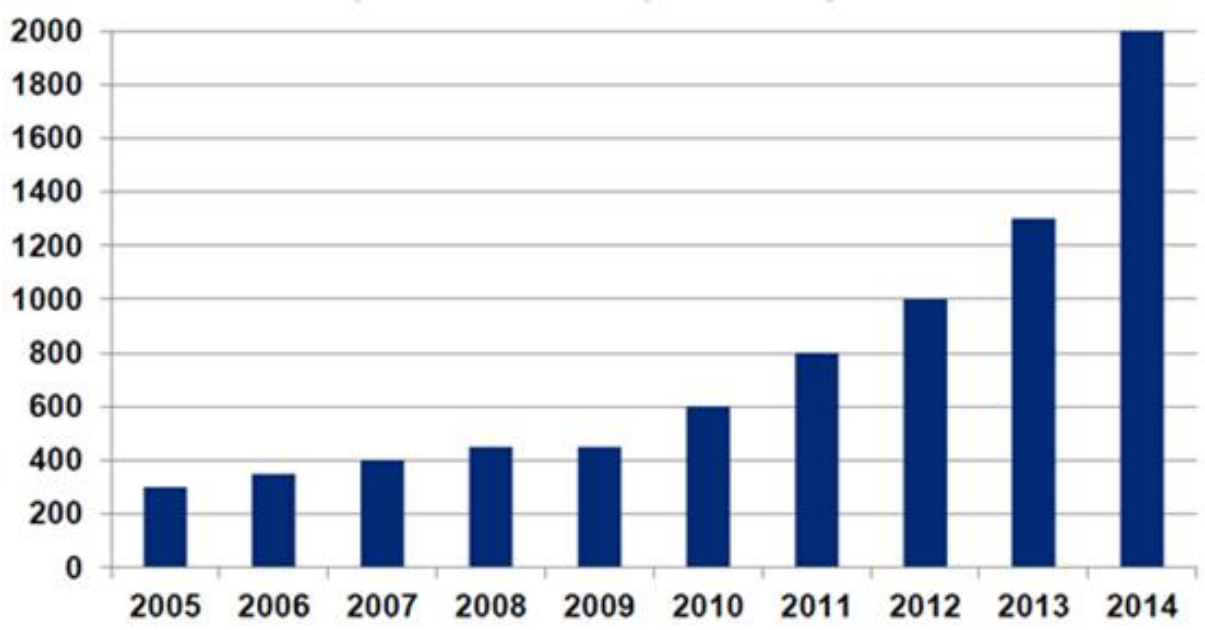
Πιο αναλυτικά οι ασφαλιστικές εταιρείες μέσω της θέσπισης του GDPR προσφέρουν πακέτα κάλυψης για τα παρακάτω θέματα:

- Cybercrime: Η ασφάλιση καλύπτει έξοδα διαχείρισης περιστατικών κοινωνικής μηχανικής τα οποία οδηγούν σε αποστολή χρημάτων σε κυβερνοεγκληματίες, εκβιασμού στον κυβερνοχώρο, επιθέσεις κακόβουλου λογισμικού (ransomware) και άσκοπη χρήση των υπολογιστικών συστημάτων της ασφαλισμένης εταιρίας .
- Reputational Harm: Καλύπτεται η απώλεια εταιρικών κερδών λόγω απώλειας πελατών από περιστατικά παραβίασης ασφάλειας. Για να υπολογισθεί αυτό το κόστος θα πρέπει να προσδιοριστεί από εγκληματολογικούς λογιστές το πλήθος των πελατών που

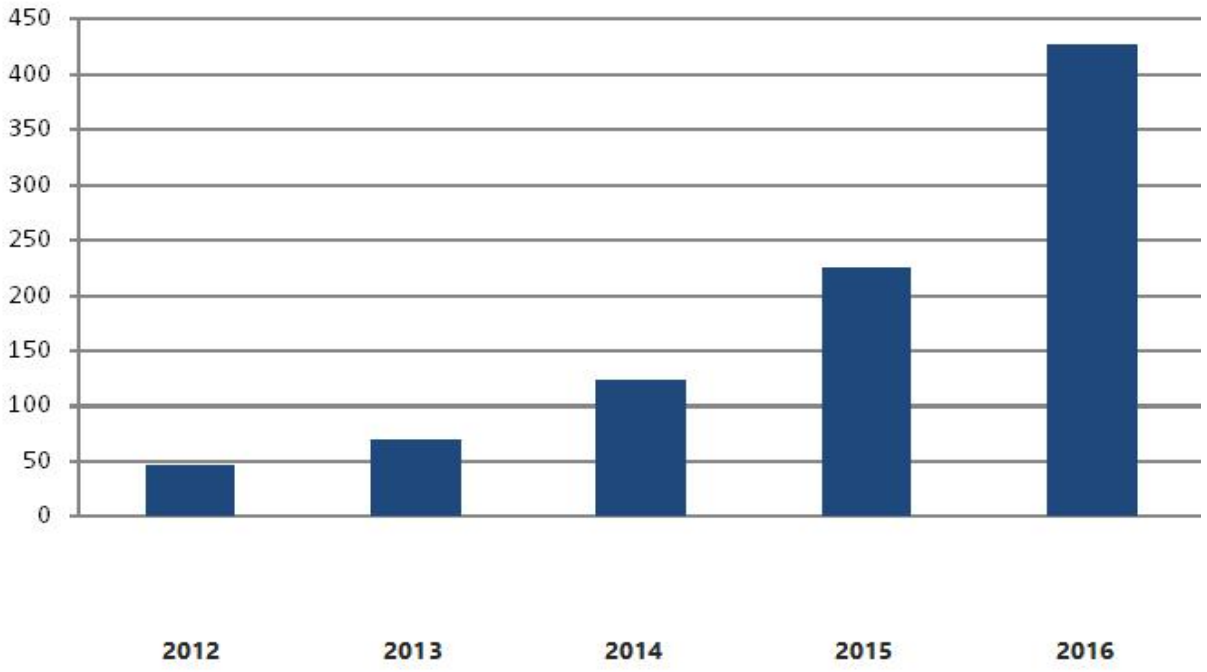
σταμάτησαν την συνεργασία με την εταιρία συνεπεία του περιστατικού παραβίασης ασφάλειας και το αρνητικό οικονομικό αποτέλεσμα που δημιούργησε το περιστατικό στην εταιρία. Είναι μια κάλυψη που η ενεργοποίησή της δεν συνδέεται με την διακοπή δραστηριότητας της επιχείρησης και δεν αποζημιώνεται από την αυτή και συνήθως δεν προσφέρουν όλα τα ασφαλιστήρια συμβόλαια.

- Dependent Business Interruption: Οι σύγχρονες επιχειρήσεις έχουν σύνθετες εφοδιαστικές αλυσίδες οι οποίες συχνά εξαρτώνται από την διαθεσιμότητα συστημάτων τρίτων προμηθευτών, όπως η διακοπή παροχής υπηρεσιών υπολογιστικού νέφους από τρίτους
- Telephone Hacking: Τηλεπικοινωνιακές χρεώσεις λόγω παράνομης πρόσβασης στο τηλεφωνικό κέντρο της επιχείρησης.

Στα παρακάτω διαγράμματα περιγράφονται αρχικά η εξέλιξη της αμερικανικής αγοράς κυβερνοασφάλισης και έπειτα της ευρωπαϊκής,όπου και στα δύο παρατηρούμε ότι το μέγεθος της ασφάλισης που αναπτύσσεται είναι πολύ μεγάλο όπως αποδεικνύεται και το εκτιμώμενο μέγεθος αυξάνεται συνεχώς σε πολλά εκατομμύρια ευρώ.

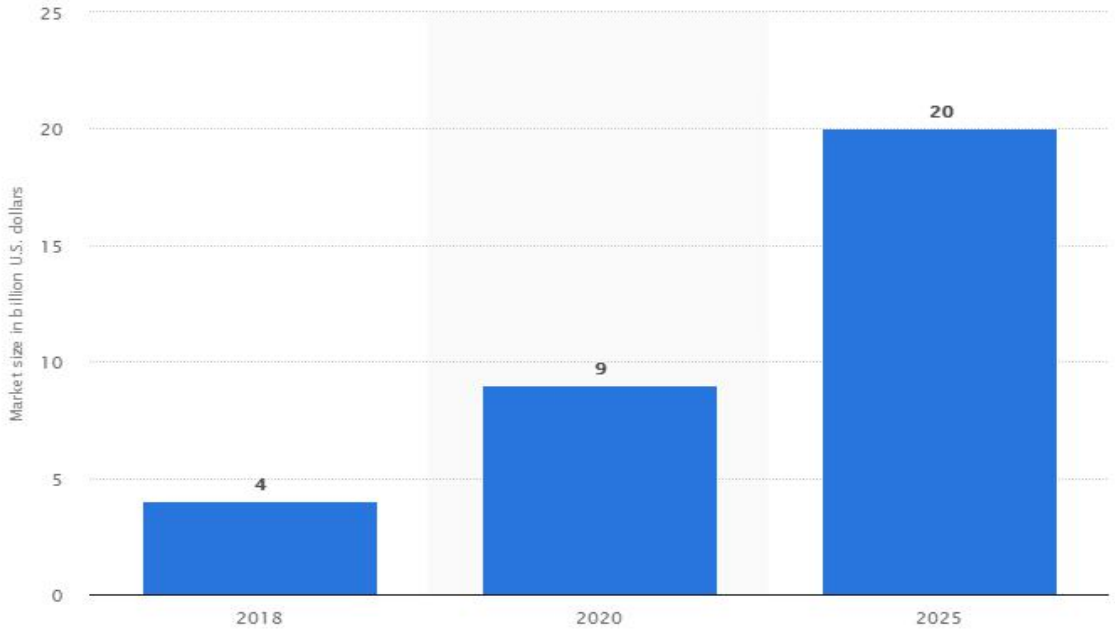


Διάγραμμα 17: Η εξέλιξη των δαπανων της αμερικανικής αγοράς κυβερνοασφάλισης σε εκατομμύρια ευρώ (EUR) άνα έτος (2005-2014). (Πηγή: www.cyberinsurancegreece.com)



Διάγραμμα 18: Η εξέλιξη των δαπανων της ευρωπαϊκής αγοράς κυβερνοασφάλισης σε εκατομμύρια ευρώ (EUR) άνα έτος (2012-2016). (Πηγή: www.advisenltd.com)

Εκτιμώμενη αξία των ασφαλίστρων ασφάλισης στον Κυβερνοχώρο σε παγκόσμιο επίπεδο το 2018, το 2020 και το 2025 σε δισεκατομμύρια δολάρια ΗΠΑ. Λόγω της ζήτησης και λόγω των ασφαλιστικών καλύψεων που πληθαίνουν παρατηρούμε συνεχώς αυξανόμενα ποσά.



Διάγραμμα 19: Η εκτιμώμενη αξία των ασφαλίστρων κυβερνοασφάλισης σε δισεκατομμύρια δολάρια (USD). (Πηγή: www.statista.com)

Από τα παραπάνω μπορεί να γίνει αντιληπτό ότι το κόστος για την ασφάλεια της παραβίασης προσωπικών δεδομένων από κυβερνοαπειλή δεν μπορεί να είναι σταθερό και μεταβάλλεται σύμφωνα με διάφορους αστάθμητους παράγοντες για τους οποίους πρέπει η επιχείρηση να λάβει γνώση και να τους διαχειριστεί. Επίσης, υπάρχουν και θέματα που πρέπει να τακτοποιηθούν όπως για παράδειγμα: Νομικές συμβουλές και υποστήριξη για την αξιολόγηση των νομικών συνεπειών της παραβίασης και τις ενέργειες που απαιτούνται για το μετριασμό τους Απώλεια Κερδών λόγω Διακοπής Λειτουργίας Εταιρικού Δικτύου που οφείλεται σε παραβίαση ασφάλειάς του Εξειδικευμένους Διαπραγματευτές σε περίπτωση Εκβιασμού για αποκάλυψη δεδομένων, αποζημιώσεις σε τρίτους που υπέστησαν ζημία λόγω διαρροής δεδομένων Ανάλυση Ζημιών που έχουν πληρωθεί από Ασφαλιστικές Εταιρείες στην Αμερική.

Καθώς οι κίνδυνοι και οι υποχρεώσεις του Κυβερνοχώρου είναι καλύτερα κατανοητοί, οι ασφαλιστές του κυβερνοχώρου θα μπορούσαν να αναλάβουν ηγετικό ρόλο στην ανάπτυξη ασφαλιστικών πινάκων από τους οποίους πωλούν ασφάλειες σε μοντέλο βασισμένο σε κινδύνους. Όσο καλύτερη είναι η ασφάλεια μιας εταιρείας, τόσο λιγότερα ασφάλιστρα πληρώνει η οικονομική μονάδα. Αυτές οι λύσεις που βασίζονται στην αγορά θα ωθούσαν τον ιδιωτικό τομέα να επενδύσει σε κατάλληλα επίπεδα ασφάλειας του κυβερνοχώρου χωρίς την απειλή των ξεπερασμένων και επαχθών κυβερνητικών κανονισμών[43].

4.6 Οικονομικό έγκλημα

Τα στελέχη κατονομάζουν ως κορυφαίους κινδύνους: τις κυβερνο-απειλές (80%), τις παρατεταμένες τεχνολογικές διακοπές στο εσωτερικό της τράπεζας (64%), τις διακοπές λειτουργίας τρίτων (64%), τη διαθεσιμότητα δεδομένων (41%), τις απαρχαιωμένες τεχνολογίες (39%), την καταστροφή σημαντικών δεδομένων (39%), την οικονομική ανθεκτικότητα (32%).

Η Ευρωπαϊκή Επιτροπή αναφέρει ως οργανωμένο οικονομικό έγκλημα όλες τις δραστηριότητες οργανωμένων εγκληματικών ομάδων οι οποίες κάνουν κατάχρηση χρηματοοικονομικών συστημάτων ή συστημάτων πληρωμών με σκοπό την αποκόμιση οικονομικού οφέλους[44].

Στην έρευνα της ΕΥ οι νέες τεχνολογίες θα έχουν σημαντικό αντίκτυπο: την εποπτεία απάτης (72%), το οικονομικό έγκλημα (68%), τη μοντελοποίηση (57%), την πιστωτική ανάλυση (57%), την κυβερνο-ασφάλεια (57%), και τις KYC (know-your-customer)

[43] Πληροφορίες αντλήθηκαν από την ιστοσελίδα https://solutions.heritage.org/providing-for-a-strong-defense/cybersecurity/
[44] Πληροφορίες αντλήθηκαν από την ιστοσελίδα www.insider.gr/apopseis/vlogs/48164/oikonomiko-egklima-kai-pos-antimetopizetai

δραστηριότητες (57%).

Οι επιθέσεις στον κυβερνοχώρο γίνονται πιο ελκυστικές και δυνητικά πιο καταστροφικές, καθώς η εξάρτησή μας από την τεχνολογία της πληροφορίας αυξάνεται. Σύμφωνα με την έκθεση Symantec για την εγκληματικότητα στον κυβερνοχώρο που δημοσιεύθηκε τον Απρίλιο του 2012, οι επιθέσεις στον κυβερνοχώρο κοστίζουν 114 δισεκατομμύρια δολάρια ετησίως. Αν υπολογίζεται ο χρόνος που χάνουν οι εταιρείες που προσπαθούν να ανακάμψουν από επιθέσεις στον κυβερνοχώρο, το συνολικό κόστος των επιθέσεων κυβέρνησης θα φτάσει στα 385 δισεκατομμύρια δολάρια. Τα θύματα επιθέσεων στον κυβερνοχώρο αυξάνονται επίσης σημαντικά. Με βάση την έρευνα που πραγματοποίησε η Symantec, η οποία περιελάμβανε συνέντευξη από 20.000 ανθρώπους σε 24 χώρες, το 69% ανέφερε ότι ήταν η αυτονομία μιας επιδρομής στον κυβερνοχώρο στη ζωή τους[45].

Ο Didier Lavion,διευθυντής στον τομέα Εγκληματολογικών Συμβουλευτικών Υπηρεσιών της PwC των ΗΠΑ,αναφέρει πώς τα κεφάλαια που διατίθενται για τον εντοπισμό και την πρόληψη του εγκλήματος αυξάνονται,γεγονός που έχει οδηγήσει σε ακόμη μεγαλύτερη αύξηση της κατανόησης και του εντοπισμού της απάτης. Με απλά λόγια, οι επιπτώσεις της απάτης δεν θεωρούνται πλέον αποδεκτό κόστος για μια επιχείρηση και οι δράστες έχουν πλέον στρατηγικούς στόχους χρησιμοποιώντας πιο εξελιγμένες μεθόδους. Το 68% των εξωτερικών δραστών (που ευθύνονται για το 40% των περιστατικών) είναι άνθρωποι με τους οποίους ο οργανισμός συνεργάζεται. Συνεχίζοντας ο Didier Lavion δίνει έμφαση στον μεγάλο τομέα δραστηριότητας της απάτης από μόνη της η οποία βασίζεται στην τεχνολογία, στην καινοτομία,είναι ευκαιριακή και επηρεάζει το σύνολο της λειτουργίας των οργανισμών,αποτελώντας τον μεγαλύτερο ανταγωνιστή όλων των εταιριών. Τα συχνότερα οικονομικά εγκλήματα που αντιμετωπίζουν οι οργανισμοί τα τελευταία δύο χρόνια είναι[46]:

- Η κατάχρηση περιουσιακών στοιχείων
- Το ηλεκτρονικό έγκλημα
- Η παραπλάνηση καταναλωτών
- Η ανάρμοστη επαγγελματική συμπεριφορά

Η καταπολέμηση του οικονομικού εγκλήματος αποτελεί κοινωνικό πρόβλημα που συνδέεται άρρηκτα με την οικονομική λειτουργία του υπάρχοντος κοινωνικοοικονομικού συστήματος,γίνεται μία προσπάθεια βελτίωσης του συστήματος ποινικής δικαιοσύνης και μια

[45] Στο άρθρο των Julian Jang-Jaccard Surya Nepal, (2014), A survey of emerging threats in cybersecurity _ Elsevier Enhanced Reader, Journal of compute and System Sciences, pp 935-952

[46] Πληροφορίες αντλήθηκαν από www.iefimerida.gr/news/400740/pwc-oikonomiko-egklima-therieyei-oi-pio-gnostes-apates

προσπάθεια ολοκληρωτικής αλλαγής του νομικού συστήματος. Με την πρόβλεψη της ικανοποίησης του παθόντος και τον θεσμό της ποινικής συνδιαλλαγής (στο Ν. 3904/2010) σκοπός είναι η εύρεση μιας εναλλακτικής λύσης στο ποινικό σύστημα και όχι απλώς μια βελτιωμένη εκδοχή του συστήματος ποινικής δικαιοσύνης. Τελικός σκοπός είναι μια δικαιοσύνη η οποία με τη σειρά της έχει ως στόχο την αποκατάσταση σε ασφαλείς κοινότητες της σχέσης μεταξύ θύματος και δράστη που έχουν επιλύσει τα μεταξύ τους προβλήματα, ιδιαίτερα προκειμένου για περιουσιακά εγκλήματα. Στην πράξη όμως οι διατάξεις του άρθρου 308Β του Κώδικα Ποινικής Δικονομίας εισάγουν ρυθμίσεις που φιλοδοξούν να μοιάσουν με τον θεσμό της συνδιαλλαγής στην ουσία όμως λίγο σχετίζονται με αυτόν[47].

[47] Στο άρθρο του Μυλωνόπουλου Χ.,Η «ικανοποίηση του παθόντος» και η «ποινική συνδιαλλαγή» στο Ν. 3904/2010,Νομική Σχολή Πανεπιστημίο Αθηνών(http://www.mylonopoulos.gr/publication/article/3/i-%C2%ABikanopoiisi-toy-pathontos%C2%BB-kai-i-%C2%ABpoiniki-syndiallagi%C2%BB-sto-n-3904/2010.html)

ΚΕΦΑΛΑΙΟ 5 ΣΤΡΑΤΗΓΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ

5.1 Διαχείριση κινδύνου-Διαχείριση των απειλών του Κυβερνοχώρου

Η διαχείριση των απειλών που εμφανίζονται στον Κυβερνοχώρο αποτελεί μια σύνθετη πρόκληση. Ιδιαίτερα μεγάλη σημασία δίνεται στην προστασία των δεδομένων και τη συμμόρφωση. Αυτό είναι λογικό καθώς οι οργανισμοί υπόκεινται σε πολλαπλές νομοθετικές και εταιρικές ρυθμιστικές απαιτήσεις, και καλούνται να αποδείξουν ότι διαχειρίζονται και προστατεύουν αποτελεσματικά τις πληροφορίες που έχουν στην κατοχή τους.

Για την επιτυχή διαχείριση των κινδύνων που προέρχονται από τον Κυβερνοχώρο θα πρέπει οι διοικήσεις να συνειδητοποιήσουν τον κίνδυνο αλλά και η υποστήριξη της επιχείρησης. Ο τρίτος και σημαντικότερος παράγοντας είναι η χρήση μιας ολοκληρωμένης εικόνας των πληροφοριακών πόρων του οργανισμού[48].

5.2 Κύριες στρατηγικές διαχείρισης του Κινδύνου

Είναι σημαντικό όλες οι επιχειρήσεις να συνεργαστούν και να υποστηριχτούν ανάλογα από τους δημόσιους οργανισμούς,όπου στην Ελλάδα είναι για παράδειγμα η Εθνική Υπηρεσία Πληροφοριών και η Δίωξη Ηλεκτρονικού Εγκλήματος. Η ευθύνη για τη στρατηγική διαχείριση πληροφοριακών κινδύνων πρέπει να δοθεί στα ανώτερα διοικητικά στελέχη.

Όσο οι ανησυχίες για τις απειλές στον κυβερνοχώρο έχουν αυξηθεί, ένα υψηλότερο ποσοστό επιχειρήσεων σε όλες σχεδόν τις βιομηχανίες ανέφερε ότι έλαβε προληπτικά μέτρα για την προστασία από τους κινδύνους του κυβερνοχώρου, σύμφωνα με την έρευνα - παρόλο που ένα σημαντικό ποσοστό δεν έχει εφαρμόσει τέτοιες προληπτικές βέλτιστες πρακτικές. Τα μέτρα που πρέπει να ληφθούν υπόψη είναι:

- Η αγορά ενός ασφαλιστηρίου συμβολαίου στον κυβερνοχώρο (51% των συμμετεχόντων στην έρευνα, από 39% πέρυσι).
- Η δημιουργία σχεδίου συνέχισης της επιχείρησης σε περίπτωση επιθέσεων στον κυβερνοχώρο (47%, από 38%).
- Αξιολογώντας τον εαυτό τους (49%, από 45%) και τους πωλητές τους (41%, από 37%).
- Ενημέρωση κωδικών πρόσβασης υπολογιστή (74%, από 71%).

[48]Πληροφορίες αντλήθηκαν από την ιστοσελίδα https://home.kpmg/gr/el/home/insights/2016/07/cyber-security-facts-and-figures.html

5.3 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Σύμφωνα με τον κανονισμό της Ευρωπαϊκής Ένωσης 2016/679 η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα. Ο παρών κανονισμός σκοπεύει να συμβάλλει στην επίτευξη ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης και μιας οικονομικής ένωσης, στην οικονομική και κοινωνική πρόοδο, στην ενίσχυση και σύγκλιση των οικονομιών εντός της εσωτερικής αγοράς και στην ευημερία των φυσικών προσώπων. Η τεχνολογία επιτρέπει τόσο σε ιδιωτικές επιχειρήσεις όσο και σε δημόσιες αρχές να κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτοφανή κλίμακα για την επιδίωξη των δραστηριοτήτων τους.

Σύμφωνα με τον κανονισμό αυτό τα δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. Παραδείγματα δεδομένων προσωπικού χαρακτήρα[49]:

- όνομα και επώνυμο·
- διεύθυνση κατοικίας·
- ηλεκτρονική διεύθυνση (όνομα.επώνυμο@εταιρεία.com)
- αναγνωριστικός αριθμός κάρτας·
- δεδομένα τοποθεσίας
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)·
- αναγνωριστικό cookie·
- το αναγνωριστικό διαφήμισης του τηλεφώνου σας·
- δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

Παραδείγματα δεδομένων που δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα:

- αριθμός μητρώου εταιρείας

[49] Πληροφορίες αντλήθηκαν από την ιστοσελίδα https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

· ηλεκτρονική διεύθυνση του τύπου (πληροφορίες@εταιρεία.com)

· ανώνυμα δεδομένα.

Ο όρος επεξεργασία προσωπικών δεδομένων είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων,σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή,η καταχώριση,η οργάνωση,η διάρθρωση,η αποθήκευση,η προσαρμογή ή η μεταβολή,η ανάκτηση,η αναζήτηση πληροφοριών,η χρήση, η κοινολόγηση με διαβίβαση,η διάδοση ή κάθε άλλη μορφή διάθεσης,η συσχέτιση ή ο συνδυασμός, ο περιορισμός,η διαγραφή ή η καταστροφή.

Επίσης, σύμφωνα με τον κανονισμό υπεύθυνος επεξεργασίας είναι το φυσικό ή νομικό πρόσωπο,η δημόσια αρχή,η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους,ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

Ο εκτελών την επεξεργασία,είναι το φυσικό ή νομικό πρόσωπο,η δημόσια αρχή,η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Η παραβίαση δεδομένων προσωπικού χαρακτήρα,αποτελεί την παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή,απώλεια,μεταβολή,άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν,αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

Ο συγκεκριμένος κανονισμός αφορά όλες τις επιχειρήσεις, (ιδιωτικού και δημόσιου τομέα) που με οποιοδήποτε τρόπο διαχειρίζονται προσωπικά δεδομένα εργαζομένων, συνεργατών, πελατών, ή άλλων φυσικών προσώπων. Παρόλα αυτά,για να ληφθεί υπόψη η ειδική κατάσταση των πολύ μικρών,των μικρών και των μεσαίων επιχειρήσεων,ο παρών κανονισμός περιλαμβάνει παρέκκλιση για οργανισμούς που απασχολούν λιγότερα από 250 άτομα (Άρθρο 30 παρ. 5) όσον αφορά την τήρηση αρχείων. Επιπλέον, τα θεσμικά όργανα και οι οργανισμοί της Ένωσης, καθώς και τα κράτη μέλη και οι εποπτικές αρχές τους, παροτρύνονται να λαμβάνουν υπόψη τις ειδικές ανάγκες των πολύ μικρών,των μικρών και των μεσαίων επιχειρήσεων κατά την εφαρμογή του παρόντος κανονισμού. Η έννοια των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων θα πρέπει να βασίζεται στο άρθρο 2 του παραρτήματος στη σύσταση 2003/361/ΕΚ της Επιτροπής (1). (Η κατηγορία των πολύ μικρών,

μικρών και μεσαίων επιχειρήσεων (ΜΜΕ) αποτελείται από επιχειρήσεις που απασχολούν λιγότερους από 250 εργαζόμενους και των οποίων ο ετήσιος κύκλος εργασιών δεν υπερβαίνει τα 50 εκατομμύρια ευρώ ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 43 εκατομμύρια ευρώ.)

Ο κανονισμός αυτός στην ελληνική νομοθεσία έλαβε χώρα από τις 25 Μαΐου 2018. Οι βασικές Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα (άρθρο 5):

a) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων (νομιμότητα, αντικειμενικότητα και διαφάνεια),
b) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 (περιορισμός του σκοπού),
c) είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία (ελαχιστοποίηση των δεδομένων),
d) είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας (ακρίβεια)
e) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων (περιορισμός της περιόδου αποθήκευσης),
f) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα,μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων (ακεραιότητα και

εμπιστευτικότητα).

Οι εταιρείες πλέον καλούνται να ασχοληθούν και επίσημα με την προστασία των πληροφοριακών τους συστημάτων και την προάσπιση των δεδομένων τους, κάνοντας τακτικά ελέγχους ασφάλειας δικτύων και υποδομών, υλοποιώντας πολιτικές ασφάλειας και διαδικασίες, αλλά και εκπαιδεύοντας τους χρήστες πληροφοριακών συστημάτων για την ορθή χρήση των πληροφοριακών συστημάτων τους.

Ο Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στους υπευθύνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων. Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Επίσης, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

a) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,
b) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,
c) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,
d) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

5.4 Κυβερνοασφάλεια (CyberSecurity)

Η ασφάλεια των πληροφοριών αποτελεί πλέον στην εποχή του διαδικτύου ζωτικό ζήτημα για όλους,απλοί χρήστες,ολόκληρες επιχειρήσεις αλλά και κράτη. Οι ανησυχίες για την ασφάλεια στον Κυβερνοχώρο με την κατανόηση των περιβαλλοντικών ζητημάτων των διαφόρων επιθέσεων στον Κυβερνοχώρο και την εκπόνηση αμυντικών στρατηγικών-αντιμέτρων που διαφυλάσσουν την εμπιστευτικότητα,την ακεραιότητα και τη διαθεσιμότητα οποιωνδήποτε ψηφιακών τεχνολογιών και τεχνολογιών πληροφόρησης. Ο εμπιστευτικός χαρακτήρας είναι ο όρος που χρησιμοποιείται για την αποτροπή της αποκάλυψης πληροφοριών σε μη

εξουσιοδοτημένα άτομα ή σε συστήματα

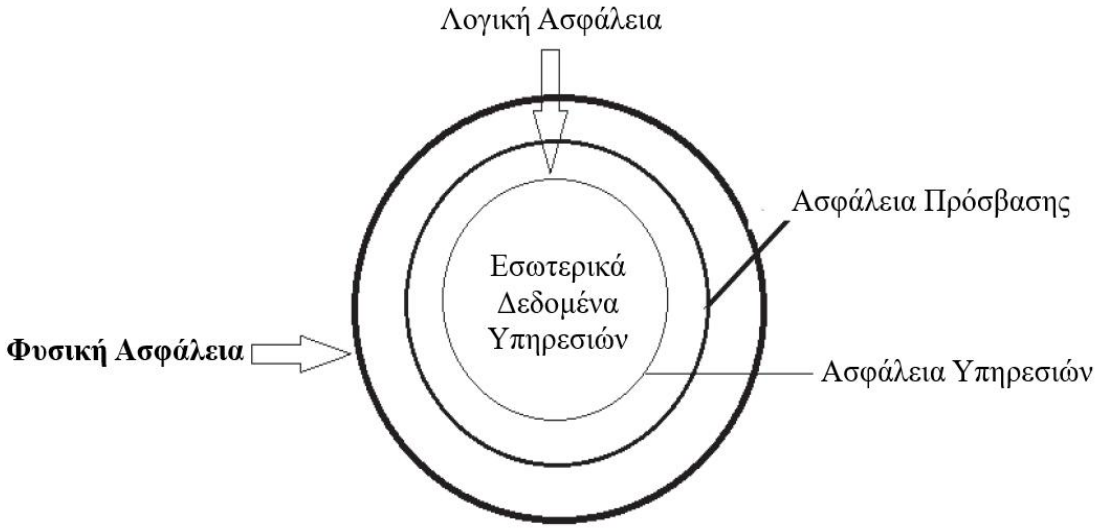
Πολλοί ειδικοί στον Κυβερνοχώρο πιστεύουν ότι το κακόβουλο λογισμικό είναι η βασική επιλογή του όπλου για τη διεξαγωγή κακόβουλων προθέσεων για την παραβίαση των προσπαθειών ασφάλειας στον Κυβερνοχώρο. Το κακόβουλο λογισμικό αναφέρεται σε μια ευρεία κατηγορία επιθέσεων που φορτώνεται σε ένα σύστημα, συνήθως χωρίς τη γνώση του νόμιμου κατόχου, για να υπονομεύσει το σύστημα προς όφελος ενός αντιπάλου. Ορισμένες παραδειγματικές τάξεις κακόβουλου λογισμικού περιλαμβάνουν ιούς, σκουλήκια,τρωικά άλογα,λογισμικά κατασκοπείας και εκτελέσιμα αρχεία bot. Το κακόβουλο λογισμικό μολύνει τα συστήματα με την ανυπαρξία τρόπων για την αναπαραγωγή των παραδειγμάτων από τα μολυσμένα μηχανήματα, εξαπατώντας τον χρήστη να ανοίξει τα μολυσμένα αρχεία ή τους δελεαστικούς χρήστες να επισκέπτονται το διαδικτυακό διαδικτυακό τόπο διαφήμισης. Σε πιο συγκεκριμένα παραδείγματα μόλυνσης από κακόβουλο λογισμικό, το κακόβουλο λογισμικό μπορεί να φορτωθεί σε μια μονάδα USB που έχει ενσωματωθεί σε μια μολυσμένη συσκευή και στη συνέχεια να μολύνει κάθε άλλο σύστημα στο οποίο εισάγεται στη συνέχεια αυτή η συσκευή. Το Malwaremay,τύπος λογισμικού υποκλοπής δεδομένων,διαδίδεται από συσκευές και εξοπλισμό που περιέχουν ενσωματωμένα συστήματα και υπολογιστική λογική. Τα θύματα κακόβουλου λογισμικού μπορούν να διαφέρουν από τα συστήματα τελικών χρηστών, τους διακομιστές, τις συσκευές δικτύου (π.χ. δρομολογητές, διακόπτες κλπ.). Ο πολλαπλασιασμός και η πολυπλοκότητα του ταχέως αυξανόμενου αριθμού κακόβουλου λογισμικού αποτελεί μείζονα ανησυχία στο διαδίκτυο σήμερα. Παραδοσιακά, οι επιθέσεις κακόβουλου λογισμικού συνέβησαν σε ένα ενιαίο σημείο επιφάνειας μεταξύ εξοπλισμού υλικού,κομματιών λογισμικού ή επιπέδου δικτύου που εκμεταλλεύονταν υπάρχοντα τρωτά σημεία σχεδιασμού και εφαρμογής σε κάθε στρώμα. Αντί να προστατεύει κάθε περιουσιακό στοιχείο, η περιμετρική αμυντική στρατηγική έχει χρησιμοποιηθεί κατά κύριο λόγο για να βάλει έναν τοίχο έξω από όλους τους εσωτερικούς πόρους για να προστατεύσει τα πάντα από κάθε ανεπιθύμητη εισβολή από το εξωτερικό.

Η γενική αποδοχή αυτού του μοντέλου περίμετρος έχει προκύψει επειδή είναι πολύ ευκολότερο και φαινομενικά λιγότερο δαπανηρό να εξασφαλιστεί μία περίμετρος από ότι είναι η εξασφάλιση μεγάλου όγκου εφαρμογών ή μεγάλος αριθμός εσωτερικών δικτύων. Για να δοθεί πιο καθορισμένη πρόσβαση σε ορισμένες εσωτερικές πηγές, οι μηχανισμοί ελέγχου πρόσβασης έχουν χρησιμοποιηθεί σε συνδυασμό με τον περιμετρικό αμυντικό μηχανισμό. Στην κορυφή της υπεράσπισης της υπεράσπισης και του ελέγχου της πρόσβασης, προστίθεται λογοδοσία για τον εντοπισμό ή την τιμωρία για τυχόν κακοδιοίκηση. Ωστόσο, οι συνδυασμένες προσπάθειες της περιμετρικής αμυντικής στρατηγικής έχουν βρεθεί όλο και

πιο αναποτελεσματικές καθώς βελτιώνεται η πρόοδος και η πολυπλοκότητα του κακόβουλου λογισμικού. Το κακόβουλο λογισμικό που εξελίσσεται πάντα φαίνεται να βρίσκει κενά για να παρακάμψει εντελώς την υπεράσπιση του υπερφόρτωσης.

Η αυξανόμενη ανάγκη για επικοινωνία συνδέεται πλέον άμεσα με την προστασία των πληροφοριών και αποτελούν δύο διαφορετικές αλλά όχι αντίθετες απαιτήσεις και σύμφωνα με την καθηγήτρια Silvia Maria Tăbuşcă η εφαρμογή ενός σύγχρονου συστήματος ασφάλεια στο Βέλγιο προβλέπει προστασία σε διάφορα επίπεδα,όπως παρουσιάζεται στο παρακάτω διάγραμμα.

Επίπεδα Ασφαλείας Πληροφοριών



Διάγραμμα 20: Προστασία των πληροφοριών σε διάφορα επίπεδα ασφαλείας. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε άρθρο των Popescu R. C.,Popescu G.,Risks of cyber attacks on financial audit activity,Audit Financiar, XVI, Nr. 1(149) p.140-147 (2018))

Τα διάφορα Επίπεδα Ασφάλειας Πληροφοριών περιγράφονται αναλυτικά παρακάτω[50]:

- Φυσική Ασφάλεια,ο πρώτο επίπεδο αποτελείται γενικά από εξοπλισμό ασφάλισης από φυσική καταστροφή και ζημιές,σκόπιμες ή άσκοπες. Αποτελεί ένα μέτρο που ισχύει για όλα τα συστήματα πληροφορικής,αλλά λιγότερο εφικτή στην περίπτωση των δικτύων.
- Λογική Ασφάλεια,το δεύτερο επίπεδο προστασίας αφορά τόσο την ασφάλεια πρόσβασης όσο και την ασφάλεια των υπηρεσιών και περιλαμβάνει το σχήμα των μεθόδων για έλεγχο της πρόσβασης σε πόρους και υπηρεσίες του συστήματος.
- Ασφάλεια Πρόσβασης,υπεύθυνο για τον καθορισμό και την διαχείριση πρόσβασης των

[50] Στο άρθρο των Popescu R. C.,Popescu G.,Risks of cyber attacks on financial audit activity,Audit Financiar, XVI, Nr. 1(149) p.140-147 (2018)

χρηστών,

- Ασφάλεια Υπηρεσιών,αφορά τον έλεγχο παροχής υπηρεσιών και δεδομένων και είναι υπεύθυνο για την προειδοποίηση και εγκατάσταση των υπηρεσιών που παρέχει το σύστημα και το δικαιώματα παροχής.
- Τελικός στόχος είναι ο πυρήνας των δεδομένων και υπηρεσιών. Σε ένα τέλειο σύστημα ασφαλείας η πρόσβαση πρέπει να γίνεται μέσω μόνο αυτών των σταδίων,χωρίς να επιτρέπεται η παράκαμψη οποιοδήποτε από αυτά.

Προέκυψε από έρευνα της Kaspersky Lab και της B2B International ότι ο ανθρώπινος παράγοντας,οι υπάλληλοι στην ασφάλεια των πληροφοριακών συστημάτων, καθιστά τις επιχειρήσεις πιο ευάλωτες από το εσωτερικό τους. Με το 46% των περιστατικών ασφάλειας πληροφοριακών συστημάτων να οφείλεται σε υπαλλήλους κάθε χρόνο, αυτή η ευπάθεια των επιχειρήσεων πρέπει να αντιμετωπιστεί σε όλα τα επίπεδα και όχι μόνο μέσω του τμήματος ασφάλειας πληροφοριακών συστημάτων. Επιπλέον διαπίστωσε ότι μόνο το 12% των απασχολουμένων έχει πλήρη επίγνωση των πολιτικών και των κανόνων ασφάλειας που καθορίζονται στους οργανισμούς όπου εργάζονται. Αυτό σε συνδυασμό με το γεγονός ότι το μισό των εργαζομένων 49% θεωρεί ότι η προστασία από τις διαδικτυακές διαφορές αποτελεί κοινή ευθύνη, παρουσιάζει πρόσθετες προκλήσεις στον καθορισμό του κατάλληλου πλαισίου για την ασφάλεια στον κυβερνοχώρο. Ηλεκτρονικό μήνυμα "ψαρέματος", αδύναμοι κωδικοί πρόσβασης, ψεύτικα τηλεφωνήματα από τμήματα τεχνολογικής υποστήριξης,αποτελούν εισόδου στην εταιρική υποδομή. Ακόμα και μία απλή flash card που μπορεί να έχει παραπέσει στο πάρκινγκ του γραφείου ή δίπλα στο γραφείο της γραμματείας μπορεί να θέσει σε κίνδυνο ολόκληρο το δίκτυο,ώστε κάποιος που βρίσκεται στο εσωτερικό της εταιρείας που δεν ξέρει ή δεν δίνει προσοχή στην ασφάλεια,συνδέοντας αυτή η συσκευή πανεύκολα με το δίκτυο προκαλώντας ολέθριες συνέπειες σχολίασε ο David Jacoby,ερευνητής ασφάλειας της Kaspersky Lab. Αυτό μας δείχνει ότι οι κυβερνοεπιθέσεις μπορούν να γίνουν με τον πιο ευφάνταστο τρόπο και ότι ηθελημένα ή άθελα οποιοσδήποτε μπορεί να είναι υποχείριο των κυβερνοπειρατών[51].

Μια επιτυχημένη προσέγγιση στον τομέα της ασφάλειας στον κυβερνοχώρο έχει πολλαπλά στρώματα προστασίας διασκορπισμένα στους υπολογιστές, τα δίκτυα, τα προγράμματα ή τα δεδομένα που πρέπει να διατηρούνται ασφαλή. Σε μια οργάνωση, οι άνθρωποι, οι διαδικασίες και η τεχνολογία πρέπει όλοι να αλληλοσυμπληρώνονται για να δημιουργήσουν μια αποτελεσματική άμυνα από επιθέσεις στον κυβερνοχώρο. Ένα ενιαίο

[51] Πληροφορίες αντλήθηκαν από την ιστοσελίδα www.kaspersky.com

σύστημα διαχείρισης απειλών μπορεί να αυτοματοποιήσει τις ολοκληρώσεις σε επιλεγμένα προϊόντα Cisco Security και να επιταχύνει τις βασικές λειτουργίες ασφάλειας: εντοπισμό, διερεύνηση και αποκατάσταση. Η ισχυρή ασφάλεια στον κυβερνοχώρο απευθύνεται στους τρεις πυλώνες ασφάλειας των δεδομένων.

- Άνθρωποι: κάθε εργαζόμενος πρέπει να γνωρίζει τον ρόλο του στην πρόληψη των απειλών στον κυβερνοχώρο και πρέπει να ενημερώνεται για τους τελευταίους κινδύνους και λύσεις. Οι χρήστες πρέπει να κατανοήσουν και να συμμορφωθούν με τις βασικές αρχές ασφάλειας δεδομένων,όπως την επιλογή ισχυρών κωδικών πρόσβασης την επιφυλακτικότητα των συνημμένων στο ηλεκτρονικό ταχυδρομείο και την δημιουργία αντιγράφων ασφαλείας των δεδομένων.

- Διαδικασίες: τεκμηριωμένες και σαφώς ορισμένες ως προς τους ρόλους,τις ευθύνες και τις αναθεωρήσεις,λόγω της συνεχόμενης εξέλιξης των απειλών. Οι οργανισμοί πρέπει να διαθέτουν ένα πλαίσιο για το πώς αντιμετωπίζουν τόσο τις απόπειρες και τις επιτυχείς επιθέσεις στον Κυβερνοχώρο. Ένα καλό και σεβαστό πλαίσιο πρέπει να οριστεί ως καθοδηγητής και να παρέχει οδηγίες για το πώς μπορούν να προσδιοριστούν οι επιθέσεις,να προστατευτούν τα συστήματα,να εντοπιστούν και να αντιμετωπιστούν οι απειλές και να πραγματοποιηθεί η ανάκαμψη του οργανισμού από επιτυχείς επιθέσεις.

  - Τεχνολογία: εγκατάσταση λογισμικού προστασίας από ιούς και αξιοποίηση τεχνογνωσίας για τη μείωση των κινδύνων στον Κυβερνοχώρο. Είναι απαραίτητη για να δοθούν στους οργανισμούς αλλά και στους ανθρώπους τα απαραίτητα εργαλεία ασφάλειας υπολογιστών που απαιτούνται για να προστατευτούν από επιθέσεις στον κυβερνοχώρο. Πρέπει να προστατευθούν τρεις κύριες οντότητες: συσκευές τελικού σημείου όπως υπολογιστές, έξυπνες συσκευές και δρομολογητές. δικτύων και την τεχνολογία υπολογιστικού νέφους. Κοινή τεχνολογία που χρησιμοποιείται για την προστασία αυτών των οντοτήτων περιλαμβάνει τείχη προστασίας(firewalls) επόμενης γενιάς,φιλτράρισμα DNS,προστασία κακόβουλου λογισμικού,λογισμικό προστασίας από ιούς και λύσεις ασφάλειας ηλεκτρονικού ταχυδρομείου.

Στον σημερινό συνδεδεμένο κόσμο, όλοι επωφελούνται από τα προηγμένα προγράμματα κυβερνοάμυνας. Σε επιμέρους επίπεδο,μια επίθεση στον Κυβερνοχώρο μπορεί να οδηγήσει σε όλα, από την κλοπή ταυτότητας, μέχρι τις προσπάθειες εκβιασμού, στην απώλεια σημαντικών δεδομένων όπως οικογενειακές φωτογραφίες. Ο καθένας βασίζεται σε

υποδομές ζωτικής σημασίας, όπως μονάδες παραγωγής ηλεκτρικής ενέργειας, νοσοκομεία και εταιρείες παροχής χρηματοοικονομικών υπηρεσιών. Η διασφάλιση αυτών και άλλων οργανώσεων είναι απαραίτητη για τη λειτουργία της κοινωνίας μας. Οι ομάδες των ερευνητών για την κυβερνοπροστασία είναι σε θέση να αποκαλύπτουν νέες αδυναμίες, εκπαιδεύουν το κοινό σχετικά με τη σημασία της ασφάλειας στον κυβερνοχώρο και ενισχύουν τα εργαλεία ανοικτού κώδικα. Η εργασία τους καθιστά το Διαδίκτυο ασφαλέστερο για όλους.

5.5 Κυβερνοασφάλιση (Cyber Insurance)

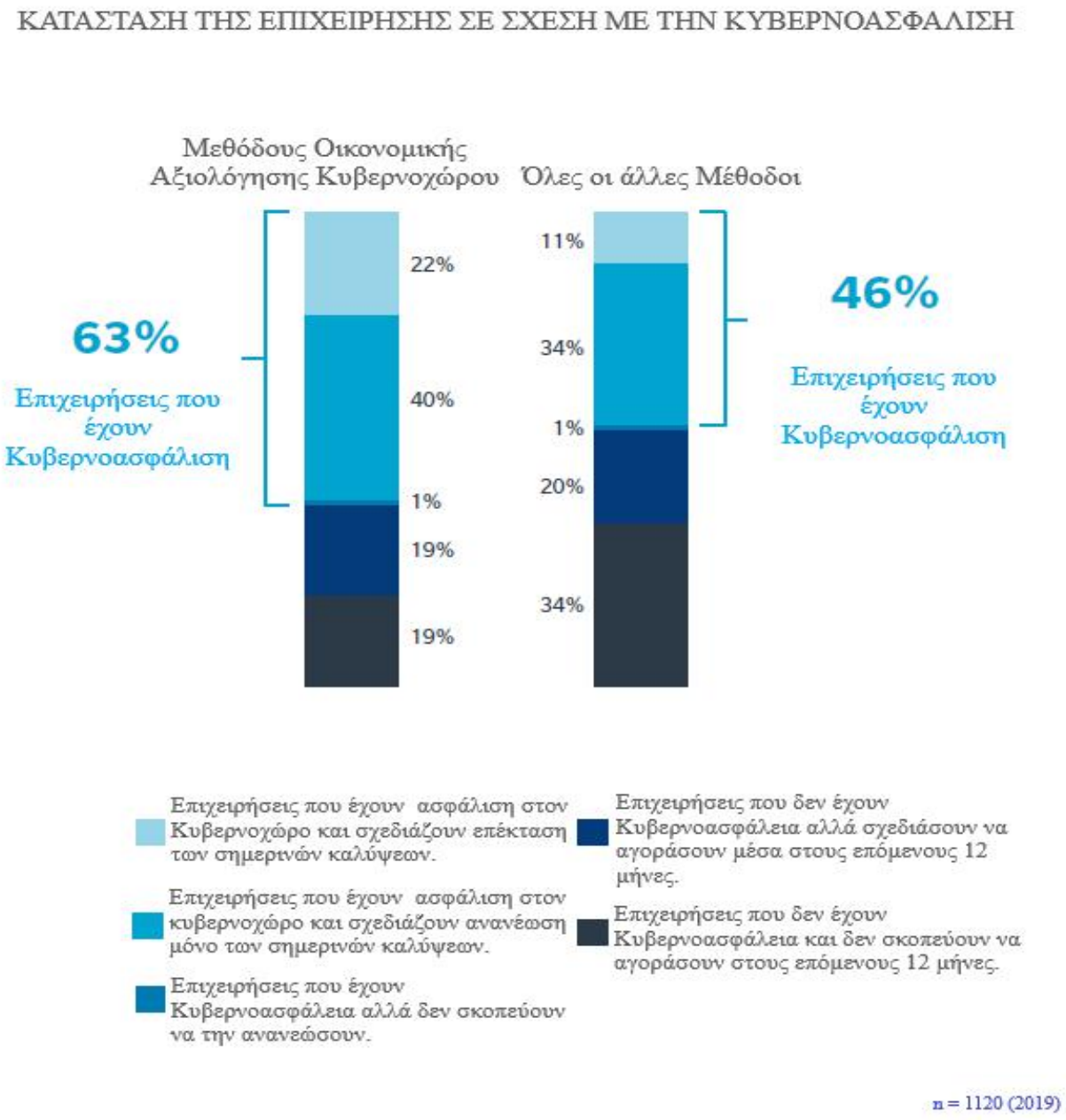
Ένας τρόπος αποκατάστασης και μείωσης του κόστους είναι η χρήση ασφάλειας έναντι των κινδύνων του Κυβερνοχώρου. Ο κλάδος της ασφάλισης κατά κυβερνοεπιθέσεων,κυβερνοασφάλιση (cyber insurance),αναμένεται να σημειώσει άνθηση σε παγκόσμιο επίπεδο, σκαρφαλώνοντας στα 5 δις δολάρια σε ετήσια ασφάλιστρα έως το 2018 και φτάνοντας τουλάχιστον τα 7,5 δις. δολάρια έως τα τέλη της δεκαετίας,σύμφωνα με τη νέα έκθεση που δημοσίευσε η PwC[52].

Διάγραμμα 21: Ετήσιες δαπάνες σε εκατομμύρια δολάρια (USD) στην κυβερνοασφάλεια και στην κυβερνοασφάλιση. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε άρθρο των Gartner,Munich Re,Global Cyber Risk Perception Survey 2019)

Σημαντικό επίσης είναι ότι οι δαπάνες για την ασφάλεια στον Κυβερνοχώρο υπερβαίνουν κατά πολύ τις δαπάνες ασφάλισης στον κυβερνοχώρο ακόμη παράγοντας που

[52] Ετήσια έκθεση της Pwc,Insurance 2020 & beyond: Reaping the dividends of cyber resilience (2019)

δείχνει την επερχόμενη άνθηση στο χώρο της ασφάλισης κατά των κινδύνων του Κυβερνοχώρου και το τεράστιο άνοιγμα και περιθώριο βελτίωσης που έχουν.



Διάγραμμα 22: Η κατάσταση της επιχείρησής σας σε σχέση με την κυβερνοασφάλιση. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο σε έρευνα των Marsh και Microsoft,Global Cyber Risk Perception Survey 2019)

Οι οργανισμοί που χρησιμοποιούν μεθόδους οικονομικής αξιολόγησης του Κυβερνοχώρου είναι πιο πιθανό για αγορά κυβερνοασφάλισης από εκείνους που χρησιμοποιούν μόνο ποιοτικές μεθόδους ή καθόλου μέθοδο για την εκτίμηση των ανοιγμάτων έναντι των κυβερνητικών κινδύνων[53]. Οι εταιρείες που ποσοτικοποιούν οικονομικά τις εκθέσεις κινδύνου του κυβερνοχώρου ενδέχεται να είναι πιο ενημερωμένες σχετικά με την

[53] Βασισμένο σε έρευνα των Marsh και Microsoft,Global Cyber Risk Perception Survey (2019)

αξία της ασφάλισης στον κυβερνοχώρο. Βλέπουμε ότι οι περισσότερες επιχειρήσεις σχεδιάζουν στην αγορά ασφάλισης στον Κυβερνοχώρο.

Οι βασικές παροχές των ασφαλιστικών προϊόντων κυβερνοεπιθέσεων είναι[54]:

- Αστική Ευθύνη,έναντι τρίτων που υπέστησαν ζημία λόγω απώλειας προσωπικών δεδομένων από την εταιρία στην οποία είχαν δώσει
- Ανταπόκριση,έξοδα και υπηρεσίες διαχείρισης περιπτώσεων παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών
- Διακοπή Εργασιών,κάλυψη για απώλεια εσόδων λόγω διακοπής της επιχειρηματικής δραστηριότητας από περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών
- Κυβερνοεκβιασμός,κάλυψη για τη διαχείριση περιπτώσεων εξαναγκασμού από απειλές που μπορεί να βλάψουν ένα δίκτυο ή να οδηγήσουν σε διαρροή εμπιστευτικών πληροφοριών.

Το ποσό που θα δαπανήσουν οι εταιρείες για την ασφάλιση τους έναντι των κινδύνων του Κυβερνοχώρου είναι μία απόφαση των διοικητικών αξιωματούχων της. Δεν υπάρχει σωστή απάντηση στο ερώτημα ποιο είναι το ύψος μιας ασφαλιστικής κάλυψης του κυβερνοχώρου. Οι εταιρείες θα πρέπει να εξετάσουν ορισμένους παράγοντες ως βασικά κριτήρια προκειμένου να λάβουν αυτή την απόφαση,όπως είναι[55]:

- Το μέγεθος του ασφαλισμένου οργανισμού
- Το ποσό των ευαίσθητων δεδομένων που αποθηκεύονται
- Την βιομηχανία δραστηριοποίησης
- Ο βαθμός των πιθανών κινδύνων της φήμης και των απειλών.

Η ασφάλιση έναντι των κινδύνων αποτελεί μία προστασία,ωστόσο οι εταιρείες πρέπει να εξετάζουν προσεκτικά όλες τις επιλογές κάλυψης που τους παρέχονται και να βρεθούν οι βέλτιστες λύσεις για την προστασία τόσο του εμπορικού σήματος,της φήμης,της λειτουργίας και των οικονομικών απωλειών από τυχόν παραβίαση. Πρέπει και είναι σημαντικό αρχικά να μειωθεί η απειλή για όλους τους χρήστες και επιπρόσθετα να χρησιμοποιηθούν οι ασφάλειες. Αποτελεί μία πολύ σημαντική απόφαση των διοικητικών αξιωματούχων,κυρίως του διευθύνοντα συμβούλου,που πρέπει να βρούν την χρυσή τομή μεταξύ κόστους και ασφάλειας.

[54] Πληροφορίες αντλήθηκαν από τον ιστότοπο www.cyberinsurancequote.gr/insurance
[55] Πληροφορίες αντλήθηκαν από τον ιστότοπο www.cyberinsurancequote.gr/insurance

ΚΕΦΑΛΑΙΟ 6 ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΣΤΟ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΟ ΤΟΜΕΑ ΚΑΙ ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ (CASE STUDY)

6.1 Κυβερνοεπιθέσεις και Χρηματοοικονομικός τομέας

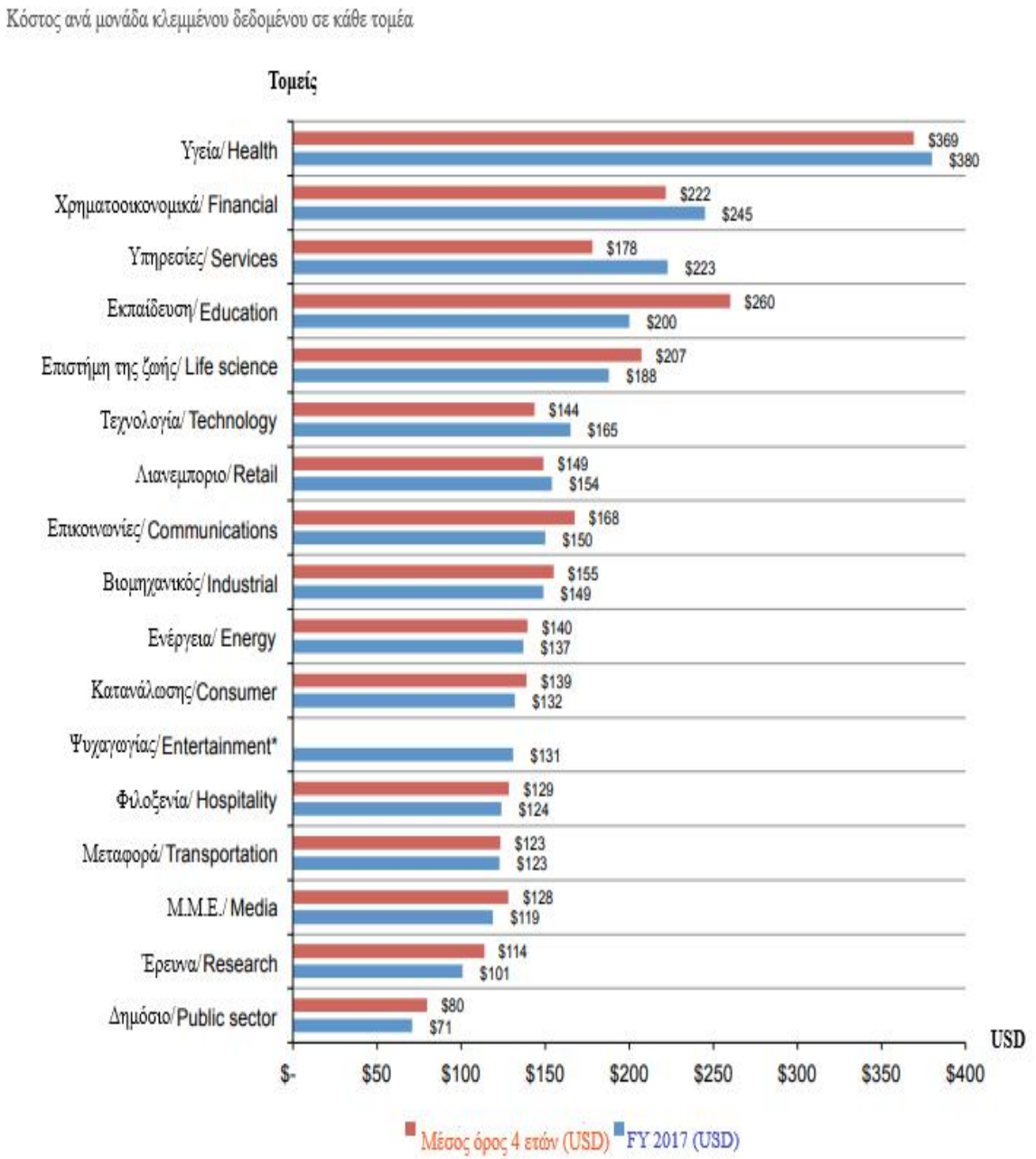
Διανύουμε μία εποχή όπου η χρηματοπιστωτική σταθερότητα αποτελεί κρίσιμη προϋπόθεση για την επίτευξη των κοινών στόχων και την ευημερία της κοινωνίας,μετά από μία δύσκολη οικονομική παγκόσμια κρίση. Οι επιθέσεις στον Κυβερνοχώρο συνεχώς αυξάνονται όπως αυξάνεται και κάθε μορφή εγκληματικότητας σε παγκόσμιο επίπεδο. Ο χρηματοοικονομικός τομέας έρχεται δεύτερος στο κόστος ανά μονάδα κλεμμένου δεδομένου στα 245$ σημειώνοντας μία αύξηση σε σχέση με τα προηγούμενα χρόνια,με το μέσο κόστος να υπολογίζετε στα 141$.[56]Σημαντικό επίσης είναι ότι το μέσο κόστος για τις επιχειρήσεις των ΗΠΑ ανά το αρχείο που χάθηκε ή κλαπεί σε παραβίαση ήταν 225$ σε όλες τις βιομηχανίες ενώ το κόστος για τις επιχειρήσεις στον χρηματοπιστωτικό τομέα ήταν 33614$[57]. Το σύνολο των τελευταίων ετών ο τομέας των χρηματοπιστωτικών υπηρεσιών παγκοσμίως ήταν πρωταρχικός στόχος κυβερνοεπιθέσεις εξαιτίας των τεράστιων διαθέσιμων πληροφοριών και της οικονομικής τους αξίας. Οι επιχειρήσεις χρηματοπιστωτικών υπηρεσιών που φέρονται να έχουν πληγεί από συμβάντα ασφαλείας είναι κατά πολλές περισσότερες από άλλους κλάδους της οικονομίας και των επιχειρήσεων[58]. Επιπρόσθετα και οι δαπάνες από μία ενδεχόμενη κυβερνοεπίθεση στον χρηματοοικονομικό τομέα είναι εκθετικά μεγαλύτερες.

Τα χρηματοπιστωτικά ιδρύματα πρέπει να είναι ευέλικτα και γρήγορα στην ενημέρωση των μεταβολών της υπάρχουσας τεχνολογίας και στην προσθήκη νέων λύσεων,να παραμένει ουσιαστικά ένα βήμα μπροστά στις τεχνολογικές εξελίξεις ώστε να μένει και μπροστά από αυτούς που κινδυνεύει[59].

Η ανάπτυξη και επέκταση της χρήσης Πληροφοριακών Συστημάτων και διασύνδεσης με το Διαδίκτυο αποτελεί μία σχέση εξάρτησης στην διασύνδεση επιχειρήσεων και

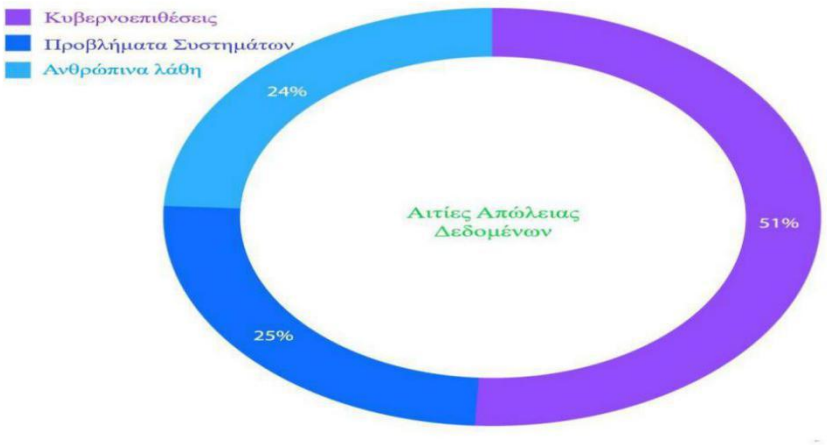
[56] Στην έρευνα Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2017)
[57] ibid (ό.π.)
[58] Στο άρθρο του Muncaster P.,Finance Hit by 300 Times More Attacks Than Other Industries (2015)
[59] Στην έρευνα των Generali Global Assistance (GGA) και Identity Theft Resource Center (ITRC),The Impact of Cybersecurity Incidents on Financial Institutions (2018)

κυβερνοχώρου όπου σε συνδυασμό με την αύξηση των απειλών κάνουν αντιληπτή τη σπουδαιότητα έρευνας και μελέτης των κινδύνων στο συγκεκριμένο χώρο. Όλα τα παραπάνω υπογραμμίζουν την αναγκαιότητα και επαγωγικά την βαρύτητα που οφείλουν να δώσουν όλες οι επιχειρήσεις του χρηματοοικονομικού τομέα στην αντιμετώπιση και την πρόληψη των κινδύνων του Κυβερνοχώρου. Όπως θα δούμε και τα στατιστικά δεδομένα ερευνών δείχνουν το πελώριο φάσμα του προβλήματος και τις οικονομικές επιπτώσεις που έχει η παραβίαση και απώλεια δεδομένων.



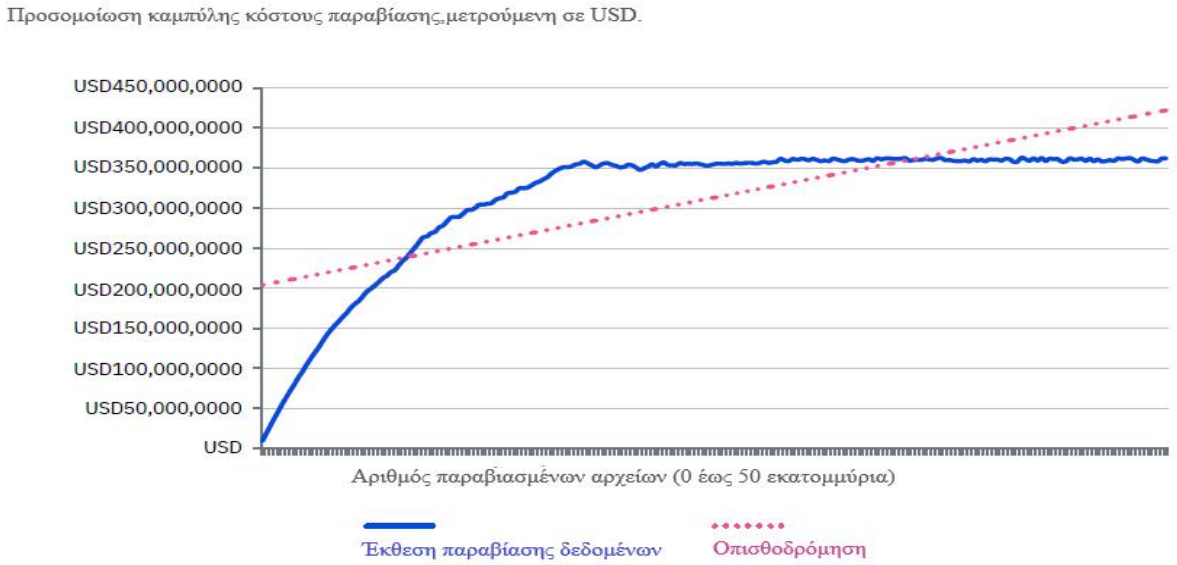
Διάγραμμα 23: Κόστος ανά μονάδα κλεμμένου δεδομένου σε κάθε τομέα και διαφοροποίηση μεταξύ του μέσου όρου των τελευταίων 4 ετών και του 2017,σε δολάρια (USD). (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2017))

Σημαντικό είναι ότι οι κυριότερες αιτίες απώλειες δεδομένων παραμένουν οι κυβερνοεπιθέσεις. Η πιθανή αντιμετώπισή τους αποτελεί το σημαντικότερο παράγοντα μείωσης των απωλειών των δεδομένων και κατά συνέπεια των οικονομικών επιπτώσεων για κάθε επιχείρηση.



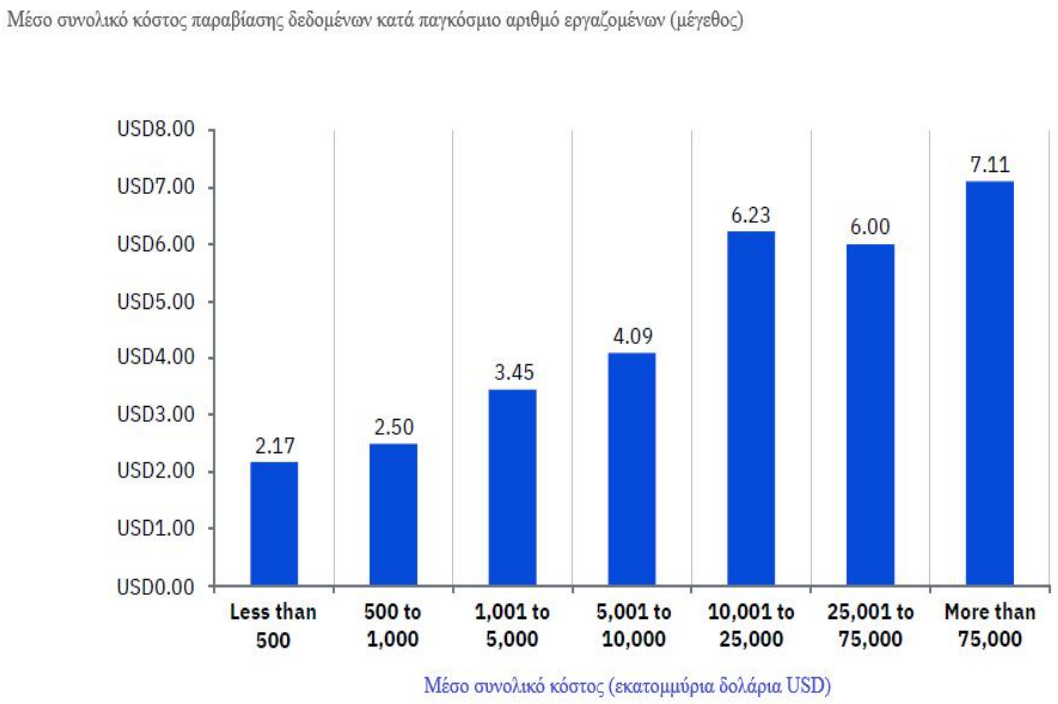
Διάγραμμα 24: Κυριότερες αιτίες απώλειες δεδομένων. (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2019))

Το κόστος των παραβιάσεων δεδομένων που αφορούν περισσότερο από ένα εκατομμύριο καταγεγραμμένα αρχεία τα τελευταία τέσσερα χρόνια. Η ανάλυση αποκαλύπτει μια παραβολική καμπύλη κόστους όπου ο ρυθμός αύξησης του κόστους μειώνεται καθώς το μέγεθος της παραβίασης προσεγγίζει τις 50 εκατομμύρια εγγραφές.



Διάγραμμα 25: Παραβολική καμπύλη κόστους παραβίασης,σε δολάρια (USD). (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2018))

Στο παρακάτω διάγραμμα φαίνεται επίσης μία συστηματική αλληλεπίδραση μεταξύ του συνολικού αριθμού εργαζομένων και του συνολικού κόστους παραβίασης δεδομένων. Εταιρείες με λιγότερους εργαζόμενους έχουν και μικρότερο μέσο συνολικό κόστος.



Διάγραμμα 26: Αλληλεπίδραση μεταξύ του συνολικού αριθμού εργαζομένων και του συνολικού κόστους παραβίασης δεδομένων,σε εκατομμύρια δολάρια (USD). (Πηγή: Ιδια επεξεργασία και μετάφραση, βασισμένο στην έκθεση Cost of Data Breach Study,Global Overview Benchmark research sponsored by IBM Security,Independently conducted by Ponemon Institute LLC (2018))

Ο κλάδος των χρηματοπιστωτικών υπηρεσιών διατρέχει τον μεγαλύτερο κίνδυνο επίθεσης από τον άνθρωπο. Ο αυξανόμενος αριθμός απειλών θα μπορούσε να είναι το αποτέλεσμα της δημόσιας χρήσης ασύρματης σύνδεσης στο διαδίκτυο (WiFi) καθώς και της ταξιδιωτικής δραστηριότητας υψηλότερης από την κανονική, ανέφερε η έκθεση. Οι οργανισμοί χρηματοπιστωτικών υπηρεσιών πλήττονται από τον αυξανόμενο αριθμό επιθέσεων ηλεκτρονικού ψαρέματος (phishing),σύμφωνα με νέα έκθεση της Mobile Security στις χρηματοπιστωτικές υπηρεσίες, που δημοσιεύθηκε από την Wandera. Οι ερευνητές ανέλυσαν 4,7 εκατομμύρια συμβάντα σε ολόκληρο το υποσύνολο των συσκευών κατά τη διάρκεια της περιόδου των 6 μηνών. Μόνο για κινητά, κάθε οργανισμός είχε κατά μέσο όρο 21.000 γεγονότα. Η έκθεση διαπίστωσε ότι σε άλλες βιομηχανίες, το phishing αντιπροσωπεύει το 42% των επιθέσεων, οι οποίες είναι σημαντικά χαμηλότερες από εκείνες του κλάδου των χρηματοπιστωτικών υπηρεσιών, δηλαδή το 57%. Οι κυβερνοεπιθέσεις έπληξαν τις εταιρείες χρηματοπιστωτικών υπηρεσιών κατά 300 φορές περισσότερο από άλλες

εταιρείες, σύμφωνα με έκθεση της Boston Consulting Group (BCG). Ακόμη και με τις επίμονες απειλές, οι χρηματοπιστωτικές επιχειρήσεις αποτυγχάνουν να προετοιμάσουν και να ανταποκριθούν σε επιθέσεις, σύμφωνα με την BCG,και η ηγεσία της εταιρείας δεν δίνει έμφαση στην ασφάλεια στον κυβερνοχώρο ούτε εργάζεται για να πλέξει την εταιρική κουλτούρα.

Πρέπει να εξεταστούν ενδεχόμενα θέσπισης νέων επιλογών όπως ενσωμάτωση τεχνητής νοημοσύνης,μηχανικής μάθησης και βιομετρικών διαπιστευτηρίων στους λογαριασμούς ώστε να βοηθήσει στην αύξηση της εμπιστοσύνης των πελατών και στην αποκατάστασης από ενδεχόμενη επίθεση[60].

6.2 Μελέτη Περίπτωσης της εταιρείας Equifax Inc (EFX.N)

Την Πέμπτη 7 Σεπτεμβρίου 2017 ανακοινώθηκε μία από τις μεγαλύτερες κυβερνοεπιθέσεις και απώλεια προσωπικών δεδομένων. Είχε προηγηθεί αρκετούς μήνες πριν μία από τις μεγαλύτερες απώλειες προσωπικών δεδομένων και πληροφοριών. Η Equifax Inc (EFX.N) δήλωσε ότι το κόστος που σχετίζεται με τη μαζική παράβαση δεδομένων του 2017 είχε αυξηθεί κατά 275 εκατομμύρια δολάρια μόνο το επόμενο έτος, γεγονός που υποδηλώνει ότι το περιστατικό θα μπορούσε να αποδειχθεί η πιο δαπανηρή κυβερνοεπίθεση στην εταιρική ιστορία. Επιπλέον η Equifax πρόκειται να πληρώσει ένα τεράστιο πρόστιμο περίπου 650 εκατομμυρίων δολαρίω[61]ν. Σημαντικό είναι επιπλέον ότι το περιστατικό παραβίασης κρίθηκε με βάση το νόμο περί προστασίας δεδομένων του 1998 και όχι με το GDPR γιατί η διαρροή έλαβε χώρα το 2017. Η ποινή θα ήταν αυστηρότερη αν η ίδια διαρροή είχε κριθεί με την τωρινή νομοθεσία. Συνολικά σε περίπου 145,5 εκατομμύρια ανθρώπους είχαν κλέψει τις πληροφορίες τους, κυρίως στις Ηνωμένες Πολιτείες,συμπεριλαμβανομένων των αριθμών κοινωνικής ασφάλισης,ημερομηνιών γέννησης,διευθύνσεων και σε ορισμένες περιπτώσεις των αδειών οδήγησης. Ενδέχεται να επηρεάσει περίπου 145,5 εκατομμύρια καταναλωτές από τις ΗΠΑ και μέχρι 44 εκατομμύρια κατοίκους στη Μεγάλη Βρετανία. Αν και η επίθεση είχε δηλωθεί ότι ξεκίνησε στα μέσα Μαΐου η παραβίαση δεν παρατηρηθεί μέχρι τις 29 Ιουλίου,σύμφωνα με τον τότε διευθύνοντα σύμβουλο της Equifax Richard F. Smith.

Η Equifax Inc (EFX.N) ιδρύθηκε από τους Cator και Guy Woolford στην Ατλάντα της Γεωργίας, ως Λιανική Πιστωτική Εταιρεία το 1899. Η εταιρεία αναπτύχθηκε γρήγορα και μέχρι το 1920 είχε γραφεία σε όλες τις Ηνωμένες Πολιτείες και τον Καναδά. Αποτελεί

[60] Στην έρευνα των Generali Global Assistance (GGA) και Identity Theft Resource Center (ITRC),The Impact of Cybersecurity Incidents on Financial Institutions (2018)

[61] Πληροφορίες αντλήθηκαν από τον ιστότοπο https://www.secnews.gr/186524/equifax-paraviasi-prostimo/?fbclid=IwAR0pjBiTten7mC7lnYF8DBkdLiPGsr2WJf_COJf9R7Qwe3mniQtjYbvj-tw

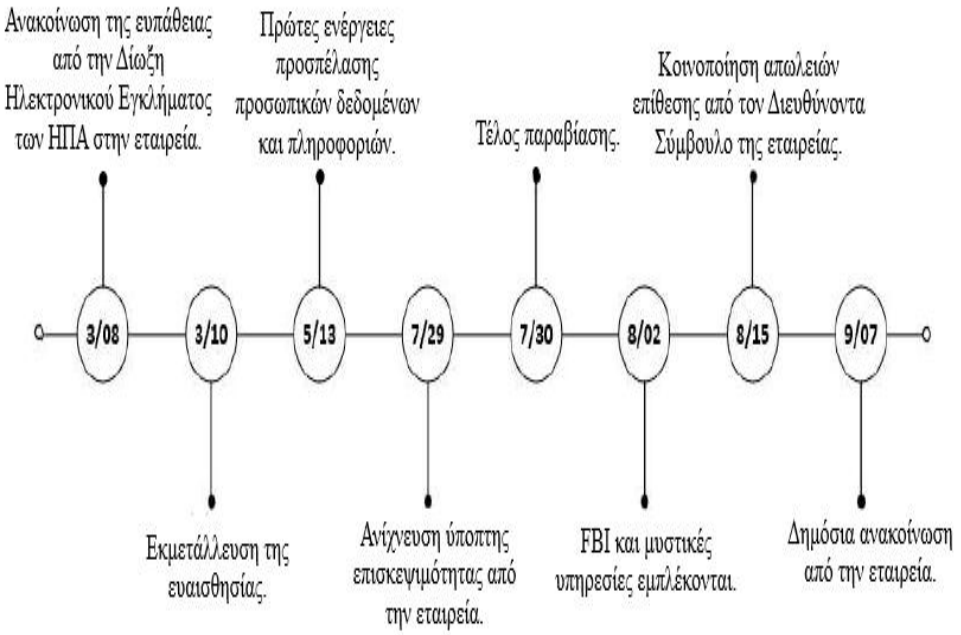
οργανισμό διαχείρισης πιστωτικών καρτών. Είναι ένας από τους τρεις μεγαλύτερους πιστωτικούς οργανισμούς, μαζί με την Experian και την TransUnion (γνωστές και ως Big 3). Λειτουργεί και διαθέτει επενδύσεις σε 24 χώρες σε όλο τον κόσμο,κυρίως σε ολόκληρη την Αμερική, την Ευρώπη και την Ασία. Είναι μέλος του Standard & Poor's (S & P) 500® και απασχολεί 11.000 υπαλλήλους παγκοσμίως. Η Equifax συλλέγει και συγκεντρώνει πληροφορίες για πάνω από 800 εκατομμύρια μεμονωμένους καταναλωτές και πάνω από 88 εκατομμύρια επιχειρήσεις παγκοσμίως. Δραστηριοποιείται επιπλέον στην παροχή πιστωτικών και δημογραφικών δεδομένων και υπηρεσιών σε επιχειρήσεις, κυβερνήσεις και καταναλωτές. Παρέχει επιπλέον παρακολούθηση της πιστωτικής πρόληψης απάτης απευθείας στους καταναλωτές. Είναι μια παγκόσμια εταιρεία ανάλυσης στοιχείων δεδομένων και τεχνολογίας. Είναι ανάδοχος εργασιών τους ιστότοπους του Υπουργείου Υγείας και Ανθρωπίνων Υπηρεσιών των Ηνωμένων Πολιτειών,και άλλους φορείς δημόσιο τομέα.

Σημαντικότερος παράγοντας παραβίασης,όπως προκύπτει από αναφορές και από τον Διευθύνοντα Σύμβουλο της εταιρείας,ήταν η καθυστέρηση ή η αδυναμία υλοποίησης μιας επιδιόρθωσης σε ένα εργαλείο εφαρμογών ιστού που ονομάζεται Apache Struts. Η κουλτούρα της εταιρείας μπορεί να είναι ένας λόγος για την αμέλεια να εφαρμόσει ένα διορθωτικό που γνώριζαν[62].

Άλλοι παράγοντες που συνέβαλαν σε αυτήν την τεράστια καταστροφή της εταιρεία ήταν:

- Μη ασφαλισμένος σχεδιασμός του δικτύου.
- Ανεπάρκεια κρυπτογράφησης προσωπικών πληροφοριών ταυτοποίησης.
- Ύπαρξη αναποτελεσματικών μηχανισμών ανίχνευσης παραβίασης.
- Ανεπαρκής κατακερματισμός και επικοινωνίας τμημάτων και υπομονάδων με τους επικεφαλής τους και τους ανώτατους αξιωματούχους της διοίκησης.
- Υπερβολική αυτοπεποίθηση ικανοτήτων λόγω του μεγέθους της εταιρείας.
- Στο παρακάτω χρονολογικό διάγραμμα παρουσιάζονται με λεπτομέρεια το ιστορικό παραβίασης.

[62] Στο άρθρο των Walia J.,Kulkarni V.,Pyne S.,ELEC-E7470 –Cybersecurity (Group Work – Case Study Article),Aalto University



Χρονολογική σειρά που απεικονίζει την παραβίαση δεδομένων της Equifax

Διάγραμμα 27: Χρονολογική σειρά παρουσίασης των κυριών περιστατικών της παραβίασης Δεδομένων. (Πηγή: Ιδια επεξεργασία, βασισμένο σε άρθρο των Ping Wang, Robert Morris,Christopher Johnson,Cybersecurity Incident Handling,Issues in Information Systems,Volume 19, Issue 3, pp. 150-159 (2018))

Το Apache Struts είναι ένα πλαίσιο εφαρμογών ανοιχτού κώδικα, το οποίο κυκλοφόρησε για πρώτη φορά το 2000 και χρησιμοποιείται από προγραμματιστές ιστού για εφαρμογές ιστού Java EE που υιοθετούν μια αρχιτεκτονική ελεγκτή μοντέλου-προβολής. Το ίδρυμα Apache δημιούργησε ένα πλαίσιο με την ονομασία WebWork που αναπτύχθηκε περαιτέρω για να ενισχύσει το υπάρχον πλαίσιο διατηρώντας παράλληλα την αρχική αρχιτεκτονική. Αργότερα, το 2007 εγκρίθηκε το πλαίσιο WebWork ως Apache Struts 2[63]. Το Apache struts 2 είναι η έκδοση-πλαίσιο που χρησιμοποιήθηκε από τους προγραμματιστές ιστού της Equifax. Λόγω ενός προβλήματος που αντιμετώπισε η συγκεκριμένη έκδοση παρότρυνε τους χρήστες να ενημερώνονται τακτικά για να αποφεύγουν οι 70 τεκμηριωμένες ευπαθείς,κάτι που παρέλειψε η Equifax[64]. Αυτό είχε σαν συνέπεια οι κυβερνοεγκληματίες να εκμεταλλευτούν τα τρωτά σημεία της εφαρμογής .

Κύρια αιτία της παραβίασης των δεδομένων θεωρείται η χρήση και εκμετάλλευση της

[63] Πληροφορίες αντλήθηκαν από τον ιστότοπο www.struts.apache.org
[64] Στο άρθρο των Walia J.,Kulkarni V.,Pyne S.,ELEC-E7470 –Cybersecurity (Group Work – Case Study Article),Aalto University

ταυτότητας των χρηστών ανοίγοντας ψευδείς λογαριασμούς χρησιμοποιώντας προσωπικά στοιχεία των θυμάτων. Οι επιτιθέμενοι ενδέχεται να χρησιμοποιήσουν τα δεδομένα για να μεταφέρουν χρήματα από έναν λογαριασμό σε άλλο,την δημιουργία ψεύτικων λογαριασμών κάτω από το όνομα του χρήστη και μπορούν επίσης να προσπαθήσουν να χρησιμοποιήσουν αυτά τα διαπιστευτήρια για πρόσβαση σε λογαριασμούς σε άλλες επιχειρήσεις ή ιδρύματα, εκμεταλλευόμενοι το γεγονός ότι οι άνθρωποι χρησιμοποιούν συχνά τον ίδιο κωδικό πρόσβασης για πολλούς λογαριασμούς[65]. Μόλις ανακοινώθηκε η παραβίαση της Equifax,οι εμπειρογνώμονες άρχισαν να κρατούν καρτέλες σε σκοτεινούς ιστότοπους περιμένοντας τεράστιες χωματερές δεδομένων που θα μπορούσαν να συνδεθούν με αυτό. Τα δεδομένα όμως δεν εμφανίστηκαν ποτέ αλλά ούτε και χρησιμοποιήθηκαν για οικονομικό όφελος,με αποτέλεσμα να οδηγεί σε μία θεωρία που έγινε ευρέως διαδεδομένη και σκοπός της παραβίασης δεν ήταν η κλοπή. Πιθανότερο είναι να πραγματοποιήθηκε από Κινέζους κατασκόπους υποστηριζόμενη από το κράτο τους[66].

Πίνακας 4: Χρονοδιάγραμμα των γεγονότων που περιβάλλουν την παραβίαση Δεδομένων,αμέσως μετά την ανακοίνωση από την εταιρεία. (Πηγή: Ιδία επεξεργασία)

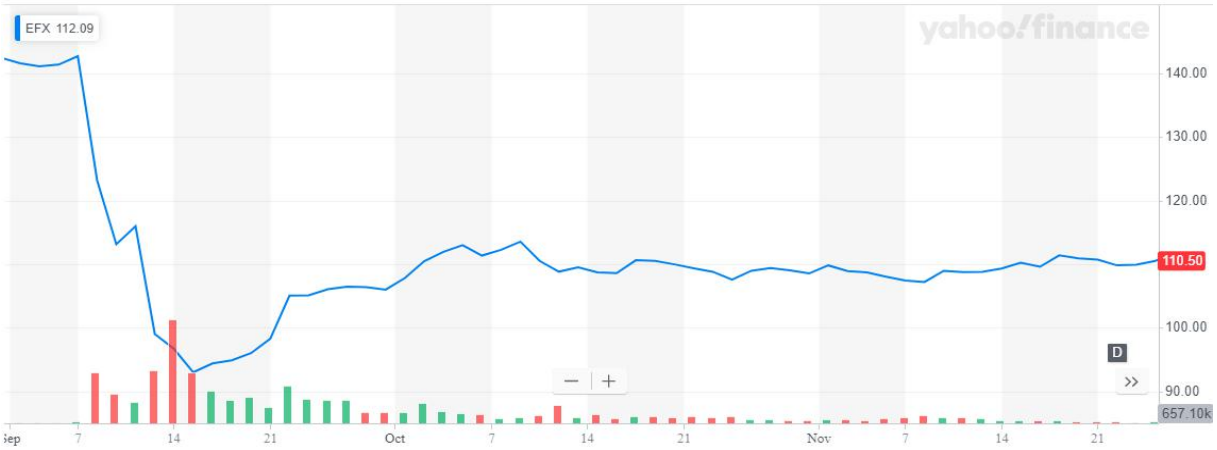
7 Σεπτεμβρίου	Ανακοίνωση της παραβίασης δημόσια από την Equifax
8 Σεπτεμβρίου	Υποχώρησε το μετοχών κατά 13,5% την πρώτη ημέρα διαπραγμάτευσης μετά την ανακοίνωση της παραβίασης.
12 Σεπτεμβρίου	Ανακοίνωση από την εταιρεία ότι δύο ανώτερα στελέχη στον τομέα της ασφάλειας ηλεκτρονικών υπολογιστών στην εταιρεία συνταξιοδοτούνται.
12 Σεπτεμβρίου	Ο Διευθύνων Σύμβουλος της Equifax απολογείται στις Η.Π.Α.
15 Σεπτεμβρίου	Η Equifax ανακοινώνει ότι ο επικεφαλής της υπεύθυνης πληροφόρησης Susan Mauldin και ο επικεφαλής του τμήματος ασφάλειας David Webb αποχωρούν άμεσα.
21 Σεπτεμβρίου	Η Equifax παραδέχεται ότι έστειλε τα θύματα παραβίασης δεδομένων σε έναν ψεύτικο ιστότοπο που μοιράστηκε μια παρόμοια διεύθυνση με εκείνη που δημιούργησε για να βοηθήσει τα θύματα.
26 Σεπτεμβρίου	Η Equifax ανακοινώνει ότι ο CEO της, Richard Smith, αποσύρεται. Ανακηρύσσει ως προσωρινό Διευθύνων Σύμβουλο τον Paulino do Rego Barros.
2 Οκτωβρίου	Η Equifax κυκλοφορεί πληροφορίες από μια έκθεση της εταιρίας Mandiant για την ασφάλεια των υπολογιστών, η οποία εντόπισε επιπλέον 2,5 εκατομμύρια ανθρώπους των οποίων οι πληροφορίες είχαν κλαπεί.
3 Οκτωβρίου	Ο πρώην CEO της Equifax Richard Smith εξετάζεται από την υποεπιτροπή της Προστασίας Καταναλωτών όπου αναφέρει τα λάθη που έγιναν.

Μετά τη δημοσίευση των συμβάντων η τιμή της μετοχής έπεσε κατά 13% με το άνοιγμα των χρηματιστηρίων την επόμενη μέρα. Η μετοχή της Equifax σημείωσε επιπλέον μία πτώση της αξίας κατά 36 % ,σε διάστημα μίας εβδομάδας, μετά από τις αναφορές ότι οι

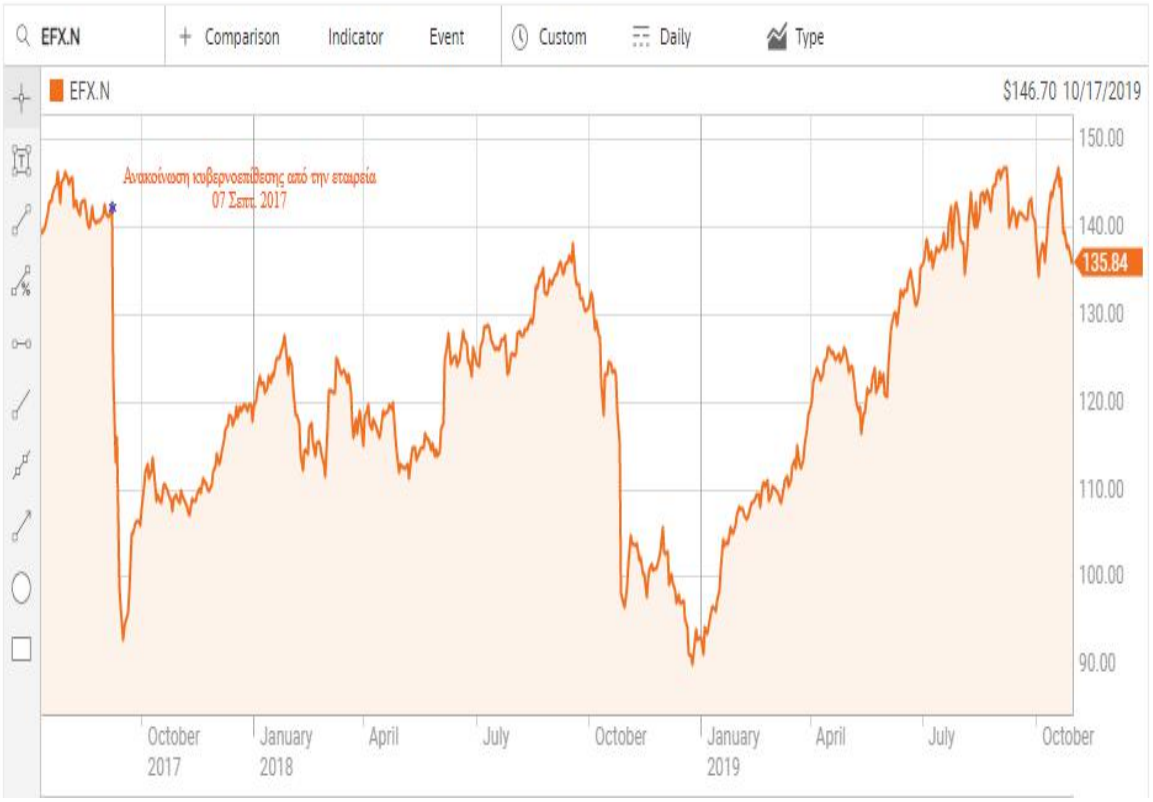
[65] ibid (ό.π.)

[66] Πληροφορίες αντλήθηκαν από τον ιστότοπο www.csoonline.com

εγκληματίες του κυβερνοχώρου είχαν πρόσβαση σε όλα τα προσωπικά δεδομένα. Έτσι όπως φαίνεται και στο διάγραμμα παρά τις προσπάθειες καθησυχασμού παρέμεινε σε πολύ χαμηλά επίπεδα για μεγάλο διάστημα,και την ζημιά δισεκατομμυρίων δολαρίων που προκλήθηκε από την πτώση της μετοχής. Στα παρακάτω διάγραμμα φαίνονται η πορεία της αξίας της μετοχής κατά τις πρώτες δύο εβδομάδες μετά την ανακοίνωση της επιτυχημένης κυβερνοεπίθεσης και της απώλειας των δεδομένων και έπειτα σε όλη αυτή την περίοδο έως και σήμερα.



Διάγραμμα 28: Η τιμή της μετοχής της Equifax τις πρώτες μέρες μετά τη δημοσίευση των συμβάντων παραβιάσεων δεδομένων. (Πηγή: www.finance.yahoo.com)



Διάγραμμα 29: Η τιμή της μετοχής της Equifax από τη δημοσίευση των συμβάντων παραβιάσεων δεδομένων σε διάστημα δύο ετών. (Πηγή: Ιδια επεξεργασία βασισμένο σε άρθρο στο www.reuters.com)

Σημαντικό επίσης είναι να τονιστεί ότι δεν ήταν η πρώτη φορά που η Equifax δέχεται επίθεση,όπως επίσης έχουν δεχτεί και παρόμοιες επιθέσεις κατά το παρελθόν τόσο η Experian όσο και η TransUnion. Το 2013 είχε ανακοινωθεί επίσης από την εταιρεία ότι κάποιοι απέκτησαν μη εγκεκριμενη πρόσβαση στα δεδομένα τεσσάρων σημαντικών ατόμων. Απλά στη συγκεκριμένη περίπτωση απώλεια του 2017,ο όγκος των στοιχείων που εκλάπησαν ήταν τεράστιος όσο και η κρισιμοτητα των πληροφοριών.

Για την αποκατάσταση του προβλήματος καθώς και για την αναβάθμιση του λογισμικού,για την αντιμετώπιση της ευπάθειας του,δαπανήθηκαν περίπου 20 εκατομμύρια δολάρια. Οι New York Times δημοσίευσαν μια έκθεση (2017) στην οποία αναφέρουν ότι η Equifax,σύμφωνα πάντα με πληροφορίες από την ίδια, έχει διαθέσει 690 εκατομμύρια δολάρια για την αποκατάσταση των ζημιών. Πρέπει επιπλέον να συνυπολογιστούν οι δωρεάν παροχές υπηρεσιών που χορηγήθηκαν στους καταναλωτές,με αποτέλεσμα την απώλεια αυτών των εσόδων εκατομμυρίων. Υπήρξαν επιπλέον ακυρώσεις συμβολαίων εκατομμυρίων δολαρίων,κυρίως από κρατικές υπηρεσίες των ΗΠΑ και ακολούθησαν πολλές αγωγές εναντίον της εταιρείας από πελάτες,καταναλωτές και εταιρείες,που ζητούσαν για την κλοπή των προσωπικών στοιχείων τους τεράστιες αποζημιώσεις. Περίπου 240 ατομικές αγωγές και άλλες 60 έρευνες στις οποίες συμμετέχουν οι κυβερνήσεις των Ηνωμένων Πολιτειών,του Ηνωμένου Βασιλείου και του Καναδά. Τέλος έχει χάσει από παραιτήσεις τρία ανώτατα διοικητικά στελέχη και αγωνίζεται συνεχώς για την ανοικοδόμηση της εμπιστοσύνης από τους πελάτες της. Ας μη λησμονούμε ότι τα μεγάλα κάστρα πέφτουν ευκολότερα γιατί έχουν περισσότερες κερκόπορτες.

Σημαντικές είναι οι εξελίξεις στην πρόοδο των αλγορίθμων διαφορικής ιδιωτικής ζωής και των ασφαλιστικών μεθόδων επαλήθευσης δύο παραγόντων είναι μερικές από τις νέες τεχνικές που πρέπει να επενδύσουν η Equifax και άλλοι οργανισμοί παροχής στοιχείων πιστοληπτικής ικανότητας για να περιορίσουν την πρόκληση ζημιών στους καταναλωτές. Κανένα δίκτυο δεν είναι άτρωτο και κάθε εταιρία πρέπει να προσπαθεί να επιτύχει και να διασφαλίσει κάθε βασική ευπάθεια. Η δαπάνη εκατομμυρίων δεν σηματοδοτεί πάντοτε και την προστασία αλλά χρειάζεται και η σωστή διαχείριση από τη διοίκηση της εταιρείας. Οι χρήστες θα πρέπει να έχουν μικρότερη πρόσβαση στις βάσεις δεδομένων μιας εταιρείας έτσι ώστε να μπορεί να εκμεταλλευτεί όσο το δυνατόν λιγότερα δεδομένα από αυτές. Τέλος η χρήση των στρατηγικών διαχείρισης που έχουν αναφερθεί στο προηγούμενο κεφάλαιο θα μπορούσαν να περιορίσουν τα κόστη και τις συνέπειες για την Equifax,όπως και για κάθε άλλη εταιρεία.

ΚΕΦΑΛΑΙΟ 7 ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

Αρχικά μελετήσαμε και ορίσαμε τον Κυβερνοχώρο και τους κινδύνους του. Στοχεύσαμε στην ανάλυση τους σε οικονομικό επίπεδο,ως προς τα κόστη,τις επιπτώσεις και τον χρηματοοικονομικό αντίκτυπο των εταιρειών. Προσδιορίσαμε τις στρατηγικές πρόληψης,διαχείρισης και αντιμετώπισης των κινδύνων του κυβερνοχώρου και εστιάσαμε στις επίθεσης του χρηματοοικονομικού τομέα και στη μελέτη περίπτωσης της εταιρείας Equifax Inc (EFX.N). Με βάση τα δεδομένα των προηγούμενων κεφαλαίων προκύπτουν τα ανάλογα συμπεράσματα που παρατίθενται παρακάτω.

Όλα τα μεμονωμένα άτομα αλλά και οι επιχειρήσεις υιοθετούν τεχνολογίες σύννεφου, ρομποτικής και τεχνητής νοημοσύνης αλλά ελάχιστοι αξιολογούν τους κινδύνους του Κυβερνοχώρου. Αν θέλεις ειρήνη ετοιμάσου για πόλεμο,συμβούλευαν οι Ρωμαίοι στρατηγοί. Για πολλούς οργανισμούς η στρατηγική διαχείριση των κινδύνων του κυβερνοχώρου παραμένει μόνο η πρόληψη. Μόνο όμως ο συνδυασμός της πρόληψης και των σχεδιασμένων στρατηγικών αντιμετώπισης σε περίπτωση του χτυπήματος θα μπορούσαν να εκμηδενίσουν την απώλεια δεδομένων και επομένως τις οικονομικές επιπτώσεις μιας κυβερνοεπίθεσης.

Οι επιχειρήσεις εστιάζουν στο πρωταρχικό ρόλο σύσταση τους και προσπαθούν με το βέλτιστο τρόπο για την επιβίωση και την κερδοφορία τους. Έτσι είναι πολύ πιθανό να αμελούν την ασφάλεια. Η έλλειψη χρόνου των ανώτερων στελεχών για να επικεντρωθούν στους κινδύνους του κυβερνοχώρου δημιουργεί ανησυχία, την ίδια στιγμή που οι απειλές στον κυβερνοχώρο βρίσκονται στο υψηλότερο σημείο όλων των εποχών και η εμπιστοσύνη στην ικανότητα ενός οργανισμού να τις διαχειρίζεται έχει μειωθεί. Με τη σωστή αντιμετώπιση των κινδύνων του Κυβερνοχώρου θα πρέπει όλα τα τμήματα της επιχείρησης να ενημερώνουν τον προϊστάμενό του και αυτοί στη συνέχεια τους ανώτατους αξιωματούχους της διοίκησης. Η συνεργασία του Διευθυντής Πληροφοριών (CIO),του Διευθυντή Τεχνολογίας (CTO),του Οικονομικού Διευθυντή (CFO) και του επικεφαλή Διευθύνοντα Συμβούλου (CEO) θα έχει σαν συνέπεια να εκμηδενίσει τον κίνδυνο απώλειας δεδομένων και πληροφοριών και κατά συνέπεια της οικονομικής ζημιάς. Η ποσοτικοποίηση,η αξιολόγηση και η διαχείριση του κινδύνου και των επιπτώσεων μέσω της στήριξης των εταιρικών σχέσεων και ο καθοριστικός ρόλος των υψηλόβαθμων αξιωματούχων στην ολιστική αντιμετώπιση αυτού του κινδύνου με την οργάνωση και σχεδίαση στρατηγικών προλήψεις και διαχείρισης θα επιφέρει την απόκρουση ενδεχόμενων επιθέσεων και την μείωση της ζημιάς σε περίπτωση επιτυχίας. Ο στρατηγικός άξονας στοχευμένης

αντιμετώπισης των απειλών μέσα από τη συνεχόμενη ενημέρωση των χρηστών σε συνδυασμό με τη βελτίωση των καινοτομων εφαρμογών και συστημάτων Κυβερνοασφάλειας δύναται να εξαλείψουν την αβεβαιότητα των κυβερνοεπιθέσεων.

Ο χρηματοοικονομικός τομέας είναι ένας από τους βασικούς στόχους κυβερνοεπιθέσεων. Αυτό οφείλεται στο μεγάλο όγκο συναλλαγών που πραγματοποιούνται καθημερινά και σε μεγάλο βαθμό στον ηλεκτρονικό τρόπο συναλλαγών τους,κάτι που χαρακτηρίζει την εποχή μας. Τα κόστη των εταιρειών λόγω της απώλειας δεδομένων είναι πολύ μεγάλα αν και στοιχεία κυβερνοεπιθέσεων στον χρηματοοικονομικό τομέα είναι ελάχιστα,διότι οι εταιρείες που πλήττονται αποφεύγουν τη δημοσίευση τους. Οι οικονομικές απώλειες από τη δημοσίευση αυτών των στοιχείων είναι τεράστιες. Ο τρόπος εισβολής στα συστήματα των πληγέντων επιχειρήσεων καθώς και το μέγεθος της ζημιάς είναι δύσκολο να προσδιοριστεί. Στην σχετική έκθεση του Ινστιτούτου Ponemon και της IBM το μέσο συνολικό κόστος μιας παραβίασης των δεδομένων υπολογίζεται περίπου 7,35 εκατομμύρια δολάρια για κάθε Κυβερνοεπίθεση. Σε μία μεγάλη Κυβερνοεπίθεση το κόστος εκτοξεύονται σε εκατοντάδες εκατομμύρια. Το άμεσο κόστος που θα προκύψει στην επιχείρηση λόγω της ελλιπούς ασφάλειας λόγω των αγωγών, των αποζημιώσεων,των ρητρών και των ακυρώσεων των συμβολαίων καθώς και το έμμεσο κόστος της μειώσης των πωλήσεων και επαγωγικά της μείωση του μεριδίου της αγοράς, λόγω της απώλεια της εμπιστοσύνης των πελατών και της δυσφήμισης. Σημαντικό είναι επίσης να σημειωθεί ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) αυξάνει τα ποσά λόγω των αυστηρότερων ποινών και αποζημιώσεων που πρέπει να καταβληθούν, ενώ πρέπει να υπολογιστούν τα αυξημένα κόστη αποκατάστασης και αναβαθμίσεις των συστημάτων ασφαλείας. Οι ηλεκτρονικοί και διαδικτυακοί κίνδυνοι έχουν αρνητική επίδραση σε σχέση με την αγορά και τη διαμόρφωση της χρηματιστηριακής αξίας της μετοχής στην επιχείρηση που πλήττεται. Τέλος πρέπει να επισημάνουμε ότι το κόστος προετοιμασίας και προστασίας από κυβερνοεπιθέσεις είναι πάντοτε μικρότερο από τον οικονομικό αντίκτυπο μιας κυβερνοεπίθεσης.

Παρόλες τις δυσκολίες και τους φόβους η μελλοντική εικόνα της αντιμετώπισης των κινδύνων του Κυβερνοχώρου φαίνεται ιδιαίτερα ενθαρρυντική,δεδομένου ότι αποτελεί κοινή γνώμη ότι υπάρχει τεράστιο περιθώριο ανάπτυξης. Επιπρόσθετα ολοένα και περισσότερες εταιρείες εφαρμόζουν στρατηγικές πρόληψης και αντιμετώπισης,ενώ ενθαρρυντικό είναι η επέκταση αγορών ασφάλισης έναντι αυτής της μορφής των κινδύνων και αποτελεί ένα θέμα με αυξανόμενο ενδιαφέρον της επαγγελματικής και επιστημονικής παγκόσμιας κοινότητας. Αποτελεί μία πολλά υποσχόμενη εναλλακτική αποδοτικής διαχείρισης των κινδύνων του Κυβερνοχώρου.

Πρέπει να γίνει αντιληπτό από όλους ότι περικοπές σε δαπάνες που αφορούν την ασφάλεια του κυβερνοχώρου αυξάνουν τις πιθανότητες να χαθούν τεράστια ποσά. Η ελάχιστη ασφάλεια των επιχειρήσεων γίνεται στόχος κυβερνοεπίθεσης,με αποτέλεσμα τον κίνδυνο απώλειας πνευματικής ιδιοκτησίας και προσωπικών πληροφοριών. Το σύνολο των επιχειρήσεων οφείλουν να υπόκεινται στους νομικούς περιορισμούς και τις διεθνείς συμφωνίες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

- Αλεξανδροπούλου - Αιγυπτιάδου Ε.,Προσωπικά δεδομένα,Εκδόσεις Νομική Βιβλιοθήκη,Αθήνα (2016)
- Γκίνογλου Δ.,Ταχυνάκης Π.,Πρωτόγερος Ν.,Λογιστικά Πληροφοριακά Συστήματα Μηχανογραφημένη Λογιστική, Εκδόσεις Rosili (2004)
- Ελευθεριάδης, Ι.,Διοίκηση Εταιρικών Κινδύνων,Πανεπιστημιακές Σημειώσεις,Πανεπιστήμιο Μακεδονίας (2018), (https://docplayer.gr/23848931-Analysi-epiheirimatikon-kindynon.html)
- Ιγγλεζάκης Ι., Ευαίσθητα Προσωπικά Δεδομένα,Εκδόσεις Σάκκουλα (2003)
- Καλογήρου Ι.,Παναγιωτόπουλος Π.,Τσακανίκας Α.,Σιώκας Ε.,Κοινωνία της Πληροφορίας & Οικονομία της Γνώσης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015)
- Καράκωστας Ι.,Δίκαιο και Ίντερνετ,Εκδόσεις Σάκκουλα,Θεσσαλονίκη (2009)
- Καρασαββίδου – Χατζηγρηγορίου Ε.,Λήψη επιχειρηματικών Αποφάσεων: Προσέγγιση με την επιχειρησιακή έρευνα,University Studio Press (1986)
- Κιουντούζης Ε.,Μεθοδολογίες Ανάλυσης και Σχεδιασμού Πληροφοριακών Συστημάτων,Εκδόσεις Ε. Μπένου,Γ' Έκδοση (2009)
- Μητάκος Θ.,Πληροφοριακά Συστήματα Διοίκησης,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015)
- Πάγκαλος Γ.,Μαυρίδης Ι., Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων,Εκδόσεις Ανικούλα,Θεσσαλονίκη (2002)
- Τριανταφύλλου Β.,Παρασκευάς Μ.,Ασημακόπουλος Γ.,Κοινωνία της Πληροφορίας,Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,Εθνικό Μετσόβιο Πολυτεχνείο,Αθήνα (2015)
- Antonucci D.,The Cyber Risk Handbook,Creating and Measuring Effective Cybersecurity Capabilities, Published by John Wiley & Sons Inc. Hoboken, New Jersey (2017)
- Betz D. J.,Stevens T.,Cyberspace and the State,Toward strategy for cyber-power,Cyber Security Strategic Studies,Adelphi series,iiss,Routledge First Edition (2012)
- Beynon-Davies P.,Business Information Systems,Palgrave Basingstoke (2009)
- Damodaran A.,Εφαρμοσμένη Χρηματοοικονομική για Επιχειρήσεις,Broken Hill (2013)

- Eling M.,Wirfs J.,Cyber Risk: Too Big to Insure?Risk Transfer Options for a Mercurial Risk Class,Institute of Insurance Economics I.VW-HSG,University of St. Gallen (2016)
- Karanzogianni A.,Cyber-Conflict and Global Politics,Contemporary Security Studies, Abingdon Routledge (2009)
- Laudon, K.C.,Laudon, J.P.,Management Information Systems,Macmillan,Second Edition (1988)
- Lefebvre H.,La production de l'espace,Anthropos,Fourth Edition (1974)
- Libicki M.,Cyberdeterrence and Cyberwar,RAND Project Air Force (2009)
- Richard C.,Robert K.,Cyber War: The Next Threat to National Security and What to Do About It,Harpercollins Publishers,First Edition,New York (2010)
- Piccoli G.,Pigni F.,Information systems for managers: with case Louisiana State University,Grenoble School of Management,Prospect Press (2018)

ΑΡΘΡΑ

- Anderson R.,Moore T.,The Economics of Information Security,Science, 314 (5799),(paper-cambridge),p.610-623 (2006)
- Badea L.,Rangu C. M.,Cyber-risk insurance-A big challenge facing contemporary economies,Review of Financial Studies RFS (2018)
- Becker G. S.,Crime and Punishment:An Economic Approach,The Journal of Political Economy,Vol. 76, No. 2,p. 169-217 (1968)
- Bendovschi A.,Cyber-attacks–trends,patterns and security countermeasures,Article in Procedia Economics and Finance (2015)
- Berliner B.,Large Risks and Limits of Insurability,The Geneva Papers on Risk and Insurance-Issues and Practice, 10 (4) p.313-329 (1985)
- Betz D.,Cyberpower in Strategic Affairs:Neither Unthinkable nor Blessed,The Journal of Strategic Studies,Vol. 35, No. 5,p.689–711 (2012)
- Beynon-Davies P.,Business Information Systems,Palgrave Basingstoke (2009)
- Biener C.,Pricing in Microinsurance Markets,World Development,41 (1),p.132– 144 (2013)
- Biener C.,Pricing in Microinsurance Markets,Chair for Risk Management and Insurance,Edited by Schmeiser H.,Working Papers on Risk Management and Insurance No.106,University of St. Gallen (2011)
- Biener C.,Eling M.,Wirfs J.,Insurability of Cyber Risk,The Geneva Papers on Insurance

and Finance,No.14 (2014)

- Biener C.,Eling M.,Wirfs J.,Insurability of Cyber Risk: An Empirical Analysis,The Geneva Papers on Risk and Insurance - Issues and Practice,40 (1),p.131- 158 (2015)
- Bodin D.,Gordon A.,Loeb P.,Wang A.,Cybersecurity insurance and risk-sharing, Journal of Accounting and Public Policy, 37 (6),p.527-544 (2018)
- Böhme R.,Cyber-Insurance Revisited,Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge MA (2005)
- Böhme, R. και Kataria, G.,Models and measures for correlation in cyber-insurance, Workshop on Economics of Information Security-WEIS (2006)
- Bolot J.,Lelarge M.,Cyber Insurance as an Incentive for Internet Security,Managing Information Risk and the Economics of Security,New York: Springer,p.269-290 (2009)
- Brockett P. L.,Golden L. L.,Wolman W.,Enterprise Cyber Risk Management,Risk Management for the Future - Theory and Cases,University of Texas at Austin USA,Chapter 14,p. 319-340 (2012)
- Cebula, J. J.,Young, L. R.,A Taxonomy of Operational Cyber Security Risks, Technical Note, Software Engineering Institute,Carnegie Mellon University (2010)
- Cebula, J. J.,Young, L. R.,Popeck M.,A Taxonomy of Operational Cyber Security Risks Version 2, Technical Note, Software Engineering Institute,Carnegie Mellon University (2014)
- Eling M.,Wirfs J.,What are the actual costs of cyber risk events?, European Journal of Operational Research,Vol. 272,p.1109-1119 (2019)
- Eling M.,Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research,The Geneva Papers (43),p.175–179 (2018)
- Franke, U.,The cyber insurance market in Sweden, Computers & Security,Vol. 68,p.130-144 (2017)
- Geer E. D.,Jr., Sc.D.,Cybersecurity and National Policy,ESSAY Vol. 1 (2010)
- Gordon L.,Loeb M.,Sohail T.,A Framework for Using Insurance for Cyber-Risk Management,Communications of the ACM,Vol. 46,No. 3 (2003)
- Jang-Jaccard J.,Nepal S.,A survey of emerging threats in cybersecurity,Elsevier Enhanced Reader,Journal of Compute and System Sciences, pp 935-9521 (2014)
- Kabay M. E,CISSP Director of Education,Anonymity and Pseudonymity in Cyberspace:Deindividuation,Incivility and Lawlessness Versus Freedom and Privacy Paper, Annual Conference of the European Institute for Computer Anti-virus (1998)

- Khanse A.,Cyber Attacks – Definition Types,Prevention (2016)
- Livanis E.,Financial Aspects of Cyber Risks and Taxonomy for the Efficient Handling of these Risks,14th International Scientific Conference on Economic and Social Development Belgrade,Serbia (2016)
- Lucas R.E. Jr.,Making a miracle,Econometrica,Vol. 61, No. 2,p. 251-272(1993)
- Lyle M. Artz,NetSPA: A Network Security Planning Architecture,MIT (2002)
- Moore T.,Anderson R.,The Economics of Information Security,University of Cambridge, Computer Laboratory (2006)
- Mukhopadhyay A., Saha, D.,Chakrabarti, B., Mahanti, A. and Podder, A., Insurance for Cyber-risk:A Utility Model,Decision, 32 (1),p. 1-19 (2005)
- O'Hara M.,Watson R.,Cavan B.,Managing the three levels of change,Information Systems Management. 16 (3) (1999)
- Patterson R.,Silencing the Call to Arms:A Shift Away From Cyber Attacks as Warfare,Loyola Marymount University and Loyola Law School,Vol. 48:969 (2015)
- Popescu R. C.,Popescu G.,Risks of cyber attacks on financial audit activity,Audit Financiar, XVI, Nr. 1(149) p.140-147 (2018)
- Radanliev P.,De Roure D.,Cannady S.,Mantilla R.,Montalvo R.,Nicolescu R.,Huth M.,Analysing IoT cyber risk for estimating IoT cyber insurance (2018)
- Radanliev P.,De Roure D.,Cannady S.,Mantilla R.,Montalvo R.,Nicolescu R.,Huth M.,Analysing IoT cyber risk for estimating IoT cyber insurance,MPRA Paper No. 92566 (2019)
- Shevchenko P. V.,Peters G. W.,Cohen R. D.,Understanding Cyber-Risk and Cyber-Insurance,Working paper 18-01 (2018)
- Uma M.,Padmavathi G.,A Survey on Various Cyber Attacks and Their Classification,International Journal of Network Security,Vol.15,No.5,p.390-396 (2013)
- Walia J.,Kulkarni V.,Pyne S.,ELEC-E7470 –Cybersecurity (Group Work – Case Study Article),Aalto University
- Wang P.,Morris R.,Johnson C.,Cybersecurity Incident Handling:A case study of the Equifax data breach,Issues in Information Systems,Vol. 19, Issue 3,p.150-159 (2018)
- Waxman M. C.,Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),Yale Journal of International Law Vol. 36,Issue 2,Article 5 (2011)
- Φυσεντζίδης Κ.,Η Σημασία της Ενσωμάτωσης του Κυβερνοχώρου στις Κοινωνικοχωρικές Δομές:Η Κυβερνόπολη,Πανεπιστήμιο Θεσσαλίας,Διδακτορική

Διατριβή,Βόλος (2012)

- Allianz Global Corporate Specialty,A Guide to Cyber Risk (2015)
- A Director's Guide Business Risk,A practical guide for board members,Director Publications Ltd.(2012)
- Basel Committee on Banking Supervision,Operational Risk: Supporting Document to the New Basel Capital Accord Document, Bank for International Settlements (2001)
- Cost of Data Breach Study,Global Analysis 2017,Benchmark research sponsored by IBM,Independently conducted by Ponemon Institute LLC (2017)
- Cost of Data Breach Study:Impact of Business Continuity Management 2018,Benchmark research sponsored by IBM Independently and conducted by Ponemon Institute LLC (2018)
- Cybersecurity in the Boardroom,A 2015 SURVEY ,NYSE Governance Services (2015)
- Deloitte,Assessing Cyber Risk. Critical questions for the board and the C-suite (2016)
- Financial Management of Cyber Risk:An Implementation Framework for CFOs (2010)
- Generali Global Assistance (GGA) και Identity Theft Resource Center (ITRC),The Impact of Cybersecurity Incidents on Financial Institutions (2018)
- Grant Thornton,Taking AIM at Cyber Risk (2018)
- Internet Security Alliance (ISA) and American National Standards Institute (ANSI),The Grant RepRisk,Reprisk Case Study Equifax Data Breach Scandal (2018)
- Joint Publication 1-02,Department of Defense Dictionary of Military and Associated Terms(8 November 2010,As Amended Through 15 February 2016)
- Marsh και Microsoft,Global Cyber Risk Perception Survey (2019)
- Pwc,Insurance 2020 & beyond: Reaping the dividends of cyber resilience (2019)
- State of Cybersecurity,F-Secure (2017)
- Take control of Cybersecurity:A Practical Guide for Officers and Directors,Foley's Cybersecurity Team (2015)
- The National Strategy to Secure Cyberspace,White House Washington DC (2018)
- The cost of incidents affecting CIIs Systematic review of studies concerning the economic impact of cyber-security incidents on critical information,F-Secureenisa (2016)
- Thornton,Taking AIM at cyber risk (2018)
- Πολιτική Κυβερνοάμυνας στις ΕΔ,Γενικό Επιτελείο Εθνικής Άμυνας,Διεύθυνση Κυβερνοάμυνας (2014)

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

- www.google.com/finance
- www.finance.yahoo.com
- www.ft.com
- www.reuters.com
- www.theguardian.com
- www.markets.businessinsider.com
- www.kaspersky.com
- www.livepedia.gr
- www.wikipedia.org
- www.equifax.com
- www.intechopen.com
- www.reprisk.com
- www.iod.com
- www.ibm.com/security/data-breach
- www.ec.europa.eu
- www.warandstrategy.gr
- www.ics.forth.gr
- www.repository.edulll.gr/edulll
- www.ekt.gr/library#0|horizontalTab1
- www.cyberinsurancegreece.com/ereynes
- www.kedisa.gr/kybernoxwros-kybernoepitheseis-kybe
- www.kedisa.gr/kybernoxwros-kybernoepitheseis-kybe
- https://insuranceworld.gr/38069/eidiseis/asfalistikes-eidiseis/psifiopiisi-digitalization-ke-asfalistiki-agora/
- https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/
- http://insuranceinnovation.gr/forum/lloyds-sta-53-dis-to-kostos-mias-pagkosmias-kyvernoepithesis/ | Insurance Innovation
- https://innovationatwork.ieee.org/cyber-security-cyber-attack/
- https://solutions.heritage.org/providing-for-a-strong-defense/cybersecurity/
- https://home.kpmg/gr/el/home/insights/2016/07/cyber-security-facts-and-figures.html
- www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks
- www.struts.apache.org
- www.advisenltd.com

- www.cyberinsurancegreece.com
- www.cyberinsurancequote.gr/insurance
- www.statista.com

- Ζοπουνίδης Κ. και Λιβάνης Ε.,Διαχείριση κινδύνων κυβερνοχώρου:Η νέα πρόκληση για τους CEOs και CFOs.(22/06/2018) www.naftemporiki.gr/printStory/1363646
- Fruhlinger J. CSO,Equifax data breach FAQ: What happened, who was affected, what was the impact?(14/10/2019) www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
- Finance Hit by 300 Times More Attacks Than Other Industries. www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks
- Μυλώπουλος Χ.,Η «ικανοποίηση του παθόντος» και η «ποινική συνδιαλλαγή» στο Ν. 3904/2010. www.mylonopoulos.gr/publication/article/3/i-%C2%ABikanopoiisi-toy-pathontos%C2%BB-kai-i-%C2%ABpoiniki-syndiallagi%C2%BB-sto-n-3904/2010.html
- Clayton M., What's a 'rootkit' again? Hint: It has nothing to do with the stump in your backyard. (07/03/2011) www.csmonitor.com/USA/Military/2011/0307/Cyberwar-glossary
- PwC: Το οικονομικό έγκλημα θεριεύει-Οι πιο γνωστές απάτες.(06/03/2018) www.iefimerida.gr/news/400740/pwc-oikonomiko-egklima-therieyei-oi-pio-gnostes-apates
- Equifax: Πρόστιμο 650 εκατομμυρίων δολαρίων για το hacking του 2017.(22/07/2019) https://www.secnews.gr/186524/equifax-paraviasi-prostimo/?fbclid=IwAR0pjBiTten7mC7lnYF8DBkdLiPGsr2WJf_COJf9R7Qwe3mniQtjYbvj-tw