ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Τμήμα Δημόσιας Διοίκησης

Πρόγραμμα Μεταπτυχιακών Σπουδών

κατεύθυνσης «Φορολογία και Ελεγκτική»

Διπλωματική Εργασία

Διακυβέρνηση Πληροφοριακών Συστημάτων: Διερεύνηση Επάρκειας και του Βαθμού Συμμόρφωσης Πριν την Εφαρμογή του Ευρωπαϊκού Κανονισμού 2016/679

ΚΟΥΛΕΝΤΙΑΝΟΣ ΑΘΑΝΑΣΙΟΣ

Τριμελής Επιτροπή:
Αναπλ. Καθ. Κωνσταντίνος Λιάπης
Ομ. Καθ. Αναστάσιος Τσάμης
Αναπλ. Καθ. Ιωάννης Φίλος

Αθήνα, Ιανουάριος 2018

PANTEION UNIVERSITY

SOCIAL & POLITICAL SCIENCES

Department of Public Administration

Master Program in Taxation and Auditing

Master Thesis

Governance of Enterprise IT: Investigating the Proficiency and Rate of Compliance Before the Establishment of the Regulation (EU) 2016/679.

KOULENTIANOS ATHANASIOS

Examiners Committee:
Assoc. Prof. Konstantinos Liapis.
Prof. AnastasiosTsamis.
Assoc. Prof. Ioannis Filos

Athens, January 2018

Στην Οικογένειά μου,

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά όλους τους Καθηγητές του Μεταπτυχιακού Προγράμματος για τις Πολύτιμες Γνώσεις που μου μετέδωσαν καθ' όλη τη διάρκεια των Σπουδών μου, για την καθοδήγηση τους, καθώς και για την προσπάθεια τους να κάνουν όλη την κοινωνία μας καλύτερη μέσω της πιο καίριας και βασικής μεθόδου, την Εκπαίδευση. Επιπρόσθετα, θα ήθελα να ευχαριστήσω τους επιβλέποντες καθηγητές της τριμελούς εξεταστικής επιτροπής μου (κκ **Κωνσταντίνο Λιάπη, Αναστάσιο Τσάμη** και **Ιωάννη Φίλο**) για την επίβλεψη, συμπαράσταση, στήριξη και συνεργασία που μου προσέφεραν κατά την εκπόνηση της διπλωματικής μου εργασίας, καθώς και για τις υποδείξεις τους σε όλη τη διάρκεια συγγραφής αυτής. Ιδιαίτερα, θα ήθελα να ευχαριστήσω τον υποψήφιο Διδάκτορα **Σταμάτη Πασσά** για την κομβική συμβολή του, ο οποίος με το ήθος του, τα πλούσια πνευματικά του προσόντα και τις υποδείξεις του στάθηκε σημαντικός αρωγός στην προσπάθεια εκπόνησης αυτής της εργασίας.

Επιπροσθέτως, θα ήθελα να ευχαριστήσω όλους όσους ανταποκρίθηκαν στην αποστολή των ερωτηματολογίων. Θα ήθελα να ευχαριστήσω επίσης τους συμφοιτητές και φίλους που με βοήθησαν, ο καθένας με τον δικό του τρόπο.

Τέλος, θερμές ευχαριστίες θα ήθελα να εκφράσω στην οικογένειά μου για την ηθική στήριξη που μου προσέφερε τόσο κατά τη διάρκεια των προπτυχιακών όσο και κατά τη διάρκεια των μεταπτυχιακών σπουδών μου.

Αθανάσιος Κουλεντιανός

Περίληψη

Έχει παρατηρηθεί εντόνως τα τελευταία χρόνια η αύξηση των αναγκών των Οργανισμών, Δημόσιων και Ιδιωτικών, για ορθότερα και αυστηρότερα μέτρα της Ηλεκτρονικής Διακυβέρνησης των φορέων. Τα Πληροφοριακά Συστήματα αποτελούν πλέον αναπόσπαστο στοιχείο των Οργανισμών και των λειτουργιών/ διαδικασιών τους, αυξάνοντας τις αρμοδιότητες της Ηλεκτρονικής Διακυβέρνησης . Ο ρόλος της Ηλεκτρονικής Διακυβέρνησης δεν είναι μόνο η εξασφάλιση και η βελτίωση αυτών των διαδικασιών αλλά και η ασφάλεια τους από εξωτερικούς και εσωτερικούς παράγοντες.

Ο σκοπός της παρούσας διπλωματικής είναι να μελετήσει κατά πόσο οι Ιδιωτικοί Φορείς είναι σε θέση να προσφέρουν την απαραίτητη ασφάλεια στα συστήματα τους σε συνδυασμό με τη συμμόρφωσή τους με το Νέο Γενικό Κανονισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Προσωπικών Δεδομένων(GDPR)

Η εν λόγω εργασία χωρίζεται σε δύο κύρια μέρη. Στο πρώτο μέρος πραγματοποιείται η απαραίτητη βιβλιογραφική επισκόπηση. Στο δεύτερο μέρος παρουσιάζεται η έρευνα που διενεργήθηκε σε Ελληνικούς Ιδιωτικούς Φορείς, με τα αποτελέσματά της, τα συμπεράσματα, τους περιορισμούς της έρευνας καθώς και τις προτάσεις για περαιτέρω μελέτη του φαινομένου.

Ειδικότερα, το πρώτο μέρος της Διπλωματικής Εργασίας είναι το θεωρητικό κομμάτι της. Απαρτίζεται από την Ανάλυση του Γενικού Κανονισμού περί Ασφάλειας Προσωπικών Δεδομένων. Αναλύονται διαδικασίες που πρέπει να συντονίσει η Ηλεκτρονική Διακυβέρνηση και το τμήμα Πληροφοριακών Συστημάτων, για την εξέλιξη, την ασφάλεια και την σωστή χρήση των συστημάτων αυτών. Περιγράφονται τέλος οι εν λόγω απειλές που πρέπει να αντιμετωπίσει η Ηλεκτρονική Διακυβέρνηση.

Το δεύτερο μέρος της εργασίας περιλαμβάνει την έρευνα μαζί με τα αποτελέσματά της και τα συμπεράσματα επ' αυτών. Συγκεκριμένα, στο δεύτερο μέρος περιλαμβάνονται τα ερευνητικά ερωτήματα της παρούσας έρευνας, η μεθοδολογία της, ο πληθυσμός του ενδιαφέροντος, το υπό εξέταση δείγμα, το όργανο μέτρησης και η μέθοδος χορήγησης καθώς και το ερωτηματολόγιο με τη δομή του. Επίσης, περιλαμβάνεται η επεξεργασία των δεδομένων, η χρονική διάρκεια της

έρευνας και η ανάλυσή τους με τη χρήση του Microsoft Excel και διαγραμμάτων. Επιπροσθέτως, παρουσιάζεται το ποσοστό ανταπόκρισης του δείγματος, καθώς και τα αποτελέσματα.

Καταληκτικά, παρουσιάζονται τα συμπεράσματα και η συζήτηση επ' αυτών, οι περιορισμοί της έρευνας και οι προτάσεις για περαιτέρω μελέτη του φαινομένου αυτού καθ' αυτού, αλλά και των λοιπών παραγόντων που σχετίζονται μαζί του.

Ειδικότερα, το δείγμα γνωρίζει σε προσωπικό επίπεδο για τα δικαιώματα που παραχωρεί στους διάφορους φορείς. Οι εταιρίες δεν έχουν προβεί, κατά 1 σημαντικό βαθμό, σε ενέργειες για την ενημέρωση του προσωπικού τους σχετικά με τις αλλαγές που φέρνει ο νέος κανονισμός GDPR. Το δείγμα μας έρχεται τουλάχιστον σε πολύ συχνή επαφή με τα προσωπικά δεδομένα πελατών και παρόλα αυτά δεν έχουν υπάρξει σοβαρές ενημερώσεις και σεμινάρια για τις αλλαγές. Εν συνεχεία αξίζει να σημειωθεί πως το δείγμα δεν έχει αντιμετωπίσει προβλήματα διαρροής δεδομένων και κυβερνοεπιθέσεων.

Λέξεις Κλειδιά: Ηλεκτρονική Διακυβέρνηση, Πληροφοριακά Συστήματα, Ασφάλεια, Διαρροή Δεδομένων, Κυβερνοεπιθέσεις, Ελλάδα, Ιδιωτικός Τομέας, Γενικός Κανονισμός Προσωπικών Δεδομένων.

Abstract

In the recent years, we have to face the needs of both Public and Private sector for more efficient and stricter e-Government measures. The IT systems have grown to be an inseparable part of the Organizational Structure. Furthermore the IT functions are necessary for the everyday working processes of every Organization. The role of E-Governance is not only to ensure and improve these processes, but also to ensure and improve their security by external and internal factors.

The purpose of this Master's Thesis is to analyze if the Private Organizations are in position to offer the security needed for their systems, and in the same time to comply with European's Union General Data Protection and Regulation(GDPR).

This Master's Thesis consists of two main parts. The first part has the necessary bibliographic overview. In the second part presents the research that is carried out to in Hellenic Private Organizations. The second part also includes the results, the limitations of this research, as well as some proposals for further study of this phenomenon.

More specifically, the first part is the theoretical part of this Thesis. It is comprised of the analysis of GDPR. We study the processes that e-Governance and IT department have to coordinate for the evolution, security and the proper use of these systems. Finally, we describe the threats that e-Governance and IT department have to address.

The second part includes the research and the research's results and conclusions. It has the questions used for the purposes of this Thesis, the methodology used, the interest population, the measuring instruments and the questionnaire with its structure. In addition, the second part contains the data processing, research time and the analysis results of Microsoft Excel and some charts for the better understanding of this thesis. The final part explains the results and the response rate of the sample.

Finally, we present the conclusions, the limitations of the research and proposals for further study of this phenomenon and the factors associated with them.

More specifically about the research, the sample appears to be up to date on a personal basis for the rights they provide to the electronic services they use. On the other hand most of the companies in Greece have yet to inform their personnel about the changes that the new European Regulation (GDPR) brings. Furthermore, the sample has not faced neither data leakage nor cyber attacks.

Key Words: e-Governance, Information Systems, Security, Data Leakage, Cyber-attacks, Greece, Private Sector, General Data Protection Regulation (GDPR).

Αρκτικόλεξο

1	ALE	Annualized Loss Expectancy
2	ARO	Annualized Rate of Occurrence
3	BPR	Business Process Re-Engineering-BPR
4	BYOD	Bring Your Own Device
5	CCTA	Central Computer and Telecommunication Agency
6	EDI	Electronic Data Interchange
7	GDPR	General Data Protection Regulation
8	ICT	Internet and Communication Technology
9	ISS	Information System Security
10	IT	Information Technologies
11	MIS	Management of Information Technologies
12	SLE	Single Loss Expectancy
13	ΕΔ	Εταιρική Διακυβέρνηση
14	ΠΣ	Πληροφοριακά Συστήματα
15	Σ.Ε.Ε.	Σύστημα Εσωτερικού Ελέγχου

Περιεχόμενα

Μέρος Πρώτο.

1.1 Εισαγωγή.

Μία εταιρεία αποτελεί έναν ζωντανό οργανισμό, που μεγαλώνει, ακμάζει, προσαρμόζεται στις αλλαγές, πολιτικές, οικονομικές, καθώς και τεχνολογικές προκειμένου να επιβιώσει να συνεχίσει να μεγαλώνει και να συνεχίζει να ακμάζει. Απαρχής κάθε εταιρεία είχε και έχει τις νέες τεχνολογίες και μεθόδους ως «σύμμαχο» στον αγώνα της να παραμείνει ανταγωνιστική και ενημερωμένη.

Με τη μεγάλη άνθιση του Παγκόσμιου Ιστού το 1989, από τον Τιμ Μπέρνερς-Λι και το ερευνητικό Ίδρυμα CERN, άλλαξε μια για πάντα την φιλοσοφία των εταιριών. Με την εισαγωγή του Διαδικτύου ξεκινάει η εποχή της πληροφόρησης. Για τη διαχείριση της πληροφορίας δημιουργούνται νέα τμήματα στις εταιρίες και εν καιρώ αλλάζει το μάρκετινγκ καθώς και η Διακυβέρνηση τους.

Γενικότερα, τα τελευταία 20 χρόνια μπροστά από πάρα πολλές έννοιες μπαίνει η λέξη ηλεκτρονική ή στα αγγλικά το πρόσθετο «e-» τροποποιώντας αυτές τις έννοιες, χαρακτηρίζοντας τις ως ηλεκτρονικές. Η ερώτηση που θα πρέπει να γίνεται κατά αυτή την τροποποίηση είναι κατά πόσο οι επιπτώσεις στην επικοινωνιακή και στην πληροφοριακή τεχνολογία(Information and Communication Technologies-ICT) είναι θετικές.

Στο κομμάτι της Εταιρικής Διακυβέρνησης μπαίνει η έννοια της Ηλεκτρονικής Εταιρικής Διακυβέρνησης. Δημιουργούνται συστήματα εσωτερικής επικοινωνίας όπως εταιρικά ηλεκτρονικά ταχυδρομεία, συστήματα κοινής διαχείρισης και αποθήκευσης πληροφορίας. Οι οργανισμοί αναπτύσσουν τρόπους και μεθόδους αποθήκευσης, διασφάλισης και διαφύλαξης της πληροφορίας. Οι κυβερνοαπειλές και κυβερνοεπιθέσεις αποτελούν καθημερινότητα. Η διαρροή και η απώλεια πληροφοριών μπορεί πλέον να καταστρέψουν τη φήμη και κατά συνέπεια μία εταιρία.

Φτάνοντας στα πιο πρόσφατα χρόνια, η Εταιρική Ηλεκτρονική Διακυβέρνηση καλείται να περιορίσει το ποιος έχει πρόσβαση και που, μέσα στον Οργανισμό. Καλείται να κάνει σωστό επιμερισμό εργασιών και τέλος να θέσουν βάσεις και να

εκπαιδεύσουν το προσωπικό για τις ηθικές διαστάσεις των πληροφοριακών συστημάτων.

1.2 Ηθικές Διαστάσεις και Νέα Νομοθεσία.

Οι εταιρείες στην προσπάθεια τους να μειώσουν την απώλεια πληροφοριών καθώς και την εταιρική κατασκοπεία, έχουν αναπτύξει τέτοια πληροφοριακά συστήματα ώστε να ξέρουν ποιος έχει πρόσβαση και που, καθώς και περιορισμούς ανά χρήστη. Επιπλέον έχουν βρει τρόπους ώστε να ακολουθούν τα ίχνη αυτών που μπορεί να προκάλεσαν κάποια απώλεια κλπ. Στην προσπάθεια αυτή όμως υπεισέρχονται έννοιες διαφύλαξης των προσωπικών δεδομένων, αφού για να επιτευχθεί ο αρχικός στόχος πρέπει να γίνει χρήση και έλεγχος σε προσωπικά δεδομένα των χρηστών. Η έννοια της ηθικής αποκτά διττή έννοια, αφού πρέπει να υπάρξει επαγγελματική ηθική από τους χρήστες και σεβασμός των προσωπικών δεδομένων από το σύστημα ή διαφορετικά υπευθυνότητα και έλεγχος.

Οι πέντε βασικές ηθικές διαστάσεις της εποχής μας:

i. Δικαιώματα και υποχρεώσεις στις πληροφορίες
ii. Δικαιώματα και υποχρεώσεις στην ιδιοκτησία
iii. Υπευθυνότητα και έλεγχος
iv. Ποιότητα συστημάτων
v. Ποιότητα ζωής

Σε όλες τις διαστάσεις πρέπει να διασφαλίζονται και ο χρήστης και το σύστημα εξίσου και οι ισορροπίες αυτών είναι πολύ λεπτές και εύθραυστες. Για την καλύτερη αποσαφήνιση αυτών των εννοιών έχουν αναπτυχθεί διάφοροι εννοιολογικοί κώδικες όπως το *ISACA code of professional ethics* καθώς και *ACM code of ethics.* Ο πρώτος αποτελεί οδηγό επαγγελματικής καθοδήγησης συμπεριφοράς των μελών και των κατόχων του, ενώ ο δεύτερος συγκεκριμενοποιεί κανόνες και περιορισμούς υπό την αιγίδα των επαγγελματικών υποχρεώσεων, οργανωτικής διοίκησης, ηθικές επιταγές και συμμόρφωσης κανονισμών και νόμων.

Ακόμα πιο πρόσφατος είναι ο Νέος Κανονισμός της ΕΕ με αριθμό 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ής Απριλίου 2016, που

αφορά την προστασία των φυσικών προσώπων όσων αφορά την επεξεργασία των προσωπικών δεδομένων και την ελεύθερη χρήση και διακίνηση αυτών, γνωστός και ως Γενική Προστασία Προσωπικών Δεδομένων(GDPR). Ο νέος κανονισμός θα τεθεί σε ισχύ στις 25 Μάη του 2018.

1.3 Ορολογία.

1.3.1 Ηλεκτρονική Διακυβέρνηση.

Για να μπορέσει να ορισθεί η έννοια της Ηλεκτρονικής Διακυβέρνησης, θα πρέπει πρώτα να ορισθεί η έννοια της Διακυβέρνησης. Όπως έχει αναφέρει και ο Rhodes η έννοια της Διακυβέρνησης έχει πάρα πολλές έννοιες για να είναι χρήσιμη (Rhodes, 1997)[1]. Αντίστοιχα, εννοιολογικά αποτελεί μία ζούγκλα σύμφωνα με τον Jordan, ο οποίος τονίζει ότι δεν υπάρχει ένας ορισμός που να γίνεται παγκόσμια αποδεκτός (Jordan, 2008)[2].

Όπως υπάρχει μία ζούγκλα ορισμών για τη Διακυβέρνηση, αντίστοιχα υπάρχει και για την ηλεκτρονική Διακυβέρνηση. Κατά μία απλή αναζήτηση σε κάποια ηλεκτρονική μηχανή αναζήτησης θα προκύψουν ορισμοί όπως:

- Η χρήση πληροφοριακών και επικοινωνιακών συστημάτων σε τομείς όπως δημόσιες υπηρεσίες, στον ιδιωτικό τομέα κλπ.
- Ένα ακόμα μοντέλο Διακυβέρνησης.
- Μία δέσμευση με την Τεχνολογία.
- Η χρήση πληροφοριακών και επικοινωνιακών συστημάτων για καλύτερη ποιότητα υπηρεσιών.

[1] Rhodes, 1997. *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability.* s.l.:s.n.

[2] Jordan, A., 2008. *The Rise of 'New' Policy Instruments in Comparative Perspecive: Has Governance Eclipsed.* s.l.:s.n.

Σύμφωνα με την Palvia και Sharma η εταιρική ηλεκτρονική διακυβέρνηση ασχολείται με τον Ρόλο τον Πληροφοριακών και Επικοινωνιακών Συστημάτων στη διαχείριση οργανωτικών δομών, διαδικασιών και πολιτικών (Palvia, 2007)[3].

Προς αποφυγή συγχύσεων, Ηλεκτρονική Διακυβέρνηση είναι η χρήση των ICT's με τους εξής τρόπους:

- Αλλαγή των δομών διακυβέρνησης με τρόπους ώστε δεν είναι εφικτοί χωρίς τα ICT.
- Δημιουργία νέων δομών και διαδικασιών που δεν είναι εφικτοί χωρίς τα ICT.
- Επισήμανση των νέων ιδεών κανονιστικής Διακυβέρνησης.

Η παραπάνω επισήμανση γίνεται σύμφωνα με τους Frank Bannister και Regina Connolly (F.Bannister, 2016)[4].

1.3.2 Εταιρική Διακυβέρνηση.

Η έννοια της Εταιρικής Διακυβέρνησης, καθότι αφορά μία πολύπλοκη έννοια εναλλασσόμενων δυναμικών και δυνατοτήτων, κατέχει πληθώρα ορισμών στην Παγκόσμια βιβλιογραφία. Σύμφωνα με τον ΟΟΣΑ (OECD, 1999)[5] η Εταιρική Διακυβέρνηση ορίζεται ως ένα σύστημα με το οποίο παρακολουθούνται και ελέγχονται οι επιχειρήσεις. Σύμφωνα με τον La Porta (La Porta, 2000)[6] η Εταιρική Διακυβέρνηση ασχολείται με τους μηχανισμούς, οι οποίοι προστατεύουν τα συμφέροντα των εξωτερικών επενδυτών (μέτοχοι και πιστωτές) ενάντια στις ατασθαλίες των εσωτερικών (διοίκηση / μάνατζερ). Σύμφωνα με τους Shleifer και

[3] Palvia, S. a. S. S., 2007. *E-Government and E-Governance: Definitions/Domain Framework and Status.* s.l.:s.n.

[4] F.Bannister, R., 2016. Defining e-Governance. *INDIANA UNIVERSITY PRESS*, 6, pp. 3-25.

[5] OECD, 1999. *OECD Principles of Corporate Governance.* s.l.:s.n.

[6] La Porta, R. L.-d.-S. F. S. A. a. V. R. W., 2000. *Agency Problems and Dividend Policies around theWorld.* s.l.:Journal of Finance.

Vishny (Shleifer, 1989)[7] η Εταιρική Διακυβέρνηση ασχολείται με το πώς οι χρηματοδότες των επιχειρήσεων θα πάρουν πίσω τα χρήματά τους, εξασφαλίζοντας φυσικά κάποια απόδοση για την επένδυσή τους.

Ο Tricker (Tricker, 1984)[8] αναφέρει ότι εάν η διοίκηση σχετίζεται με τη λειτουργία της επιχείρησης , η Εταιρική Διακυβέρνηση σχετίζεται με το εάν λειτουργεί σωστά.

Η Aguillera (Aguillera, 2005)[9] ορίζουν την ΕΔ ως τη μελέτη της κατανομής των δικαιωμάτων και των ευθυνών μεταξύ των διαφόρων συμμετεχόντων στην εταιρία . Οι συμμετέχοντες είναι τα στελέχη ,οι μέτοχοι ,το Διοικητικό συμβούλιο και άλλα ενδιαφερόμενα μέρη(π.χ. εργαζόμενοι, προμηθευτές και πελάτες).

Ο Monks (Monks, 2002)[10] δηλώνει ότι η Εταιρική Διακυβέρνηση είναι μία διαδικασία αποτελεσματικής λογοδοσίας της διοίκησης σε ενημερωμένους και ενεργούς ιδιοκτήτες.

Οι Gillan and Starks (Gillan and Starks, 1998)[11] ορίζουν την ΕΔ ως ένα σύστημα νόμων, κανόνων και παραγόντων που ελέγχουν τις λειτουργίες μίας εταιρίας. Σύμφωνα με την Ελληνική Επιτροπή Κεφαλαιαγοράς, ως Εταιρική Διακυβέρνηση ορίζεται το σύνολο πρακτικών που υιοθετεί μια επιχείρηση προκειμένου να εξασφαλίσει την αποδοτική λειτουργία της, την προστασία των μετόχων της, αλλά και το σύνολο αυτών που έχουν νόμιμα συμφέροντα στην εταιρία.

---

[7] Shleifer, A. a. V. R. W., 1989. *Management entrenchment: The case of manager specific investments.* s.l.: Journal of Financial Economics.

[8] Tricker, R. (., 1984. *Corporate Governance.* s.l.:Gower Publishing Company.

[9] Aguillera, R., 2005. *Corporate Governance.* s.l.:International Encyclopedia of Economic Sociology.
[10] Monks, R., 2002. *Creating value through corporate governance.* s.l.: Corporate Governance: An international review.

[11] Gillan and Starks, L., 1998. *A survey of shareholder activism: motivation and empirical evidence.* s.l.:Contemporary Finance Digest, Vol. 2, No. 3.

Το βασικό ερώτημα που θα πρέπει να τίθεται, είναι το κατά πόσο η επιλεγμένη Διακυβέρνηση είναι και η «καλή» Διακυβέρνηση.

Τέλος, ένας κοινά αποδεκτός ορισμός είναι ο ακόλουθος: «Εταιρική Διακυβέρνηση είναι το σύνολο νομικών, θεσμικών και εθιμικών ρυθμίσεων, οι οποίες πρέπει να χαρακτηρίζουν τη δραστηριότητα κυρίως των εισηγμένων στα χρηματιστήρια εταιριών, αλλά όχι μόνο αυτών. Απαντά δε, στα ερωτήματα ποιος και πώς ελέγχει τις δραστηριότητες των εταιριών, καθώς και σε ποιους κατανέμονται τα οφέλη, αλλά και οι κίνδυνοι που απορρέουν από την εταιρική δραστηριότητα» (Anon., 2006)[12].

1.3.3 Έννοια Εσωτερικού Ελέγχου.

Ως έννοια ο **εσωτερικός έλεγχος** (internal audit) διακρίνεται για το εύρος και το υψηλό επίπεδο των προσφερόμενων υπηρεσιών του (Drogalas, 2011)[13]. Συχνά όμως, η άγνοια των διοικούντων, υπονομεύει την προσέγγιση και τη σημασία που του αποδίδεται στο σύγχρονο επιχειρηματικό γίγνεσθαι. Το γεγονός αυτό τεκμηριώνει τη μεγάλη έμφαση που καταλογίζεται στην οπτική της στρατηγικής αξιολόγησής του, ως αποτελεσματικό μέσο εκπλήρωσης και επίτευξης των επιχειρησιακών στόχων. Σήμερα, ο ρόλος που καλείται να διαδραματίσει ένα αποτελεσματικό Σύστημα Εσωτερικού Έλεγχου είναι τόσο από την πλευρά της πρόληψης των ενδοεπιχειρησιακών παραλήψεων και ατασθαλιών, όσο και από την οπτική της ελαχιστοποίησης των δυσμενών επιδράσεών τους στην οικονομική μονάδα και στους περιβάλλοντες φορείς της.

[12] Anon., 2006. *ΟικονομικάΧρονικά.* s.l.:s.n.

[13] *Drogalas, G., Pantelidis, P., Tsakpinidou, A.,* Drogalas, G. and Kesisi, E. *(2011) "Internal Audit and Risk Assessment", ESDO 2011*, Greece, Conference Proceedings.

1.3.4 Σύστημα Εσωτερικού Ελέγχου.

Με σκοπό την πληρέστερη εννοιολογική προσέγγιση του εσωτερικού ελέγχου, παρατίθεται η διάκριση των όρων «Σύστημα Εσωτερικού Ελέγχου» και «Εσωτερικός Έλεγχος». Στα πλαίσια της παραπάνω διάκρισης, οι Cook και Winkle (Winkle, 1976)[14] προσομοίωσαν το Σύστημα Εσωτερικού Ελέγχου με το νευρικό σύστημα του ανθρώπου το οποίο απλώνεται στην οικονομική μονάδα μεταφέροντας εντολές και αντιδράσεις από και προς τη Διοίκησή της. Ήτοι, το Σύστημα Εσωτερικού Ελέγχου της οικονομικής μονάδας συνδέεται άμεσα με την οργανωτική της δομή και τους γενικούς κανόνες λειτουργίας της.

Σύμφωνα με έναν ευρύτερο ορισμό, το Σύστημα Εσωτερικού Ελέγχου ορίζεται ως το πλάνο της επιχείρησης και το σύνολο των μεθόδων και διαδικασιών που ακολουθεί η Διοίκηση για να διασφαλίσει την αποδοτική συνεργασία με τη διεύθυνση της επιχείρησης, την πρόληψη και τον εντοπισμό της απάτης και του λάθους, την ακρίβεια και ολοκλήρωση των λογιστικών αρχείων και την έγκαιρη προετοιμασία όλων των χρήσιμων οικονομικών πληροφοριών.

Πιο πρόσφατα, ο Φίλος (Ι., 2004)[15] τονίζοντας τη συνεισφορά του Συστήματος Εσωτερικού Ελέγχου στην επίτευξη των στόχων της οικονομικής μονάδας, όρισε το Σ.Ε.Ε. ως το οργανωμένο σύνολο ελέγχων λειτουργιών και διαδικασιών που καθιερώνεται από τη Διοίκηση με σκοπό την εξάλειψη των αρνητικών επιπτώσεων του οργανισμού, την αποτελεσματική του λειτουργία και την ικανοποίηση των στόχων του.

Ειδικότερα, το Σύστημα Εσωτερικού Ελέγχου περιλαμβάνει τις αρμοδιότητες του προσωπικού, τα εισερχόμενα και εκδιδόμενα δικαιολογητικά, τη διαδρομή και τον έλεγχό τους, και τέλος τους τηρούμενους λογαριασμούς, τον τρόπο και τη μέθοδο ενημέρωσής τους.

Συγκεντρωτικά από όλες τις παραπάνω απόψεις συμπεραίνεται ότι το Σύστημα Εσωτερικού Ελέγχου αποτελεί το πλέγμα όλων των διαδικασιών και

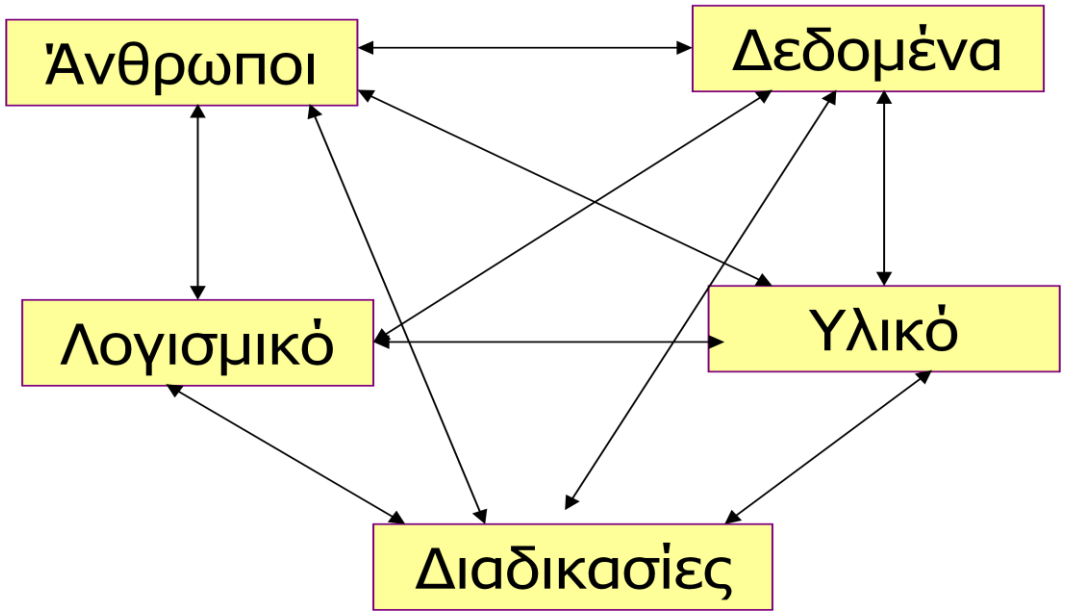
[14] Winkle, C. a., 1976. *Auditing Philosophy and Technique.* s.l.:s.n.

[15] Ιωάννης Φίλος., 2004. *Σύστημα Εσωτερικού Ελέγχου Επιχειρήσεων.* s.l.:s.n.

πολιτικών που: προάγουν την ακρίβεια και αξιοπιστία των λογιστικών και επιχειρησιακών δεδομένων, προστατεύουν τους πόρους της οικονομικής μονάδας από τη σπατάλη και την απάτη, εκτιμούν την πιστή εφαρμογή της πολιτικής της Διοίκησης από τα διάφορα τμήματα και γενικότερα αξιολογούν τη συνολική αποτελεσματικότητα και απόδοση των λειτουργιών της οικονομικής μονάδας (Alexander Hamilton Institute, 2005) (Institute, 2005)[16].

2.1 Πληροφοριακά Συστήματα.

Ένα ολοκληρωμένο Πληροφοριακό Σύστημα αποτελείται από ένα σύνολο αρχών, διαδικασιών και μίας ορισμένης από την επιχείρηση οργανωτικής δομής. Τα παραπάνω σε συνδυασμό με το προσωπικό, τα δεδομένα της εταιρίας, τις εγκαταστάσεις, τα επικοινωνιακά συστήματα και το λογισμικό δημιουργούν την έννοια του Πληροφοριακού Συστήματος.



[16] Institute, A. H., 2005. *Survey of Modern Business Science*. s.l.:s.n.

2.2 Κίνδυνος.

Όταν αναφερόμαστε στην έννοια του κινδύνου, μιλάμε για τη δυνητική πιθανότητα ζημίας που μπορεί να προκύψει είτε άμεσα σε μία διαδικασία, είτε έμμεσα από κάποιο μελλοντικό γεγονός. Οι οργανισμοί στην προσπάθεια τους για τη μείωση της ζημίας αυτή αρχικά προσπαθούν μέσω διαδικασιών, συστημάτων, κανονισμών και αρχών προσπαθούν να την προλάβουν από το να συμβεί.

Λόγω του κινδύνου αναπτύχθηκε και η έννοια της επικινδυνότητας, της πιθανότητας να πραγματοποιηθεί ο επικείμενος κίνδυνος. Για την ανάλυση και τον καλύτερο προσδιορισμό της επικινδυνότητας υπάρχουν κάποιες ερωτήσεις που πρέπει να γίνουν:

- Τι μπορεί να συμβεί; (Αναγνώριση Απειλής)
- Ποιες θα είναι οι συνέπειες; (Αναγνώριση Πιθανών Συνεπειών)
- Ποια είναι η πιθανότητα επανάληψης του γεγονότος; (Συχνότητα)
- Εξακρίβωση βαθμού αβεβαιότητας. (Αβεβαιότητα)

Ο βασικός τύπος για την Επικινδυνότητα ορίζεται ως το γινόμενο της Πιθανότητας να συμβεί επί του Επικείμενου Προσδιορισθέντος Κόστους (Ε=Π*Κ). Διαφορετικά σύμφωνα με τον Σωκράτη Κάτσικα (Κάτσικας, n.d.)[17] Β>Ρ*L, όπου Β το κόστος Πρόληψης, Ρ η πιθανότητα και L το συνολικό Κόστος της Απώλειας. Η λογική του παραπάνω τύπου έγκειται στο αν συμφέρει τον οργανισμό να πληρώσει το κόστος της πρόληψης.

Παρόλη την απλότητα του παραπάνω τύπου, αξίζει να σημειωθεί ότι η προσέγγιση των επιμέρους μερών του είναι αρκετά δύσκολη, έως και αδύνατη σε συγκεκριμένες περιπτώσεις. Πιο συγκεκριμένα, θα μπορούσαν οι επιπτώσεις να επηρεάσουν τη φήμη της εταιρίας, όπου το κόστος εκτός από υπέρογκο, δεν είναι και υπολογίσιμο.

[17] Κάτσικας, Σ. Π., n.d. *Ανάλυση, Αποτίμηση και Διαχείρηση Επικινδυνότητας Πληροφοριακών Συστημάτων.* s.l.:s.n.

2.2.1 Διαχείριση Κινδύνου στα Πληροφοριακά Συστήματα.

Η διαχείριση του κινδύνου από τα Πληροφοριακά Συστήματα γίνεται μέσα από την ουσιαστική κατανόηση και αντιμετώπιση παραγόντων που δυνητικά θα μπορούσαν να οδηγήσουν τον οργανισμό σε έλλειψη εμπιστευτικότητας, από το κοινό της, ακεραιότητας ή και της διαθεσιμότητας του πληροφοριακού της συστήματος. Κίνδυνος για τα Πληροφοριακά Συστήματα θα μπορούσε να προκληθεί από μία βλάβη σε κάποια διαδικασία, ή από την απώλεια κάποιας πληροφορίας. Με λίγα λόγια ο κίνδυνος των πληροφοριακών συστημάτων προκύπτει σε συνάρτηση της αξίας των εταιρικών περιουσιακών στοιχείων, των ευπαθειών του και των πιθανών απειλών που μπορεί να προκύψουν.

2.2.2 Ευπάθειες.

Ευπάθεια είναι ένα ελάττωμα ή μία αδυναμία σε κάποιο σημείο του συστήματος. Η Ευπάθεια μπορεί να οφείλεται στην μη ύπαρξη σαφούς πολιτικής και εταιρικής ιεραρχίας στις προσβάσεις. Μπορεί να οφείλεται στην ελλιπή εκπαίδευση του προσωπικού, στην μη ύπαρξη σχεδίου εκτάκτου ανάγκης, στην έλλειψη αντιγράφων ασφαλείας και μεθόδων άμεσης ανάκτησης τους και πολλά άλλα γεγονότα που δημιουργούν λειτουργικά προβλήματα στην εταιρία.

2.2.3 Απειλές.

Ως απειλή ορίζουμε μία μη επιθυμητή ενέργεια η οποία μπορεί να προκαλέσει κάποια δυσλειτουργία στις οργανικές διαδικασίες. Πιο συγκεκριμένα θα μπορούσαμε να μιλήσουμε για τις Απειλές-Πηγές (threats-sources), όπου εκεί έχουμε την πρόθεση ή ενέργεια με την οποία παραποιείται κάποια διαδικασία, υπάρχει εκμετάλλευση μία ευπάθειας για τη δημιουργία ζημίας στην εταιρία. Αναλυτικότερα διαχωρίζουμε στα εξής:

- Λανθασμένη/Τυχαία Γνωστοποίηση: η μη εξουσιοδοτημένη δημοσιοποίηση διαβαθμισμένων και προσωπικών δεδομένων.

- Φυσικές Καταστροφές.
- Τροποποίηση Λογισμικού: Μία εκ προθέσεως τροποποίηση λογισμικού, που οδηγεί σε απώλεια δεδομένων, θέτει σε κίνδυνο το απόρρητο και τις διαδικασίες τις εταιρίας. Παραδείγματα αυτών είναι ο Κακόβουλος Κώδικας, Λογικές Βόμβες, Δούρειοι Ίπποι, Καταπακτές και Ιοί.
- Χρήση Εύρους Ζώνης: Η τυχαία και λανθασμένη χρήση του εύρους ζώνης των επικοινωνιών.
- Σκόπιμη Αλλοίωση Δεδομένων.
- Σφάλμα Ρυθμίσεων.
- Δυσλειτουργία/Διακοπή Λειτουργιών και Τηλεπικοινωνιών.

2.2.4 Κατηγοριοποίηση Κινδύνων - Απειλών Πληροφοριακών Συστημάτων.

Βάση των βασικών πόρων των πληροφοριακών συστημάτων, δηλαδή το υλικό (hardware) από το οποίο αποτελούνται, το λογισμικό (software) και φυσικά τα δεδομένα, οι εταιρίες αντιμετωπίζουν τις εξής απειλές βάση του Pfleeger (Pfleeger, 1997)[18]:

- Υποκλοπή (interception): Η διαδικασία κατά την οποία ένα μη εξουσιοδοτημένο μέλος καταφέρνει να υποκλέψει κάποια πληροφορία, να αντιγράψει κάποιο πρόγραμμα, παρακολούθηση ροής δεδομένων και επικοινωνιών κ.α. προσπελάζοντας την ασφάλεια των δικτύων και της εταιρίας. Αφορά και επηρεάζει το κομμάτι της εμπιστευτικότητας.
- Μεταβολή (modification): Κάποιο μη εξουσιοδοτημένο μέλος αφού καταφέρει και αποκτά έγκριση πρόσβασης, καταφέρνει και παραποιεί και τα δεδομένα, προγράμματα κλπ. Με αυτό τον τρόπο μπορεί κάποια εργασιακή διαδικασία να αχρηστευθεί ή να χάσει το νόημα της, τα αποτελέσματα κάποιας έρευνας να είναι αναληθή. Η απειλή αυτή αφορά την ακεραιότητα του συστήματος.
- Πλαστογραφία (fabrication): Μία διαδικασία που επηρεάζει μόνο τα δεδομένα της εταιρίας. Επιτυγχάνεται μόνο με την εισαγωγή παραποιημένων/

[18] Pfleeger, C., 1997. *Security Computing, Prentice Hall International*. s.l.:ISBN.

εσφαλμένων εγγράφων και δεδομένων για την παραποίηση αποτελεσμάτων. Η απειλή αυτή είναι κατά της ακεραιότητας του συστήματος.

- Διακοπή (interruption): Η αδρανοποίηση ή αχρήστευση ενός κομματιού του συστήματος ή ακόμα και παντελής διαγραφής του. Αυτό θα μπορούσε να σημαίνει καταστροφή μίας συσκευής ακόμα και απώλεια δεδομένων ή προγραμμάτων. Η απειλή αφορά τη διαθεσιμότητα του συστήματος και αυτό μπορεί να σημάνει μεγάλη απώλεια κερδών.

2.3 Ανάλυση και Αξιολόγηση Κινδύνου.

Οι μάνατζερ των εταιρειών, καλούνται πολύ συχνά να λάβουν κάποιες αποφάσεις σχετικά με τους υποκείμενους κινδύνους. Για την εύστοχη απόφαση πρέπει να γίνει ορθή ανάλυση και αξιολόγηση του κίνδυνου. Οι απόφαση έχει να κάνει με την αποτροπή του κινδύνου, την αποδοχή του ακόμα και τη μείωση του μέσω μέτρων. Στην απόφαση αυτή συμβάλει το κόστος του μέτρου και το κόστος αποδοχής του κινδύνου, που όπως ήδη αναφέρθηκε δεν μπορούμε να είμαστε σίγουροι για τις επιπτώσεις του. Πολλές φορές οι εταιρίες μειώνουν το κόστος τους δίνοντας σε άλλη εταιρία να αναλάβει τον προκείμενο κίνδυνο (outsourcing).

Η ανάλυση του κινδύνου περιλαμβάνει:

- Διαδικασίες Εντοπισμού.
- Ανάλυση.
- Μέτρα αντιμετώπισης.
- Πρόβλεψη.
- Διορθωτικές Ενέργειες.

Τέλος υπάρχουν δύο βασικοί μέθοδοι ανάλυσης κινδύνου, η ποσοτική μέθοδος (quantitative) και η ποιοτική (qualitative).

2.3.1 Ποσοτική Μέθοδος.

Η ποσοτική μέθοδος χρησιμοποιείται κυρίως από ασφαλιστικές εταιρίες, τράπεζες κλπ, όπου στην ουσία με τι κατάλληλες ποσοτικές πληροφορίες αναλύονται ο κίνδυνος και οι επιπτώσεις ως έμμεσες και άμεσες δαπάνες. Το μειονέκτημα της μεθόδου οφείλεται στο ότι δεν είναι εύκολο να ποσοτικοποιηθούν όλες οι συνιστώσες του κινδύνου.

Μαθηματικά θα μπορούσε να προσδιορισθεί ως η Ετησιοποιημένη Απώλεια Προσδόκιμου (Annualized Loss Expectancy (ALE). Η ετησιοποιημένη Απώλεια Προσδόκιμου υπολογίζεται ως το γινόμενο του Ενιαίου Προσδόκιμου Απώλειας (Single Loss Expectancy) επί του Ετησιοποιημένου Ρυθμού Εμφάνισης (Annualized Rate of Occurrence) ALE=SLE*ARO (Steve, n.d.).

Ο υπολογισμός συναντά δυσκολίες στατιστικής φύσης, καθώς και δεν είναι από να υπολογισθούν με ακρίβεια έννοιες όπως η αξία των πληροφοριών, το κόστος ανάκτησης κ.α.. Αντίστοιχα είναι σχεδόν αδύνατο να υπολογισθεί το ποσοστό του κινδύνου κατά απόλυτο νούμερο.

2.3.2 Ποιοτική Αξιολόγηση Κινδύνου.

Οι ποιοτικές εκτιμήσεις κινδύνου έχουν ως δεδομένο την μεγάλη αβεβαιότητα της πιθανότητας και των επιπτώσεων του κινδύνου. Όπως και στην ποσοτική μέθοδο, έτσι και στην ποιοτική δυσκολίες προκύπτουν κατά τον υπολογισμό του κινδύνου. Για αυτό η εκτίμηση του θα πρέπει να γίνεται σε κλίμακες πολλαπλής εκτίμησης του κινδύνου.

Από τον υπολογισμό και μετά ο Κίνδυνος χαρακτηρίζεται ως «Υψηλός», «Μέτριος» και «Χαμηλός. Η κοινοποίηση των αποτελεσμάτων μπορεί να γίνει σε συνδυασμό με τον κίνδυνο, την περιγραφή των αποτελεσμάτων τους και την πιθανότητα να συμβεί.

Τα άτομα που διαχειρίζονται τον Κίνδυνο είναι υπεύθυνα στο να συντάξουν ένα τέτοιο που πίνακα, που θα πρέπει όμως να αναθεωρείται από τους ίδιους. Ο

παραπάνω κατάλογος θα μπορούσε να συνδυαστεί με ένα κατάλογο μεθόδων αντιμετώπισης τους.

2.4 Εύρεση Ευπαθειών.

Όλα τα συστήματα έχουν ευπάθειες, σημεία στα οποία καιροφυλακτούν κίνδυνοι. Σημαντικό λοιπόν για τους οργανισμούς είναι να εντοπίσουν τις ευπάθειες τους και να τις διορθώσουν ή να τις κάνουν λιγότερο ευπαθείς. Ένα βασικό πρώτο βήμα είναι ο έλεγχος και επανεξέταση του ήδη υπάρχοντα καταλόγου αδυναμιών, εφόσον υπάρχει, διαφορετικά πρέπει να ξεκινήσουν να χωρίζουν τα πεδία σε περιοχές ελέγχου. Εν συνεχεία, σε συνεργασία με τα άτομα που γνωρίζουν καλύτερα τις περιοχές, γίνεται ο εντοπισμός των αδύναμων και πιθανώς τρωτών σημείων.

Κάποια γνωστά εργαλεία:

- *Σαρωτές Ευπαθειών*: Αποτελείται από λογισμικό που εξετάζει το λειτουργικό σύστημα, και αναζητά συγκεκριμένα σημεία με βάση δεδομένων ελαττωματικών υπογραφών.
- *Δοκιμές Εισχώρησης:* Εύρεση τρωτών σημείων από αναλυτές, μέσω της προσπάθειας να ασκήσουν απειλές κατά του συστήματος.
- *Διαχειριστικός Έλεγχος Λειτουργιών:* Τα τελευταία χρόνια έχουν αναπτυχθεί βέλτιστες μέθοδοι διακυβέρνησης όπως το ISO 17799, και πολλά άλλα φυσικά. Πάντα μπορεί να γίνει αναθεώρηση διαδικασιών με βάση αυτές τις βέλτιστες μεθόδους. Δεν είναι τυχαίο που οι εταιρείες προσπαθούν εντόνως τα τελευταία χρόνια να λάβουν πιστοποιήσεις από αυτές τις βέλτιστες μεθόδους διακυβέρνησης. Οι πιστοποιήσεις αυτές φέρουν αξιοπιστία και κύρος στις εταιρίες που τις κατέχουν και εξακολουθούν να τροποποιούν και να αλλάζουν τα συστήματα τους βάση των βέλτιστων μεθόδων.
- *Λίστα Ευπαθειών:* Όπως έχει ήδη αναφερθεί, είναι σημαντικό να διατηρείται λίστα με γνωστές ή παλαιότερες ευπάθειες. Η τεχνική αυτή βοηθάει στις μελλοντικές εκτιμήσεις καθώς και στη συνοχή μεταξύ των ελέγχων.

2.5 Διαχείριση Κινδύνου.

Η διαχείριση του Κινδύνου γίνεται σε 3 στάδια. Το πρώτο στάδιο περιλαμβάνει την εκτίμηση του. Το δεύτερο στάδιο περιλαμβάνει τον περιορισμό του και το τρίτο στάδιο την αξιολόγηση του κινδύνου. Το πρώτο βήμα περιλαμβάνει τον καθορισμό του και την αξιολόγηση του κινδύνου, όπως και τη σύσταση μέτρων για περιορισμό και τη μείωση του κινδύνου. Στο δεύτερο βήμα θέτονται προτεραιότητες και μέτρα για την καταπολέμηση του κινδύνου, καθώς και αξιολόγηση των μέτρων αυτών. Το τρίτο και τελευταίο βήμα περιλαμβάνει τη διαδικασία συνεχούς αξιολόγησης του κινδύνου.

Η Διαχείριση Κινδύνου θα μπορούσε να χαρακτηρισθεί ως η διαδικασία που προσφέρει ισορροπία των λειτουργικών, οικονομικών μέτρων για την καταπολέμηση του Κινδύνου σε σχέση με τα οφέλη που αυτά φέρουν στον οργανισμό. Η διαδικασία αυτή δεν συναντάται μόνο στα Πληροφοριακά Συστήματα.

2.5.1 Εκτίμηση Κινδύνου.

Η εκτίμηση του Κινδύνου είναι η πρώτη διαδικασία που λαμβάνει χώρο κατά τη Διαχείρισης ενός Κινδύνου. Οι εταιρίες προσπαθούν κατά τη διάρκεια της διαδικασίας να προσδιορίσουν τον κίνδυνο και να κατανοήσουν την έκταση του κατά τη διάρκεια ζωής του πληροφοριακού συστήματος. Το αποτέλεσμα αυτού είναι η καταλληλότερη προσέγγιση και μείωση των αποτελεσμάτων του κινδύνου.

2.5.2 Βασικές Μέθοδοι Διαχείρισης Κινδύνου.

Οι τέσσερις βασικές στρατηγικές Διαχείρισης Κινδύνου είναι ο Μετριασμός, η Μεταβίβαση, η Αποδοχή και η Αποφυγή.

Ο Μετριασμός περιλαμβάνει τον καθορισμό των Ευπαθειών και τον καθορισμό αντισταθμιστικών ελέγχων και μεθόδων για τον περιορισμό του κινδύνου.

Μεταβίβαση είναι η διαδικασία που η εταιρία προσλαμβάνει ένα τρίτο εξειδικευμένο μέλος για να αναλάβει τον κίνδυνο. Αυτό δε σημαίνει απαραίτητα ότι διορθώνονται οι ατέλειες και οι ευπάθειες, αλλά σίγουρα μειώνεται το οικονομικό κόστος των επιπτώσεων.

Η Αποδοχή συνεπάγεται αποδοχή των χαμηλών κινδύνων και έτσι το σύστημα συνεχίζει με να δουλεύει με αυτούς. Παρόλα αυτά θα πρέπει να γίνεται έλεγχος και εκτίμηση των κινδύνων ακόμα και μετά την αποδοχή τους.

Τέλος η Αποφυγή είναι η στρατηγική στην οποία αφαιρούνται ή αντικαθίστανται τα ευάλωτα σημεία του συστήματος.

Όποια στρατηγική και να ακολουθηθεί θα πρέπει να πρώτα να καταγραφεί σε επίσημα έγγραφα και να γίνει αποδεκτή από τους Διαχειριστές του Κινδύνου.

2.5.3 Αντίμετρα.

Τα μέτρα ασφαλείας ή αντίμετρα αποτελούνται από ενέργειες, διαδικασίες, τεχνικές ή ακόμα κατασκευές ή συσκευές που περιορίζουν τις ευπάθειες του συστήματος. Η διαφορετικές φύσεις των μέτρων συμβάλουν στην ανάλυση των πληροφοριακών συστημάτων στις εξής συνιστώσες (G.Pangalos, 1997)[19]:

- Φυσική Ασφάλεια Συστήματος (physical security): Μέθοδοι προστασίας του εξοπλισμού και των εγκαταστάσεων από φυσικές καταστροφές, κλοπές, βανδαλισμούς, φωτιές κλπ.
- Ασφάλεια Υπολογιστικού Συστήματος (computer security): Η αναφορά γίνεται για την προστασία της πληροφορίας που είναι άμεσα προσβάσιμη από τον ηλεκτρονικό υπολογιστή (προγράμματα, εφαρμογές, αρχεία δεδομένων).
- Ασφάλεια Βάσεων Δεδομένων (database security): Η ασφάλεια αυτή αφορά εφαρμογή πολιτικής ως προς τις εξουσιοδοτήσεις του ποιος μπορεί να δει τι και του ποιος μπορεί να τροποποιήσει τι.

[19] G.Pangalos, 1997. *Security of Medical Database Systems for Health Care IT and Security Personnel.* s.l.:s.n.

- Ασφάλεια Δικτύων (network security): Αναφέρεται στην ασφάλεια και προστασία των πληροφοριών κατά την επεξεργασία τους, μετάδοση τους μέσω τηλεφωνικών γραμμών, ηλεκτρονική μετάδοση τους κλπ.

2.5.4 Αποτελεσματικότητα Μέτρων.

Η αποτελεσματικότητα των μέτρων/αντίμετρων ασφαλείας εξαρτώνται από την αποτελεσματικότητα τους (effectiveness). Αναφορικά μερικοί παράγοντες που συμβάλουν στην αποτελεσματικότητα σύμφωνα με τον Pfleeger (Pfleeger, 1997) [20]είναι οι εξής:

- Επίγνωση του μεγέθους του προβλήματος. Οι υπεύθυνοι για την εφαρμογή των μέτρων θα πρέπει αρχικά να έχουν πειστεί για την αναγκαιότητα και το επίπεδο της ασφάλειας, το οποίο έχουν λάβει.
- Περιοδικές και συστηματικές αναθεωρήσεις. Η αμφισβήτηση της συνέπειας ενός μέτρου πρέπει να γίνεται συνεχώς, ώστε να υπάρχει αναθεώρηση του ανά πάσα ώρα και στιγμή. Θα πρέπει να μην ξεχνάμε ποτέ τη δυναμικότητα του συστήματος. Αυτό συνεπάγεται πως οι συνθήκες, οι ανάγκες και απειλές του συστήματος δεν σταματούν ποτέ να αλλάζουν και να εξελίσσονται. Οπότε τα μέτρα για να παραμένουν αποτελεσματικά θα πρέπει να προσαρμόζονται ή να αντικαθίστανται.
- Συσχέτιση μέτρων. Είναι πιθανό ένα μέτρο να λειτουργήσει σε παραπάνω από μία διαφορετικές απειλές. Τα μέτρα θα πρέπει να επικοινωνούν και να συνεργάζονται μεταξύ τους για να είναι πιο αποτελεσματικά, να αλληλοσυμπληρώνονται. Αυτό όμως δεν σημαίνει ότι μπορεί ένα αντίμετρο να είναι αδύναμο ή μη ικανό να αντιμετωπίσει την απειλή για την οποία έχει δημιουργηθεί. Δεν πρέπει να παραβλέπεται το γεγονός ότι οι κίνδυνοι προκύπτουν στα πιο αδύναμα ή λιγότερο ασφαλή σημεία(weakest point philosophy).

[20] Pfleeger, C., 1997. *Security Computing, Prentice Hall International*. s.l.:ISBN.

- Σύμφωνα με την αρχή της αποτελεσματικότητας, τα μέτρα θα πρέπει να είναι επαρκή, κατάλληλα διαμορφωμένα και εύκολα στη χρήση τους την κρίσιμη στιγμή.

3.1 Γενική Προστασία Προσωπικών Δεμένων(GDPR).

Ο νέος κανονισμός σε σύγκριση με αυτόν που αντικαθιστά, στην ουσία προσπαθεί να μεγαλώσει την έκταση της νομοθεσίας περί προστασίας προσωπικών δεδομένων της ΕΕ. Ελεγκτές και διαχειριστές των προσωπικών δεδομένων, καθώς και οι μέθοδοι που χρησιμοποιούνται, αποτελούν το βασικό πεδίο που μπαίνει στο μικροσκόπιο της νέας νομοθεσίας. Ισχύει όταν σε μία Ευρωπαϊκή κατοικία επεξεργάζονται οι διασυνδέσεις των αγαθών/υπηρεσιών που χρησιμοποιεί, ακόμα και όταν επεξεργάζονται «συμπεριφορές» μη Ευρωπαίων Πολιτών. Οι επιχειρήσεις που δεν βρίσκονται στην Ευρώπη αλλά έχουν ως στόχο Ευρωπαίους Πολίτες, πρέπει να κατανοήσουν τις επιπτώσεις του GDPR όπως και να δράσουν για τη συμμόρφωση τους στους νέους κανόνες. Ο Κανονισμός δεν έχει ισχύει σε θέματα επεξεργασίας δεδομένων από νομοθετικές επιχειρήσεις όπως Εκτελεστικοί Φορείς του Νόμου.

Ο νέος κανονισμός εισάγει νέες «έννοιες» και αλλαγές στα ακόλουθα:

- *Διαφάνεια και συναίνεση*, οι πληροφορίες και οι συναινέσεις που ζητούνται για χρήση από τρίτους, θα είναι ξεκάθαρα.
- *Ανήλικα άτομα και συγκατάθεση*, σε αυτή τη περίπτωση θα πρέπει να υπάρχει συγκατάθεση από 13 χρονών και κάτω, κάποιου ενήλικου προσώπου. Εάν δεν υπάρξει συγκατάθεση η χρήση και συγκατάθεση θα είναι δυνατή για ηλικίες άνω των 16 χρόνων.
- *Ρυθμιζόμενα Δεδομένα*, όπου οι έννοιες Προσωπικά Δεδομένα και Ευαίσθητα Δεδομένα επεκτείνονται και μπορεί να περιλαμβάνουν και Βιομετρικά Στοιχεία για παράδειγμα.
- *Ψευδώνυμο,* μία νέα μέθοδος για την προστασία δεδομένων, ώστε να μην αποδίδονται τα χαρακτηριστικά σε ένα συγκεκριμένο πρόσωπο.
- *Παραβίαση Προσωπικών Δεδομένων,* νέα μέθοδος για ενημέρωση κάθε παραβίασης, ανεξάρτητα από τον τομέα.

- *Προστασία Δεδομένων* από τον σχεδιασμό και τη λογοδοσία. Οι εταιρίες και οι Οργανισμοί πρέπει να βρουν τρόπους και να υιοθετήσουν νέες μεθόδους και τεχνικές που αποδεικνύουν την συμμόρφωση τους με το Νέο Κανονισμό.
- *Ενισχυμένα Δικαιώματα,* όπως το «Δικαίωμα στη Λήθη», η αντίσταση στις αυτόματες αποφάσεις και μεταφορά δεδομένων.
- *Εποπτικές Αρχές,* η έννοια αυτή αλλάζει δραματικά εισάγοντας την έννοια του ενιαίου σημείου αναφοράς ακόμα και σε Πολυεθνικά Γκρουπ.

3.2 Βασικές Αρχές Προστασίας Δεδομένων:

Οι βασικές αρχές προστασίας Δεδομένων είναι ίδιες όπως και παλαιότερα. Πιο συγκεκριμένα:

- Δικαιοσύνη
- Νόμοι με Διαφάνεια
- Περιορισμοί Σκοπών
- Ελαχιστοποίηση Δεδομένων
- Ποιότητα Δεδομένων
- Ασφάλεια
- Ακεραιότητα και Εμπιστευτικότητα.

Σε όλα αυτά έρχεται και προστίθεται μία Νέα Αρχή που κρίνει ποιοι έλεγχοι και ποιοι κανονισμοί υποδεικνύουν την συμμόρφωση στις Αρχές Προστασίας Δεδομένων.

3.3 Έλεγχοι Δεδομένων.

Όπως αναφέρθηκε ήδη, θα πρέπει να υπάρχουν ξεκάθαρα controls που να υποδεικνύουν την συμμόρφωση στο GDPR. Αυτά τα controls πρέπει να περιλαμβάνουν ειδοποιήσεις που εξηγούν την διαφάνεια της επεξεργασίας. Παρόλα αυτά κάποιες πληροφορίες πρέπει να παρέχονται, όμως θα πρέπει να υπάρχουν ξεκάθαρες ειδοποιήσεις, καθώς και κάποιο χρονικό περιθώριο για την αποδοχή. Για παράδειγμα αν κάποιο άτομο επιθυμεί να μάθει αν τα δεδομένα του επεξεργάζονται,

μπορεί να ζητήσει να δει τα δεδομένα καθώς και κάποιο επεξηγηματικό σημείωμα για τη χρήση και τα αποτελέσματα τους. Τα αποτελέσματα αυτά πρέπει να δίνονται εντός μήνα, κατόπιν ζήτησης τους, ή να δίδεται επεξήγηση για τη μη συμμόρφωση. Έτσι θα πρέπει οι Εταιρίες να αναπτύξουν μεθόδους και απαντητικά κείμενα για την άμεση εξυπηρέτηση τους. Επιπλέον θα μπορούσαν να αναπτυχθούν διαδικτυακοί σύνδεσμοι που να οδηγούν στα αποτελέσματα αυτά, για πιο άμεση εξυπηρέτηση.

3.4 Δικαίωμα άρνησης.

Κάτι ακόμα σημαντικότερο είναι το δικαίωμα της άρνησης, που γίνεται κατά πολύ εντονότερο με το νέο κανονισμό. Ο καθένας πλέον έχει δικαίωμα να αρνηθεί άμεσο μάρκετινγκ, να γίνουν οι αναζητήσεις του μέρος στατιστικής ανάλυσης και πολλά άλλα τέτοια παραδείγματα. Τέτοιοι μέθοδοι πρέπει να ειδοποιούν τον χρήστη με αυτοματοποιημένο τρόπο, ώστε να μπορέσει να ενημερωθεί και κατόπιν να αποδεχτεί ή να αρνηθεί να γίνει μέρος της προκείμενης επεξεργασίας.

Βέβαια μπορεί να δίνεται η δυνατότητα της επιλογής μέχρι πιο σημείο δέχεται ο χρήστης αν επεξεργαστούν τα δεδομένα του. Επιπροσθέτως θα πρέπει να δίνεται και η δυνατότητα διαγραφής υπαρχόντων στοιχείων, δεδομένων και αποτελεσμάτων επεξεργασίας.

Ειδικά μέσα στις υποχρεώσεις της Διακυβέρνησης Δεδομένων, υπάρχει η ανάγκη της απόδειξης ότι έχουν παρθεί μέτρα ώστε να μην παραβιάζονται οι αρχές του GDPR. Αυτό περιλαμβάνει μέτρα όπως Αξιολογήσεις επιπτώσεων στην Ιδιωτική Ζωή, Ελέγχους, Αξιολογήσεις πολιτικών και μεθόδων, Εγγραφές Δραστηριοτήτων καθώς και τον διορισμό για Υπευθύνου για την Προστασία Δεδομένων. Τέλος απαγορεύεται η μεταφορά δεδομένων εκτός των χωρών της Ευρωπαϊκής Ένωσης. Ένα θέμα που επηρεάζει και περιορίζει σημαντικά τους Πολυεθνικούς Ομίλους, καθώς και τα πρόσθημα σε μη συμμόρφωση, μπορούν να οδηγήσουν σε 4% πρόστιμο του ετήσιου Ομιλικού Τζίρου.

Εν τέλει, ο νέος κανονισμός, με υποχρεωτική εφαρμογή από το Μάιο του 2018, υποχρεώνει όλες τις επιχειρήσεις που χειρίζονται προσωπικά δεδομένα Ευρωπαίων πολιτών να συμμορφώνονται πλήρως με τις απαιτήσεις του, που αφορούν

ασφάλεια δεδομένων και προστασία των δικαιωμάτων των φυσικών προσώπων. Προβλέπει αυστηρά πρόστιμα έως 20 εκατομμύρια ευρώ ή το 4% του ετήσιου παγκόσμιου κύκλου εργασιών (Passas, 2018)[21].

3.5 Εποπτικές Αρχές.

Ίσως το κομμάτι κλειδί του GDPR να είναι Εποπτικές Αρχές. Οι Εθνικές Αρχές θα συνεχίσουν να υπάρχουν, θα πρέπει όμως να συνεργάζονται μεταξύ τους για την διασφάλιση της εφαρμογής του GDPR. Οι αρχές αυτές θα πρέπει να είναι ανεξάρτητες καθώς και το προσωπικό τους εκπαιδευμένο, επαρκές και κατάλληλο για την προστασία δεδομένων.

3.6 Βασικές Πρωτοβουλίες Συμμόρφωσης με το GDPR.

Το πρώτο και βασικότερο κομμάτι είναι η *Επίγνωση.* Αυτό επιτυγχάνεται βεβαιώνοντας ότι οι εργαζόμενοι της εταιρίας γνωρίζουν πως ο κανονισμός αλλάζει και ακολουθεί τις αρχές του GDPR. Πρέπει να γίνει εκτίμηση του αντίκτυπου και βρεθούν κομμάτια που μπορεί να προκαλέσουν παραβιάσεις του GDPR. Αν εταιρία έχει «Εγγραφές Κινδύνου», αυτό θα πρέπει να αποτελέσει μία από αυτές.

Ένα δεύτερο σκέλος θα μπορούσε να αποτελέσει η *Διαχείριση της Πληροφορίας* που υπάρχει. Για παράδειγμα θα μπορούσε αρχειοθετηθεί βάση του που προήλθε και με ποιον «μοιράζεται». Αυτό θα μπορούσε να αποτελέσει και θέμα ελέγχου, ώστε να βρεθεί και να διαπιστωθεί ποιος έχει και πως διαχειρίζεται τα Δεδομένα και τις Πληροφορίες.

Ένα τρίτο κομμάτι μπορεί να αποτελέσει ο *Τρόπος Επικοινωνίας του Απορρήτου.* Θα πρέπει να εξετασθούν και να ενημερωθούν οι τρόποι που ενημερώνονται οι χρήστες για τη διαχείριση των προσωπικών τους δεδομένων, καθώς και για τα δικαιώματα τους. Επιπροσθέτως πρέπει αν ελεγχθούν οι μέθοδοι που εξασφαλίζουν τα δικαιώματα των χρηστών.

[21] Passas S., Adaptability in the era of digital transformation - The privacy perspective, Money Show Conference, 2018

Πλέον οι χρήστες έχουν δικαίωμα να δουν πως επεξεργάζονται τα δεδομένα τους, τα αποτελέσματα τους και πολλά άλλα αιτήματα τα οποία μπορούν να προκύψουν από τους χρήστες. Θα πρέπει να δημιουργηθούν φόρμες επικοινωνίας (πχ διαδικτυακοί σύνδεσμοι, επιστολές κλπ) που θα ανταποκρίνονται σε τέτοιου τύπου αιτήματα.

Έλεγχος θα πρέπει να υπάρξει και στις διαδικασίες επεξεργασίας δεδομένων, να εξετασθούν το κατά πόσο έχουν πάρει τις απαραίτητες εγκρίσεις και τις νομικές βάσεις στις οποίες βασίζονται.

Θα πρέπει να γίνει αναθεώρηση των τρόπων που βρίσκουν και αποκτούν τις πληροφορίες καθώς και αντίστοιχη αρχειοθέτηση. Το κομμάτι της συγκατάθεσης είναι ίσως το πιο βασικό στις αρχές του GDPR και εταιρίες θα καλούνται να αποδείξουν ότι υπάρχουν οι απαραίτητες συγκαταθέσεις για την απόκτηση των πληροφοριών. Εκτός αυτού θα πρέπει να βρεθούν μέθοδοι εξασφάλισης της ηλικίας των χρηστών, καθότι το θέμα «παιδί» απασχολεί εξίσου τα θέματα εξέτασης του GDPR.

Πρέπει επίσης να εξετασθούν και να ελεγχθούν οι μέθοδοι εύρεσης και διερεύνησης για την παραβίαση προσωπικών δεδομένων. Σε περίπτωση παραβίασης θα πρέπει να γίνουν περαιτέρω έλεγχοι, αξιολόγηση της παραβίασης, ενημέρωση των ενδιαφερόμενων μερών και φυσικά τροποποιήσεις και αλλαγές στις διαδικασίες.

Τέλος, σε περίπτωση που μιλάμε για κάποιο παγκόσμιο οργανισμό, θα πρέπει να βεβαιωθεί υπό ποιους κανονισμούς πρέπει να διενεργούνται οι επεξεργασίες δεδομένων και ποιες είναι οι εποπτικές αρχές.

4.1 Δομή Ηλεκτρονικής Διακυβέρνησης.

Σύντομα μετά την εισαγωγή της Ηλεκτρονικής Διακυβέρνησης, εισήλθε μία νέα μόδα στις εταιρίες γνωστή ως Επιχειρησιακός Ανασχεδιασμός Διαδικασιών (Business Process Re-Engineering-BPR). Η θεωρία του BPR έλεγε πως μέσω των νέων ηλεκτρονικών συστημάτων περιορίζονται και απλοποιούνται διαδικασίες, που συνήθως γίνονταν από μεσαίου επιπέδου τζούνιορ μάνατζερ. Βασικό χαρακτηριστικό

αποτελούσε η ιδιότητα των τεχνολογιών για πιο γρήγορη επεξεργασία και ανάλυση πληροφοριών. Η τεχνολογία αποτέλεσε τον «οδηγό» σε αυτές τις αλλαγές (Osborne, 1992)[22]. Παράλληλα με τις αλλαγές υπήρξαν και νέες ιδέες για νέες δομές και νέες διαδικασίες. Τρεις νέες βασικές δομές εμφανίστηκαν στην εξωτερική ανάθεση διαδικασιών(Outsourcing), στα δίκτυα επικοινωνίας και πληροφόρησης καθώς και στο μάνατζμεντ της αλυσίδας εφοδιασμούς (Supply Chain).

Επιπροσθέτως εισήχθησαν νέες έννοιες στην επιχειρηματική διακυβέρνηση όπως νέες ιεραρχικές δομές, νέες δομές στην αγορά και στην έννοια της έμμεση διακυβέρνησης (Barney, 1999)[23].

Ενώ τα ICT επιτρέπουν ή διευκολύνουν αυτές τις αλλαγές των δομών, υπάρχουν παρανοήσεις στο πόσο θεμελιώδες είναι το κομμάτι της τεχνολογίας και το πόσο εξαρτώνται από αυτή. Ενώ σε δομές όπως αυτές των Κοινωνικών Δικτύων, διαδικτυακών κοινοτήτων και ψηφιακών κόσμων βρίσκεται με ουσιαστικό τρόπο η έννοια της Ηλεκτρονικής Διακυβέρνησης, υπάρχουν και δομές που όμως δεν θα μπορούσαν να χαρακτηριστούν ως μορφές Ηλεκτρονικής Διακυβέρνησης διότι δεν παρέχουν καμία αλλαγή στο υπάρχων μοντέλο. Για αποφυγή των παρανοήσεων θα πρέπει να σχολιαστούν οι έννοιες των ηλεκτρονικών διαδικασιών και συστημάτων, εφόσον υπάρχουν, σε σχέση με τις προκάτοχες διαδικασίες/ συστήματα.

Απαραίτητη συνθήκη για το BPR και κατά συνέπεια της Ηλεκτρονικής Διακυβέρνησης, αποτελεί η διατύπωση της συνολικής λειτουργίας της επιχείρησης ως ένα πλέγμα αλληλεξαρτώμενων λειτουργιών (Armistead C., 1999)[24]. Η παραδοχή αυτής της ενότητας μεταξύ των τμημάτων υποδεικνύει επί της ουσίας ολόκληρη την Διοίκηση.

Ο κριτικός ρόλος της Ηλεκτρονικής Διακυβέρνησης είναι να διοικεί, να υποστηρίζει και να διευκολύνει τους αντικειμενικούς σκοπούς της εταιρίας. Όπως

[22] Osborne, D. a. T. G., 1992. *Reinventing government : How the entrepreneurial spirit is transforming the public sector.* s.l.:s.n.

[23] Barney, J., 1999. *How a Firm's Capabilities Affect Boundary Decisions,* s.l.: Sloan Management Review.

[24] Armistead C., P. J. &. M. S., 1999. *Strategic business process management for organisational effectiveness.* s.l.:s.n.

επίσης θα πρέπει να μετριάζει τον κίνδυνο. Το στρατηγικό εταιρικό πλάνο αυξάνει τις ευθύνες και τις αρχές της Ηλεκτρονικής Διακυβέρνησης με τη χρήση μίας νέας δομής για μία πιο αποτελεσματική και πιο αποδοτική χρήση των ICT. Τα λογισμικά συστήματα και οι παλαιές δομές πρέπει να μετατραπούν σε σαφή καθορισμένα συστήματα που να μπορούν να υποστηρίξουν μελλοντικά επιχειρηματικά μοντέλα (Bernroider, 2008)[25]. Οι επιχειρησιακές ανάγκες πρέπει να δίνουν έναυσμα για οργανωτικές αλλαγές στις υπάρχουσες δομές και συστήματα. Με αυτές τις αλλαγές θα πρέπει να αυξάνεται και η «αξία» της εταιρίας.

Τα συστήματα θα πρέπει να βοηθάνε στη διαχείριση της ποικιλομορφίας των κοινωνικών αναγκών, καθώς και η αποφυγή προβλημάτων επικοινωνίας και η έλλειψη νομιμοποίησης διαδικασιών είναι αναγκαία. Επιπροσθέτως θα πρέπει να δημιουργηθούν εσωτερικές και εξωτερικές διεπαφές για να επιλυθεί το πρόβλημα της οργανωτικής δομής. Να δημιουργηθούν δηλαδή ορθά συστήματα που θα επιτρέπουν την καλύτερη ενδό-διοίκηση καθώς και την εξωτερική διεπαφή με την κοινωνία και τον ευρύτερο χώρο δραστηριοποίησης, για την επίτευξη οργανωτικής ολοκλήρωσης.

Η διαμόρφωση της δομής θα πρέπει να γίνεται λαμβάνοντας υπόψη, αλλά ταυτόχρονα βοηθώντας την επίτευξη τους στους εξής τομείς:

- *Η Πολιτικής της Εταιρίας*, αφού πρέπει να υπάρχει ένα όραμα και ένας στόχος, τα οποία θα πρέπει να επιτυγχάνονται και μέσω των διαδικασιών των Πληροφοριακών Συστημάτων.
- *Εταιρικές Αξίες,* τα πιστεύω, η ιδεολογία και οι αρχές της.
- *Αποστολή της Εταιρίας,* με την έννοια του μακροχρόνιου σχεδιασμού της εταιρίας και όλοι οι επιχειρησιακοί σκοποί της.
- *Δομή Εξουσίας* που αφορά ένα σύνολο αντικρουόμενων συμφερόντων και ενδιαφερόντων που επηρεάζουν τις διαδικασίες. Θα πρέπει να υπάρχουν ελεγχόμενες προσβάσεις για όλους για αποφυγή θεμάτων.
- *Οι ανάγκες* της εταιρίας σε γενικότερο επίπεδο.
- *Η γνώση,* δηλαδή σωστή καταχώρηση και μετάδοση της κατά την απόκτηση της, καθώς και μέθοδοι απόκτησης της.

[25] Bernroider, E. W., 2008. *IT governance for enterprise resource planning supported by the DeLone–McLean model of information systems success.* s.l.:s.n.

- *Εταιρικό Σχέδιο Δράσης,* στην διευκόλυνση επίτευξης του στρατηγικού της πλάνου.

4.2 Σχέση BPR με IT.

Αξίζει να σημειωθεί η σημαντικότητα της αμφίδρομης σχέσης του BPR με το IT. Η σχέση αφορά την εκμετάλλευση των τεχνολογιών για επιτάχυνση μέσω της αυτοματοποίησης και την απλοποίηση μέσω του ανασχεδιασμού των διεργασιών (Nath, 1997)[26]. Η αυτοματοποίηση των υφιστάμενων διεργασιών αποτελεί μία μόνο δυνατότητα της Πληροφοριακής Τεχνολογίας. Η σημαντικότερη συνεισφορά της, εντούτοις, έγκειται στις ευκαιρίες που προσφέρει για το ριζικό ανασχεδιασμό των διεργασιών αυτών (Attaran, 2004)[27].

Αναλυτικότερα, δύνονται ευκαιρίες ριζικού ανασχεδιασμού και η δημιουργία αυτοματισμών σε εργασίες μέσω της Πληροφορικής της Τεχνολογίας, αφού μέσω αυτής μπορούν να προσπεραστούν κάποιες επιμέρους εργασίες. Κατά συνέπεια δημιουργείται όφελος από άποψη κόστους και χρόνου.

Αναφορικά, ο ρόλος της Πληροφοριακής Τεχνολογίας στο BPR είναι πολύπλευρος και αφορά σε όλες τις φάσεις του project αλλαγής: (α) πριν την υλοποίηση του ανασχεδιασμού, (β) κατά τη διάρκεια του ανασχεδιασμού και (γ) κατά τη διάρκεια της εφαρμογής (Attaran, 2004)[28]. Σε κάθε περίπτωση, για την υποστήριξη του project αλλαγής απαιτείται να εξεταστεί εξ' αρχής η επάρκεια της υπάρχουσας υποδομής της Πληροφοριακής Τεχνολογίας, καθώς, έχει αποδειχθεί ότι, όσο μεγαλύτερες είναι οι δυνατότητες που αυτή προσφέρει, τόσο μεγαλύτερα περιθώρια έχει μία επιχείρηση να προχωρήσει σε ριζικές αλλαγές και να πετύχει (Aladwani,

[26] Nath, B. G. A. &., 1997. *The role of information technology in business process reengineering.*. s.l.:International Journal of Production Economics 50(2-3), 91-104.

[27] Attaran, M., 2004. *Exploring the relationship between information technology and business process reengineering.* s.l.:Information & Management 41(5), 585-596.

[28] Attaran, M., 2004. *Exploring the relationship between information technology and business process reengineering.* s.l.:Information & Management 41(5), 585-596.

1999)[29]. Επιπλέον, τονίζεται ότι, οι ιδιαίτερες απαιτήσεις για τη χρήση Πληροφοριακής Τεχνολογίας καθιστούν επιτακτική την ανάγκη ανάλογης εκπαίδευσης των εργαζομένων (Buzacott, 1996)[30].

5.1 Ο Ρόλος των Πληροφοριακών Συστημάτων.

Ο βασικότεροι ρόλοι είναι οι εξής (Melone, 1990)[31]:

- Η συλλογή, η αποθήκευση και η διασφάλιση δεδομένων τα οποία μπορούν αν επεξεργαστούν και να προσφέρουν αναγκαίες πληροφορίες στην Διοίκηση.
- Η επεξεργασία δεδομένων για την καλύτερη πληροφόρηση που αφορά είτε εσωτερικές διεργασίες οι οποίες μπορούν να βελτιώσουν εσωτερικές δομές, είτε πληροφορία για καλύτερη λήψη αποφάσεων (πχ βάση πελατολογίου).
- Βελτίωση οργάνωσης και επικοινωνίας πληροφοριών εντός και εκτός της εταιρίας.
- Ασφάλεια ως προς τη διαρροή δεδομένων (Data Leakage).
- Άμεση πληροφόρηση, εφόσον ζητηθεί.
- Καλύτερα επικοινωνιακά συστήματα με προμηθευτές, πελάτες κλπ (πχ after sales service).
- Καταγραφή σφαλμάτων και εύρεση μεθόδων για αποφυγή τους στο μέλλον.
- Καλύτερος έλεγχος εσωτερικών διεργασιών.
- Αύξηση παραγωγικότητας και αποδοτικότητας υπαλλήλων.
- Βελτίωση μεθόδων εκμάθησης και εκπαίδευσης (πχ e-learning).
- Εκσυγχρονισμός εργασιακού περιβάλλοντος.
- Ευκαιρίες για καινοτομίες μέσω βελτίωσης διαδικασιών έρευνας και ανάλυσης.

---

[29] Aladwani, A. M., 1999. *Implications of some of the recent improvement philosophies for the management of the information systems organization.* s.l.:Industrial Management & Data Systems 99(1-2), 33-39.

[30] Buzacott, J. A., 1996. *Commonalities in reengineered business processes: models and issues.* s.l.:Management Science 42(5), 768-782.

[31] Melone, 1990. *Theoretical Assessment of the User-Satisfaction Construct in Information Systems Reshearch :* Management Science

- Ορθή αξιολόγηση προσωπικού.

5.2 Ανάπτυξη και Δομή Πληροφοριακών Συστημάτων.

- Προγραμματισμός Πραγματοποιήσεως Πληροφοριακών Συστημάτων (Project Management).
- Οργάνωση Έργου Αναπτύξεως Πληροφοριακού Συστήματος (Project Organization).
- Οργάνωση Κέντρου Πληροφορικής (EDP Center Organization).
- Πρόβλεψη Χρόνων Αναπτύξεως του Συστήματος (Project Forecasting).
- Έλεγχος Αναπτύξεως Συστήματος (Project Control).
- Αξιοπιστία Πληροφοριακών Συστημάτων (Project Reliability).
- Αξιολόγηση Πληροφοριακών Συστημάτων (Project Effectiveness and Evaluation).
- Έλεγχος Ασφάλειας Πληροφοριακών Συστημάτων (Information System Security). (Γεωργίου, 2001)[32].

5.3 Βασικές Αρχές/Χαρακτηριστικά.

Πριν την ανάπτυξη, τροποποίηση ή αντικατάσταση των ήδη υπαρχόντων συστημάτων, θα πρέπει να σκεφτούμε και να αναλύσουμε τις αρχές και τα βασικά χαρακτηριστικά που θα πρέπει να διέπουν τα νέα συστήματα. Σύμφωνα με τον Χαράμη (Χαράμης, 2001) ένα πληροφοριακό σύστημα θα πρέπει να χαρακτηρίζεται από εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity) και διαθεσιμότητα (availability).

Η *εμπιστευτικότητα* είναι έννοια που συνδέεται άμεσα με τις έννοιες ιδιωτικότητα (privacy) και τη μυστικότητα (secrecy). Η εμπιστευτικότητα αφορά την μη αποκάλυψη ευαίσθητων ή μη κατάλληλων πληροφοριών σε μη

[32] Ανικούλα Ε., Χαράμης Γ., 2001. *Διοικητική Της Αναπτύξεως Πληροφοριακών Συστημάτων.* s.l.:s.n.

εξουσιοδοτημένους χρήστες εντός του συστήματος. Ας μην ξεχνάμε κιόλας ότι αποτελεί μία βασική αρχή που αφορά τη σχέση Πελάτη-Εταιρίας.

Η *ακεραιότητα* αποτελεί βασικό χαρακτηριστικό της πληροφορίας. Η επίτευξή της γίνεται μέσω τη δημιουργία αυστηρά εξουσιοδοτημένων χρηστών, ο οποίοι θα είναι οι μόνοι υπεύθυνοι και οι μόνοι ικανοί για οποιαδήποτε αλλαγή ή τροποποίηση των πληροφοριών. Γενικότερα πρέπει να υπάρχουν τρόποι και μέθοδοι διατήρησης της πληρότητας και αξιοπιστίας που κατέχει η εταιρία.

Τέλος η *διαθεσιμότητα* εξασφαλίζει την άμεση πρόσβαση στην πληροφορία, όταν είναι απαραίτητη, χωρίς καθυστερήσεις.

5.4 Διάκριση Πληροφοριακών Συστημάτων.

Τα πληροφοριακά συστήματα θα μπορούσαν να διακριθούν στα εξής επιμέρους μέρη:

- Συστήματα Επεξεργασίας συναλλαγών ηλεκτρονικής επεξεργασίας δεδομένων.
- Συστήματα Υποστήριξης Διοίκησης:
  i) Συστήματα υποστήριξης αποφάσεων.
  ii) Έμπειρα Συστήματα.
  iii) Στρατηγικά Πληροφοριακά Συστήματα.
- Πληροφοριακά Συστήματα.

Τα συστήματα επεξεργασίας συναλλαγών αποτελούν μέρος των λειτουργικών πληροφοριακών συστημάτων. Μέσα στις αρμοδιότητες τους, πέραν τις επεξεργασίας των δεδομένων, αποτελεί και η ενημέρωση των ήδη υπαρχόντων αρχείων και φυσικά η δημιουργία των εγγράφων συναλλαγής. Ένα τέτοιου τύπου σύστημα δύναται να συνεργάζεται με κάποιο άλλο μηχανογραφικό σύστημα ηλεκτρονικής μετάβασης δεδομένων (Electronic Data Interchange).

Συνήθως εξυπηρετούν βασικές επιχειρησιακές λειτουργίες όπως πωλήσεις, προμήθειες, μισθοδοσία προσωπικού, πληρωμές κλπ. Αυτό μεταφράζεται πως μία

διακοπή του συστήματος αυτού θα μπορούσε να καθηλώσει την εταιρία, προκαλώντας τεράστιες ζημίες.

Τα Πληροφοριακά Συστήματα Διοίκησης, γνωστά και ως MIS, έχουν άμεση συσχέτιση με τις αρμοδιότητες και λειτουργίες των στελεχών της εταιρίας, με σκοπό να βοηθήσουν τα στελέχη των εταιρειών στην λήψη αποφάσεων. Η διαδικασίες που ακολουθούν τα συστήματα αυτά είναι η συλλογή και αποθήκευση δεδομένων τα οποία θα επεξεργαστούν από μοντέλα απόφασης για την εξαγωγή των απαιτούμενων πληροφοριών.

Τα έμπειρα συστήματα είναι αυτά που επεξεργάζονται προβλήματα που χαρακτηρίζονται από ασάφεια, υποκειμενικότητα, ελλιπή πληροφόρηση και αβεβαιότητα, προσφέροντας μία λίστα εναλλακτικών λύσεων. Αυτά τα προβλήματα λύνονται με τη λήψη τουλάχιστον ικανοποιητικών αποφάσεων.

Όταν τα προβλήματα χαρακτηρίζονται από σαφήνεια, αντικειμενικότητα, αρκετή ή και πλήρη πληροφόρηση χρησιμοποιούνται τα Στρατηγικά Συστήματα. Τα στρατηγικά συστήματα παρέχουν μία ημί-δομημένη αν όχι ολοκληρωμένη απόφαση (Noe Hollenbeck, n.d.)[33].

Εν ολίγοις θα μπορούσε να παρομοιάσει κανείς την επιχείρηση και το περιβάλλον της ως τις εισροές των πληροφοριακών μας συστημάτων. Υπό την κατάλληλη επεξεργασία των δεδομένων αυτών από τα πληροφοριακά μας συστήματα, παράγονται οι κατάλληλες αποφάσεις για τις νέες επενδύσεις, νέες επιχειρηματικές αποφάσεις κλπ. Τα Πληροφοριακά Συστήματα δηλαδή αποτελούνται από μία πολύπλευρη και διεπιστημονική πλατφόρμα επεξεργασίας δεδομένων και ένα σωρό άλλες επιχειρησιακές συνιστώσες .

5.5 Υλοποίηση Νέου Πληροφοριακού Συστήματος.

[33] Noe Hollenbeck, Gerhert Wright, 2003. *Human Resource Management: Gaining Competitive Advantage.*

5.5.1 Ανάλυση Πληροφοριακού Συστήματος.

Τα πληροφοριακά συστήματα, όπως ήδη έχει αναφερθεί, χαρακτηρίζονται από την αέναη εξέλιξη της τεχνολογίας. Οι εξελίξεις αυτές, ανά περιόδους θα πρέπει να φέρουν αλλαγές. Προκειμένου όμως να αποφασισθεί από το αρμόδιο τμήμα ποιες αλλαγές είναι σημαντικές και απαραίτητες, θα πρέπει πρώτα να αναλυθεί το υπάρχων Πληροφοριακό Σύστημα. Η ανάλυση γίνεται μέσω ερωτηματολογίων, συνεντεύξεων, μεθόδων δειγματοληψίας κ.α. Σκοπός των αναλύσεων όμως είναι και η εύρεση αδύνατων σημείων και ελλείψεων σε διάφορα επίπεδα. Τα επίπεδα αυτά Ιεραρχικά πρέπει να ξεκινούν από την ποιότητα της Ανώτατης Διοίκησης, να συνεχίζουν με την αξιολόγηση της υπάρχουσας επιχειρησιακής δομής, τον έλεγχο των πολιτικών και του επιπέδου των εργαζομένων και φυσικά την ποιότητα των επικοινωνιών και ελέγχου.

Γενικά η διαδικασία της ανάλυσης του υπάρχοντος πληροφοριακού συστήματος θα πρέπει να γίνεται ανά τακτά χρονικά διαστήματα, ώστε τα συστήματα να παραμένουν ενημερωμένα, ασφαλή, εύχρηστα και να πετυχαίνουν το σκοπό τους και φυσικά τους στόχους της εταιρίας.

5.5.2 Προκαταρκτική Έρευνα.

Αφότου εντοπισθεί κάποια νέα τεχνολογική εξέλιξη, θα πρέπει να γίνει αρχικά μία προκαταρκτική έρευνα για την ανάγκη της εγκατάστασης της στα ήδη υπάρχοντα πληροφοριακά συστήματα ή τη δημιουργία νέων πληροφοριακών συστημάτων. Βασικές ερωτήσεις που περιλαμβάνει αυτή η έρευνα είναι εξής:

- Ποιες είναι οι νέες δυνατότητες του νέου πληροφοριακού συστήματος/νέας τεχνολογίας;
- Λόγοι Χρησιμότητας;
- Ποιες ανάγκες θα καλυφθούν από το νέο σύστημα;
- Ποιες διευκολύνσεις θα προσφέρει στην καθημερινότητα και στις εργασίες/διαδικασίες της εταιρίας;
- Ποιοι αντικειμενικοί Σκοποί του στην επιχείρηση;

Αφότου ολοκληρωθεί αυτή η διαδικασία, πρέπει να γίνει καθορισμός της κατάστασης του υπάρχοντος συστήματος. Κατά τη διερεύνηση πρέπει να βρεθούν και οι απαραίτητες τροποποιήσεις που μπορεί να χρειαστούν (OECD, 2004)[34].

Από τις διαδικασίες αυτές εύλογα συμπεραίνουμε τις απαραίτητες ενέργειες για την ανάπτυξη του νέου συστήματος. Γίνεται δημιουργία μίας ομάδας που θα το αναλάβει και φυσικά φτιάχνεται το πλάνο του σχεδιασμού του όλου συστήματος.

5.5.3 Μελέτη Εφικτότητας.

Εν συνεχεία ακολουθεί η σύνταξη της μελέτης εφικτότητας, μία διαδικασία κατά την οποία εξετάζονται η σκοπιμότητα του έργου αυτού και κατά πόσο δυνατών είναι ως προς την υλοποίηση του (Bill, 1999)[35].

Αναλυτικότερα από άποψη τεχνικών απαιτήσεων, αναλύονται ο αριθμός των χρηστών που είναι απαραίτητοι, ο όγκος των αρχείων και δεδομένων, οι χρήσης τις οποίες θα εξυπηρετεί, πιθανότητες ταυτόχρονης επεξεργασίας κ.α. Φυσικά αναλύονται τα υπάρχοντα συστήματα και πως οι παροχές (υπάρχουσες τεχνολογίες και τεχνογνωσία προσωπικού) τους μπορούν να διευκολύνουν τα νέα συστήματα (Peeka, n.d.)[36].

Κατά τη σύνταξη της μελέτης αυτής πρέπει να αναλυθούν και στόχοι, δυνατότητες, διευκολύνσεις και οι υπόλοιποι σκοποί που θα εξυπηρετήσει το νέο σύστημα. Όπως είναι σαφές θα πρέπει να γίνουν έλεγχοι στα τμήματα και στις διαδικασίες που θα επηρεαστούν από το νέο σύστημα. Απαραίτητη είναι η ανάλυση και η θέσπιση των ορίων και των προσβάσεων στο σύστημα αυτό, όπως και νέες διαδικασίες που πιθανώς θα προκύψουν από αυτό.

---

[34] www.oecd.org ,2004. OECD Information and Technology Outlook.

[35] Gates Bill, 1999. *Επιχειρηματικές ευκαιρίες στην Ψηφιακή Οικονομία/ Μέσα από την Καλύτερη Χρήση της Τεχνολογίας.* Εκδόσεις Κλειδάριθμος.

[36] Peeka, Oikonomou Victoria, Lykogianni Vasiliki. *The Human Factor as a source of competitive advancement in the new Globalization Market.* University of Peiraious, Panteion University.

Ένας παράγοντας που είναι αναπόσπαστος και ο πιο καθοριστικός σε κάθε τμήμα είναι το προσωπικό του (Peeka, n.d.)[37]. Συνεπώς δεν θα μπορούσε να λείπει η ανάλυση της κατάστασης του προσωπικού των τμημάτων που θα επηρεαστούν από το νέο σύστημα. Για την σύνταξη αυτού του κομματιού πρέπει να γίνουν σαφείς οι σχέσεις του υπάρχοντος τμήματος με το υπάρχων ΠΣ(πχ δυσκολίες, κολλήματα, bugs κλπ). Το προσωπικό είναι αυτό που γνωρίζει καλύτερα τις δυνατότητες και ανάγκες του ΠΣ, αφού και η επαφή τους είναι συνεχής, καθημερινή και αδιάκοπη. Οπότε και στις προσεγγίσεις αυτές η οπτική γωνία του προσωπικού είναι ίσως η σημαντικότερη. Θα πρέπει να γίνουν περεταίρω αναλύσεις για τις σχέσεις του προσωπικού το υπάρχων σύστημα, ανάλυση για την ετοιμότητα του για την υποδοχή του νέου, ανάλυση των υπαρχόντων καθηκόντων. Τέλος θα πρέπει να γίνει ανάλυση, πιθανών ανακατατάξεων, εκπαιδευτικών αναγκών για την υποδοχή του νέου συστήματός κλπ.

5.5.4 Σχεδιασμός του Νέου Πληροφοριακού Συστήματος.

Η διαδικασία αυτή γίνεται φυσικά για τον ορθό καθορισμό και επιμερισμό των νέων εργασιών από τους αναλυτές και τους τελικούς χρήστες, την διαχείριση της ενημερότητας του συστήματος και τέλος για την εύρεση λύσεων σε θέματα που πιθανώς προέκυψαν κατά τα δύο προηγούμενα βήματα. Το κομμάτι αυτό χωρίζεται σε δύο επιμέρους ενέργειες τον γενικό σχεδιασμό και τον τεχνικό/ειδικό σχεδιασμό (Pavlou PA, 2006)[38].

[37] Peeka, Oikonomou Victoria, Lykogianni Vasiliki. *The Human Factor as a source of competitive advancement in the new Globalization Market.* University of Peiraious, Panteion University.

[38] Pavlou PA, El Sawy OA, 2006. *From IT Leveraging competence to competitive advantage in turbulent environment: the case of new product development.* Information Technology Research.

Γενικός Σχεδιασμός (Samia, 2006)[39]:

- Οργανωτική δομή ΠΣ: περιλαμβάνει τη διαχείριση, τον έλεγχο και την συσχέτιση των διεργασιών, προσανατολισμό εργασιών και λήψη αποφάσεων.
- Βασικές Σχεδιαστικές Επιλογές ΠΣ: περιλαμβάνει το στρατηγικό σχέδιο που κρύβεται πίσω από το νέο ΠΣ, την κατανομή του συστήματος, το δίκτυο εργασιών, υποσυστήματα και τις συσχετιζόμενες εφαρμογές.
- Σχεδιασμός Ροής Δεδομένων: αποτελείται από τα διαγράμματα που περιγράφουν την ροή δεδομένων. Το κομμάτι αυτής της διεργασίας αποτελεί κομμάτι κλειδί στα νέα συστήματα διότι οι διαδικασίες τροποποιούνται, καταργούνται ή δημιουργούνται νέες, ενώ το μέγεθος των δεδομένων αλλάζει.
- Ανάλυση Κόστους: Στο σημείο αυτό γίνεται ανάλυση του κόστους και του οφέλους που θα έχει η εταιρία από τα νέα ΠΣ.

Ειδικός Σχεδιασμός**:**

- Οργάνωση Αρχείων: μία διαδικασία που καθορίζει τα αρχεία, την αποθήκευσης τους και φυσικά την ασφάλεια τους.
- Σχεδιασμός Εισόδου Δεδομένων: περιλαμβάνει τα απαραίτητα φίλτρα πριν την είσοδο δεδομένων στο νέο σύστημα, την συλλογή δεδομένων, τα μέσα που χρησιμοποιούμε για την είσοδο τους, τον έλεγχο ορθότητας τους και φυσικά τον σχεδιασμό επικοινωνίας χρήστη-συστήματος.
- Σχεδιασμός Εξόδων Δεδομένων/Αποτελεσμάτων: προσδιορίζονται τα μέσα εξόδου δεδομένων και αποτελεσμάτων, την φόρμα εξόδου αποτελεσμάτων και τους ελέγχους που πρέπει να γίνονται κατά τη διανομή και στις πληροφορίες εξόδου.
- Σχεδιασμός Τεχνικών Προδιαγραφών Συστημάτων και το Απαραίτητο Λογισμικό.

5.5.5 Υλοποίηση Νέου Πληροφοριακού Συστήματος.

[39] Chreim Samia, "Managerial Frames and Institutional Discourses of Frame: Employee Appropriation Resistance", Organizational Studies, University of Ottawa, Ontario Canada, 2006

Η υλοποίηση του Νέου Πληροφοριακού συστήματος είναι το προτελευταίο βήμα στη δημιουργία του Πληροφοριακού Συστήματος.

Το βήμα αυτό μπορεί να γίνει αρκετά χρονοβόρο, διότι πρέπει να περάσει υπό την επεξεργασία πολλών παραμέτρων και λειτουργικών τεστ.

Σιγά σιγά οριστικοποιούνται διαδικασίες και παίρνει την τελική μορφή του Νέο Πληροφοριακό Σύστημα. Οι επιδράσεις από το νέο εξοπλισμό, τις νέες διαδικασίες και φυσικά οι επιδράσεις στην παραγωγή και τα οφέλη του γίνονται ορατά. Γίνεται ο πρώτος χαρακτηρισμός των ποιοτικών χαρακτηριστικών ως προς την αποτελεσματικότητα, την απλότητα, την ευκαμψία, την συμβατότητα και την τεκμηρίωση του νέου συστήματος.

Όπως έχει ήδη αναφερθεί ο ανθρώπινος παράγοντας είναι ο παράγοντας που έχει την τελευταία λέξη στην ολοκλήρωση του Νέου Συστήματος. Συνεχής ανατροφοδότηση κατά την αρχική περίοδο λειτουργίας του συστήματος, μέχρι την οριστική του εγκατάσταση, είναι το τελευταίο κομμάτι της διαδικασίας.

5.5.6 Συντήρηση Πληροφοριακού Συστήματος.

Η συντήρηση του Πληροφοριακού Συστήματος είναι το κομμάτι που το κρατά το σύστημα ενημερωμένο, προσαρμοσμένο στις νέες συνθήκες και στις καθημερινές αλλαγές αναγκών, στόχων κλπ. Η διαδικασία αυτή ονομάζεται συντήρηση Πληροφοριακού Συστήματος.

Οι νέες ανάγκες για πληροφοριακές απαιτήσεις, τηλεπικοινωνιακές ανάγκες καθώς και η κουλτούρα της εταιρίας πρέπει να υπηρετούνται από το Πληροφοριακό Σύστημα.

Φυσικά στην έννοια αυτή συγκαταλέγονται η συντήρηση του Πληροφοριακού υλικού και λογισμικού, την διατήρηση ενός λειτουργικού οργανωτικού πλαισίου και φυσικά ενός λειτουργικού επικοινωνιακού συστήματος.

Συμπερασματικά οι παραπάνω διαδικασίες συντήρησης κρατάνε το Πληροφοριακό Σύστημα ανταγωνιστικό και λειτουργικό και φυσικά εν ζωή.

5.5.7 Συμπεράσματα Διαδικασίας Δημιουργίας Πληροφοριακού Συστήματος.

Συμπερασματικά θα μπορούσε να πει κανείς ότι τα πληροφοριακά συστήματα τροποποιούνται, αλλάζουν, μεταβάλλονται, αναπτύσσονται και δημιουργούνται νέα για την συνεχή βελτίωση των σύγχρονων επιχειρήσεων. Απαραίτητα είναι τα στοιχεία του ελέγχου και η διαρκής ανατροφοδότηση πληροφοριών με το προσωπικό.

6.1 Διαχείριση Τεχνολογιών-Προσωπικού.

Το σύγχρονο εταιρικό περιβάλλον χαρακτηρίζεται από τον αυξανόμενο ανταγωνισμό και τις συνεχείς τεχνολογικές εξελίξεις. Η ανάγκη της επιχείρησης να παραμείνει ανταγωνιστική είναι πιο έντονη από ποτέ. Για να μπορέσει να ανταποκριθεί και να συναγωνιστεί, όπως και να μείνει ενήμερη με τις εξελίξεις η εταιρία καλείτε να επενδύσει. Οι επενδύσεις δεν αφορούν μόνο νέες μεθόδους παραγωγής, την παραγωγή φθηνότερων και πιο ανταγωνιστικών προϊόντων, αλλά καλείται να κάνει μία συγκριτική διαφορά με τους ανταγωνιστές της. Οι επενδύσεις αυτές αφορούν τις νέες τεχνολογίες και φυσικά στον ανθρώπινο παράγοντα μέσω των συνεχών ενημερώσεων και εκπαιδεύσεων.

Ένα πρώτο βήμα είναι η εισαγωγή νέου πληροφοριακού συστήματος. Όπως έχουμε αναφέρει, ένα νέο πληροφοριακό σύστημα συμβάλει στην παραγωγικότητα και ανταγωνιστικότητα, εξασφαλίζοντας έγκυρη πληροφόρηση σε όλα τα ιεραρχικά επίπεδα που συνιστούν την εταιρία.

Ωστόσο, η απλή εισαγωγή ενός πληροφοριακού συστήματος ενώ ενισχύει την επικοινωνία και την ορθή πληροφόρηση, δεν εγγυάται την ενίσχυση του συγκριτικού πλεονεκτήματος. Ας μην ξεχνάμε άλλωστε την πολυπλοκότητα της εγκατάστασης του ΠΣ.

Η εταιρία θα πρέπει να δημιουργήσει ένα νέο στρατηγικό πλάνο που θα στηρίζεται στα πλεονεκτήματα του νέου πληροφοριακού συστήματος. Ένα αλάνθαστο μέσο με το οποίο το στρατηγικό πλάνο δημιουργεί το συγκριτικό του

πλεονέκτημα είναι η εκπαίδευση των χρηστών του νέου πληροφοριακού συστήματος και γενικότερα του προσωπικού.

6.1.1 Συμμετοχή Ανθρωπίνου Παράγοντα.

Αποτελεί παραδοχή το γεγονός ότι η συμμετοχή όλου του προσωπικού της εταιρίας είναι βασικό και αναπόσπαστο κομμάτι της Διοίκησης Ολικής Ποιότητας. Στην μέγιστη αξιοποίηση των πληροφοριακών συστημάτων, ο ανθρώπινος παράγοντας παίζει τον σημαντικότερο ρόλο, όντας χρήστης και αποδέκτης όλων αυτών των αλλαγών.

Στην προσπάθεια των εταιριών να δημιουργήσουν το συγκριτικό πλεονέκτημα σε σχέση με τον ανταγωνισμό, ο ανθρώπινος παράγοντας είναι ο σημαντικότερος. Η διατήρηση του συγκριτικού πλεονεκτήματος, πρέπει να απασχολεί και είναι κομμάτι του στρατηγικού πλάνου της εταιρίας. Με ορθή ηγεσία είναι εφικτό οι δυνατότητες του ανθρωπίνου δυναμικού να χρησιμοποιούνται στο μέγιστο για το όφελος της εταιρίας (Bill, 1999)[40].

Ο ανθρώπινος παράγοντας αποτελεί σημαντική παράμετρο για τον αν το Πληροφοριακό Σύστημα θα αυξήσει την παραγωγικότητα. Ο συνδυασμός ανθρώπινου παράγοντα με το νέο πληροφοριακό σύστημα, είναι η πιο κρίσιμη παράμετρος κατά την υιοθέτηση του νέου πληροφοριακού συστήματος.

Ανάλογα με τις μεθόδους εμπλοκής του εργαζομένου στις εταιρικές δραστηριότητες, διακρίνουμε 3 τύπων ενσωματώσεις (Peeka, n.d.)[41]:

i. Εσωτερική Ενσωμάτωση, κατά την οποία κάθε εργαζόμενος ξεχωριστά καλείται να υιοθετήσει και να χρησιμοποιήσει τη νέα πρακτική.

[40] Gates Bill, 1999. *Επιχειρηματικές ευκαιρίες στην Ψηφιακή Οικονομία/ Μέσα από την Καλύτερη Χρήση της Τεχνολογίας.* Εκδόσεις Κλειδάριθμος.

[41] Peeka, Oikonomou Victoria, Lykogianni Vasiliki. *The Human Factor as a source of competitive advancement in the new Globalization Market.* University of Peiraious, Panteion University.

ii. Οργανωτική Ενσωμάτωση, η οποία περιλαμβάνει την εμπλοκή όλων των ενδιαφερόμενων μελών για την υιοθέτηση και χρήση των νέων πρακτικών.

iii. Στρατηγική Ενσωμάτωση, που συνεπάγεται όλων των πολιτικών της εταιρίας και του ανθρωπίνου παράγοντα με το επιχειρησιακό στρατηγικό πλάνο της εταιρίας, για αύξηση της αποδοτικότητας και διατήρηση του συγκριτικού πλεονεκτήματος.

Στη συγκεκριμένη περίπτωση που αναφερόμαστε στη σχέση του ανθρώπινου παράγοντα με τα πληροφοριακά συστήματα, η καλύτερη επένδυση είναι η εκπαίδευση. Δεν είναι τυχαίο άλλωστε το γεγονός ότι όλοι οι μεγάλοι οργανισμοί ακολουθούν προγράμματα κατάρτισης των εργαζομένων τους. Άλλωστε όταν έχεις ανταγωνιστικό ανθρώπινο δυναμικό έχεις έναν ανταγωνιστικό οργανισμό. Η εκπαίδευση αυτή πρέπει να περιλαμβάνει θέματα πληροφοριακών συστημάτων, για την καλύτερη και αποδοτικότερη χρήση τους, αλλά και θέματα εξειδίκευσης και ενημέρωσης των εργαζομένων ανάλογα με την θέση την οποία κατέχουν (Melone, 1990)[42].

6.1.2 Προβλήματα κατά την Υιοθέτηση Νέου Πληροφοριακού Συστήματος.

Ένας από τους πιο βασικούς νόμους της φυσικής είναι ο νόμος της αδράνειας. Σύμφωνα με αυτό το νόμο το αντικείμενο της μελέτης αντιστέκεται στην αλλαγή της κατάστασης της οποίας βρίσκεται ήδη. Μία αντίστοιχη περίπτωση μπορεί να αντιμετωπισθεί κατά την προσπάθεια ενσωμάτωσης νέων εφαρμογών, πολιτικών, διαδικασιών και φυσικά νέων πληροφοριακών συστημάτων από το ανθρώπινο δυναμικό. Ειδικότερα, μπορεί να υπάρξει άρνηση, αντιδράσεις λόγω έλλειψης εξοικείωσης, έλλειψης εκπαίδευσης κ.α.

Κάποιες βασικές αντιδράσεις είναι οι εξής (Λεωνίδας, 2001) [43]:

[42] Melone, 1990. *Theoretical Assessment of the User-Satisfaction Construct in Information Systems Reshearch :* Management Science.

[43] Χυτήρης Λεωνίδας, 2001. *Οργανωσιακή Συμπεριφορά: Η ανθρώπινη συμπεριφορά σε οργανισμούς και επιχειρήσεις.* Εκδοτικός Οίκος Interbooks.

- Απόρριψη αλλαγής λόγω φόβου μείωσης αποδοχών ή κύρους της εργασίας τους, ή και ακόμα απώλεια της δουλειάς τους.
- Αντίσταση στην αλλαγή, η οποία μειώνει την απόδοση του εργαζομένου.
- Ανοχή στην αλλαγή, δηλαδή διατήρηση ουδέτερης στάσης. Ο εργαζόμενος θεωρεί ότι ούτε ωφελείται ούτε χάνει κάτι όμως και από την αλλαγή, γεγονός που συνεπάγεται την μη αύξηση της παραγωγικότητας.
- Τέλος η αποδοχή της αλλαγής συνεπάγεται θετική αντίδραση του εργαζομένου. Ο εργαζόμενος θεωρεί ότι θα επωφεληθεί των αλλαγών και θα αυξήσει την παραγωγικότητα του.

Αποτελεί σημαντικό παράγοντα η συνεχής ανατροφοδότηση πληροφοριών, ιδιαίτερα όταν οι αλλαγές έχουν συμβεί πρόσφατα. Θα πρέπει να υπάρχουν άμεσες διορθωτικές ενέργειες σε οποιαδήποτε περίπτωση από διοικητικό προσωπικό, καθώς και να γνωρίζουν ποια η σχέση του ανθρώπινου δυναμικού με το σύστημα επικοινωνίας της εταιρίας, το πληροφοριακό σύστημα και φυσικά με τις πολιτικές που ακολουθεί η εταιρία.

7.1 Μεθοδολογίες και Εργαλεία Διαχείρισης και Αξιολόγησης Κινδύνου στα ΠΣ.

Όπως έχει ήδη αναφερθεί ένα αναπόσπαστο κομμάτι σε όλους τους οργανισμούς είναι η Διαχείριση του Κινδύνου. Στην προσπάθεια συστηματοποίησης του κινδύνου δημιουργηθήκαν κάποια εργαλεία για την καλύτερη αξιολόγηση και διαχείριση του τα οποία ξεχώρισαν και άρχισαν να υιοθετούνται από διάφορους οργανισμούς.

Κάποια από τα πιο γνωστά εργαλεία και μεθοδολογίες διαχείρισης κινδύνου είναι οι εξής:

- Μεθοδολογία NIST – National Institute of Standards and Technology.
- Μεθοδολογία CRAMM - Central Computer and Telecommunication Agency.
- Μεθοδολογία FRAP – Facilitated Risk Assessment Process.
- Μεθοδολογία Magerit – Minestirio de Administraciones Publicas (Spanish Ministry of Public Admininstration)
- Μεθοδολογία IT - Grundschutz (BSI)

- Μεθοδολογία OCTAVE – Operational Critical, Threat, Asset and Vulnerability Evaluation.
- Μεθοδολογία EBIOS (Expression des Besoin et Indification des Objectifs de Securite – Έκφραση Αναγκών και Προσδιορισμός Στόχων Ασφαλείας).
- Μεθοδολογία COBRA

7.2 Μεθοδολογία OCTAVE - Operational Critical, Threat, Asset and Vulnerability Evaluation.

Μία από τις πιο πολυχρησιμοποιημένες μεθοδολογίες για την διαχείριση και αξιολόγηση του Κινδύνου στα Πληροφοριακά Συστήματα είναι η OCTAVE, η οποία θα αναλυθεί στα πλαίσια αυτού του κεφαλαίου. Το Software Engineering Institute (SEI) του Carnegie Mellon University ανέπτυξε αυτή τη μοθοδολογία. Βασικός λόγος δημιουργίας της συγκεκριμένης μεθοδολογίας είναι η βελτίωση μεθόδων προστασίας των οργανισμών από τους κινδύνους και την ασφάλεια πληροφοριών. Η μεθοδολογία αυτή ακολουθεί μία διαφορετική μέθοδο αξιολόγησης και κατανόησης του κινδύνου καθώς και των συνιστωσών που το αποτελούν, δημιουργώντας μία εκτεταμένη και ουσιώδη ασφάλεια. Βασική αρχή είναι ότι ο Οργανισμός θα κατανοήσει καλύτερα τον κίνδυνο από το εργαλεία και κατά συνέπεια θα λάβει καλύτερη απόφαση διαχείρισης κινδύνου από το εργαλείο.

Υπάρχουν 3 βασικές φάσεις που Ακολουθούνται:

1) Στην φάση αυτή συλλέγονται όλες οι σχετικές πληροφορίες για τις ενδεχόμενες απειλές, καθώς και σχετικές πληροφορίες στρατηγικών που ακολουθεί ο οργανισμός.
   a) Διαδικασία 1: Εντοπισμός Πληροφοριών που προέρχονται από την Ανώτερη Διοίκηση.
   b) Διαδικασία 2: Καθολικός Προσδιορισμός και Διαχείριση Γνώσεων σε Επιχειρησιακό Επίπεδο.
   c) Διαδικασία 3: Προσδιορισμός Γνώσεων σε επίπεδο Προσωπικού.
   d) Διαδικασία 4: Δημιουργία Προφίλ Απειλών.

2) Στην δεύτερη φάση συγκεντρώνονται οι γνώσεις των διαχειριστών στο επιχειρησιακό κομμάτι
   a) Διαδικασία 5: Επισήμανση βασικών συστατικών.
   b) Διαδικασία 6: Αξιολόγηση των συστατικών αυτών.
3) Ακολουθεί η φάση 3, η οποία περιλαμβάνει την συλλογή γνώσης του προσωπικού, αναλυτικότερα:
   a) Διαδικασία 7: Ανάλυση Κινδύνου.
   b) Διαδικασία 8: Δημιουργία Στρατηγικής κατά των απειλών και ταυτόχρονη επισκόπηση, αναθεώρηση και έγκριση στρατηγικής.

Το συγκριτικό πλεονέκτημα της μεθόδου OCTAVE είναι ότι λαμβάνει ανατροφοδότηση και πληροφορίες από όλο τον οργανισμό, κερδίζοντας μία πιο σφαιρική άποψη για αυτόν σε σύντομο χρονικό διάστημα, ώστε να αντιδράσει εγκαίρως στον κίνδυνο. Η μέθοδος αυτή παρέχει 3 βασικά αποτελέσματα, την στρατηγική προστασίας, ένα σχέδιο μετριασμού και ένα κατάλογο ενεργειών ανά περίπτωση. Τέλος θα μπορούσε κανείς να πει ότι η OCTAVE στοχεύει περισσότερο στο Προσωπικό.

8.1 Μεθοδολογίες και Εργαλεία Ανάλυσης και Διαχείρισης επικινδυνότητας σε έργα Πληροφοριακών Συστημάτων.

Οι συνεχείς και αυξανόμενες ανάγκες για ασφάλεια κατά την υλοποίηση έργων πληροφορικής και έργων Ηλεκτρονικής Διακυβέρνησης, έχουν ωθήσει τους Οργανισμούς στην δημιουργία αποτελεσματικών εργαλείων και μεθοδολογιών για να καλύψουν την ανάγκη αυτή.

Κάποιες από τις πιο σημαντικές μεθοδολογίες είναι οι εξής:

- PRINCE (Projects In Controlled Environments).
- GDPM (Goal Directed Project Management).
- RiskNav.
- PBMOK.

Στα πλαίσια του Κεφαλαίου αυτού θα αναλυθεί η μεθοδολογία Prince, καθότι αποτελεί μία μεθοδολογία που χρησιμοποιείται και από δημόσιους όσο και ιδιωτικούς φορείς. Αποτελεί επίσης μία σύγχρονη και δοκιμασμένα πετυχημένη μεθοδολογία.

8.2 Μεθοδολογία Prince.

Η μεθοδολογία Prince αποτελεί μία λειτουργική μέθοδο διαχείρισης δημοσίων έργων εγκεκριμένη από το Ηνωμένο Βασίλειο. Για την ακρίβεια δημιουργήθηκε το 1989 από την CCTA (Central Computer and Telecommunication Agency), ενώ η PRINCE2 που δημοσιεύθηκε το 1996, έχει συμβάλει στην κοινοπραξία 150 ευρωπαϊκών οργανώσεων.

Αναλυτικότερα τα χαρακτηριστικά της είναι:

- Εστίαση στην Δικαίωση των Επιχειρήσεων.
- Δημιουργία Καθορισμένης Δομής της Ομάδας Διαχείρισης του Έργου.
- Ο σχεδιασμός γίνεται βάση των Προϊόντων.
- Διαίρεση του έργου σε επιμέρους κομμάτια για καλύτερη διαχείριση και έλεγχο.
- Δημιουργία Ευελιξίας όσο είναι απαραίτητη για τη διαχείριση του έργου.

Αρχικά ορίζεται το έργο και η ομάδα που θα το αναλάβει. Αναλύεται ο τρόπος προσέγγισης και γίνεται και το πρόγραμμα υλοποίησης του. Στη συνέχεια δίνεται η εντολής για την έναρξη του έργου. Στο στάδιο αυτό αναλύεται το σχέδιο του έργου, η διύλιση επιχειρηματικού ενδιαφέροντος, οι κίνδυνοι του, ενώ διασφαλίζεται η ποιότητα του.

Όπως έχει αναφερθεί το έργο θα πρέπει να αναλύονται σε στάδια και να ελέγχονται. Με αυτό τον τρόπο αξιολογείται η πρόοδος και οι παράμετροι του έργου, ενώ διευκολύνονται πιθανές διορθωτικές ενέργειες.

Η διαδικασία του ελέγχου και της διαχείρισης των ορίων του έργου, υπαγορεύουν τι πρέπει να γίνει σε κάθε στάδιο και τον τρόπο ολοκλήρωσής του. Επιπροσθέτως θα πρέπει να ελεγχθούν και να αναλυθούν πιθανοί κίνδυνοι.

Ακολουθούν οι ενέργειες της Διεύθυνσης Παράδοσης του Έργου/Προϊόντος και η περάτωση του έργου. Στο σημείο αυτό γίνεται αξιολόγηση και αναθεώρηση, εφόσον είναι απαραίτητη του έργου.

Συνοπτικά θα μπορούσε να τονισθεί ότι ο έλεγχος με τη μεθοδολογία PRINCE είναι απλούστερος, αμεσότερος και συντομότερος αφού αποτελείται από επιμέρους μέρη, τα οποία αναλύονται ευκολότερα. Αυστηρός επιμερισμός εργασίας και σωστή Διακυβέρνηση και Ιεραρχία διευκολύνουν την επίτευξη του οποιοδήποτε έργου.

9.1 Διαρροή Δεδομένων.

Ένα βασικό πρόβλημα που αντιμετωπίζουν όλοι οι οργανισμοί είναι η διαρροή δεδομένων. Η διαρροή δεδομένων συνεπάγεται αδυναμία προστασίας τους από τον οργανισμό, με συνέπεια την δημιουργία έλλειψης εμπιστοσύνης της κοινής γνώμης. Ας μην ξεχνάμε πόσο μεγάλη ζημία μπορεί να προκαλέσει στην φήμη ενός οργανισμού ένα τέτοιο γεγονός. Υπάρχουν άλλωστε αμέτρητες περιπτώσεις εταιριών και οργανισμών που δεν κατάφεραν ποτέ να ανακάμψουν από τέτοια γεγονότα. Σκοπός κάθε οργανισμού είναι η προστασία των δεδομένων και έμμεσα προστασία της φήμης του οργανισμού.

Αναφορικά με την έννοια Δεδομένα εννοούμε τα εξής:

- Οικονομικές Πληροφορίες.
- Στοιχεία Πελατών.
- Δεδομένα Πνευματικής Ιδιοκτησίας.
- Επιχειρηματικά Πλάνα.
- Αναπτυξιακά Πλάνα.
- Προσωπικά Στοιχεία Δεδομένων.
- Πληροφορίες Προϊόντων και Υπηρεσιών.
- Πληροφορίες Διαφημιστικών Εκστρατειών.

9.2 Βασικά αίτια απωλειών.

Βασικά Αίτια Απώλειας Δεδομένων Από Εξωτερικές Πηγές:

- Δούρειος Ίππος (Trojan Horse).
- Κακόβουλος Κώδικας (Malware).
- Λογικές Βόμβες (Logic Bombs).
- Καταπακτές (Trapdoors).
- Ιοί (Viruses).
- Ηλεκτρονική Πειρατεία (Hacking).
- Φυσική Απώλεια.

Όσον αφορά την εσωτερική απώλεια δεδομένων από εσωτερικές πηγές για ακόμη μία φορά πάλι ο ανθρώπινος παράγοντας έχει πρωταγωνιστικό ρόλο. Υπάρχουν εργασιακά λάθη, υπάρχουν όμως και οι περιπτώσεις που εργαζόμενοι της εταιρίας διαρρέουν πληροφορίες για προσωπικό όφελος. Πρακτικές όπως ο καθένας να φέρνει τη δικιά του ηλεκτρονική συσκευή στον χώρο εργασίας και δουλεύει σε αυτή, ή μη κρυπτογραφημένα αρχεία από πλευράς εταιρίας, έχουν διευκολύνει αρκετά αυτά τα γεγονότα.

9.3 Έμμεσες και Άμεσες Απώλειες Δεδομένων.

Οι συνέπειες από την απώλεια Δεδομένων μπορούν χαρακτηριστούν ως άμεσες ή έμμεσες απώλειες. Ο διαχωρισμός τους γίνεται βάση του χρονικού περιθωρίου που γίνονται ορατές. Άμεσες είναι οι απώλειες που γίνονται άμεσα εμφανείς και είναι και εύκολα μετρήσιμες από άποψη κόστους. Έμμεσες είναι οι απώλειες μπορεί να μην γίνουν άμεσα αντιληπτές, δεν προσδιορίζονται εύκολα ως προς τον χρόνο που συνέβησαν και το κόστος, αφού είναι πιθανόν να επιφέρουν και αρνητική δημοσιότητα.

9.4 Τεχνολογικά Εργαλεία Πρόληψης.

Με την πάροδο του χρόνου και λόγω των αυξημένων επιθέσεων και λόγω της ανάγκης για πρόληψη, έχουν αναπτυχθεί τεχνολογικά εργαλεία για τον εντοπισμό και την πρόληψη διαρροής δεδομένων.

Βασικά Μέτρα Προστασίας:

- Τείχος Προστασίας (firewall).
- Αντιιοί (Antivirus).
- Συστήματα Εντοπισμού Εισβολών.
- Εξαρτημένα Τερματικά.
- Πολιτικές του Οργανισμού.

Προχωρημένα Μέτρα Προστασίας:

- Εντοπισμός Ανωμαλιών.
- Επιβεβαίωση Ανάλογη της Δραστηριότητας.
- Παγίδες.
- Δοχείο Μελιού (honeypots).

Έλεγχος Προσβάσεων και Κρυπτογράφηση:

- Έλεγχος Συσκευών.
- Κρυπτογράφηση.
- Υπηρεσία Διαχείρισης Δικαιωμάτων (Rights Management Services).

Καθορισμένα Συστήματα Αποτροπής Απώλειας Δεδομένων:

- Σαρώσεις Κινούμενων Δεδομένων, δηλαδή των δεδομένων που βρίσκονται σε υπολογιστή και σε άλλα αποθηκευτικά μέσα.
- Σαρώσεις Χρησιμοποιούμενων Δεδομένων, δηλαδή όλα τα Δεδομένα με τα οποία αλληλεπιδρά ο χρήστης.
- Σαρώσεις Δεδομένων που Βρίσκονται σε Κίνηση, δηλαδή των Δεδομένων που ανταλλάσσονται Διαδικτυακά.

9.5 Αντικειμενικοί Στόχοι και Σκοποί του τμήματος Πληροφοριακών Δεδομένων.

Ο αντικειμενικός σκοπός του τμήματος Πληροφοριακών Συστημάτων είναι η εξασφάλιση ότι η αποτυχία συστήματος, η ανεπιθύμητη αποκάλυψη πληροφοριών, η απάτη, η διακοπή εργασιακών διαδικασιών, διαρροή δεδομένων και μη πιστοποιημένες προσβάσεις σε δεδομένα, δεν μπορούν να πραγματοποιηθούν από εγκληματίες του κυβερνοχώρου. Θα ακολουθήσει τμηματοποίηση των βασικότερων κινδύνων που καλείται να αντιμετωπίσει το τμήμα Πληροφοριακών Συστημάτων, ή κάποιο τρίτο μέλος που έχει αναλάβει την ασφάλεια, και οι απαραίτητες ενέργειες αποτροπής και πρόληψης τους.

9.5.1 Αποτυχία Συστήματος.

Η αποτυχία συστήματος μπορεί να προκληθεί από ιούς, κακόβουλο λογισμικό όπως δούρειοι ίπποι κλπ και να οδηγήσουν στη διακοπή των εργασιακών διαδικασιών. Στην περίπτωση αυτή πρέπει να ληφθούν ενέργειες αντιιών και διαχείριση κακόβουλου λογισμικού. Αναλυτικότερα, πρέπει να επιβεβαιωθεί ότι η βάση του προγράμματος αντιιών(software) είναι ενημερωμένη(updated) με την πιο πρόσφατη έκδοση για τους, όπως και αντίστοιχα οι πιο νέοι ορισμοί ιών(virus definitions) είναι εγκατεστημένη. Αυτοί οι έλεγχοι πρέπει να γίνονται μηνιαίοι για το λογισμικό και εβδομαδιαίοι για τους ορισμούς των ιών.

9.5.2 Ανεπαρκής Ασφάλεια Συστημάτων.

Η αποτυχία συστήματος μπορεί να προκύψει από την μη συμμόρφωση των διαμορφωμένων ρυθμίσεων(configuration settings) με τα προβλεπόμενα πρότυπα(agreed standards). Η παράλειψη αυτή μπορεί να οδηγήσει σε μη επιθυμητή αποκάλυψη πληροφοριών, απάτη και διακοπή εργασιακών διαδικασιών.

Το πρώτο μέτρο που πρέπει να ληφθεί αφορά τη γραμμή βάσης ασφαλείας(security baseline). Θα πρέπει να γίνεται τουλάχιστον κάθε τρεις μήνες έλεγχος για την εξασφάλιση της εύρυθμης λειτουργίας της.

Ακολουθεί η διαδικασία ελέγχων των καλυμμάτων ασφαλείας (security patches), η οποία θα πρέπει να γίνεται περιοδικά.

Θα πρέπει να γίνονται έλεγχοι αδυναμιών (vulnerability scans). Για την ακρίβεια θα πρέπει να ελέγχονται τα συστήματα υποδοχής(host systems), και οι δικτυακές συσκευές(network devices) που φημίζονται για τις αδυναμίες τους. Έλεγχος πρέπει να γίνεται και σε μη αναγκαίες διαδικασίες, εντολές και υπηρεσίες που έχουν τεθεί σε αχρηστία. Βασικός έλεγχος πρέπει να γίνεται επίσης για την εύρεση μη εξουσιοδοτημένων δικτύων και συστημάτων στον χώρο εργασίας με τη χρήση εργαλείων χαρτογράφησης.

Πρέπει επίσης να εξασφαλίζεται και η χρήση και η ασφάλεια των φορητών συσκευών (πχ laptop,tablet,κινητά) μέσω κρυπτογράφησης.

Τέλος απαραίτητη είναι η κρυπτογράφηση και η ασφάλιση των εφεδρικών μέσων(backup mediums encryption).

9.5.3 Μη εξουσιοδοτημένες προσβάσεις.

Μη εξουσιοδοτημένες προσβάσεις σε εμπιστευτικές πληροφορίες και έγγραφά είναι πιθανών να συμβούν μέσω αυτοματοποιημένων εξωτερικών συνδέσμων(links). Ο λόγος που μπορεί να συμβεί το παραπάνω γεγονός είναι η ανεπάρκεια των μέτρων που χρησιμοποιούνται για ασφάλεια. Η ανεπάρκεια αυτή οδηγεί σε μη επιθυμητή αποκάλυψη πληροφοριών και απάτη.

Η λύση είναι ο έλεγχος των εξωτερικών συνδέσμων. Θα πρέπει να γίνεται ανάλυση ρίσκου των συνδέσμων από την Ασφάλεια Πληροφοριακών Συστημάτων, τον Υπεύθυνο Ασφάλειας Πληροφοριών και τη Διοίκηση Πληροφοριακού Ρίσκου και συλλογικά να αποφασίσουν για την υλοποίηση του εξωτερικού συνδέσμου. Περιοδικά θα πρέπει να αξιολογούνται τα μέτρα και να αντικαθίστανται αυτά που κρίνονται ως ανεπαρκή. Οι έλεγχοι πρέπει να γίνονται λαμβάνοντας υπόψη την αρχιτεκτονική δομή των συστημάτων, των αρχών του συστήματος, την πολιτική ασφαλείας κλπ.

9.5.4 Απώλεια Κρυπτογραφημένων Κλειδιών.

Είναι πιθανό κρυπτογραφημένα κλειδιά να βρεθούν σε μη εξουσιοδοτημένα άτομα από απρόσεκτη έκδοση, από λανθασμένες ανανεώσεις προσβάσεων κλπ, οι οποίες οδηγούν σε λανθασμένες και μη εξουσιοδοτημένες προσβάσεις σε ευαίσθητα δεδομένα και συστήματα.

Το τμήμα πληροφοριακών συστημάτων πρέπει να εξασφαλίζει ότι τα εξουσιοδοτημένα κλειδιά, δίνονται με ασφάλεια στους κατόχους τους, ανανεώνονται και ανακαλούνται ορθά.

9.5.5 Απειλές από τρίτους.

Μία από τις σημαντικότερες και πιο απρόβλεπτες απειλές είναι αυτή των κυβερνό-εγκλημάτων. Τα εγκλήματα αυτά συμβαίνουν ευκολότερα όταν δεν υπάρχουν επαρκή μέτρα ασφάλειας στο διαδικτυακό περιβάλλον και έχουν ως συνέπεια την απώλεια δεδομένων, την απάτη και τη διακοπή των εργασιών.

Αρχικά θα πρέπει να γίνονται τεστ διείσδυσης. Τα τεστ αυτά πρέπει να γίνονται πριν την εκτέλεση νέων πληροφοριακών συστημάτων. Η θεωρητική βάση των τεστ αυτών πρέπει να περιλαμβάνει τις βασικές αρχές της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Στην χειρότερη περίπτωση τα τεστ αυτά πρέπει να γίνονται κάθε 3 χρόνια.

Ένα ακόμα μέτρο πρόληψης είναι η παρακολούθηση της ασφάλειας και διαχείριση των περιστατικών ασφάλειας. Για την ακρίβεια πρέπει να γίνονται αναλύσεις πιθανών επιθέσεων και μη επιθυμητών συμβάντων. Σύμφωνα με αυτούς τους έλεγχους πρέπει να τίθενται σε λειτουργία νέα διαδικαστικά μέτρα ασφαλείας.

Φυσικά πρέπει να γίνονται αναλύσεις των πιθανών και υφιστάμενων κινδύνων του δικτύου κίνησης. Το τμήμα ασφάλειας πληροφοριακών συστημάτων σε συνεργασία με τον υπεύθυνο ασφάλειας των πληροφοριών πρέπει να ελέγχουν τον επιχειρηματικό κίνδυνο βάση του διαθέσιμου δικτύου κίνησης πληροφοριών.

Τέλος σε αυτό το κομμάτι πρέπει να γίνονται και έλεγχοι στους κανόνες βάσης του τοίχους προστασίας (firewall). Μία διαδικασία που πρέπει να εκτελείται τουλάχιστον μία φορά το μήνα σε όλα τα τοίχοι προστασίας. Οι ενεργοί κανονισμοί της βάσης του τοίχους προστασίας θα πρέπει να ανταποκρίνονται στις

υποβαλλόμενες αιτήσεις και απαιτήσεις. Οι πιθανές αποκλίσεις που πιθανώς διαπιστωθούν, θα πρέπει να αναλύονται, να διορθώνονται ή να δέχονται επίσημες αποδοχές από τη Διοίκηση.

9.5.6 Προβλήματα Προστασίας Εταιρικών Ιστοσελίδων.

Η πιθανή αδυναμία ασφάλειας των ιστοσελίδων και των εφαρμογών μπορούν να οδηγήσουν σε απώλεια δεδομένων και διακοπή εργασιών.

Ο διαχειριστής των ιστοσελίδων και των εφαρμογών σε συνεργασία με το τμήμα πληροφοριακών συστημάτων πρέπει να δημιουργήσουν μία πλήρη λίστα με τις πιστοποιήσεις, τις προσβάσεις και τα ονόματα των τομέων (domain names).

Επιπροσθέτως, περιοδικά θα πρέπει να γίνεται ανεξάρτητη λειτουργία ασφάλειας που θα ελέγχει και θα εξακριβώνει πως μόνο ασφαλής ιστότοποι (website) και εφαρμογές έχουν τεθεί ή θα τεθούν σε λειτουργία.

9.5.7 Ανάληψη Πληροφοριακών Κινδύνων.

Η μη συμμόρφωση λειτουργιών ασφαλείας με τους εθνικούς και διεθνής κανονισμούς, περιορισμούς, εσωτερικές πολιτικές και βέλτιστες πρακτικές, οδηγεί στους πληροφοριακούς κινδύνους/ ρίσκο.

Η ορθή λύση των πληροφοριακών κινδύνων/ ρίσκο είναι η σωστή συνεργασία τμημάτων και ατόμων εντός του οργανισμού. Ειδικότερα θα πρέπει ο Υπεύθυνος Ασφάλειας Πληροφοριών και ο Υπεύθυνος Κυβερνοασφάλισης να αποτελέσουν μέλος του Συμβουλίου. Αυτό θα δημιουργήσει ένα καλύτερο ορισμό για την πληροφοριακή και διαδικτυακή ασφάλεια. Θα πρέπει να ορισθούν οι εξής υπεύθυνοι:

- Υπεύθυνος Ασφάλειας Πληροφορίας(Information Security Officer).
- Υπεύθυνος Ασφαλειών(Security Officer).
- Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων(Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων).
- Ομάδα που Συντελείται από τους παραπάνω Υπεύθυνους.

Ετησίως και ανεξαρτήτως των οργανωτικών αλλαγών, θα πρέπει ο Υπεύθυνος Ασφάλειας Πληροφορίας να εξασφαλίζει ότι οι Πολιτικές Ασφαλείας Πληροφοριών είναι ενημερωμένες και ότι ακολουθούνται πιστά.

Ετησίως θα πρέπει να συντελείται επίσης ένα σχέδιο ασφάλειας πληροφοριών από τον Υπεύθυνο Ασφάλειας Πληροφοριών και να επιβεβαιώνει συχνά το κατά πόσο ακολουθείται το σχέδιο αυτό.

Αναγκαία είναι και η ετήσια διασφάλιση πως οι διαδικασίες και καθοδηγητικές γραμμές είναι διαθέσιμες και ενημερωμένες, σύμφωνα με την πολιτική ασφάλειας πληροφοριών και πως δεν λείπει καμία διαδικασία και καθοδηγητική γραμμή. Μια διαδικασία που εκτελείται πάλι από τον Υπεύθυνο Ασφάλειας Πληροφοριών.

Τέλος, θα πρέπει να εκτελείται ένα σχέδιο για την ευαισθητοποίηση και ενημέρωση των εργαζομένων για την ασφάλεια πληροφοριών. Έλεγχος των αποτελεσμάτων του σχεδίου αυτού θα πρέπει να γίνονται τουλάχιστον μία φορά στους 3 μήνες.

9.5.8 Ανεπαρκής Φυσική Πρόσβαση.

Ένα ακόμα θέμα για επίλυση είναι η ανεπαρκής φυσική πρόσβαση και περιβαλλοντική ασφάλεια εντός και εκτός του Δωματίου του Κεντρικού Υπολογιστή (server).

Μία λύση είναι η Φυσική Ασφάλεια, δηλαδή με την ύπαρξη ατόμου που εξασφαλίζει την ασφάλεια του Δωματίου του Κεντρικού Υπολογιστή. Τα άτομα που θα δικαιούνται πρόσβαση είτε φυσική είτε απομακρυσμένη θα πρέπει να ελέγχεται και να επαναπροσδιορίζεται με μεγάλη συχνότητα. Επίσης αναγκαία είναι η ύπαρξη κλειστού καλωδιακού τύπου κάμερας καταγραφής εντός και εκτός του Δωματίου.

Επισκέπτες και τρίτα μέλη θα πρέπει να συνοδεύονται από προσωπικό του τμήματος Πληροφοριακών Συστημάτων, από την είσοδο τους έως και την αποχώρηση τους. Τέλος απαραίτητη είναι η καταγραφή των επισκεπτών.

Τέλος το Δωμάτιο του Κεντρικού Υπολογιστή πρέπει να προστατεύεται και από φυσικές περιβαλλοντολογικές καταστροφές. Μερικά μέτρα κατά των φυσικών καταστροφών αναφορικά είναι :

- Συστήματα εντοπισμού και καταστολής φωτιάς.
- Ανεξάρτητες Πηγές Ηλεκτρισμού σε περίπτωση διακοπής Ρεύματος.
- Υπερυψωμένο πάτωμα για τυχών πλημύρες.
- Σωστή υποδομή ταβανιού και καλωδίων.

Τα μέτρα αυτά θα πρέπει να ελέγχονται με υψηλή συχνότητα.

9.6 Συμπεράσματα.

Συμπερασματικά θα πρέπει υπάρχει ασφάλεια για την διαρροή πληροφοριών εντός και εκτός της εταιρίας. Θα πρέπει το προσωπικό να είναι σωστά προετοιμασμένο, εκπαιδευμένο και ευαισθητοποιημένο. Απαραίτητες είναι οι ενέργειες ασφάλειας από το τμήμα Πληροφοριακών Συστημάτων σε τεχνικό και τεχνολογικό επίπεδο, καθώς και η ανάθεση επιβλεπόντων των αποτελεσμάτων. Η ασφάλεια των Πληροφοριών αποτελεί νούμερο ένα προτεραιότητα για όλους τους Οργανισμούς πλέον με τη νέα Νομοθεσία του GDPR.

Τέλος η αξία της πληροφορίας εξαρτάται από το ποιος την κατέχει. Π.χ. ευαίσθητες πληροφορίες και εταιρικά δεδομένα και πρακτικές στα χέρια των ανταγωνιστών μπορεί να είναι πιο προβληματική από ότι στα χέρια ενός εφήβου (Brian Cashell, 2004)[44].

[44] Brian Cashell, W. D. J. M. J. a. B. W., 2004. *The Economic Impact of Cyber-Attacks.* s.l.:s.n.

Πίνακας με Γνωστά Γεγονότα Απώλειας Δεδομένων από www.datalossdb.org.

Ημερομηνία	**Οργανισμός**	**Περιγραφή**
2003	Βρετανική Υπηρεσία Πληροφοριών	Μια αναφορά της Βρετανικής Υπηρεσίας Πληροφοριών υπό μορφή εγγράφου Word περιείχε τα ονόματα συγγραφέων μιας μελέτης, η οποία στη σύνοψη των μεταδιδόμενων είχε αναφορές από τις ΗΠΑ και παρουσιάστηκε σε ομιλία στα Ηνωμένα Έθνη. Τα μεταδεδομένα έδειξαν ότι η αναφορά στην πραγματικότητα γράφτηκε από

		Αμερικανούς ερευνητές
Ιούλιος 2008	Google	Δεδομένα εκλάπησαν από τα κεντρικά γραφεία της θυγατρικής της εταιρείας, Colt Express. Οι κλέφτες εισέβαλλαν και έκλεψαν υπολογιστές της εταιρείας που περιείχαν αποκρυπτογραφημένα δεδομένα ονομάτων, διευθύνσεων και αριθμών Κοινωνικής Ασφάλισης υπαλλήλων της Google. Ως αποτέλεσμα, η Google τερμάτισε τη συνεργασία της με την Colt Express
Οκτώβριος 2008	UPS	Από φορητό υπολογιστή υπαλλήλου της UPS εκλάπησαν πληροφορίες μισθοδοσίας 9000 υπαλλήλων της Μ. Βρετανίας. Ως απάντηση η UPS ανακοίνωσε ότι θα κρυπτογραφεί όλα τα αποθηκευμένα δεδομένα σε όλες τις φορητές συσκευές της επιχείρησης.
Ιανουάριος 2009	Συστήματα πληρωμών Heartland	Κακόβουλο λογισμικό παραβίασε 10 εκατομμύρια συναλλαγές πιστωτικών και χρεωστικών καρτών.
Οκτώβριος 2009	Εθνικό Αρχείο των ΗΠΑ	Η διεύθυνση του Εθνικού Αρχείου των ΗΠΑ απέρριψε με ακατάλληλο τρόπο σκληρούς δίσκους που περιείχαν 76 εκατομμύρια ονόματα, διευθύνσεις και αριθμούς Κοινωνικής Ασφάλισης

		βετεράνων στρατιωτικών
Σεπτέμβριος 2011	Science Applications	Κασέτες αντιγράφων ασφαλείας εκλάπησαν από αυτοκίνητο και περιείχαν 5.117.799 ονόματα ασθενών, νούμερα τηλεφώνων, αριθμούς Κοινωνικής Ασφάλισης, και ιατρικές πληροφορίες
Μάρτιος 2012	Shanghai Roadway D&B Marketing Services Co. Ltd	Παράνομη αγοραπωλησία πληροφοριών 150.000.000 πελατών
Μάρτιος 2013	LivingSocial Inc (ΗΠΑ)	Hacker κατάφερε να υπεξαιρέσει ονόματα, emails και ημερομηνίες γεννήσεως 50.000.000 πελατών

10.1 Έννοιες που Αφορούν, Απασχολούν και Επηρεάζουν τα Πληροφοριακά Συστήματα.

Τα πληροφοριακά συστήματα ασχολούνται ίσως με ένα από τα πιο διαδραστικά θέματα που μπορούν να απασχολήσουν έναν οργανισμό. Οι συχνές αλλαγές και εξελίξεις εισάγουν νέες έννοιες. Αναφορικά μερικές έννοιες που θα απασχολήσουν το κεφάλαιο αυτό είναι:

- Φέρε τη Δικιά σου Συσκευή (Bring Your Own Device BYOD).
- Χρήση Διαδικτυακού Αποθηκευτικού Χώρου (Cloud).
- Διαχείριση Προμηθευτών (Vendor Management-Outsourcing).
- Σκιά Πληροφοριακών Συστημάτων (Shadow IT).
- Διακυβέρνηση Δεδομένων.

10.2 Φέρε τη Δικιά σου Συσκευή (Bring Your Own Device BYOD).

Ζούμε σε μία εποχή που χάρη στις τεχνολογικές εξελίξεις τα τεχνολογικά gadget μικραίνουν, έχουν μεγαλύτερη αυτονομία στην διάρκεια μπαταρίας τους και εύκολα συναγωνίζονται έναν Ηλεκτρονικό Υπολογιστή. Στον αντίποδα όμως ένας επαγγελματίας έχει μία συσκευή για το σπίτι, μία για τη δουλειά και μία για το δρόμο. Αυτό δημιουργεί προβλήματα με τα αρχεία, τις ρυθμίσεις, πιθανώς της συμβατότητα των λογισμικών κ.α. Τεχνικά, και πολλές εταιρίες το δέχονται, υπάρχει η δυνατότητα του να συμπιεστούν όλες οι συσκευές σε μία, λόγω των τεχνολογικών διαθέσιμων δυνατοτήτων.

Ενώ αποτελεί μία μέθοδο που έχει προοπτικές αύξησης της ατομικής αποδοτικότητας, προκύπτουν θέματα ασφαλείας. Από τη στιγμή κιόλας που η συσκευή συνδεθεί σε κάποιο εταιρικό δίκτυο, ξεκινούν οι ανησυχίες για την ασφάλεια (Keith W. Miller, 2012)[45]. Η πρώτη ανησυχία αφορά τα Δεδομένα, τα οποία θα καταλήξουν σε κάποιον Προσωπικό Υπολογιστή και όταν συμβεί αυτό δεν υπάρχει δυνατότητα ελέγχου των Δεδομένων από την εταιρία. Με την καθημερινή μεταφορά αυτών των δεδομένων σε συνδυασμό με την συνεχή μετακίνηση της συσκευής αυξάνονται οι πιθανότητες εσκεμμένης κλοπής. Επιπροσθέτως, όταν το laptop δεν ανήκει στην εταιρία δεν είναι εύκολη η εγκατάσταση των πολιτικών ασφαλείας της εταιρίας. Ένα τελευταίο πρόβλημα είναι ότι η εταιρία θα μπορεί και αυτή με τη σειρά της να έχει πρόσβαση στα Δεδομένα της συσκευής όταν αυτή συνδεθεί στο δίκτυο της εταιρίας. Το πρόβλημα έγκειται στα βιομετρικά στοιχεία που πλέον έχουν οι συσκευές, καθώς και στα γενικότερα προσωπικά δεδομένα του χρήστη.

Σαν λύσεις θα μπορούσαν να δημιουργηθούν ξεχωριστά προφίλ στη συσκευή από τμήμα του IT, ώστε ο χρήστης να μπορεί να διαχωρίζει την προσωπική του ζωή από την εργασία του. Τα εργασιακά δεδομένα να μπορούν να έχουν κάποιον κρυπτογραφημένο κώδικα, για την εύκολη εύρεση του, όπως για τη μη δυνατότητα μεταφοράς του όταν η συσκευή βρίσκεται σε μη εξουσιοδοτημένο σύστημα.

Τέλος, η εγκατάσταση κωδικών ασφαλείας και GPS σε περίπτωση κλοπής είναι μία άμεση λύση.

[45] Keith W. Miller, J. V. F. H., 2012. *BYOD: Security and Privacy Considerations.* s.l.:IEEE Computer Society.

10.3 Χρήση Διαδικτυακού Αποθηκευτικού Χώρου (Cloud)/ Cloud Computing.

Ο ορισμός του Cloud Computing η διανεμόμενη αρχιτεκτονική που συγκεντρώνει όλους τους πόρους των διακομιστών (servers) σε μία κλιμακούμενη πλατφόρμα, με σκοπό την παροχή των πόρων αυτών και σε άλλους υπολογιστές (Sean Carlin, 2011)[46].

Τα 4 βασικά χαρακτηριστικά του είναι τα εξής:

- Κοινοί Πόροι, δηλαδή ενώ τα παλαιά μοντέλα έδιναν συγκεκριμένα δεδομένα σε ένα χρήστη, πλέον οι πηγές και οι εφαρμογές μπορούν να χρησιμοποιηθούν από πολλούς χρήστες.
- Μαζική Επεκτασιμότητα, αφού δίνει τη δυνατότητα να συνδυάσει αμέτρητα συστήματα ταυτόχρονα.
- Ελαστικότητα, διότι μπορεί να χρησιμοποιήσει όσο χώρο χρειάζεται για οποιαδήποτε χρήση, όσο και να τον αποδεσμεύσει.
- Γρήγορος και άμεσος εφοδιασμός, όπως επιπρόσθετα συστήματα και δικτυακές πηγές.

Αναφορικά Διάφορα Μοντέλα Cloud Computing:

- Δημόσια Cloud, φτιάχνετε και χρησιμοποιείται από διάφορους πελάτες.
- Ιδιωτικά Cloud, φτιάχνετε για ιδιοχρησία ή πωλείται μεμονωμένα σε ένα πελάτη.
- Υβριδικά Cloud, όπου στο ίδιο δίκτυο τοποθετείται και ιδιωτικό και δημόσιο Cloud

Αν έπρεπε να χαρακτηρίσουμε την τεχνολογική ωριμότητα των Cloud, θα λέγαμε ότι βρίσκονται ακόμα σε ηλικία νεογνού. Αυτό συνεπάγεται ότι ακόμα δεν έχουν προκύψει σημαντικά προβλήματα στη χρήση, οπότε δεν υπάρχουν μέτρα πρόληψης ή και μετρά περιορισμού ενός προβλήματος.

[46] Sean Carlin, K. C., 2011. *Cloud Computing Security.* s.l.:International Journal of Ambient Computing and Intelligence, 3(1), 14-19.

Αναφορικά κάποιοι προβληματισμοί είναι οι εξής:

- Ένα αρχικό πρόβλημα αφορά τους προμηθευτές και το κατά πόσο θα μπορούσαν να διατηρήσουν την απόδοση τους, ενώ το πελατολόγιο αυξάνεται. Ας μην ξεχνάμε πόσο έχει αυξηθεί η χρήση τους τα τελευταία χρόνια. Ειδικότερα σε περίπτωση που το Cloud σταματήσει να λειτουργεί για τον οποιοδήποτε λόγο, πιθανότητα θα επηρεάσει όλες τις λειτουργίες της εταιρίας.
- Ένα ακόμα ζήτημα είναι το ζήτημα της Ιδιωτικότητας. Πολύ χρήστες του Cloud πιθανώς θα αποθηκεύσουν προσωπικά ευαίσθητα δεδομένα. Δεν έχει διαπιστωθεί ακόμα το κατά πόσο η Δομή των Cloud, μπορεί να φιλοξενήσει ευαίσθητα προσωπικά δεδομένα χωρίς όμως να παραβεί κανόνες περί ιδιωτικού απορρήτου κλπ.
- Πιθανή είναι και η ανάγκη αύξησης των μέτρων ασφαλείας από την οπτική της πρόσβασης. Δεν πρέπει να μας ενδιαφέρει μόνο η γρήγορη και η εύκολη πρόσβαση στο Cloud, αλλά και η ασφαλής πρόσβαση.
- Οι χρήστες, σιγά θα αρχίσουν να αλλάζουν, πχ μπορεί κάποιος να πάψει να χρησιμοποιεί το χώρο του. Εδώ για λόγους εξοικονόμησης χρημάτων, πόρων και χρόνου, υπάρχει πιθανότητα ο κατασκευαστής να μην δημιουργήσει νέες Διευθύνσεις IP, αλλά να κρατήσει τις ίδιες. Σε αυτή την περίπτωση υπάρχει πιθανότητα ο νέος χρήστης να έχει προσβάσεις σε παλαιότερες δυνατές προσβάσεις του προηγούμενου χρήστη.
- Αλλαγές και ενημερώσεις του συστήματος μπορεί να αφήσουν το Cloud εκτεθειμένο για πολύ μικρό χρονικό διάστημα.

Συνοπτικά, μία εταιρία θα ήταν ιδανικό αν μπορούσε να δημιουργήσει το δικό της Cloud. Τα έγγραφα και τα δεδομένα παραμένουν προστατευμένα από φυσικές καταστροφές και προσβάσεις, ενώ υπάρχει άμεση προσβασιμότητα τους από εξουσιοδοτημένους χρήστες. Παρόλα αυτά πρέπει να γίνεται έλεγχος και η προστασία τους να γίνεται ολοένα και πιο ασφαλής.

10.4 Διαχείριση Προμηθευτών (Vendor Management-Outsourcing).

Η διαχείριση των Προμηθευτών (Vendor Management), αποτελεί μία αρχή η οποία επιτρέπει στις επιχειρήσεις να διαχειριστούν τα κόστη τους, τη δημιουργία της βέλτιστης υπηρεσίας/διαδικασίας για την επιχείρηση, σε συνδυασμό με τον επιμερισμό του κινδύνου για αύξηση της αξίας της ποιότητας κατά τη διάρκεια ζωής της υπηρεσίας/διαδικασίας.

Οι απειλές που απασχολούν είναι σε ένα τέτοιο έργο είναι η απόδοση του. Η απόδοση σε πρώτη φάση εξαρτάται από την αφοσίωση των ενδιαφερόμενων μελλών της (Englund, n.d.)[47]. Πιο συγκεκριμένα, τα Ανώτερα Διοικητικά Στελέχη είναι απαραίτητο να συνεισφέρουν και να εργαστούν στον έλεγχο προόδου του έργου αυτού.

Ένα δεύτερο κομμάτι για την κατανόηση του προβλήματος απόδοσης είναι ότι τα άτομα που εργάζονται για το νέο κομμάτι, δεν αποτελούν μέλη της οργάνωσης και κατά συνέπεια δεν γνωρίζουν βασικά οργανωτικά θέματα και στρατηγικούς στόχους και σκοπούς. Για ακόμη μία φορά η συνεργασία των Ανώτερων Διοικητικών Στελεχών είναι απαραίτητη για την διασφάλιση ότι όλα πηγαίνουν σύμφωνα με το πρόγραμμα της οργάνωσης (Ross, 2002)[48].

Ένα τρίτο ζήτημα σε όλα αυτά είναι η διαχείριση των διαθέσιμων πόρων για τα έργα που τρέχει η εταιρία. Άλλωστε οι μάνατζερ δεν φημίζονται για της οργανωτικές του δεξιότητες ως προς τη διαχείριση των πόρων (Li Liu, 2010)[49]. Όποτε λόγω του ανταγωνισμού των έργων (Pinto, 2000)[50] είναι απαραίτητο να υπάρχει βοήθεια από εξωτερικούς συνεργάτες ώστε να παρέχουν « κάλυψη αέρος για τους στρατιώτες» (Englund, n.d.)[51].

---

[47] Englund, R. a. B. A., n.d. *Project Sponsorship: Achieving management commitment for project success.* 2006: s.n.

[48] Ross, J. a. W. P., 2002. *Six Decisions your IT People Shouldn't Make.* s.l.:Harvard Business Review 80(11): 85–91.

[49] Li Liu, P. Y., 2010. *Sponsorship and IT vendor management of projects.* s.l.:Journal of Information Technology.

[50] Pinto, J., 2000. *Understanding the Role of Politics in Successful Project Management.* s.l.:International Journal of Project Management 18(2):85–91.

[51] Englund, R. a. B. A., n.d. *Project Sponsorship: Achieving management commitment for project success.* 2006: s.n.

Τέλος, η ουσιαστική αφοσίωση στο έργο από τους εξωτερικούς συνεργάτες είναι απαραίτητη για την σωστή και αποτελεσματική ολοκλήρωση του, καθώς πρέπει να παρέχουν κίνητρο στους εργαζομένους για την καλύτερη απόδοση τους (Miranda, 2005)[52].

10.5 Σκιά Πληροφοριακών Συστημάτων (Shadow IT).

Η σκιά των πληροφοριακών συστημάτων συνιστούν ένα συμπλήρωμα στο τμήμα πληροφοριακών συστημάτων. Η σκιά των πληροφοριακών συστημάτων αποτελείται πρόσθετες διεργασίες, από κάποια αυτόματα αναπτυγμένα συστήματα πληροφορικής και από κάποιες οργανωτικές ομάδες τοποθετημένες σε κάποια κομμάτια της επιχείρησης. Τα συστήματα αυτά συνήθως δεν είναι γνωστά σε όλους, και υποστηρίζονται από το τμήμα πληροφοριακών συστημάτων. Σύμφωνα με την οπτική της Διοίκησης και του Μάνατζμεντ της επιχείρησης το φαινόμενο αυτό θα πρέπει να είναι πάντα υπό έλεγχο (Christopher Rentrop, 2012)[53].

Σε αυτό το σημείο γεννάται η ανάγκη χαρακτηρισμού της κάθε περίπτωσης της σκιάς των πληροφοριακών συστημάτων. Για τον ορθό χαρακτηρισμό θα χρησιμοποιηθούν κριτήρια όπως αυτό της σχετικότητας, της αξίας του, του μεγέθους του, την εν δυνάμει καινοτομία του και του παραλληλισμού (Christopher Rentrop, 2012)[54].

Στο κομμάτι της σχετικότητας έχουμε την ανάγκη να χαρακτηρίσουμε το πόσο απαραίτητη είναι η σκιά στις διαδικασίες καθώς και θέματα που θα πρέπει να εξετάσει η εταιρία. Αναλύουμε τα εξής:

---

[52] Miranda, S. a. K. C., 2005. *Moments of Governance in IS Outsourcing: Conceptualizing effects of contracts on value capture and creation.* s.l.:Journal of Information Technology 20(3): 152–169..

[53] Christopher Rentrop, S. Z., 2012. *Shadow IT Evaluation Model.* s.l.:Proceedings of the Federated Conference on Computer Science and Information Systems pp. 1023–1027.

[54] Christopher Rentrop, S. Z., 2012. *Shadow IT Evaluation Model.* s.l.:Proceedings of the Federated Conference on Computer Science and Information Systems pp. 1023–1027.

- Στρατηγική Σχετικότητα: Πρέπει να ελεγχθεί πως η σκιά επηρεάζει τις στρατηγικές αποφάσεις και τις επιλογές δομής των πληροφοριακών συστημάτων. Πχ, μπορεί με τη χρήση κάποιας σκιάς να υπονομεύεται κάποια πιθανή εταιρική στρατηγική.
- Κριτική: Αναφερόμαστε σε θέματα όπως επιχειρησιακές διαδικασίες, ασφάλεια πληροφοριακών συστημάτων, συμμόρφωση με τη νομοθεσία, τη συντήρηση των πληροφοριακών συστημάτων και πως θα μπορούσε να τα επηρεάσει η συμπεριφορά της σκιάς.

Αξία: Φυσικά αναφερόμαστε στη αξία που προκύπτει ή στην αξία που χάνουμε από την ύπαρξη σκιάς. Ειδικότερα εξετάζουμε τους εξής τομείς:

- Συστημική Αξία.
- Αξία στη Συντήρηση Συστημάτων.
- Αξία της Πληροφορίας.
- Αξία στις επιχειρησιακές διαδικασίες.

Το κομμάτι του μεγέθους της σκιάς των πληροφοριακών συστημάτων είναι το τρίτο κριτήριο. Σε αυτό το κριτήριο ενδιαφερόμαστε για την χρήση των πόρων που γίνεται από τη σκιά, τον επαγγελματισμό της σκιάς και το ποσό της εισχώρησης τους στα υπάρχοντα συστήματα. Για τον περαιτέρω σχολιασμό του μεγέθους χαρακτηρίζουμε τα εξής:

- Χρήση των πόρων και επαγγελματισμός, δηλαδή το πόσα άτομα δουλεύουν για αυτό το περιστατικό της σκιάς (πχ τεχνικοί πόροι, υπάλληλοι) καθώς και ο επαγγελματισμός κατά την διεκπεραίωση των εργασιών.
- Ο αριθμός των χρηστών της σκιάς των πληροφοριακών συστημάτων.
- Τα συστατικά που συνιστούν την συγκεκριμένη σκιά πληροφοριακών συστημάτων. Συστατικά μπορεί να είναι το λογισμικό(software) που χρησιμοποιείται και τα υλικά συστήματα(hardware).
- Οι διαδικασίες της σκιάς πληροφοριακών συστημάτων: Βασική στρατηγική, σχεδιασμός, διαδικασίες εργασιών, λειτουργίες, υπηρεσίες και φυσικά διαδικασίες βελτίωσης.

Το τέταρτο κριτήριο είναι η εν δυνάμει καινοτομία. Η εν δυνάμει καινοτομία μπορεί να είναι με την χρήση καινοτόμας τεχνολογίας, μίας νέας διαδικασίας και φυσικά τα οφέλη χρήσης της σκιάς.

Το τελευταίο κριτήριο είναι το κριτήριο του παραλληλισμού, δηλαδή το κατά πόσο χρησιμοποιείται η σκιά πληροφοριακών συστημάτων παράλληλα με ένα υπάρχων επίσημο πληροφοριακό σύστημα. Ειδικότερα εξετάζουμε εάν η σκιά συμπληρώνει το υπάρχων, αν το υποκαθιστά, αν το αντικαθιστά, εάν το παραβλέπει ή εάν το βελτιώνει ως προς τις διαδικασίες τους.

Συμπερασματικά, όπως κάθε επιχειρησιακό κομμάτι έτσι και οι Σκιές Πληροφοριακών πρέπει να αναγνωρίζονται ως προς την ύπαρξη τους εντός της επιχείρησης. Θα πρέπει δηλαδή το Διοικητικό κομμάτι να γνωρίζει τις ανάγκες της, την συνεισφορά της και φυσικά του κινδύνους που εγκυμονεί. Σχέδια περί οργάνωσης και σχέδια κατά των κινδύνων είναι απαραίτητα.

10.6 Διακυβέρνηση Δεδομένων.

Οι επιχειρήσεις χρειάζονται σωστή διαχείριση ποιότητας δεδομένων (Data Quality Management - DQM) η οποία πρέπει να συνδυάζει επιχειρηματικές και τεχνικές οπτικές για να ανταπεξέλθουν στις στρατηγικές και λειτουργικές ανάγκες τις επιχείρησης (Wende, 2007)[55]. Μέχρι πρότινος αυτό το κομμάτι το αναλάμβανε το τμήμα πληροφοριακών συστημάτων. Το πρόβλημα έγκειται στην αγνόηση επιχειρησιακών θεμάτων, με τη χρήση των οποίων όμως θα μπορούσε να επιτευχθεί η καλύτερη διαχείριση της ποιότητας της πληροφορίας. Για μια πιο ολοκληρωμένη διαχείριση ποιότητας της πληροφορίας πρέπει να συνεργαστούν άτομα από διαφορετικά τμήματα. Ιδανικά η ομάδα αυτή θα αποτελείται από άτομα από το επιχειρηματικό τμήμα σε συνεργασία με το τμήμα πληροφοριακών συστημάτων. Η ομάδα αυτή θα αναλάβει γενικότερα την Διακυβέρνηση Δεδομένων και φυσικά την ασφάλεια ποιότητας της.

[55] Wende, K., 2007. *A Model for Data Governance – Organising Accountabilities for Data Quality Management.* s.l.:18th Australasian Conference on Information Systems.

Η αναφορά στη Διακυβέρνηση Δεδομένων σημαίνει ποιοτική διαχείριση δεδομένων. Ειδικότερα αναφερόμαστε στην συλλογή των δεδομένων, την οργάνωση και αποθήκευση τους, στις διαδικασίες με τις οποίες τα επεξεργαζόμαστε για να λάβουμε δεδομένα αποτελέσματα υψηλών προδιαγραφών (Price, 2005)[56].

Από την Οργανωτική σκοπιά πρέπει αν ελέγχουμε την διατήρηση των χορηγιών, να ανταπεξέρχονται στις προσδοκίες και στη συμμόρφωση των κανονισμών, να καθοριστούν οι απαραίτητες ευθύνες και φυσικά την εύρυθμη λειτουργία του τμήματος(καλή συνεργασία τμημάτων).

Το τμήμα πληροφοριακών συστημάτων αναλαμβάνει πιο πρακτικά ζητήματα για τη διαχείριση της πληροφορίας και τις μεθόδους επεξεργασίας τους, αφότου λάβει τις απαραίτητες κατευθυντήριες γραμμές από το επιχειρηματικό τμήμα.

Οργανωτικά, η Εταιρική Διακυβέρνηση δίνει τα ζητούμενα στο τμήμα της Διακυβέρνησης Δεδομένων, το οποίο σε συνεργασία με το τμήμα Πληροφοριακών Συστημάτων παράγουν την ζητούμενη Πληροφορία. Από εκεί αναλαμβάνει το τμήμα Μάνατζμεντ τη χρήση της για Στρατηγικά Ζητήματα, για θέματα Προτύπων και Πολιτικών, για τις Διαδικασίες Διαχείρισης Πληροφορίας, για τη Δομή της Πληροφορίας και της Πληροφόρησης κ.α.

10.7 Σύνοψη.

Συνοπτικά, το τμήμα πληροφοριακών συστημάτων έχει να ασχοληθεί με όλα τα παραπάνω θέματα και ζητήματα και γενικότερα με όλες τις αλλαγές, προσθήκες, ανάγκες και γενικότερα με οτιδήποτε μπορεί να προκύψει. Όλες αυτές οι ενασχολήσεις του τμήματος αυξάνουν καθημερινά την ανάγκη για σωστή διαχείριση του τμήματος, σωστή διαχείριση πόρων, μεγέθυνσης του και ταυτόχρονα επιμερισμό εργασιών σε ομάδες/τμήματα. Απαραίτητη είναι η και η συνεχής εκπαίδευση του προσωπικού και η συνεργασία του με τα υπόλοιπα τμήματα της εταιρίας.

[56] Price, R. &. S. G., 2005. *A semiotic information quality framework: development and comparative analysis.* s.l.:Journal of Information Technology, vol. 2005, no. 20, pp. 88-102.

Εάν υπάρχει, τελικά, μια καθοριστική γραμμή άμυνας για τον χρήστη, αυτή είναι η εξειδικευμένη εκπαίδευση που μπορεί να λάβει για να μάθει να προστατεύει τα προσωπικά του δεδομένα από τρίτους στο διαδίκτυο, να διαβάζει την εκάστοτε πολιτική χρήσης μιας υπηρεσίας και να ξέρει τι ισχύει από τον νόμο, αναφορικά με την προστασία των προσωπικών του δεδομένων και πώς μπορεί να απαιτήσει αποζημίωση σε περίπτωση μη-εγκεκριμένης εγγραφής τους σε αρχείο ή διαρροής των προσωπικών δεδομένων του (Πασσάς Σ., n.d.)[57].

11.1 Κυβερνοεπιθέσεις (Cyber Attacks).

Η ασφάλεια των συστημάτων σε συνδυασμό με την ανάγκη για ασφάλεια των πληροφοριών έχει αναγνωρισθεί ως κρίσιμο ζήτημα σε επίπεδο τόσο εθνικό όσο και σε κάθε επιχείρηση/οργανισμό ξεχωριστά. Επιπροσθέτως έχουμε να αντιμετωπίσουμε τις παραβιάσεις, που συμβαίνουν σχεδόν καθημερινά, στην ασφάλεια πληροφοριών. Με την αύξηση συχνότητας των παραβιάσεων και των επιθέσεων αυξάνεται και η πιθανότητα για μελλοντικές επιθέσεις με επιπτώσεις κατά πολύ σοβαρότερες από αυτές που έχουν ήδη αντιμετωπισθεί.

Η ερώτηση που γεννάται είναι κατά πόσο διαθέτουμε αρκετούς πόρους, τόσο δημόσιους όσο και ιδιωτικούς για την προστασία και την πρόληψη από μελλοντικές επιθέσεις. Η αλήθεια είναι πως η ποσοτικοποίηση κάποιων δεδομένων που καθορίζουν την παραπάνω ερώτηση, είναι δύσκολο να προσδιορισθεί.

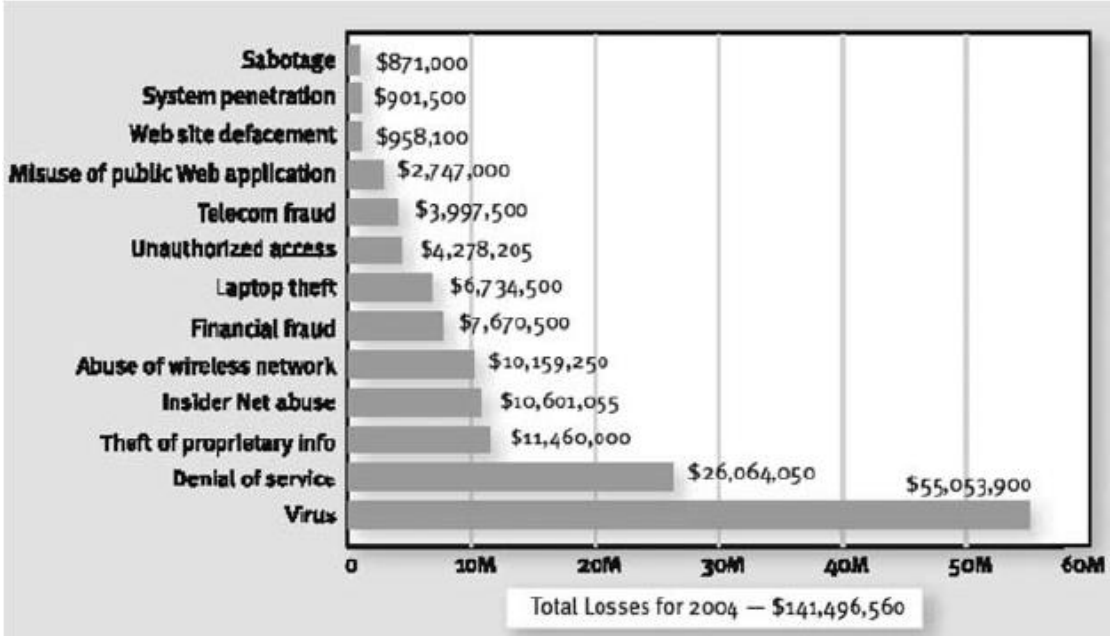
11.2 Προσδιορισμός Οικονομικού Αντίκτυπου των Κυβερνοεπιθέσεων.

Ένα από τα πρώτα πράγματα που επηρεάζονται από μία σοβαρή κυβερνοεπίθεση, είναι η αξία της μετοχής. Τα νέα για την κυβερνοεπίθεση διαδίδονται ολοένα και γρηγορότερα, δημιουργώντας ανησυχητικό κλίμα και κατά

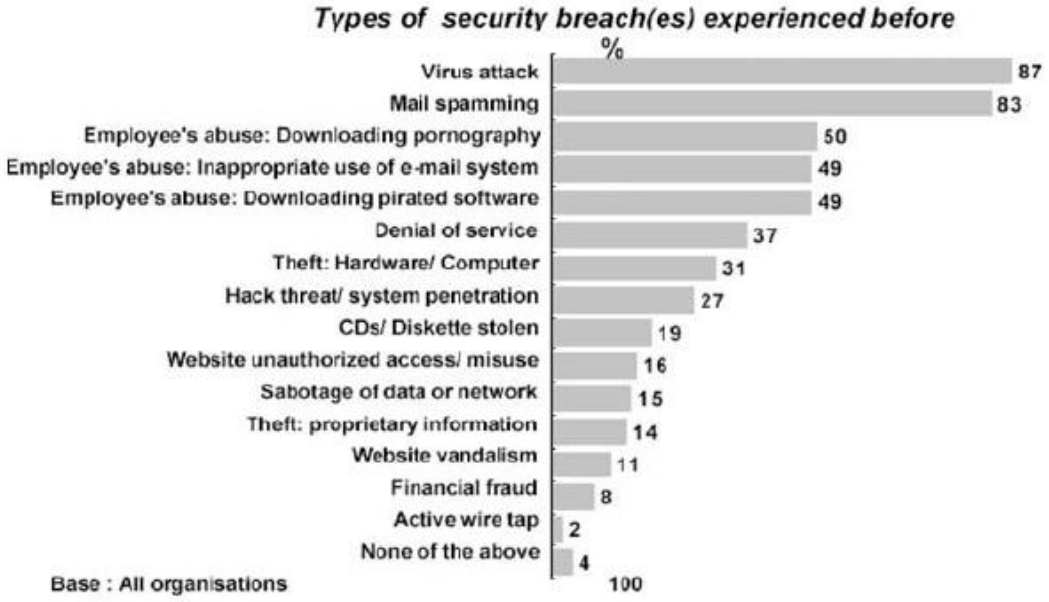
[57] Πασσάς Σ., Ράικος Γ., Ιδιωτικότητα & εμπιστευτικότητα: η σημερινή πραγματικότητα, Netweek - Boussias Communications, 2015

συνέπεια αλλαγή πεποιθήσεων του κοινού(επενδυτές), με αποτέλεσμα στην πτώση της αξίας της μετοχής.

Ποσοστά Απωλειών από Παραβιάσεις CSI/FBI Ινστιτούτο Ασφάλειας Υπολογιστών 2004.



Τύποι Παραβιάσεων που έχουν αντιμετωπισθεί στο παρελθών NISER ISMS 2003



Τα παραπάνω σχεδιαγράμματα δείχνουν την αξία απωλειών από παραβιάσεις και κυβερνοεπιθέσεις και τους τύπους των παραβιάσεων που μπορεί να τις έχουν προκαλέσει. Παρόλα αυτά δεν είναι εύκολο να προσδιορίσουμε το κόστος παραβιάσεων, κυβερνοεπιθέσεων και της απώλειας δεδομένων. Έτσι καθίσταται δύσκολο σε μία επιχείρηση/ οργανισμό να λάβει μία απόφαση ως προς το κόστος και άρα της επένδυσης στα μέτρα που πρέπει να λάβει. Μία μέθοδος που ακολουθείται είναι να χωρίσουμε τα κόστη σε έμμεσα και άμεσα.

Άμεσα κόστη είναι αυτά κατά την επαναφορά του συστήματος μετά από ένα τέτοιο συμβάν. Το άμεσο κόστος περιλαμβάνει υλικά και ώρες εργασίας, καθιστώντας το ευκολότερο στον υπολογισμό του. Βέβαια από λογιστικής άποψης, κόστη όπως αναβαθμίσεις, νέα μέτρα, εκπαιδεύσεις κλπ, μπορούν να δυσκολέψουν τον υπολογισμό του άμεσου κόστους, καθότι δεν είναι εύκολο να αξιολογήσουμε τα ποσά που δόθηκαν λόγω της επίθεσης ή ως μία νέα επένδυση (Brian Cashell, 2004)[58]. Τέλος ένα γεγονός που δυσκολεύει ακόμα περισσότερο την αξιολόγηση του άμεσου κόστους έγκειται στην αξιολόγηση των απωλειών λόγω διακοπής εργασιών κλπ.

Το έμμεσο κόστος είναι το κόστος που προκύπτει αφού έχει αποδοθεί το άμεσο κόστος για την επαναφορά του συστήματος στην αρχική του κατάσταση. Παραδείγματα έμμεσου κόστους είναι οι απώλειες λόγω κακής φήμης της επωνυμίας που δέχθηκε την επίθεση. Ο ανταγωνισμός σίγουρα θα εκμεταλλευτεί την ευκαιρία να αυξήσει το πελατολόγιο του και όπως ήδη αναφέρθηκε η τιμή του χρηματιστηρίου αποκλείεται να μείνει ανεπηρέαστη. Είναι εύκολο να αποφανθεί κανείς πως το έμμεσο κόστος, παρά τις δυσκολίες προσδιορισμού του φέρει μεγαλύτερη σημαντικότητα από το άμεσο.

Ο προσδιορισμός του κόστους είναι χρήσιμος για μελλοντική πρόληψη και μετριασμό των μελλοντικών απωλειών. Σε ότι αφορά την κυβερνοασφάλεια πρέπει να κοιτάμε τις μελλοντικές δραστηριότητες και πιθανότητες για επιθέσεις (Brian Cashell, 2004)[59].

[58] Brian Cashell, W. D. J. M. J. a. B. W., 2004. *The Economic Impact of Cyber-Attacks.* s.l.:s.n.

[59] Brian Cashell, W. D. J. M. J. a. B. W., 2004. *The Economic Impact of Cyber-Attacks.* s.l.:s.n.

11.2.1 Κόστος Κυβερνοασφάλισης.

Σαν κόστος μπορεί να υπολογισθεί και το κόστος της Κυβερνοασφάλισης. Ασφαλιστικές εταιρίες έχουν αναλάβει να ασφαλίζουν οργανισμούς και εταιρίες για τις κυβερνοεπιθέσεις. Το κόστος εξαρτάται από τις παροχές. Π.χ. υπάρχουν πακέτα ασφάλισης εσωτερικών και εξωτερικών απωλειών. Διάφορες περιπτώσεις ασφάλισης αφορούν την ασφάλεια των συστημάτων, περιεχόμενα ιστοσελίδων, διακοπή επιχειρηματικών λειτουργιών κ.α.

11.2.2 Μακροοικονομικό Κόστος.

Ένα εξίσου σημαντικό κόστος είναι το Μακροοικονομικό Κόστος. Μία επίθεση σε μία επιχείρηση μπορεί να την καταστρέψει μακροπρόθεσμα ή να δυσκολέψει την ανάπτυξη της. Μία λύση πάνω σε αυτό είναι ο υπολογισμός Μακροοικονομικού Κόστους. Ο Γενικός κανόνας λέει ότι όσο μικρότερη και πιο κατανοητή είναι μία επίθεση και η διάρκεια της ζωή της εξίσου μικρή, τότε το μακροοικονομικό κόστος θα είναι μικρό. Παρόλα αυτά, κρίσιμο παράγοντα αποτελεί το πόσο γρήγορα μπορεί να ανακάμψει μία εταιρία (Brian Cashell, 2004)[60].

11.3 Σενάρια Αναγνώρισης.

Πάντα σε μία Κυβερνοεπίθεση, τα πρώτα μέτρα που λαμβάνουμε είναι αυτά της πρόληψης. Σε αυτά τα μέτρα θα μπορούσαν να προστεθούν σενάρια αναγνώρισης επιθέσεων. Το βασικό σενάριο είναι η θέσπιση μοτίβων των επιθέσεων για γρηγορότερο εντοπισμό τους και φυσικά την πρόληψη τους.

[60] Brian Cashell, W. D. J. M. J. a. B. W., 2004. *The Economic Impact of Cyber-Attacks.* s.l.:s.n.

Σίγουρα ο αυτοματοποίηση αυτών το διαδικασιών θα ήταν ιδανική αλλά αντιμετωπίζει κάποιες σημαντικές προκλήσεις (Steven Cheung, 2003)[61]:

- Η γνώση για τα σενάρια των επιθέσεων θα πρέπει να συσχετισθούν με μία αντίστοιχη τεχνολογία.
- Λόγω της ανομοιογένειας των ειδοποιήσεων πρώτου επιπέδου, αλλάζει το περιεχόμενο των ειδοποιήσεων.
- Η κατηγοριοποίηση των επιθέσεων του ίδιου σεναρίου, μπορεί να καταχωρηθούν βάση κάποια άλλου κριτηρίου, εκτός της επίθεσης.
- Η ειδοποιήσεις πρώτου επιπέδου μπορεί να είναι αρκετά συχνές και όχι πάντα σωστές.
- Μία επίθεση μπορεί να έχει διάφορες μορφές ανάλογα με τον στόχο του επιτιθέμενου με αποτέλεσμα να μην είναι ξεκάθαρο το σενάριο.
- Υπάρχει πιθανότητα μία επίθεση να έχει στοιχεία από διάφορα σενάρια, αφού οι επιθέσεις δεν συνεπάγονται πάντα ένα συγκεκριμένο στόχο, άρα και η συσχέτιση της με ένα σενάριο δεν είναι εφικτή.

Αρχικά είναι απαραίτητος ο χαρακτηρισμός διάφορων ορισμών:

- Ο ορισμός του *Τρωτού Σημείου*, είναι ο πρώτος χαρακτηρισμός που πρέπει να γίνει ανά περίσταση. Τρωτό σημείο θεωρείται εκείνο το κομμάτι ή διαδικασία του συστήματος που είναι πιθανό να δεχθεί κάποια λειτουργία που παραβιάζει την ασφάλεια και τις πολιτικές των συστημάτων.
- Η έννοια της *Εκμετάλλευσης*, σύμφωνα με την οποία αποτελεί την χρήση ενός Τρωτού Σημείου.
- Το *Βήμα της Επίθεσης,* το οποίο αποτελείται από την εκμετάλλευση ενός τρωτού σημείου και χρήση του για την εκστρατεία της επίθεσης.
- Τέλος η έννοια της *Επίθεσης*, σύμφωνα με την οποία είναι συλλογή των *Βημάτων Επίθεσης.*

Σαν δεύτερο βήμα στην δημιουργία Σεναρίου Αναγνώρισης αποτελείται από 3 κομμάτια (Steven Cheung, 2003)[62] :

[61] Steven Cheung, U. L. M. W. F., 2003. *Modeling Multistep Cyber Attacks for Scenario Recognition.* In Proceedings of the Third DARPA Information Survivability Conference and Exposition (DISCEX III) επιμ. s.l.:s.n.

- Αναγνώριση των λογικών επιθέσεων μέσα στα σενάρια. Σύμφωνα με αυτό το κομμάτι κάθε επίθεση έχει ένα σκοπό. Θα πρέπει να βρεθεί και να καταχωρηθεί στους «αισθητήρες» αναγνώρισης.
- Χαρακτηρισμός Λογικών Βημάτων Επιθέσεων από τη σκοπιά της Αναγνώρισης τους. Αυτό συνεπάγεται έλεγχο και παρατήρηση συγκεκριμένων διαδικασιών, γεγονότων, κατάσταση συστημάτων κ.α.
- Συγκεκριμενοποίηση Σχέσεων Μεταξύ των Επιθέσεων. Μερικά παραδείγματα είναι οι χρονική σχέση (χρόνος μεταξύ των επιθέσεων), σχέσεις αξίας (τι στόχο είχαν οι επιθέσεις) και μία γενικότερη σχέση του αν η μία επίθεση διευκολύνει σε κάποιο κομμάτι κάποια άλλη επίθεση.

Στο τρίτο βήμα πρέπει να δημιουργηθεί μία προγραμματιστική γλώσσα για καλύτερη επικοινωνία των σεναρίων με τους «αισθητήρες» ανίχνευσης. Ειδικότερα αυτή γλώσσα θα πρέπει να έχει τα εξής χαρακτηριστικά (Steven Cheung, 2003)[63]:

- Ένα βασικό χαρακτηριστικό είναι οι *Επεκτάσεις* για καλύτερο χειρισμό των αισθητήρων επίθεσης.
- Θα πρέπει να κατέχει την *Εκφραστική Δυνατότητα* ώστε να καλύπτει το πλήθος τον επιθέσεων που μας ενδιαφέρει.
- Η γλώσσα θα πρέπει να είναι *Ξεκάθαρη* ώστε να μπορεί να υπάρχει άμεση μηχανοποίηση.
- Η γλώσσα καλό θα είναι να μπορεί να διευκολύνει ξεχωρίζοντας τα σημαντικά γεγονότα από τα σχεδόν ασήμαντα.
- Η γλώσσα θα πρέπει να δίνει τη δυνατότητα για αποδοτικότητα των εφαρμογών.

---

[62] Steven Cheung, U. L. M. W. F., 2003. *Modeling Multistep Cyber Attacks for Scenario Recognition.* In Proceedings of the Third DARPA Information Survivability Conference and Exposition (DISCEX III) επιμ. s.l.:s.n.

[63] Steven Cheung, U. L. M. W. F., 2003. *Modeling Multistep Cyber Attacks for Scenario Recognition.* In Proceedings of the Third DARPA Information Survivability Conference and Exposition (DISCEX III) επιμ. s.l.:s.n.

- Τέλος η γλώσσα θα πρέπει να είναι ανεξάρτητη από την χρησιμοποιούμενη τεχνολογία.

Τα σενάρια αναγνώρισης μπορούν σε σημαντικό βαθμό να διευκολύνουν διαδικασίες ασφάλειας, όπως όμως και να συμβάλλουν στην πρόληψη.

11.4 Περίπτωση Επίθεσης – WannaCry Ransomware Attack.

Μία από τις πιο γνωστές κυβερνοεπιθέσεις που συνέβησαν τα τελευταία χρόνια είναι η περίπτωση της WannaCry Ransomware Attack. Η επίθεση ξεκίνησε 12 Μαΐου το 2017 και διήρκησε τρεις ολόκληρες μέρες, έως το 15 Μαΐου. Κατά αυτή την περίπτωση χρήστες του γνωστού λογισμικού συστήματος Microsoft δέχτηκαν ένα αναδυόμενο παράθυρο, το οποίο ενημέρωνε τον χρήστης πως ο υπολογιστής και τα αρχεία του έχουν κρυπτογραφηθεί, περιορίζοντας το χρήστη στο να μην μπορεί να χρησιμοποιήσει τον υπολογιστή. Το παράθυρο έδινε ένα χρονικό διάστημα στο οποίο ο χρήστης μπορούσε να πληρώσει λύτρα (ransom) υπό την μορφή bitcoin(ψηφιακό νόμισμα που χρησιμοποιείται σε διαδικτυακές συναλλαγές). Ενημέρωνε πως εάν δεν τα λύτρα δεν πληρωνόντουσαν μέχρι κάποια συγκεκριμένη ημερομηνία ο χρήστης θα έχανε τα αρχεία του.

Πάνω από 230,000 υπολογιστές δέχθηκαν αυτή την επίθεση σε 150 χώρες. Ένα σημαντικό να σημειωθεί ότι από την επίθεση προσβλήθηκαν φορείς όπως Εθνικό Σύστημα Υγείας του Ηνωμένου Βασιλείου, η Ισπανική εταιρία Τηλεφωνίας Telefonica, FedEx και Deutsche Bahn.

Η λύση βρέθηκε τελικά από τον 22χρονό διαχειριστή κακόβουλου λογισμικού Marcus Hutchins, ο οποίος μείωσε την εξάπλωση κάνοντας εγγραφή ενός ονόματος που βρήκε κατά την ανάλυση του κώδικα της επίθεσης. Στο τέλος με αυτή τη διαδικασία σταμάτησε την οριστικά το αρχικό ξέσπασμα της επίθεσης. Παρόλα αυτά έχουν βρεθεί παρόμοιοι υιοί, παρόμοιας λογικής της αρχικής επίθεσης. Τέλος να σημειωθεί ότι δεν έχει επιτευχθεί η ολοκλήρωση ανάκτησης δεδομένων.

Θεωρητικά η ψηφιοποίηση μας δίνει την δυνατότητα της εύκολης πρόσβασης σε οτιδήποτε είναι ψηφιοποιημένο, ανά πάσα ώρα και στιγμή. Όλα γίνονται εύκολα και γρήγορα με το πάτημα ενός κουμπιού. Η ψηφιοποίηση έχει βελτιώσει την ζωή

των χρηστών των υπολογιστών από πάρα πολλές απόψεις, όμως πάντα υπάρχουν δύο για το ίδιο νόμισμα. Από τη μία πλευρά έχει μειώσει τις πιθανότητες γενικότερων εγκλημάτων, από συνολικής άποψής και έχει διευκολύνει σχεδόν όλες τις διαδικασίες. Από την άλλη πλευρά έχει αυξήσει τις ανάγκες για προστασία προσωπικών και εταιρικών δεδομένων (Savita Mohurle, 2017)[64]. Τέλος η επίθεση WannaCry Ransomware Attack, τονίζει την ανάγκη για τη συχνή δημιουργία αντιγράφων ασφαλείας, καθότι ακόμα δεν έχουν ανακτηθεί όλα τα δεδομένα που χάθηκαν από την επίθεση αυτή (Sahi, 2017)[65].

[64] Savita Mohurle, M. P., 2017. *A brief study of Wannacry Threat: Ransomware Attack 2017.* s.l.:International Journal of Advanced Research in Computer Science.

[65] Sahi, D. S. K., 2017. *A Study of WannaCry Ransomware Attack.* s.l.:International Journal of Engineering Research in Computer Science and Engineering.

Μέρος Δεύτερο.

12.1 Έρευνα και Ερωτηματολόγιο.

Κατά την ανάλυση του θεωρητικού/ ερευνητικού πλαισίου της παρούσας έρευνας, δημιουργούνται μία σειρά από ερωτήματα, τα οποία θα απαντηθούν μέσω ενός συγκεκριμένου ερωτηματολογίου. Τα κύρια ερευνητικά ερωτήματα που θα προσπαθήσει το συγκεκριμένο ερωτηματολόγιο να μελετήσει είναι τα εξής:

- Θα προσπαθήσει να αναλύσει το κατά πόσο οι Ελληνικές επιχειρήσεις λαμβάνουν μέτρα για την ασφάλεια των Πληροφοριακών τους Συστημάτων, καθώς και την επάρκεια τους.
- Την ευαισθητοποίηση των εργαζομένων απέναντι στην ασφάλεια των πληροφοριών των οποίων διαχειρίζονται.
- Θα αναλυθεί επίσης η συμμόρφωση των πληροφοριακών συστημάτων των Εταιριών με τους κανονισμούς, τις Εξωτερικές αρχές και τη Νομοθεσία.
- Τέλος, θα χαρακτηριστεί η ετοιμότητα και το αν έχει γίνει ανάλογη προετοιμασία για τη συμμόρφωση των εταιριών με το Νέο Γενικό Κανονισμό της Ευρωπαϊκής ένωσης περί προστασίας των προσωπικών δεδομένων GDPR.

12.2 Μεθοδολογία Έρευνας.

Ακολουθεί η περιγραφή της μεθοδολογίας που χρησιμοποιήθηκε για την ανάλυση του ερωτηματολογίου που τέθηκε για την συγκεκριμένη έρευνα.

Παρά το γεγονός ότι ένα ερωτηματολόγιο παρέχει πληρέστερη εικόνα για την έρευνα, η αξιοπιστία τους περιορίζεται από το δείγμα στο οποίο έγινε η ανάλυση. Πιο συγκεκριμένα είναι πιθανό άτομα από το δείγμα να προσπάθησαν να αποκρύψουν στοιχεία και γεγονότα ή ακόμα και να μην γνωρίζουν για περιστατικά που συνέβησαν στο εργασιακό τους περιβάλλον.

Η μεθοδολογία χαρακτηρίζεται επίσης από τον τύπο των ερωτήσεων, από το πως θα ερωτηθεί το δείγμα και φυσικά από τον ρυθμό με τον οποίο θα απαντήσουν οι ερωτηθέντες. Για την επιλογή της καλύτερης δυνατής μεθόδου θα πρέπει να ληφθεί υπόψη ο τρόπος επικοινωνίας του ερωτηματολογίου, οι ικανότητες και οι εργασιακές

θέσεις των ερωτηθέντων/ ερευνητών, καθώς και η διαθεσιμότητα των εσωτερικών πόρων και του χρόνου που διατίθενται για την διεξαγωγή της έρευνας. Η βέλτιστη λύση περιλαμβάνει τα εξής:

- Την πρόβλεψη της πιθανής ανταπόκρισης του ερωτηματολογίου.
- Η μεθοδολογία θα πρέπει να είναι η πιο εύκολη.
- Να είναι ανάλογη του χρονοδιαγράμματος της έρευνας.
- Να είναι ανάλογη του προϋπολογισμού.

Βασικές Μέθοδοι:

- Προσωπικές Συνεντεύξεις.
- Τηλεφωνικές Συνεντεύξεις.
- Τηλεομοιοτυπική αποστολή ερωτηματολογίου (συμπληρωμένο προσωπικά).
- Έρευνες μέσω ηλεκτρονικού ταχυδρομείου (συμπληρωμένες από τον καθένα μόνο του).
- Διαδικτυακές (ιστοσελίδα) συνεντεύξεις(συμπληρωμένες από τον καθένα μόνο του)

Στην παρούσα έρευνα το μέσω που χρησιμοποιήθηκε για την επικοινωνία του ερωτηματολογίου είναι το ηλεκτρονικό ταχυδρομείο. Εν συνεχεία αναλύονται τα πλεονεκτήματα και τα μειονεκτήματα της συγκεκριμένης μεθόδου.

Πλεονεκτήματα:

- Γρηγορότερη ολοκλήρωση της διαδικασίας ερωτηματολογίων.
- Χαμηλό Κόστος διεξαγωγής έρευνας.
- Υπάρχει η δυνατότητα επισύναψης πολυμέσων.
- Γρηγορότερη και πιο άμεση ανταπόκριση των ερωτηθέντων.
- Διατήρηση Ανωνυμίας και εμπιστευτικότητας των πληροφοριών που εμπεριέχονται στις απαντήσεις.
- Ευκολότερη ανάλυση απαντήσεων και εφαρμογή στατιστικών μεθοδολογιών στα ερωτηματολόγια.

Μειονεκτήματα:

- Το δείγμα μειώνεται, αφού υπάρχει σημαντικό κομμάτι του πληθυσμού που δεν είναι εξοικειωμένο με τη χρήση ηλεκτρονικών μέσων.
- Οι ερωτήσεις που διέπουν το ερωτηματολόγιο θα πρέπει να είναι απλές και να απαντώνται εύκολα.
- Θα πρέπει να βρεθούν ή να δημιουργηθούν λίστες που να περιέχουν τις ηλεκτρονικές διευθύνσεις.

12.3 Πληθυσμός Ενδιαφέροντος.

Το παρόν ερωτηματολόγιο έχει σαν πληθυσμό ενδιαφέροντός υπαλλήλους που εργάζονται σε Ελληνικές Επιχειρήσεις και πιο συγκεκριμένα άτομα που εργάζονται σε Τμήματα Πληροφοριακών Συστημάτων με ένα ποσοστό 30%, Εσωτερικών Ελεγκτών με ένα ποσοστό 20%, υπαλλήλων που έρχονται σε συχνή επαφή με προσωπικά δεδομένα πελατών και ατόμων με ποσοστό 30%, Οικονομικούς Διευθυντές ή Διευθύνοντες Συμβούλους και Εξωτερικούς Ελεγκτές με ένα ποσοστό 20%. Τέλος το μέγεθος του δείγματος μας είναι 81 (n=81).

12.4 Είδος Δειγματοληψίας.

Για την επιλογή του δείγματος χρησιμοποιήθηκε η δειγματοληψία ευκολίας (Groves, 2009) [66], με την έννοια ότι το συγκεκριμένο ερωτηματολόγιο στάλθηκε σε Οικονομικές Διευθύνσεις, σε Διευθύνσεις Εσωτερικών Ελεγκτών και σε τμήματα Πληροφοριακών Συστημάτων Ελληνικών Επιχειρήσεων, προκειμένου να αποσταλούν στα μέλη τους και να απαντηθούν από αυτά. Ο λόγος των συγκεκριμένων επιλογών είναι ότι λόγω των επαγγελματικών τους αρμοδιοτήτων και υποχρεώσεων έχουν ως βασικές τους ενασχολήσεις την αντιμετώπιση ή/και την πρόληψη ή/και η την ανίχνευση προβλημάτων των Πληροφοριακών τους Συστημάτων και θέματα που αφορούν την Προστασία Πληροφοριών και Δεδομένων. Κατά τη μέθοδο αυτή μπορεί να παραχθεί ένα τυχαίο και αξιόπιστο αντιπροσωπευτικό δείγμα.

[66] Groves, R.M. Floyd, J., Fower, Jr., Couper, M.P., Lepkowski, J.M., Singer, E., & Tourangeau, R. (2009). Survey Methodology. 2nd Edition, Wiley-Blackwell.

12.5 Μέθοδοι Χορήγησης και Όργανο Μέτρησης.

Για την συλλογή των απαραίτητων δεδομένων στην προκείμενη εργασία χρησιμοποιήθηκε ανώνυμο ερωτηματολόγιο το οποίο στάλθηκε μέσω ηλεκτρονικού ταχυδρομείου στα τυχαία δείγματα των εργαζομένων.

Η εισαγωγή του ερωτηματολογίου αποτελείται από επεξηγηματικό σημείωμα, το οποίο παρείχε τις απαραίτητες πληροφορίες σχετικά με την έρευνα. Παρείχε πληροφορίες όπως το σκοπό της διεξαγωγής, τα ερευνητικά ερωτήματα και τους συντονιστές της εργασίας. Εξαιτίας του ευαίσθητου περιεχομένου της έρευνας, έγινε επίσης αναφορά για τη διατήρηση της ανωνυμίας και της εμπιστευτικότητας των απαντήσεων. Αξίζει να σημειωθεί ότι η συμμετοχή δεν ήταν υποχρεωτική.

Η συλλογή των απαντήσεων πραγματοποιήθηκε σε φύλλο Excel, το οποίο εκδόθηκε με τη χρήση της ειδικά διαμορφωμένης πλατφόρμας της Google γνωστή ως Google Drive (drive.google.com).

Τέλος η έρευνα διεξήχθη κατά την περίοδο 10 Δεκεμβρίου έως 17 Δεκεμβρίου του 2017.

12.6 Ερωτηματολόγιο και Δομή.

Οι τύποι των ερωτήσεων που χρησιμοποιήθηκαν στο παρόν ερωτηματολόγιο είναι οι εξής:

- Ερωτήσεις κλειστού τύπου, όπου ο ερωτώμενος έχει να επιλέξει απάντηση μέσα από μία λίστα πιθανών απαντήσεων.
- Ερωτήσεις τύπου Likert οι οποίες κυμαίνονται από πολύ έως καθόλου.

Ειδικότερα οι έξι πρώτες ερωτήσεις αποτελούνται από προσωπικές πληροφορίες των συμμετεχόντων (φύλλο, ηλικία, εκπαίδευση, θέση εργασίας, χρόνος απασχόλησης στη συγκεκριμένη διεύθυνση). Ακολουθούν ερωτήσεις που αφορούν την άποψη και την εξοικείωση του ερωτηθέντος σε σχέση με το Νέο Γενικό Κανονισμό περί Προστασίας Προσωπικών Δεδομένων GDPR. Εν συνεχεία μέσω

ερωτήσεων προσπαθούν να χαρακτηριστούν τα μέτρα για την ασφάλεια των Εταιρικών Πληροφοριών και Δεδομένων. Τέλος, υπάρχουν ειδικότερες ερωτήσεις περί Διαρροής Δεδομένων και Κυβερνοεπιθέσεων.

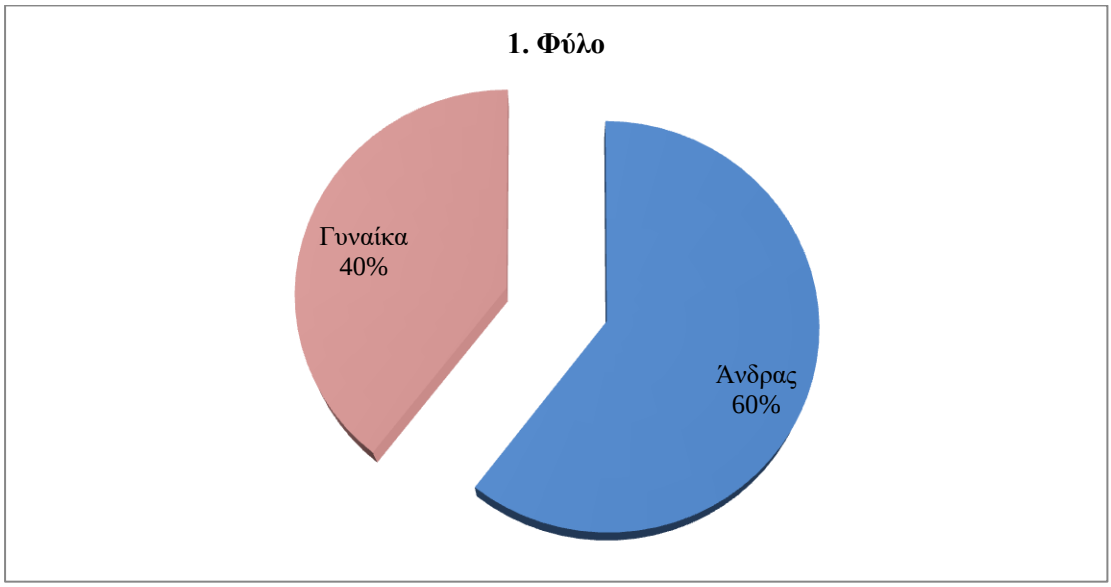
Τέλος πριν την αποστολή του ερωτηματολογίου, έγιναν τεστ από ένα μικρό γκρουπ ατόμων, ώστε να πραγματοποιηθούν οι απαραίτητες διορθώσεις. Έπειτα από τις διορθώσεις που προέκυψαν στην ορολογία, στην κατανόηση, στην σειρά των ερωτήσεων κ.α. το ερωτηματολόγιο στάλθηκε στους ερωτηθέντες.

12.7 Ανάλυση Αποτελεσμάτων Έρευνας/Ερωτηματολογίου.

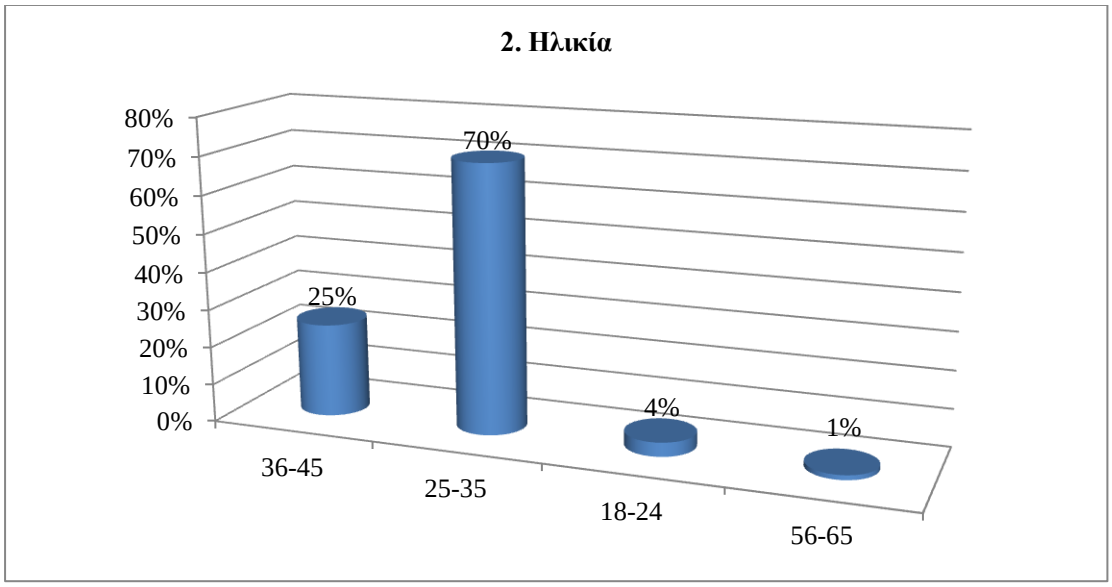
Στο κεφάλαιο αυτό παρουσιάζονται τα αποτελέσματα της εμπειρικής έρευνας που διεξήχθη στα πλαίσια της εν λόγω διπλωματικής εργασίας ,θέλοντας να δοθούν απαντήσεις στα ερευνητικά ερωτήματα που τέθηκαν και να προκύψουν ορισμένα συμπεράσματα. Το βασικότερο πρόγραμμα που χρησιμοποιήθηκε για την αποθήκευση αλλά και την ανάλυση των δεδομένων είναι το Microsoft Excel.

Οι πρώτες έξι ερωτήσεις είναι προσωπικές για να αποτυπωθεί το προφίλ των ερωτηθέντων.

Σχήμα 1, Φύλο

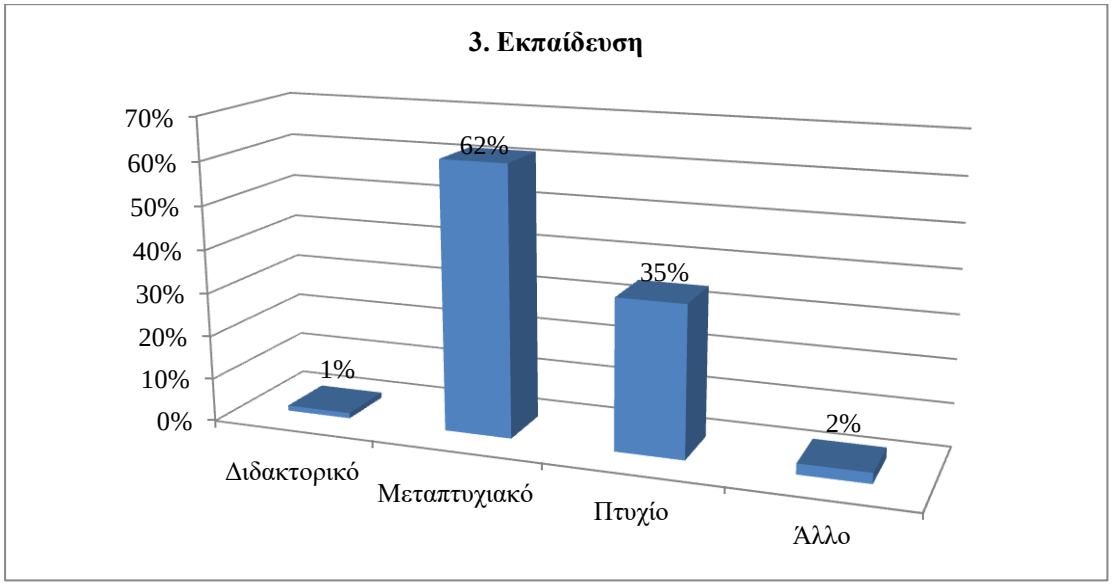


Σχήμα 2, Ηλικία

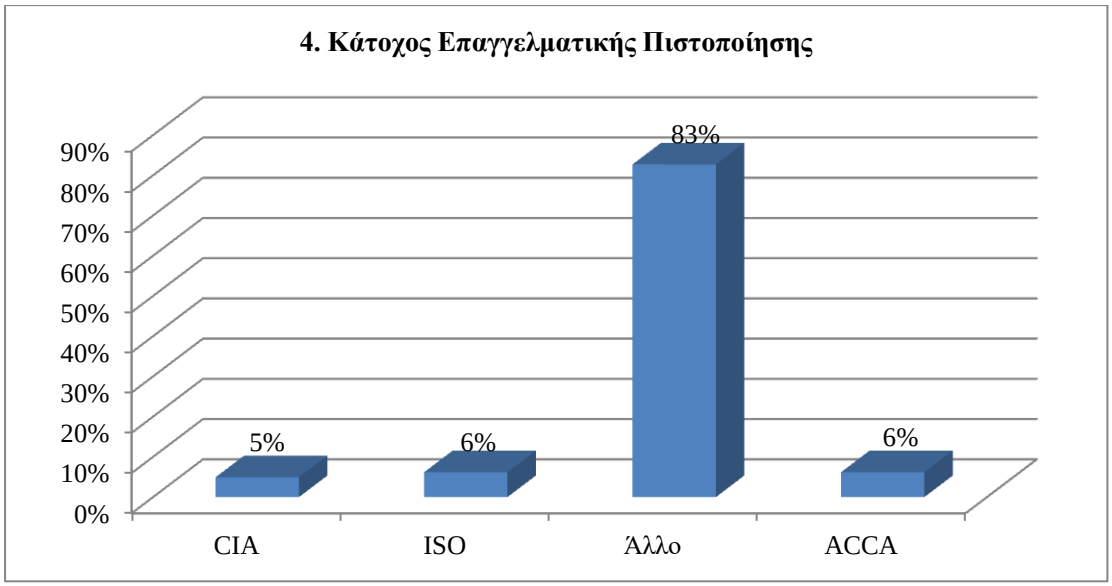


Όπως παρατηρείται από το **σχήμα 1** , έξι στους δέκα ερωτηθέντες είναι άντρες με ποσοστό στην ηλικία τους να κυμαίνεται 25-35 ετών κατά το 70% (**σχήμα 2**).

Σχήμα 3, Εκπαίδευση

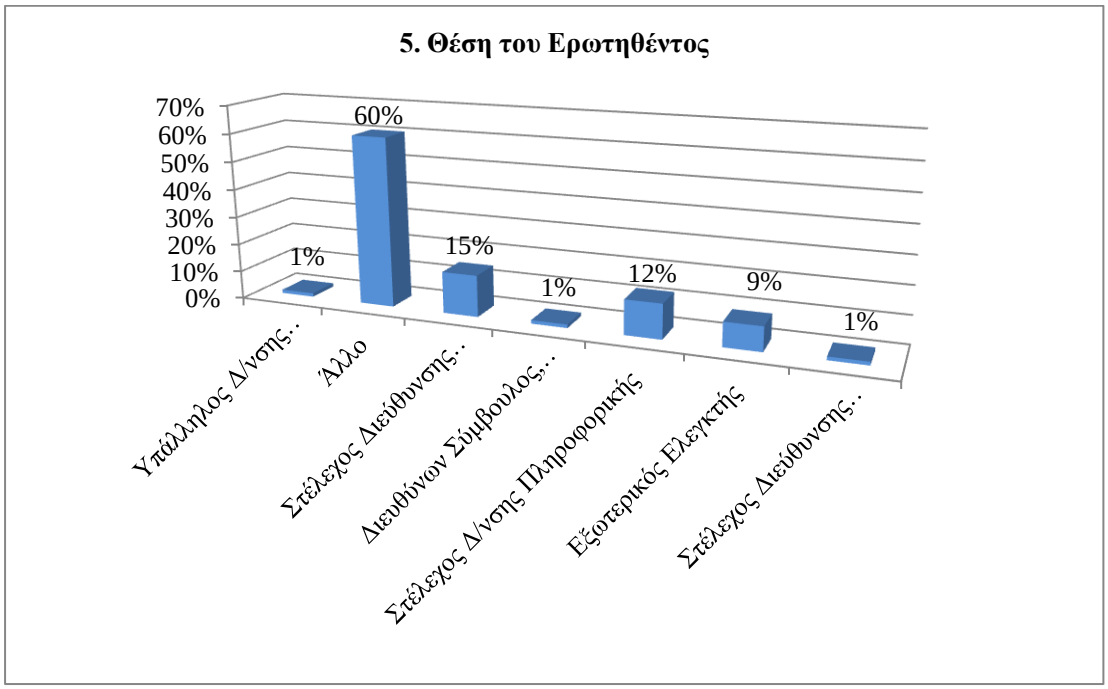


Σχήμα 4, Κάτοχος Επαγγελματικής Πιστοποίησης

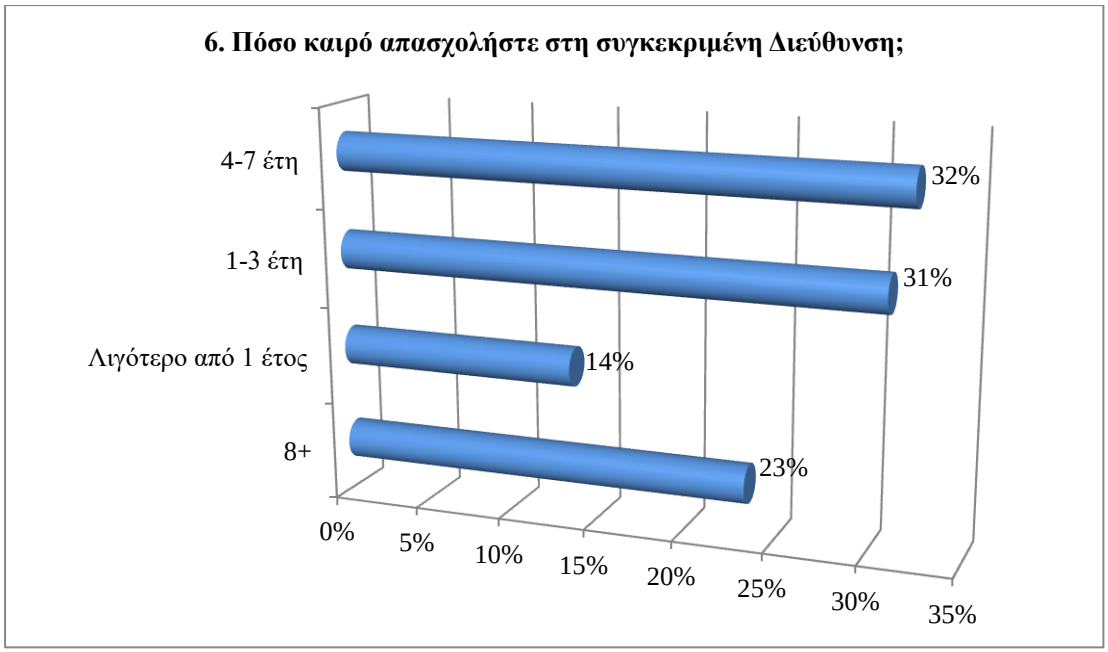


Το 62% του πληθυσμού είναι κάτοχοι μεταπτυχιακού (**σχήμα 3**), ενώ μόλις το 17% έχει αποκτήσεις επαγγελματικές πιστοποιήσεις όπως το CIA, ISO και ACCA (**σχήμα 4**).

Σχήμα 5, Θέση του Ερωτηθέντος

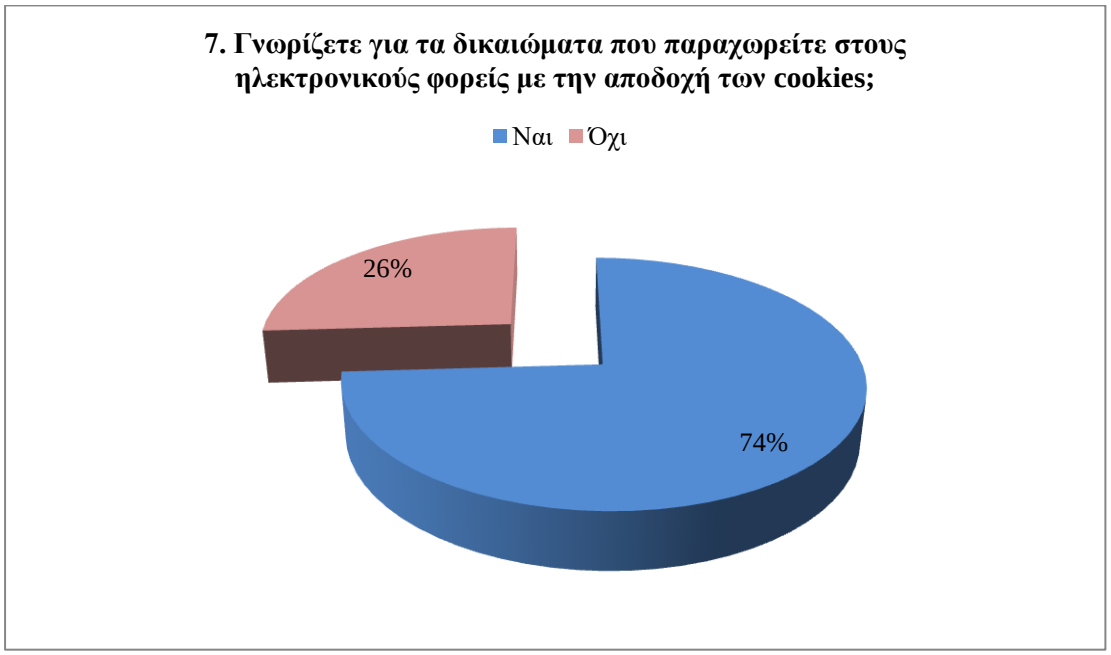


Σχήμα 6, Πόσο καιρό απασχολήστε στη συγκεκριμένη Διεύθυνση;



Οι ερωτηθέντες εργάζονται κατά ποσοστό 60% σε άλλη διεύθυνση από τις αναφερόμενες , ενώ το 15% είναι Στελέχη Εσωτερικού Ελέγχου και με ποσοστό 12% είναι τα Στελέχη Δ/νσης Πληροφορικής (**σχήμα 5**) . Η προϋπηρεσία ανέρχεται σε ποσοστό 32% στα τέσσερα έως επτά έτη που δικαιολογείται λόγω της ηλικίας του δείγματος , καθώς με ποσοστό 31% ακολουθούν τα ένα έως τρία έτη (**σχήμα 6)** .

Σχήμα 7, Γνωρίζετε για τα δικαιώματα που παραχωρείτε στους ηλεκτρονικούς φορείς με την αποδοχή των cookies;

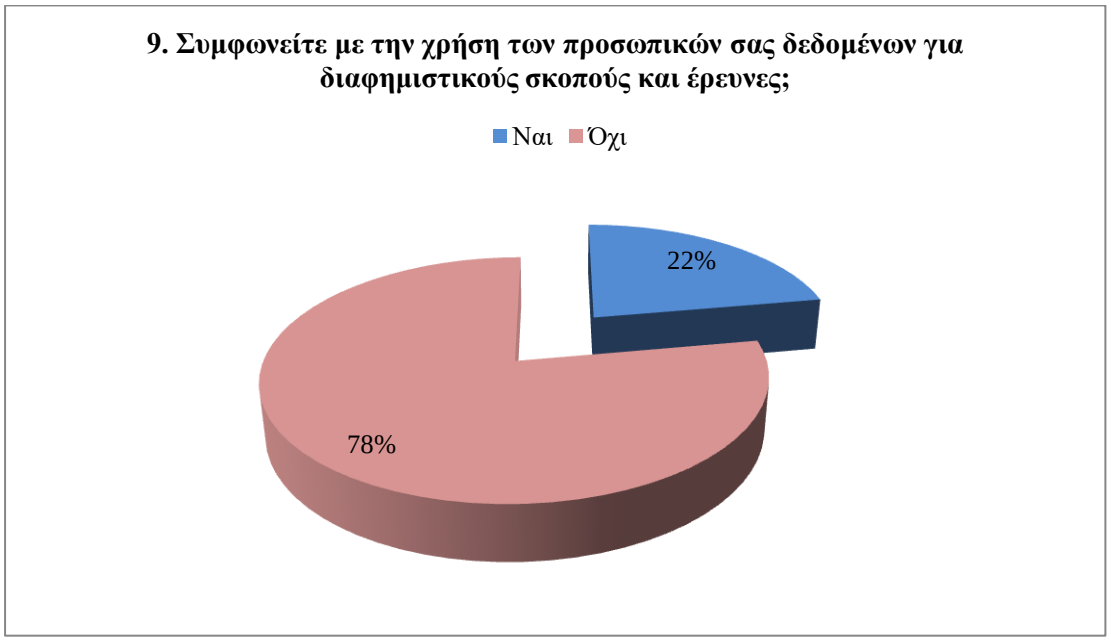


Το 74% της έρευνας γνωρίζει σχετικά με τα δικαιώματα τα οποία παραχωρεί στους ηλεκτρονικούς φορείς κατά την αποδοχή των cookies (**σχήμα 7**). Αποτελεί σημαντικό ποσοστό, διότι σημαίνει ότι έχουν ασχοληθεί με τα προσωπικά τους δεδομένα και ότι έχουν ενημερωθεί για αυτά με κάποιο μέσο. Θα υπάρξουν αλλαγές με το Νέο Κανονισμό και τα δικαιώματα θα βελτιωθούν σημαντικά, προς όφελος του χρήστη των υπηρεσιών. Οι επιλογές και τα δικαιώματα θα αλλάξουν σημαντικά προς όφελος του χρήστη των υπηρεσιών.

Σχήμα 8, Έχετε δεχθεί ηλεκτρονικό διαφημιστικό υλικό βάσει των αναζητήσεων σας στο διαδίκτυο;

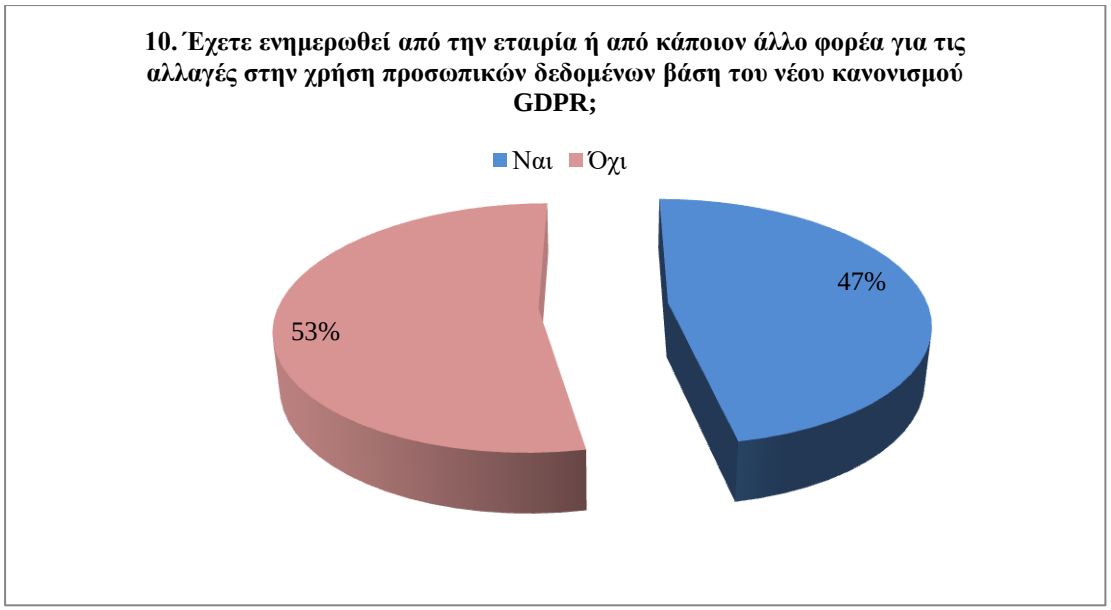
Κατά 96% ο πληθυσμός του δείγματος έχει δεχτεί διαφημιστικό υλικό βάσει αναζητήσεων που έχει πραγματοποιήσει στο διαδίκτυο (**σχήμα 8**). Αυτό το ποσοστό δείχνει ότι όλοι ανά περιόδους δέχονται ανεπιθύμητη ηλεκτρονική αλληλογραφία σε σχέση με τις αναζητήσεις τους. Το άμεσο μάρκετινγκ χρησιμοποιεί τις αναζητήσεις και τα προσωπικά δεδομένα για προώθηση προϊόντων, που σημαίνει ότι όλα τα στοιχεία που κάποιος δέχεται να παραχωρήσει χρησιμοποιούνται άμεσα και προωθούνται στις ανάλογες εταιρίες. Το παραπάνω φαινόμενο θα είναι μέσα σε αυτά που θα επηρεαστούν με τις αλλαγές του GDPR.

Σχήμα 9, Συμφωνείτε με την χρήση των προσωπικών σας δεδομένων για διαφημιστικούς σκοπούς και έρευνες;



Το 78% διαφωνεί όσο αφορά τη χρήση των προσωπικών του δεδομένων για διαφημιστικούς σκοπούς και έρευνες ,ενώ μόλις το 22% συναινεί στη χρήση των προσωπικών τους δεδομένων (**σχήμα 9**). Λόγω των νέων και αυστηρότερων μέτρων που θα ληφθούν μέχρι τις αρχές Μαΐου, θα είναι ξεκάθαρο σε τι γίνεται συναίνεση και τι όχι. Θα υπάρχει το δικαίωμα της άρνησης όπως και το δικαίωμα να διαγραφούν ανά πάσα ώρα και στιγμή τα προσωπικά δεδομένα που έχει κάποια εταιρία. Θα είναι δυνατό να γίνεται έλεγχος στις στατιστικές που προέρχονται από τα στοιχεία που έχουν αντλήσει από τον χρήστη κ.α.

Σχήμα 10 , Έχετε ενημερωθεί από την εταιρία ή από κάποιον άλλο φορέα για τις αλλαγές στην χρήση προσωπικών δεδομένων βάση του νέου κανονισμού GDPR;



Στην ερώτηση εάν οι ερωτηθέντες έχουν ενημερωθεί από την εταιρεία ή από κάποιον άλλο φορέα σχετικά με τις αλλαγές στη χρήση των προσωπικών δεδομένων βάσει του νέου κανονισμού GDPR ένας στους δύο ερωτηθέντες απάντησε πως έχει ενημερωθεί, κάτι το οποίο αποτελεί πολύ μικρό ποσοστό (**σχήμα 10**). Δεδομένης της χρονικής περιόδου στην οποία μιλάμε, δηλαδή μήνες πριν οριστικοποίηση των μέτρων και δεδομένων των προστίμων για την μη συμμόρφωση των εταιριών με τον κανονισμό, είναι εύλογο ότι οι εταιρίες πρέπει να βιαστούν και να λάβουν τα απαραίτητα μέτρα όπως και να ενημερώσουν το προσωπικό τους.

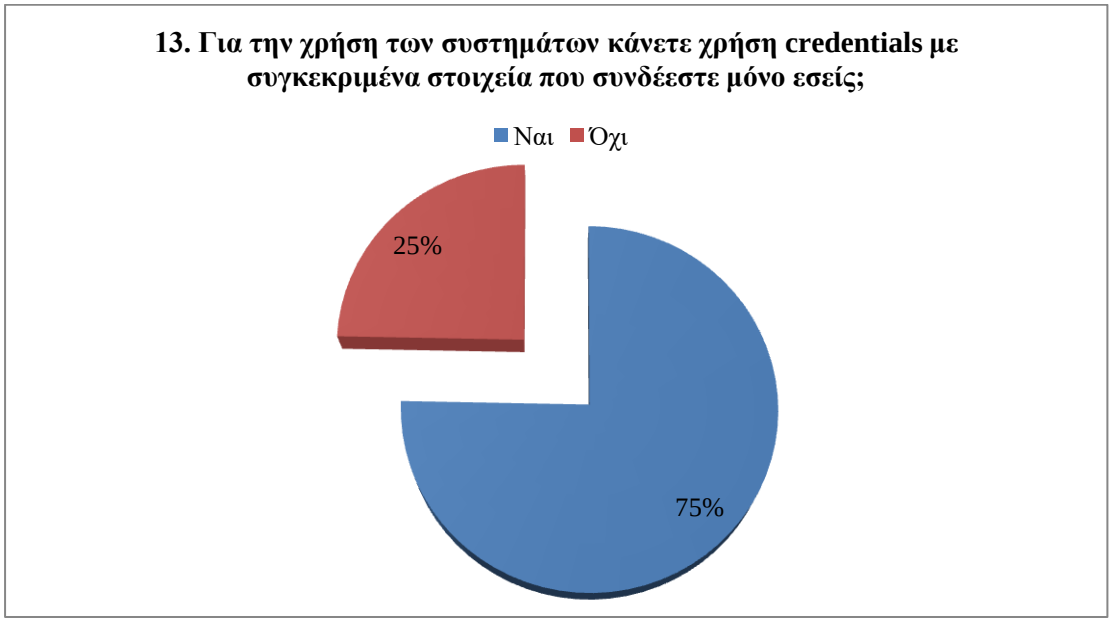
Σχήμα 11, Με τι συχνότητα έρχεστε σε επαφή με προσωπικά δεδομένα πελατών ή άλλων συσχετιζόμενων μελών κατά τη διάρκεια της εργασίας σας;

Το ποσοστό 38% του δείγματος έρχεται καθημερινά σε επαφή με προσωπικά δεδομένα πελατών ή άλλων συσχετιζόμενων μελών στη διάρκεια της εργασίας τους , το 23% συχνά , ενώ μόλις το 6% δεν έχει καθόλου επαφή με προσωπικά δεδομένα είτε πελατών είτε συσχετιζόμενων μελών (**σχήμα 11**). Τα ποσοστά που έρχονται σε επαφή με τα προσωπικά δεδομένα είναι υψηλότερα από αυτά που δεν έρχονται. Σε συνδυασμό με την παραπάνω ερώτηση, γεννάται η παρατήρηση της αναγκαιότητας για εκπαίδευση του προσωπικού. Η αποφυγή των λανθασμένης χρήσης προσωπικών δεδομένων είναι αναγκαία για την επιβίωση των οργανισμών, αφού τα πρόστιμα είναι τόσο υψηλά που θα μπορούσαν να καταστρέψουν τον οργανισμό.

Σχήμα 12, Υπάρχουν σεμινάρια και εκπαιδεύσεις σχετικά με τις αλλαγές είτε των συστημάτων, είτε των πολιτικών της εταιρίας;

Στην ερώτηση εάν πραγματοποιούνται σεμινάρια και ειδικές εκπαιδεύσεις σχετικά με τις αλλαγές των συστημάτων και των πολιτικών της εταιρείας ,μόλις το 57% απάντησε θετικά , γεγονός που αποτυπώνει ότι δεν υπάρχει καλός συντονισμός και ενημέρωση για την εξέλιξη των εργαζομένων (**σχήμα 12**).

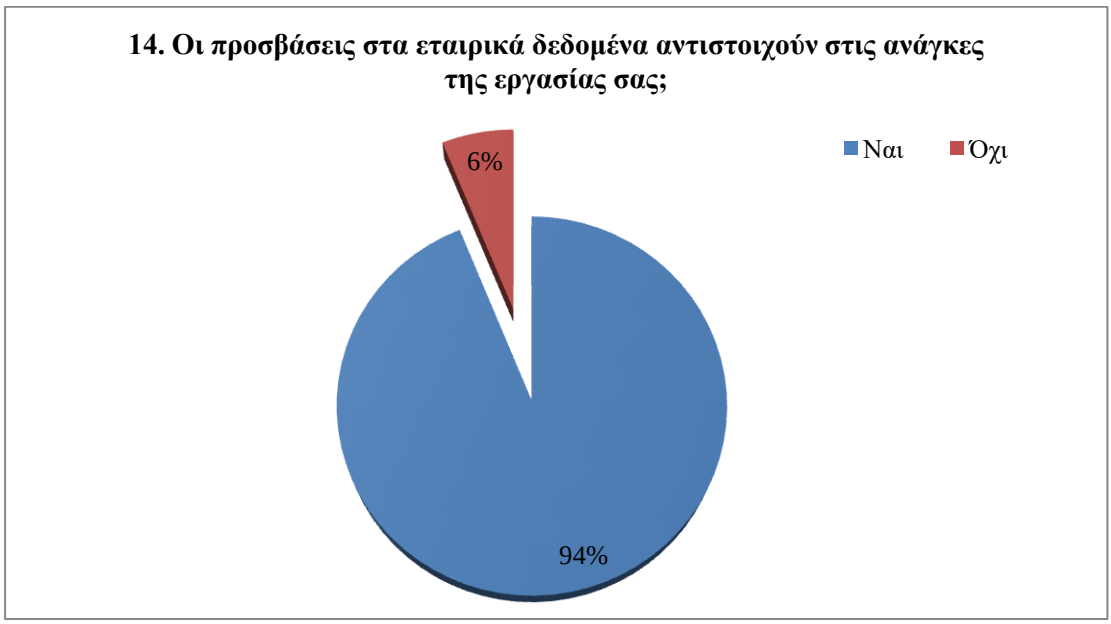
Σχήμα 13, Για την χρήση των συστημάτων κάνετε χρήση credentials με συγκεκριμένα στοιχεία που συνδέεστε μόνο εσείς;



Το 75% των ερωτηθέντων χρησιμοποιεί credentials με συγκεκριμένα στοιχεία για να συνδεθεί , γεγονός που αποδεικνύει την προσπάθεια για ασφαλή δεδομένα (**σχήμα 13**). Απαραίτητο μέτρο ασφάλειας για όλους τους οργανισμούς, διασφαλίζει την ορθή

χρήση και την ασφάλεια των πληροφοριών και των δεδομένων καθώς και την ομαλή διεξαγωγή των εργασιών του οργανισμού.

Σχήμα 14, Οι προσβάσεις στα εταιρικά δεδομένα αντιστοιχούν στις ανάγκες της εργασίας σας;

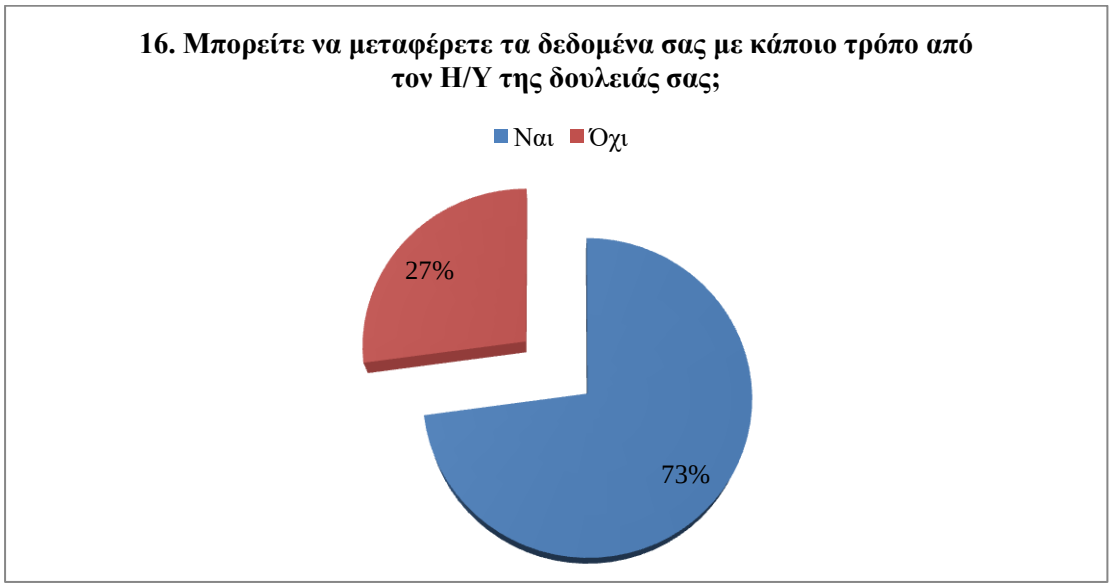


Σχετικά με τις προσβάσεις στα εταιρικά δεδομένα , το 94% του πληθυσμού απάντησε πως αντιστοιχούν στις ανάγκες της εργασίας τους, επομένως υπάρχει ορθός καταμερισμός προσβάσεων στους εργαζόμενους ώστε να έχουν στην κατοχή τους τα απαραίτητα δεδομένα για τη πραγματοποίηση των εργασιών τους (**σχήμα 14**). Οι ερωτήσεις 13 και 14 εξακριβώνουν όχι μόνο ότι έχουν ληφθεί μέτρα για την ασφάλεια των πληροφοριών, αλλά και ότι τα μέτρα αυτά είναι σωστά και ανάλογα των καταστάσεων και εργασιών του χρήστη.

Σχήμα 15, Κάνετε χρήση προσωπικών ηλεκτρονικών συσκευών για τη διεκπεραίωση των εργασιών σας;

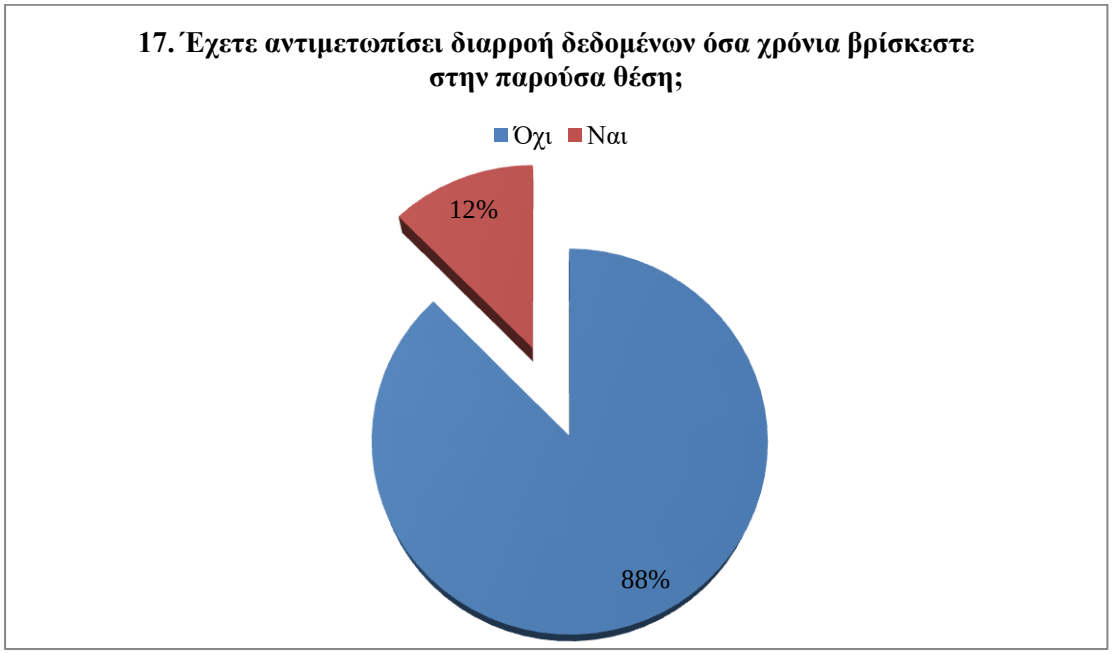
Το 54% των ερωτηθέντων κάνει χρήση προσωπικών του ηλεκτρικών συσκευών για τη διεκπεραίωση των εργασιών του, γεγονός το οποίο αποδεικνύει ότι εύκολα μπορούν να διαρρεύσουν δεδομένα χωρίς κανένα έλεγχο (**σχήμα 15**). Σίγουρα η χρήση προσωπικών συσκευών μπορεί να αυξήσει την παραγωγικότητα, αλλά με αυτό τον τρόπο μπορούν εύκολα να διαρρεύσουν δεδομένα. Εταιρίες που ακολουθούν τέτοιες πρακτικές, θα πρέπει να λάβουν και τα απαραίτητα μέτρα ασφαλείας (βλέπε κεφάλαιο 10.1).

Σχήμα 16, Μπορείτε να μεταφέρετε τα δεδομένα σας με κάποιο τρόπο από τον Η/Υ της δουλειάς σας;



Όμοια με την παραπάνω ερώτηση και με μεγαλύτερο ποσοστό της τάξης του 73% , οι ερωτηθέντες μπορούν να μεταφέρουν δεδομένα από τον υπολογιστή της εργασίας τους. Επομένως συμπεραίνεται ότι τα δεδομένα στα οποία έχουν πρόσβαση οι εργαζόμενοι δεν είναι ασφαλή, αφού εύκολα κάποιος μπορεί να μεταφέρει οποιαδήποτε πληροφορία (**σχήμα 16**). Θα πρέπει να υπάρξουν μέτρα κρυπτογράφησης, καθώς και πρωτόκολλα ηλεκτρονικής υπογραφής ώστε τα δεδομένα και οι πληροφορίες να αφήνουν «σημάδια» όταν χρησιμοποιούνται εκτός εταιρίας.

Σχήμα 17, Έχετε αντιμετωπίσει διαρροή δεδομένων όσα χρόνια βρίσκεστε στην παρούσα θέση;

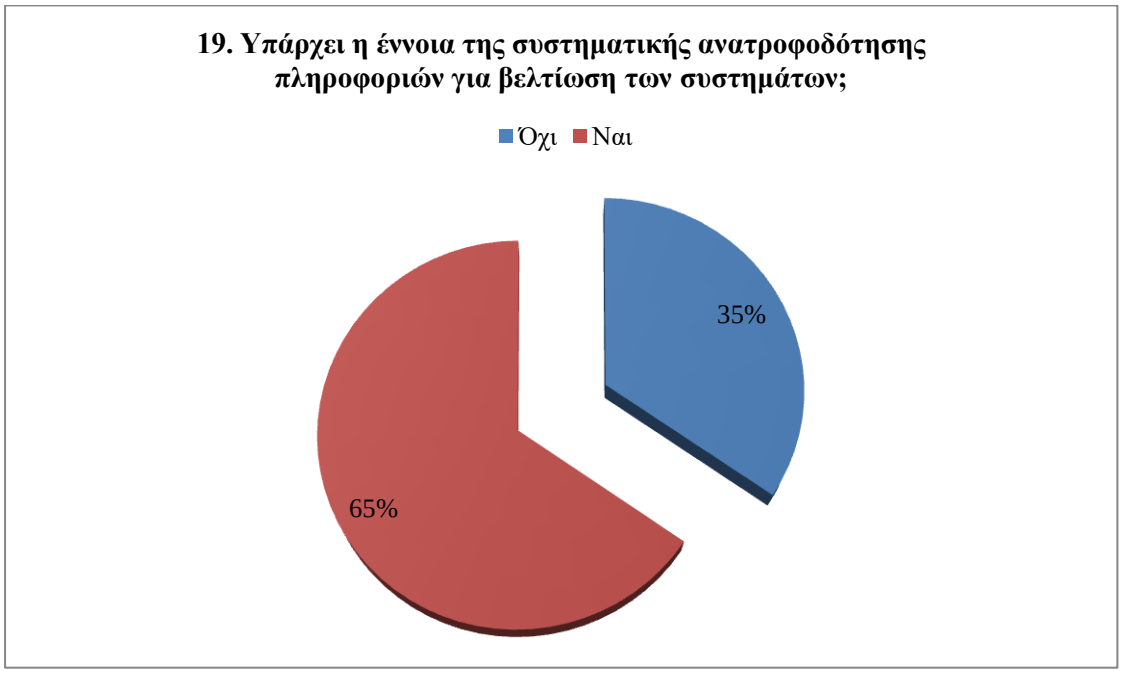


Παρότι μπορούν εύκολα να μεταφερθούν τα δεδομένα , όπως παρατηρείται στις παραπάνω ερωτήσεις , το 88% των ερωτηθέντων απαντά ότι δεν έχει αντιμετωπίσει διαρροή δεδομένων όσα χρόνια βρίσκεται στην παρούσα θέση. Συμπερασματικά θα μπορούσε λοιπόν κάποιος να πει ότι έχει καλλιεργηθεί η επιχειρηματική ηθική στους εργαζόμενους ,γεγονός το οποίο βοηθά στην προστασία των δεδομένων, όπως και τα μέτρα που πιθανώς έχουν ληφθεί είναι επαρκή (**σχήμα 17**).

Σχήμα 18, Ποια από τα παρακάτω μέτρα θεωρείτε αποτελεσματικότερα κατά της διαρροής πληροφοριών;

Σαν μέτρα αντιμετώπισης κατά της διαρροής πληροφοριών το 35% του δείγματος απάντησε ότι θεωρεί την επένδυση σε νέα λογισμικά και συστήματα που να αποτρέπουν τη διαρροή των δεδομένων. Η αμέσως επόμενη απάντηση με 31% είναι η κρυπτογράφηση και με ποσοστό 27% απαντήθηκε η χρήση ειδικών username και password ανά χρήστη και η συχνή αλλαγή των κωδικών. Σίγουρα η επένδυση σε νέα λογισμικά είναι και η πιο δαπανηρή αντιμετώπιση για τις επιχειρήσεις , όμως όπως απαντήθηκε υπάρχουν κι άλλες μέθοδοι αντιμετώπισης όπως η κρυπτογράφηση και η χρήση ειδικών username και password (**σχήμα 18**). Αξίζει να τονισθεί ότι η τεχνολογία και οι εξελίξεις που την διέπουν αποτελούν πλέον καθημερινότητα. Εύλογα δημιουργείται το συμπέρασμα ότι θα πρέπει να ακολουθηθούν αυτές οι εξελίξεις και το πιο πετυχημένο μέσο για το σκοπό αυτό είναι οι επενδύσεις σε νέες τεχνολογίες, συστήματα και λογισμικά.

Σχήμα 19, Υπάρχει η έννοια της συστηματικής ανατροφοδότησης πληροφοριών για βελτίωση των συστημάτων;

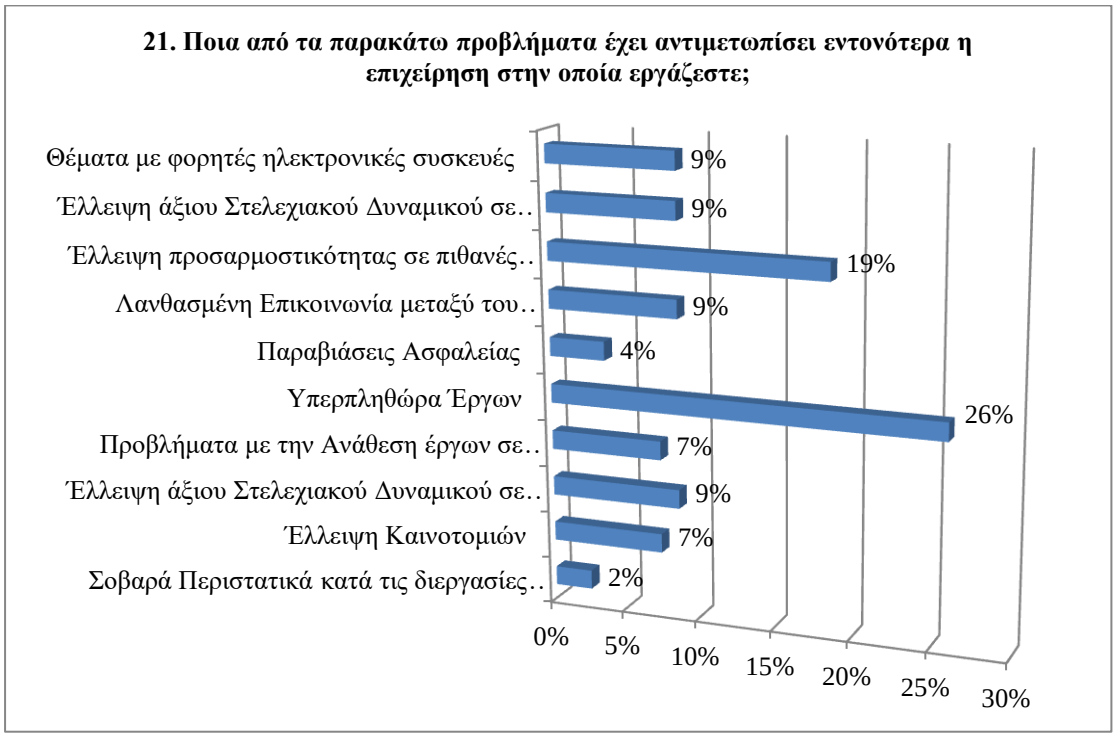


Σύμφωνα με το 65% των ερωτηθέντων υπάρχει η έννοια της συστηματικής ανατροφοδότησης πληροφοριών για τη βελτίωση των συστημάτων (**σχήμα 19**). Είναι σημαντικό εργαλείο η συστηματική ανατροφοδότηση για όλους τους τομείς ενός οργανισμού. Πιο συγκεκριμένα επιταχύνει και βελτιώνει τη συστηματική αναθεώρηση των προγραμμάτων, συστημάτων κ.α. Στο κομμάτι της ασφάλειας βοηθάει η εσωτερική οπτική του χρήστη για την πρόληψη και την βελτίωση των μεθόδων, των εργασιών, των λογισμικών, των συστημάτων κ.α.

Σχήμα 20, Πόσο σημαντική είναι για τα μέλη των επιχειρηματικών στελεχών η έννοια της πληροφορίας και η τεχνολογία ώστε να επιτευχθεί η επιχειρησιακή στρατηγική και το επιχειρηματικό όραμα του Οργανισμού;

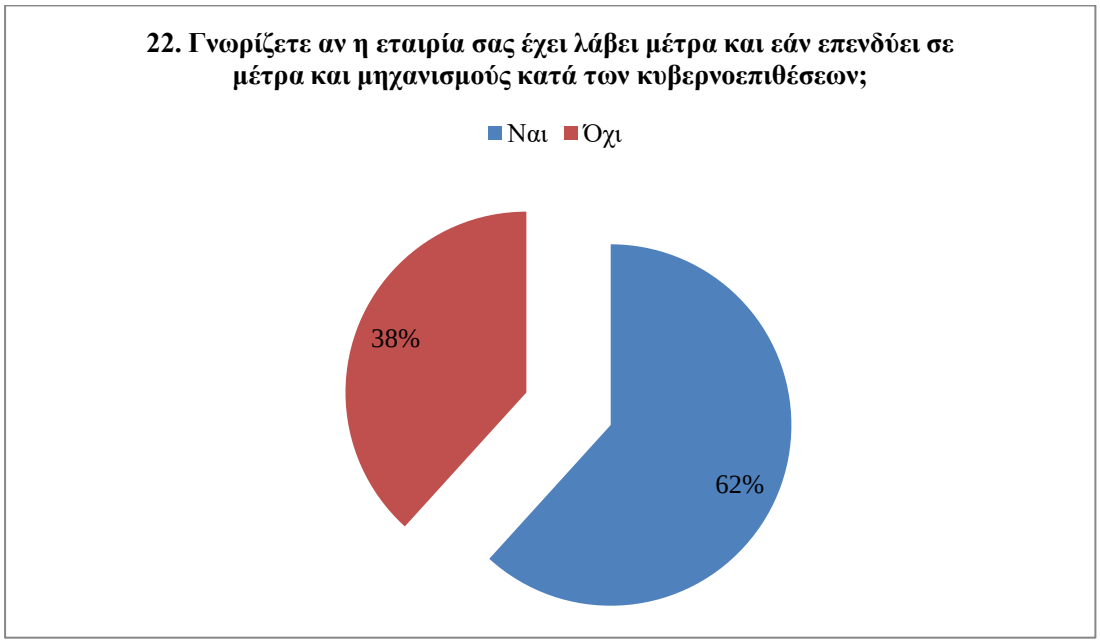
Το 51% των ερωτηθέντων απάντησε ότι τα μέλη των επιχειρηματικών στελεχών θεωρούν πολύ σημαντική την έννοια της πληροφορίας και την τεχνολογία ώστε να επιτευχθεί η επιχειρησιακή στρατηγική καθώς και το όραμα του Οργανισμού (**σχήμα 20**). Είναι θετικό ότι δίνεται η απαραίτητη αξία στην έννοια της πληροφορίας, γιατί αυτό σημαίνει ότι η εταιρία θα προσπαθεί πάντα να την προστατέψει, να την εξασφαλίσει την ορθότητα της και να την διασφαλίσει από απειλές όπως διαρροή κ.α.

Σχήμα 21, Ποια από τα παρακάτω προβλήματα έχει αντιμετωπίσει εντονότερα η επιχείρηση στην οποία εργάζεστε;



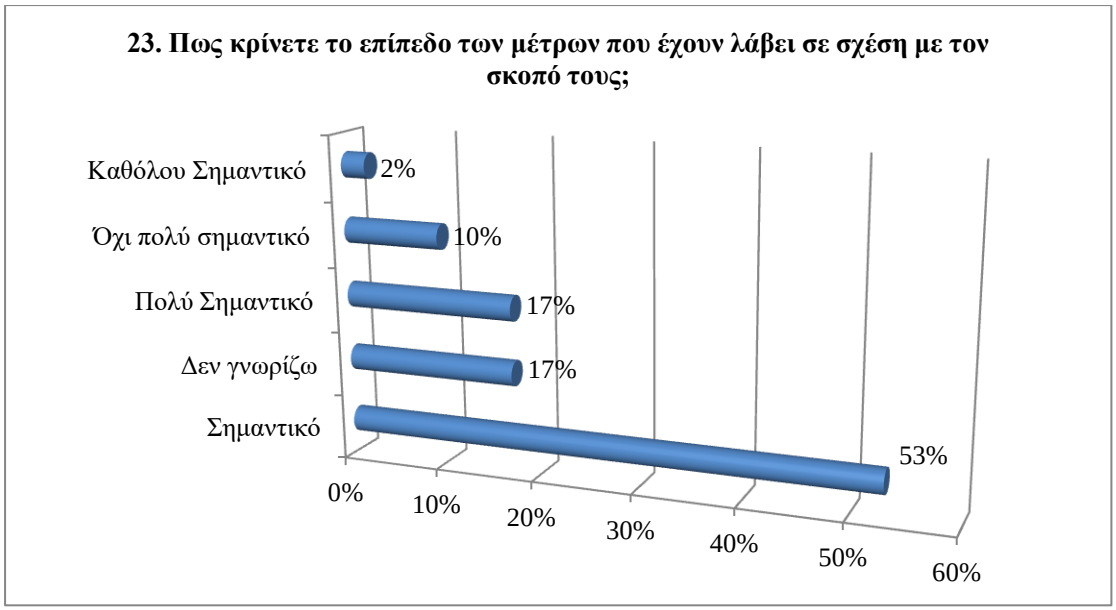
Όσο αφορά το ερώτημα ποια είναι τα προβλήματα τα οποία έχει αντιμετωπίσει εντονότερα η επιχείρηση στην οποία εργάζεστε , οι απαντήσεις είναι διάχυτες με το μεγαλύτερο ποσοστό απαντήσεων στο 26% για την υπερπληθώρα έργων και με 19% την έλλειψη προσαρμοστικότητας σε πιθανές αλλαγές (**σχήμα 21**). Είναι προφανές ότι οι Ελληνικές Επιχειρήσεις προκειμένου να είναι ανταγωνιστικές αναλαμβάνουν πολλά νέα έργα και projects. Δεν υπάρχει όμως πάντα η σωστή οργάνωση και η σωστή κατανομή των πόρων, ώστε να διεκπεραιωθούν όλα τα έργα χωρίς να επιβαρυνθεί κάποιο από το άλλα έργα.

Σχήμα 22 , Γνωρίζετε αν η εταιρία σας έχει λάβει μέτρα και εάν επενδύει σε μέτρα και μηχανισμούς κατά των κυβερνοεπιθέσεων;



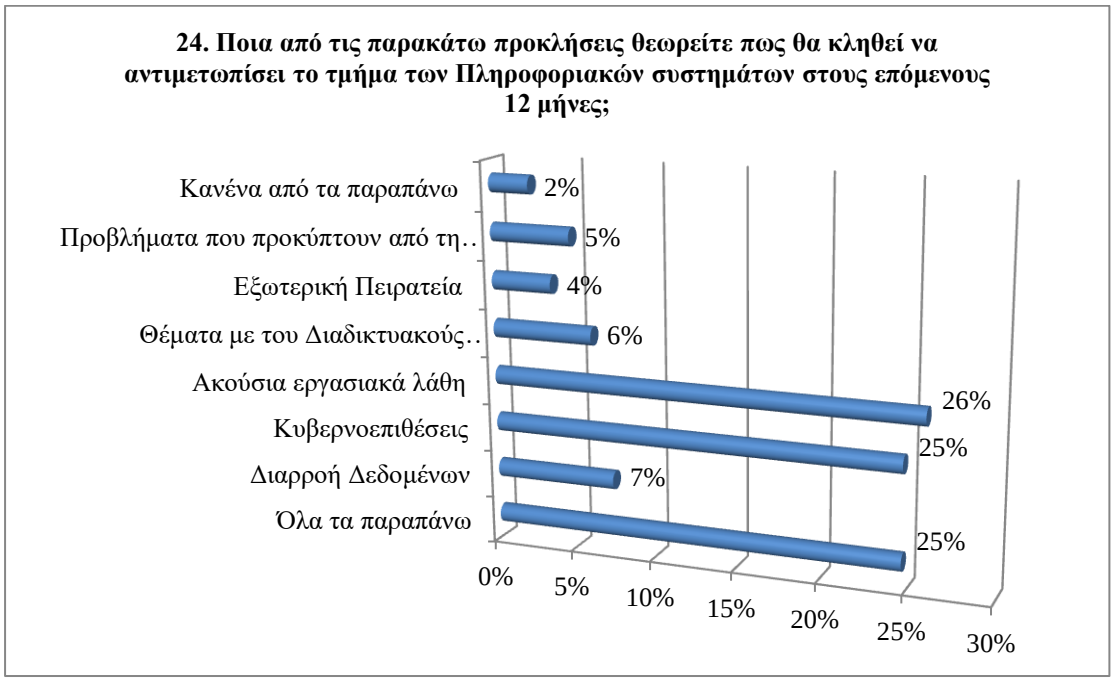
Το 62% των ερωτηθέντων απάντησε πως γνωρίζει εάν η εταιρία που εργάζεται έχει λάβει μέτρα και εάν επενδύει σε μέτρα και μηχανισμούς κατά των κυβερνοεπιθέσεων (**σχήμα 22**). Η παραπάνω ερώτηση αποδεικνύει ότι ένα καλό ποσοστό εταιριών και οργανισμών ενημερώνει τους εργαζομένους του, για τους μηχανισμούς και τα νέα που λαμβάνουν κατά των κυβερνοεπιθέσεων. Ας μην ξεχνάμε την αύξηση του ποσοστού των κυβερνοεπιθέσεων. Η απειλή αυτή μπορεί να προκαλέσει ζημίες στην εταιρία, να επηρεάσει τη θέση της στην αγορά, τη φήμη της, όπως και τις εσωτερικές εργασίες της.

Σχήμα 23, Πως κρίνετε το επίπεδο των μέτρων που έχουν λάβει σε σχέση με τον σκοπό τους;



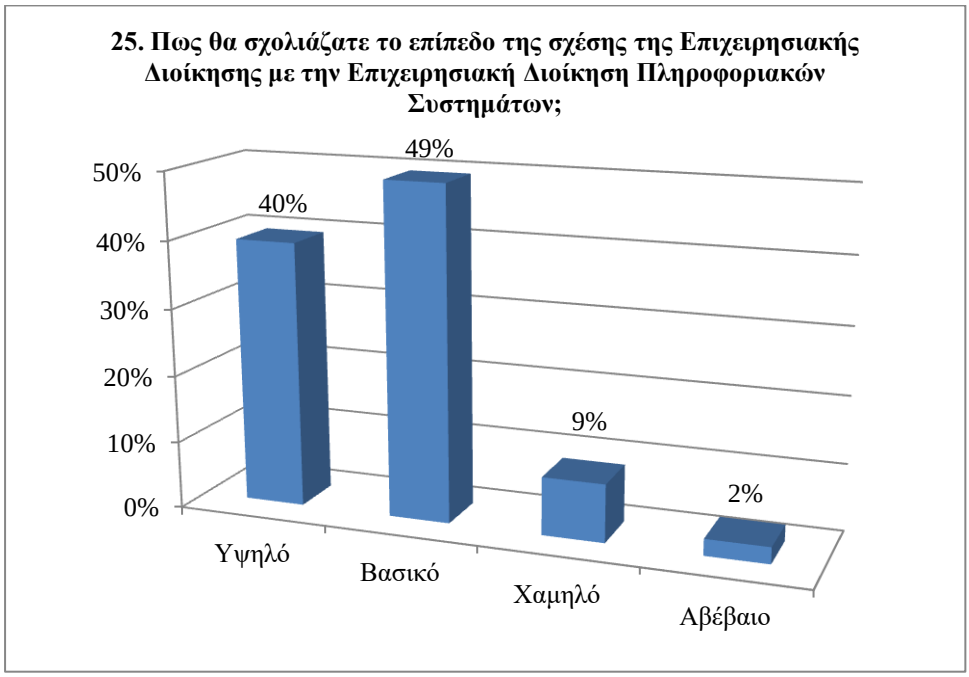
Περίπου 5 στους 10 απάντησαν πως κρίνουν σημαντικό το επίπεδο των μέτρων που έχουν λάβει σε σχέση με το σκοπό τους (**σχήμα 23**). Η ασφάλεια που αισθάνεται ο εργαζόμενος έχει άμεσο αντίκτυπο στην παραγωγικότητα του και εν συνεχεία στην συνολική απόδοση της εταιρίας.

Σχήμα 24, Ποια από τις παρακάτω προκλήσεις θεωρείτε πως θα κληθεί να αντιμετωπίσει το τμήμα των Πληροφοριακών συστημάτων στους επόμενους 12 μήνες;



Τα ακούσια λάθη θεωρεί το 26% του πληθυσμού ότι θα κληθεί να αντιμετωπίσει το τμήμα πληροφοριακών συστημάτων στους επόμενους δώδεκα μήνες σαν πρόκληση, έπειτα με 25% θεωρούνται πιθανές προκλήσεις από κυβερνοεπιθέσεις καθώς και όλα τα αναφερόμενα (**σχήμα 24**).

Σχήμα 25, Πως θα σχολιάζατε το επίπεδο της σχέσης της Επιχειρησιακής Διοίκησης με την Επιχειρησιακή Διοίκηση Πληροφοριακών Συστημάτων;



Βασικό θεωρούν το επίπεδο της σχέσης της επιχειρησιακής διοίκησης με την επιχειρησιακή διοίκηση πληροφοριακών συστημάτων σε ποσοστό 49%, ενώ το 40% θεωρεί υψηλή τη συγκεκριμένη σχέση (**σχήμα 25**).

13.1 Συμπεράσματα και Επίλογος.

Κατά τη διπλωματική εργασία αναπτύχθηκαν θέματα όπως κίνδυνοι και ευπάθειες πληροφοριακών συστημάτων, μέθοδοι για κατηγοριοποίηση και μέτρα κατά των κινδύνων και των ευπαθειών, μέθοδοι ορθής ανάπτυξης πληροφοριακών συστημάτων, αντικειμενικοί στόχοι των πληροφοριακών συστημάτων, θέματα που προέκυψαν με το Νέο Κανονισμός GDPR κ.α.

Στόχος αυτής της διπλωματικής είναι η ανάλυση για την καλύτερη κατανόηση των κινδύνων και των προκλήσεων που καλείται να αντιμετωπίσει το τμήμα πληροφοριακών συστημάτων μίας επιχείρησης, ενός οργανισμού κλπ. Το τμήμα πληροφοριακών συστημάτων ασχολείται με όλα τα κομμάτια ενός οργανισμού και ένα πρόβλημα που μπορεί να προκύψει σε αυτά σίγουρα θα αλληλεπιδράσει και με άλλα κομμάτια του οργανισμού. Στόχος λοιπόν κάθε οργανισμού είναι η προστασία

και η ομαλή λειτουργία των πληροφοριακών συστημάτων και κατά συνέπεια η διασφάλιση λειτουργίας του οργανισμού ως ολότητα.

Εν συνεχεία δημιουργήθηκε ένα ερωτηματολόγιο για να απαντηθούν διάφορα ερωτήματα που γεννήθηκαν κατά την εκπόνηση της διπλωματικής εργασίας. Το ερωτηματολόγιο προσπάθησε να εξακριβώσει την επάρκεια των μέτρων ασφαλείας και την προσαρμοστικότητα των Ελληνικών Εταιριών και Οργανισμών ως προς τις τεχνολογικές εξελίξεις και τις αλλαγές που έχουν προκύψει σε θέματα που αφορούν το Νέο Κανονισμό GDPR. Έγινε επίσης προσπάθεια για την επαλήθευση της αξίας της πληροφορίας και των δεδομένων και πως αυτά διαχειρίζονται από τις Ελληνικές Επιχειρήσεις. Ένα τελευταίο κομμάτι που προσπάθησε να εξακριβώσει το ερωτηματολόγιο είναι θέματα στα οποία ίσως αντιμετωπίζονται δυσκολότερα από άλλα και θέματα που απασχολούν περισσότερο τις διευθύνσεις των Ελληνικών Οργανισμών και Επιχειρήσεων.

Ειδικότερα στο κομμάτι του ερωτηματολογίου τα αποτελέσματα έδειξαν ότι το ενώ το δείγμα μας είναι ενημερωμένο για τα δικαιώματα που παραχωρούν στις διάφορες υπηρεσίες κατά τη χρήση τους, σε επαγγελματικό επίπεδο και δεδομένης της χρονικής περιόδου που μιλάμε, μήνες πριν την έναρξη λειτουργίας του Νέου Κανονισμού περί Προσωπικών Δεδομένων GDPR, ένα σημαντικό ποσοστό εργαζομένων δεν έχει ενημερωθεί για τις αλλαγές αυτές. Αξιοσημείωτο το γεγονός ότι το μεγαλύτερο ποσοστό του δείγματος έρχεται τουλάχιστον σε πολύ συχνή με προσωπικά δεδομένα, μόνο το 47% έχει ενημερωθεί για τις αλλαγές που φέρει το GDPR και γενικότερα μόνο το 57% των εργαζομένων ενημερώνετε σχετικά με αλλαγές είτε συστημάτων, είτε πολιτικών της εταιρίας.

Στη συνέχεια το ερωτηματολόγιο επικεντρώνεται στη Διαρροή Δεδομένων και τις Κυβερνοεπιθέσεις. Αρχικά ενώ παρατηρείται έντονα η δυνατότητα προσωπικών συσκευών για τη διεκπεραίωση εργασιών όπως και η μεταφορά δεδομένων στο σπίτι και οπουδήποτε, διαδικασίες που αυξάνουν την Διαρροή Δεδομένων, τα ποσοστά Διαρροής Δεδομένων είναι σε πολύ χαμηλό επίπεδο. Αυτό μπορεί να οφείλεται είτε από τη δημιουργία ικανών μέτρων για την αποτροπή της διαρροής δεδομένων, είτε από την καλλιέργεια επαγγελματικής ηθικής στους εργαζομένους, είτε και τα δύο παραπάνω φαινόμενα συνδυαστικά που είναι το ιδανικό. Όσον αφορά τις Κυβερνοεπιθέσεις, οι εργαζόμενοι κατά κύριο λόγο είναι ενημερωμένοι για τα μέτρα

και τα θεωρούν και τα μέτρα σημαντικά και αποτελεσματικά. Τέλος, υπάρχει η ανησυχία ότι στους επόμενους 12 μήνες θα παρατηρηθούν προβλήματα από την υπερπληθώρα έργων που έχουν αναλάβει οι εταιρίες και όχι από Κυβερνοεπιθέσεις ή Διαρροή Δεδομένων.

Συμπερασματικά η Διακυβέρνηση Πληροφοριακών Συστημάτων στον Ιδιωτικό Τομέα πρέπει να έχει ένα κομμάτι δημιουργικό ως προς τα συστήματα τους, θέματα ασφαλείας και στα θέματα ενδοεταιρικών κανονισμών. Πρέπει να προσαρμόζονται άμεσα σε όλων των ειδών τις εξελίξεις όπως και να λειτουργούν διαρκώς υπό αμερόληπτο εσωτερικό έλεγχο. Ιδανικό είναι όλα τα παραπάνω να λειτουργούν υπό το πρίσμα των Βέλτιστων Πρακτικών που έχουν δημιουργηθεί από Παγκόσμιους Οργανισμούς.

14.1 Προτάσεις για Περαιτέρω Έρευνα.

Στα πλαίσια της παρούσας Διπλωματική εργασίας έχουν αναπτυχθεί και αναλυθεί κίνδυνοι που αφορούν τα Πληροφοριακά Συστήματα και την Διοίκησή τους. Στο σημείο αυτό γεννάται το ερώτημα για το ποια είναι η σχέση του Εσωτερικού Ελέγχου και των Πληροφοριακών συστημάτων;

Θέματα όπως Ασφάλεια Πληροφοριακών Συστημάτων, Σχέδια Ανάκαμψης και οι Επενδύσεις στα Πληροφοριακά συστήματα απασχολούν ολοένα και περισσότερο τις Διοικήσεις, δημιουργώντας την ανάγκη για πιο δραστικό έλεγχο των κινδύνων των Πληροφοριακών Συστημάτων, με την πρώτη επισήμανση να γίνεται από τον Hermanson το 2003 (Hermanson, 2003)[67].

Σαν συνέχεια αυτή της διπλωματικής θα μπορούσε να γίνει ανάλυση τρόπων και μεθόδων για καλύτερη συνεργασία του Εσωτερικού Ελέγχου με τα Πληροφοριακά συστήματα, δημιουργώντας μία αμφίδρομη σχέση που να είναι επωφελής και για τα δύο τμήματα. Από τη μία ο Εσωτερικός Έλεγχος να δημιουργήσει τα απαραίτητα controls για τις διαδικασίες και την ασφάλεια των Πληροφοριακών Συστημάτων και από την άλλη τα πληροφοριακά συστήματα να

[67] Hermanson, L. B. H. a. D. R., 2003. *Is your audit commitee watching IT risks?*. The Journal of Corporate Accounting & Finance

προσφέρουν μία εσωτερική «οπτική» των διαδικασιών που επιβλέπουν ώστε να ασκηθεί και εκεί εσωτερικός έλεγχος.

Αναφορικά κάποια θέματα που χρειάζονται επίβλεψη από τον εσωτερικό έλεγχο είναι τα εξής:

- Αξιολόγηση επάρκειας μέτρων ασφαλείας των Πληροφοριακών Συστημάτων.
- Οι κίνδυνοι που αναλαμβάνουν τα Πληροφοριακά Συστήματα.
- Η διαβεβαίωση της ασφάλειας των Πληροφοριακών Συστημάτων.
- Η διασφάλιση της συνέχισης των εργασιών των Πληροφοριακών Συστημάτων.
- Η εξασφάλιση της συμμόρφωσης των Πληροφοριακών Συστημάτων με τις «Εξωτερικές» απαιτήσεις, κανονισμούς και Νομοθεσίες.
- Η απόκτηση εξωτερικής διαβεβαίωσης για τις λειτουργίες των Πληροφοριακών Συστημάτων.

Βιβλιογραφία

Aguillera, R., 2005. *Corporate Governance*. s.l.:International Encyclopedia of Economic Sociology.

Aladwani, A. M., 1999. *Implications of some of the recent improvement philosophies for the management of the information systems organization.* s.l.:Industrial Management & Data Systems 99(1-2), 33-39.

Anon., 2006. *ΟικονομικάΧρονικά.*

Armistead C., P. J. &. M. S., 1999. *Strategic business process management for organisational effectiveness.*

Attaran, M., 2004. *Exploring the relationship between information technology and business process reengineering.* s.l.:Information & Management 41(5), 585-596.

Barney, J., 1999. *How a Firm's Capabilities Affect Boundary Decisions,* s.l.: Sloan Management Review.

Bernroider, E. W., 2008. *IT governance for enterprise resource planning supported by the DeLone–McLean model of information systems success.*

Brian Cashell, 2004. *The Economic Impact of Cyber-Attacks.*

Buzacott, J. A., 1996. *Commonalities in reengineered business processes: models and issues.* s.l.:Management Science 42(5), 768-782.

Chreim Samia, "Managerial Frames and Institutional Discourses of Frame: Employee Appropriation Resistance", Organizational Studies, University of Ottawa, Ontario Canada, 2006

Christopher Rentrop, 2012. *Shadow IT Evaluation Model.* s.l.:Proceedings of the Federated Conference on Computer Science and Information Systems pp. 1023–1027.

Drogalas, G., Pantelidis, P., Tsakpinidou, A., Drogalas, G. and Kesisi, E. *(2011) "Internal Audit and Risk Assessment", ESDO 2011*, Greece, Conference Proceedings.

Englund, R. a. B. A., n.d. *Project Sponsorship: Achieving management commitment for project success.* 2006: s.n.

Evans J.R., 2005. *The management and control of quality.* Sixth Edition South Western.

F.Bannister, R., 2016. Defining e-Governance. *INDIANA UNIVERSITY PRESS*, 6, pp. 3-25.

G.Pangalos, 1997. *Security of Medical Database Systems for Health Care IT and Security Personnel.*

Gates Bill, 1999. *Επιχειρηματικές ευκαιρίες στην Ψηφιακή Οικονομία/ Μέσα από την Καλύτερη Χρήση της Τεχνολογίας.* Εκδόσεις Κλειδάριθμος.

Gillan and Starks, L., 1998. *A survey of shareholder activism: motivation and empirical evidence.* s.l.:Contemporary Finance Digest, Vol. 2, No. 3.

Gopan K. Kanji, 1996. *Implementation and pitfalls of TQM.* Total Quality Management.

Groves, R.M. Floyd, J., Fower, Jr., Couper, M.P., Lepkowski, J.M., Singer, E., & Tourangeau, R. (2009). Survey Methodology. 2nd Edition, Wiley-Blackwell

Institute, A. H., 2005. *Survey of Modern Business Science.*

Hermanson, 2003. *Is your audit commitee watching IT risks?.* The Journal of Corporate Accounting & Finance

Jordan, A., 2008. *The Rise of 'New' Policy Instruments in Comparative Perspecive: Has Governance Eclipsed.*

Keith W. Miller, 2012. *BYOD: Security and Privacy Considerations.* s.l.:IEEE Computer Society.

La Porta, 2000. *Agency Problems and Dividend Policies around theWorld.* s.l.:Journal of Finance.

Laudon Kenneth G., Laudon Jane P., 2002. *Συστήματα Πληροφοριών Διοίκησης, MIS: Οργάνωση και Διοίκηση στην Δικτυωμένη επιχείρηση.* Εκδόσεις Κλειδάριθμος.

Li Liu, 2010. *Sponsorship and IT vendor management of projects.* s.l.:Journal of Information Technology.

Marler H. Janet ,2006. *Trainning and effective employee information technology use.* Journal of Management.

Melone, 1990. *Theoretical Assessment of the User-Satisfaction Construct in Information Systems Reshearch :* Management Science.

Miranda, 2005. *Moments of Governance in IS Outsourcing: Conceptualizing effects of contracts on value capture and creation.* s.l.:Journal of Information Technology 20(3): 152–169..

Monks, R., 2002. *Creating value through corporate governance.* s.l.: Corporate Governance: An international review.

Nath, 1997. *The role of information technology in business process reengineering..* s.l.:International Journal of Production Economics 50(2-3), 91-104.

Noe Hollenbeck, Gerhert Wright, 2003. *Human Resource Management: Gaining Competitive Advantage.*

OECD, 1999. *OECD Principles of Corporate Governance.*

Osborne, 1992. *Reinventing government : How the entrepreneurial spirit is transforming the public sector.*

Palvia, S. a. S. S., 2007. *E-Government and E-Governance: Definitions/Domain Framework and Status.*

Passas S., Adaptability in the era of digital transformation - The privacy perspective, Money Show Conference, 2018

Pavlou PA, El Sawy OA, 2006. *From IT Leveraging competence to competitive advantage in turbulent environment: the case of new product development.* Information Technology Research.

Peeka, Oikonomou Victoria, Lykogianni Vasiliki. *The Human Factor as a source of competitive advancement in the new Globalization Market.* University of Peiraious, Panteion University.

Pfleeger, C., 1997. *Security Computing, Prentice Hall International.* s.l.:ISBN.

Pinto, J., 2000. *Understanding the Role of Politics in Successful Project Management.* s.l.:International Journal of Project Management 18(2):85–91..

Prashant Bordia, 2006. *Differences in sharing knowledge impersonally and via Databases: The Role of evaluation apprehension and received benefits.* European Journal of Work and Organizational Psychology.

Price, R. &. S. G., 2005. *A semiotic information quality framework: development and comparative analysis.* s.l.:Journal of Information Technology, vol. 2005, no. 20, pp. 88-102.

Rhodes, 1997. *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability.*

Ross, J. a. W. P., 2002. *Six Decisions your IT People Shouldn't Make.* s.l.:Harvard Business Review 80(11): 85–91.

Sahi, D. S. K., 2017. *A Study of WannaCry Ransomware Attack.* s.l.:International Journal of Engineering Research in Computer Science and Engineering.

Savita Mohurle, M. P., 2017. *A brief study of Wannacry Threat: Ransomware Attack 2017.* s.l.:International Journal of Advanced Research in Computer Science.

Sean Carlin, K. C., 2011. *Cloud Computing Security.* s.l.:International Journal of Ambient Computing and Intelligence, 3(1), 14-19.

Shleifer, A. a. V. R. W., 1989. *Management entrenchment: The case of manager specific investments.* s.l.: Journal of Financial Economics.

Steve, E., n.d. *An Introduction to Information System Risk Management.*

Steven Cheung, U. L. M. W. F., 2003. *Modeling Multistep Cyber Attacks for Scenario Recognition.* In Proceedings of the Third DARPA Information Survivability Conference and Exposition (DISCEX III) επιμ.

Tricker, R. (., 1984. *Corporate Governance.* s.l.:Gower Publishing Company.

Wende, K., 2007. *A Model for Data Governance – Organising Accountabilities for Data Quality Management.* s.l.:18th Australasian Conference on Information Systems.

Winkle, C. a., 1976. *Auditing Philosophy and Technique.*

Ανικούλα Ε., Χαράμης Γ., 2001. *Διοικητική Της Αναπτύξεως Πληροφοριακών Συστημάτων.*

Ιωάννης, Φίλος, 2004. *Σύστημα Εσωτερικού Ελέγχου Επιχειρήσεων.*

Κάτσικας, Σ. Π., n.d. *Ανάλυση, Αποτίμηση και Διαχείρηση Επικινδυνότητας Πληροφοριακών Συστημάτων*.

Πασσάς Σ., Ράικος Γ., Ιδιωτικότητα & εμπιστευτικότητα: η σημερινή πραγματικότητα, Netweek - Boussias Communications, 2015

Χαράμης, Γ., 2001. *Διοικητική Ανάπτυξη Πληροφοριακών Συστημάτων.* s.l.:Ανίκουλα ISBN.

Χυτήρης Λεωνίδας, 2001. *Οργανωσιακή Συμπεριφορά: Η ανθρώπινη συμπεριφορά σε οργανισμούς και επιχειρήσεις.* Εκδοτικός Οίκος Interbooks.

www.oecd.org ,2004. OECD Information and Technology Outlook.

www.datalossdb.org.

Παράρτημα.

Ερωτηματολόγιο

Πάντειο Πανεπιστήμιο: Ερωτηματολόγιο για τη Διπλωματική με Θέμα "Ηλεκτρονική Διακυβέρνηση στον Ιδιωτικό Τομέα".

ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Εμπιστευτικό Ερωτηματολόγιο έρευνας στα πλαίσια εκπόνησης Διπλωματικής εργασίας με θέμα "Ηλεκτρονική Διακυβέρνηση στον Ιδιωτικό Τομέα".

Αξιότιμοι/ες Κύριοι/Κυρίες

Το παρόν ερωτηματολόγιο αποστέλλεται στο πλαίσιο Διπλωματικής Εργασίας για το Μεταπτυχιακό Φορολογία και Ελεγκτική, που εκπονείται στο Τμήμα Δημόσιας Διοίκησης του Παντείου Πανεπιστημίου Κοινωνικών και Πολιτικών Επιστημών. Η συμπλήρωση των ερωτημάτων θα βοηθήσει στην επιτυχία της έρευνας της παρούσας Διπλωματικής Εργασίας. Με την εξέλιξη των συστημάτων τεχνολογίας σε συνδυασμό με το πόσο απαραίτητα είναι τα Πληροφοριακά Συστήματα για τις λειτουργίες ενός Οργανισμού, έχουν παρατηρηθεί εγκληματικές ενέργειες με στόχο αυτά τα συστήματα. Αυτές είναι γνωστές και ως Κυβερνοεπιθέσεις, με στόχο την καταστροφή ή την απόσπαση πληροφοριών. Πολύ συχνό είναι και το φαινόμενο της Διαρροής Πληροφοριών, κατά το οποίο Εμπιστευτικές Πληροφορίες χάνονται ή αποσπώνται με διάφορες μεθόδους και μέσα. Τέλος, έχουν δημιουργηθεί για ανάγκες τροποποίησης και αλλαγών των Πληροφοριακών Συστημάτων για τη συμμόρφωση με τον νέο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR).

Παρακαλώ στην απάντηση των ερωτηματολογίων μέχρι τις 17/12/2017. Ευχαριστώ για την Κατανόηση σας.

Η συμπλήρωση του ερωτηματολογίου θα σας πάρει λίγα μόλις λεπτά. Είναι ανώνυμο και οι απαντήσεις σας είναι αυστηρώς εμπιστευτικές.

* Απαιτείται

1. Φύλο *

Άνδρας

Γυναίκα

2. Ηλικία *

18-24

25-35

36-45

46-55

56-65

66+

3. Εκπαίδευση *

Διδακτορικό

Μεταπτυχιακό

Πτυχίο

Άλλο

4. Κάτοχος Επαγγελματικής Πιστοποίησης *

CIA

ACCA

CFSA

CSA

ACF

CISM

CISSP

CIPP

ISO

Άλλο

5. Θέση του Ερωτηθέντος *

Διευθύνων Σύμβουλος, Οικονομικός Διευθυντής

Στέλεχος Διεύθυνσης Κανονιστικής Συμμόρφωσης (compliance officer)

Στέλεχος Διεύθυνσης Εσωτερικού Ελέγχου (internal auditor)

Στέλεχος Διεύθυνσης κατά της απάτης (fraud analyst)

Εξωτερικός Ελεγκτής

Στέλεχος Δ/νσης Πληροφορικής

Άλλο

6. Πόσο καιρό απασχολήστε στη συγκεκριμένη Διεύθυνση; *

Λιγότερο από 1 έτος

1-3 έτη

4-7 έτη

8+

7. Γνωρίζετε για τα δικαιώματα που παραχωρείτε στους ηλεκτρονικούς φορείς με την αποδοχή των cookies; *

Ναι

Όχι

8. Έχετε δεχθεί ηλεκτρονικό διαφημιστικό υλικό βάσει των αναζητήσεων σας στο διαδίκτυο; *

Ναι

Όχι

9. Συμφωνείτε με την χρήση των προσωπικών σας δεδομένων για διαφημιστικούς σκοπούς και έρευνες; *

Ναι

Όχι

10. Έχετε ενημερωθεί από την εταιρία ή από κάποιον άλλο φορέα για τις αλλαγές στην χρήση προσωπικών δεδομένων βάση του νέου κανονισμού GDPR; *

Ναι

Όχι

11. Με τι συχνότητα έρχεστε σε επαφή με προσωπικά δεδομένα πελατών ή άλλων συσχετιζόμενων μελών κατά τη διάρκεια της εργασίας σας; *

Καθημερινά

Συχνά

Σπάνια

Καθόλου

12. Υπάρχουν σεμινάρια και εκπαιδεύσεις σχετικά με τις αλλαγές είτε των συστημάτων, είτε των πολιτικών της εταιρίας; *

Ναι

Όχι

13. Για την χρήση των συστημάτων κάνετε χρήση credentials με συγκεκριμένα στοιχεία που συνδέεστε μόνο εσείς; *

Ναι

Όχι

14. Οι προσβάσεις στα εταιρικά δεδομένα αντιστοιχούν στις ανάγκες της εργασίας σας; *

Ναι

Όχι

15. Κάνετε χρήση προσωπικών ηλεκτρονικών συσκευών για την διεκπεραίωση των εργασιών σας; *

Ναι

Όχι

16. Μπορείτε να μεταφέρετε τα δεδομένα σας με κάποιο τρόπο από τον Η/Υ της δουλειάς σας; *

Ναι

Όχι

17. Έχετε αντιμετωπίσει διαρροή δεδομένων όσα χρόνια βρίσκεστε στην παρούσα θέση; *

Ναι

Όχι

18. Ποια από τα παρακάτω μέτρα θεωρείτε αποτελεσματικότερα κατά της διαρροής πληροφοριών; *

Χρήση ειδικών username και password ανά χρήστη και συχνή αλλαγή κωδικών

Επένδυση σε νέα λογισμικά και συστήματα που αποτρέπουν τη διαρροή δεδομένων

Χρήση συσκευών που ανήκουν μόνο στην εταιρία.

Κρυπτογράφηση

19. Υπάρχει η έννοια της συστηματικής ανατροφοδότησης πληροφοριών για βελτίωση των συστημάτων; *

Ναι

Όχι

20. Πόσο σημαντική είναι για τα μέλη των επιχειρηματικών στελεχών η έννοια της πληροφορίας και η τεχνολογία ώστε να επιτευχθεί η επιχειρησιακή στρατηγική και το επιχειρηματικό όραμα του Οργανισμού; *

Καθόλου Σημαντική

Όχι πολύ σημαντική

Σημαντική

Πολύ Σημαντική

Δεν γνωρίζω

21. Ποια από τα παρακάτω προβλήματα έχει αντιμετωπίσει εντονότερα η επιχείρηση στην οποία εργάζεστε; *

Επενδύσεις

Υπερπληθώρα Έργων

Παραβιάσεις Ασφαλείας

Λανθασμένη Επικοινωνία μεταξύ του τμήματος Πληροφοριακών Συστημάτων σε σχέση με τους επιχειρηματικούς στόχους.

Έλλειψη άξιου Στελεχιακού Δυναμικού σε εργαζομένους Πληροφορικής

Ανεπαρκή μέτρα για την συνέχιση εργασιών σε περίπτωση καταστροφών ή επιθέσεων

Έλλειψη προσαρμοστικότητας σε πιθανές αλλαγές

Έλλειψη Καινοτομιών

Σοβαρά Περιστατικά κατά τις διεργασίες των Πληροφοριακών συστημάτων

Προβλήματα σχετικά με τη Χρήση Διαδικτυακών Αποθηκευτικών Χώρων (Cloud)

Θέματα με φορητές ηλεκτρονικές συσκευές

Θέματα με χρήση προσωπικών συσκευών των εργαζομένων για επιχειρησιακές λειτουργίες

Προβλήματα με την Ανάθεση έργων σε εξωτερικούς συνεργάτες;

22. Γνωρίζετε αν η εταιρία σας έχει λάβει μέτρα και εάν επενδύει σε μέτρα και μηχανισμούς κατά των κυβερνοεπιθέσεων; *

Ναι

Όχι

23. Πως κρίνετε το επίπεδο των μέτρων που έχουν λάβει σε σχέση με τον σκοπό τους; *

Καθόλου Σημαντικό

Όχι πολύ σημαντικό

Σημαντικό

Πολύ Σημαντικό

Δεν γνωρίζω

24. Ποια από τις παρακάτω προκλήσεις θεωρείτε πως θα κληθεί να αντιμετωπίσει το τμήμα των Πληροφοριακών συστημάτων στους επόμενους 12 μήνες; *

Προβλήματα που προκύπτουν από τη χρήση προσωπικών συσκευών σε επιχειρησιακές λειτουργίες

Κυβερνοεπιθέσεις

Εξωτερική Πειρατεία

Διαρροή Δεδομένων

Ακούσια εργασιακά λάθη

Θέματα με του Διαδικτυακούς Αποθηκευτικούς Χώρους(Cloud)

Όλα τα παραπάνω

Κανένα από τα παραπάνω

25. Πως θα σχολιάζατε το επίπεδο της σχέσης της Επιχειρησιακής Διοίκησης με την Επιχειρησιακή Διοίκηση Πληροφοριακών Συστημάτων; *

Χαμηλό

Βασικό

Υψηλό

Αβέβαιο