ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

<<Αξιολόγηση της επίδρασης της οργανωσιακής κουλτούρας στην αποτελεσματικότητα της εφαρμογής της διαχείρισης ασφάλειας πληροφοριών>>

ΒΛΑΧΟΠΟΥΛΟΥ ΕΛΕΝΗ

ΜΤΕ1802

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΚΩΝ/ΝΟΣ ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ -ΣΧΗΜΑΤΩΝ

ΠΕΡΙΛΗΨΗ

Σκοπός αυτής της εργασίας είναι να εξετάσει την επίδραση της κουλτούρας της οργάνωσης στην αποτελεσματικότητα της εφαρμογής της διαχείρισης ασφάλειας πληροφοριών (ISM).Η εργασία αυτή προσέγγισε την ασφάλεια πληροφοριακών συστημάτων μέσα από το πρίσμα της οργανωσιακής κουλτούρας , της εμπιστοσύνης και της διάχυσης γνώσης. Προκειμένου να γίνουν κατανοητές οι σχέσεις που διαμορφώνονται σχεδιάστηκε ένα ερωτηματολόγιο και μοιράστηκε σε υπαλλήλους μεγάλων εταιρειών προκειμένου να απαντήσουν σχετικά με την οργανωσιακή κουλτούρα, τα χαρακτηριστικά και την αποτελεσματικότητα του ISM σε οργανισμούς με σημαντική χρήση πληροφοριακών συστημάτων.

Για τον σχεδιασμό, τη μεθοδολογία και την προσέγγιση της έρευνας διαμορφώθηκε ,με βάση την ανασκόπηση της βιβλιογραφίας ,ένα μοντέλο της σχέσης μεταξύ οργανωσιακής κουλτούρας και διαχείρισης της ασφάλειας των πληροφοριακών συστημάτων. Αυτό είχε ως αποτέλεσμα να διερευνηθεί το πώς τα ποικίλα χαρακτηριστικά της οργανωσιακής κουλτούρας επηρεάζουν τις αρχές του συστήματος της διαχείρισης πληροφοριών.

Τα ευρήματα της έρευνας προκύπτουν από τέσσερα μοντέλα παλινδρόμησης που έχουν εμφανιστεί για την ποσοτικοποίηση του αντίκτυπου στην αποτελεσματικότητα της υλοποίησης της οργανωσιακής κουλτούρας ISM. Αν και η εταιρική κουλτούρα μπορεί να ρυθμιστεί, η εμπιστοσύνη, η διάδοση πληροφοριών, η δημιουργικότητα και η παραγωγικότητα επηρεάζουν έντονα τις αρχές του ISM. Η εφαρμογή συστημάτων ασφάλειας σε οργανισμούς συνδέεται επίσης στενά με την οργανωσιακή κουλτούρα.

Όσον αφορά τους περιορισμούς της έρευνας και τις επιπτώσεις της, αναφέρεται πως το δείγμα περιορίζεται σε οργανωτικούς παράγοντες στην Ελλάδα. Επιπλέον προτείνεται να επαναληφθεί αυτή η μελέτη σε άλλες χώρες για να επιβεβαιωθεί ξανά το αποτέλεσμα πριν από την έγκρισή των γενικότερων επιπτώσεων του.

ABSTRACT

The purpose of this paper is to examine the impact of organizational culture on the effectiveness of the implementation of information security management (ISM). This work approached the security of information systems through the prism of organizational culture, trust and knowledge dissemination. In order to understand the relationships that form a questionnaire, a questionnaire was designed and distributed to employees of large companies in order to answer about the organizational culture, characteristics and effectiveness of ISM in organizations with significant use of information systems.

For the design, methodology and approach of the research, a model of the relationship between organizational culture and information systems security management was developed, based on the literature review. This led to an investigation into how the diverse characteristics of organizational culture influence the principles of the information management system.

The research findings come from four regression models that have emerged to quantify the impact on the effectiveness of the implementation of the ISM organizational culture. Although corporate culture can be regulated, trust, information dissemination, creativity and productivity strongly influence ISM principles. The implementation of security systems in organizations is also closely linked to the organizational culture.

Regarding the limitations of the research and its effects, it is reported that the sample is limited to organizational factors in Greece. In addition, it is suggested that this study be repeated in other countries to reaffirm the result before approving its general effects.

Κεφάλαιο 1: Εισαγωγικές έννοιες

1.1. Εισαγωγή

Κατά τη διάρκεια των τελευταίων δεκαετιών η χρήση της τεχνολογίας των πληροφοριών (IT) είναι πλέον πιο διαδεδομένη από ποτέ σε όλους τους τομείς της κοινωνίας και τα είδη των δραστηριοτήτων που εκτελεί ή στηρίζει, έχουν όλο και μεγαλύτερη σημασία. Σαν αποτέλεσμα, τα πληροφοριακά συστήματα χρησιμοποιούνται πλέον σε μεγάλο βαθμό από όλους τους οργανισμούς και τις επιχειρήσεις σε τόσο μεγάλο βαθμό που θα ήταν αδύνατο να διαχειριστούν τις πληροφορίες καθημερινά χωρίς τη χρήση πληροφοριακών συστημάτων. Ειδικότερα η χρήση μεγάλων δεδομένων (big data) έγινε όλο και πιο ευρεία στις επιχειρήσεις κάτι που καθιστά τη χρήση των πληροφοριακών συστημάτων πιο αναγκαία από ποτέ.

Παράλληλα με την ανάπτυξη των πληροφοριακών συστημάτων ενισχύθηκε και η ανάγκη για ασφάλεια και προστασία από τους κινδύνους. Οι οργανωσιακοί κίνδυνοι περιλαμβάνουν πολλά είδη κινδύνων, όπως για παράδειγμα κινδύνους διαχείρισης προγραμμάτων, επενδυτικούς κινδύνους, νομικούς κινδύνους, κινδύνους ασφάλειας, αποθεμάτων, εφοδιαστικής αλυσίδας κτλ (vonSolms και Niekerk ,2013). Συγκεκριμένα ο κίνδυνος ασφάλειας σχετίζεται με τη χρήση των πληροφοριακών συστημάτων και αποτελεί μια από τις πολλές συνιστώσες του οργανωτικού κινδύνου που αποτελεί ένα σημαντικό πρόβλημα για τους διαχειριστές όταν καλούνται να ανταποκριθούν σε θέματα που άπτονται της ασφάλειας των πληροφοριακών συστημάτων. Η αποτελεσματική διαχείριση κινδύνου σημαίνει πως η επιχείρηση λειτουργεί σε ένα πολύπλοκο επιχειρησιακό περιβάλλον αλλά παρόλα αυτά επιβάλλεται να υπάρχει διασύνδεση μεταξύ των τμημάτων της επιχείρησης ,η οποία είναι σε θέση να χρησιμοποιεί τα πληροφοριακά συστήματα, αλλά και τις γνώσεις των παρελθόντων ετών, προκειμένου να περατωθούν όλες οι δραστηριότητες που σχετίζονται με την λειτουργία της επιχείρησης. Οι διαχειριστές των επιχειρήσεων πρέπει να είναι σε θέση να αναγνωρίσουν τους κινδύνους ούτως ώστε να μπορούν να πάρουν αποφάσεις για τη διαχείριση του κινδύνου και με γνώμονα τα οφέλη της κάθε διαδικασίας να αντισταθμίζουν των κινδύνων τους.

Είναι σαφές πως τα ίδια τα πληροφοριακά συστήματα αποτελούν τον δίαυλο μέσω των οποίων προκαλούνται σοβαρές επιθέσεις, περιβαλλοντικές διαταραχές ,ανθρώπινα σφάλματα ή ακόμα και επιχειρηματική αποτυχία.

Η διαχείριση του κινδύνου ασφάλειας πληροφοριών, όπως και η διαχείριση κινδύνου γενικότερα, δεν είναι μια αυτοτελής επιστήμη. Συγκεντρώνει τις καλύτερες συλλογικές πληροφορίες και ενέργειες ατόμων και ομάδων στους οργανισμούς που είναι αρμόδιοι για τον στρατηγικό σχεδιασμό, την εποπτεία, τη διαχείριση και τις καθημερινές επιχειρησιακές λειτουργίες, παρέχοντας τόσο τα απαραίτητα όσο και τα επαρκή μέτρα αντιμετώπισης των κινδύνων για την προστασία των επιχειρηματικών λειτουργιών.

Όπως γίνεται εμφανές οι επιχειρησιακοί κίνδυνοι απαιτούν προστασία. Η έλλειψη των σχετικών υπηρεσιών εμπιστευτικότητας, ειλικρίνειας, ανταπόκρισης και αξιοπιστίας των πληροφοριών μπορεί να έχουν πολύ δυσμενείς συνθήκες στους οργανισμούς. Συνεπώς είναι επιτακτική η ανάγκη να γίνει η διαχείριση του κινδύνου που αφορά στις πληροφορίες αλλά και στα πληροφοριακά συστήματα μέσα στις επιχειρήσεις. Αυτή η επιτακτική ανάγκη για ασφάλεια είναι ακόμα πιο έντονη σήμερα που πολλές επιχειρήσεις έχουν ενοποιήσει όλες τις λειτουργίες τους, εσωτερικές αλλά και εξωτερικές, μέσω ενός δικτύου πληροφοριακών συστημάτων. Συνεπώς είναι αναγκαία η ύπαρξη ενός συνολικού πλάνου διαχείρισης στα πλαίσια ενός οργανισμού. Είναι λογικό πως οι αλλαγές στην τεχνολογία των ηλεκτρονικών υπολογιστών έχουν επιφέρει ανάλογες απειλές και κινδύνους απέναντι σε αυτή την επιχειρησιακή λειτουργία αλλά και στην πληροφορία γενικότερα. Υπό αυτές τις συνθήκες μια νέα σκοπιά της οργανωσιακής ασφάλειας πρέπει να αναπτυχθεί με βάση την οποία η πληροφορία και η ασφάλεια των πληροφοριών θα περιλαμβάνει προληπτικές ενέργειες με στοχευμένο σχέδιο παρά μια αντίδραση απέναντι στις τεχνολογικές αλλαγές μέσα στα πλαίσια του οργανισμού. Συνεπώς είναι σημαντικό να ακολουθούν οι οργανισμοί ένα δομημένο σχέδιο εφαρμογής και διατήρησης του συστήματος διαχείρισης και ασφάλειας των πληροφοριακών συστημάτων.

Η εργασία αυτή έχει ως σκοπό να καταδείξει τον τρόπο με τον οποίο οι επιχειρήσεις αντιμετωπίζουν την αλλαγή που προέρχεται από την εφαρμογή της ασφάλειας πληροφοριακών συστημάτων μέσα στα πλαίσια ενός οργανισμού. Προκειμένου να εξυπηρετηθούν οι σκοποί του θέματος αυτού, η εργασία χωρίζεται σε πέντε (5) ενότητες.

Η πρώτη ενότητα περιλαμβάνει την εισαγωγή και την αποσαφήνιση όλων εκείνων των όρων που θα χρησιμοποιηθούν καθώς επίσης και τους σκοπούς της παρούσας έρευνας.

Το δεύτερο κεφάλαιο παρουσιάζει τα δευτερογενή στοιχεία της έρευνας, δηλαδή τις βιβλιογραφικές αναφορές πάνω στις οποίες στηρίζεται το θέμα της εργασίας, με ιδιαίτερη έμφαση στην οργανωσιακή κουλτούρα και τις προσεγγίσεις της διαχείρισης αλλαγής σε οργανωτικό επίπεδο.

Το τρίτο κεφάλαιο αποτελεί μια παρουσίαση της μεθοδολογίας της παρούσας έρευνας στο οποίο θα αναλυθούν η φιλοσοφία, ο σχεδιασμός της έρευνας, η μέθοδος δειγματοληψίας και ο τρόπος ανάλυσης του δείγματος.

Το τέταρτο κεφάλαιο περιλαμβάνει την παρουσίαση των δεδομένων της έρευνας και στην ανάλυση των αποτελεσμάτων που προέκυψαν.

Το πέμπτο κεφάλαιο αναφέρεται στα συμπεράσματα της έρευνας.

1.2. Πληροφοριακά συστήματα

Στο σημείο αυτό είναι απαραίτητο να δοθεί ένας ορισμός για τα πληροφοριακά συστήματα. Το πληροφοριακό σύστημα είναι ένα δυναμικό και ολοκληρωμένο σύστημα μεταξύ χρήστη και μηχανής που έχει ως σκοπό την υποστήριξη διοικητικών και επιχειρησιακών λειτουργιών, διαδικασιών λήψης αποφάσεων και λοιπών εργασιών (Βασιλακόπουλος και Χρυσικόπουλος ,1990).

Ο όρος "ολοκληρωμένο" υποδεικνύει μια σύνδεση μεταξύ των χρήσιμων τμημάτων του πληροφοριακού συστήματος. Επομένως, η συλλογή των δεδομένων και η εκτέλεση εφαρμογών-διεργασιών πάνω σε αυτά περιλαμβάνονται σε ένα πλήρες πληροφοριακό σύστημα. Ένα ολοκληρωμένο πληροφοριακό σύστημα αποτελείται από ενιαίες εφαρμογές που αποσκοπούν στην ικανοποίηση των απαιτήσεων πληροφόρησης ενός συγκεκριμένου οργανωτικού σκοπού. Ο σχεδιασμός αυτών των εφαρμογών βασίζεται σε μια ολιστική άποψη των γνώσεων του οργανισμού. Αυτό σημαίνει πως οι λειτουργίες δεν αντιμετωπίζονται μεμονωμένα αλλά ολιστικά, και πάντα σε σχέση με ολόκληρο το δίκτυο.

Προκειμένου να ικανοποιηθούν οι ανάγκες πληροφόρησης των διαφόρων ομάδων χρηστών, δημιουργούνται μεμονωμένες εφαρμογές ενός συστήματος πληροφοριών. Κατά συνέπεια, αυτά τα μεμονωμένα συστήματα θα είναι μη συμβατά μεταξύ τους εάν δεν υπάρχουν πλήρεις και σωστές διαδικασίες.

Ένας άλλος ορισμός του πληροφοριακού συστήματος περιλαμβάνει τα αλληλένδετα στοιχεία που συλλέγουν, επεξεργάζονται, αποθηκεύουν και διαχέουν τις πληροφορίες για την υποστήριξη της λήψης αποφάσεων, του συντονισμού, της παρακολούθησης, της ανάλυσης και της απεικόνισης.

Οι δραστηριότητες τις οποίες αναλαμβάνει να φέρει εις πέρας ένα πληροφοριακό σύστημα είναι οι εξής (PMI Institute, 2013):

- Εισαγωγή ή συλλογή πρωτογενών δεδομένων από τον οργανισμό ή το εξωτερικό περιβάλλον για επεξεργασία πληροφοριών συστήματος.
- Επεξεργασία, Η διαχείριση και ανάλυση πρωτογενών εισροών, που πρέπει να μετασχηματιστούν (επεξεργασία), κατά τρόπο κατανοητό.
- Διανομή πληροφοριών σχετικά με τα μεταποιημένα προϊόντα σε άτομα ή δραστηριότητες που πρόκειται να χρησιμοποιηθούν.
- Ανατροφοδότηση . Δημιουργία σχολίων για να υποστηριχθεί η αξιολόγηση ή η διόρθωση των στοιχείων από τα μέλη της οργάνωσης που έχουν την δικαιοδοσία να το κάνουν.

Το πληροφοριακό σύστημα περιλαμβάνει μια ποικιλία τεχνολογιών πληροφορικής (IT).Την υλοποίηση, την επικοινωνία ή την εκπαίδευση διαφόρων ενδιαφερομένων σε συγκεκριμένα οργανωτικά και κοινωνικά πλαίσια, συμπεριλαμβανομένων υπολογιστών, εφαρμογών, βάσεων δεδομένων, δικτύων επικοινωνίας ,διαδικτύου, κινητών συσκευών κ.α. Όλες οι πτυχές του σχεδιασμού, της υλοποίησης, της χρήσης και του επηρεασμού των οργανισμών και της κοινωνίας είναι γενικού ενδιαφέροντος για τον τομέα της κοινωνίας της πληροφορίας.

Ωστόσο, ο τομέας της κοινωνίας της πληροφορίας δεν έχει να κάνει κυρίως με τις τεχνολογικές και ηλεκτρονικές πτυχές της πληροφορικής. Αυτό που έχει σημασία για το πληροφοριακό σύστημα είναι ο τρόπος με τον οποίο οι τεχνικές καινοτομίες έχουν αξιοποιηθεί και δημιουργηθεί για να επιτρέψουν στην κοινωνία των πληροφοριών να ανταποκριθεί στις ανάγκες και τις απαιτήσεις της γνώσης καθώς και στους συγκεκριμένους στόχους και πρακτικές των διαφορετικών οντοτήτων, όπως άτομα, ομάδες ή οργανώσεις.

1.2.1. Η ασφάλεια των πληροφοριακών συστημάτων

Η ασφάλεια σύμφωνα με τους vonSolms και vanNiekerk (2013) αναφέρεται ως η προστασία των διαφόρων περιουσιακών στοιχείων από διάφορες απειλές στις οποίες μπορεί να εκτίθενται. Η διαδικασία της ασφάλειας δεν είναι μια στατική διαδικασία αλλά ένα σύνολο δραστηριοτήτων μέσω των οποίων μετασχηματίζονται οι πόροι. Στη διεθνή βιβλιογραφία ο τομέας της ασφάλειας αφορά σε διάφορες έννοιες που σχετίζονται μεταξύ τους. Συγκεκριμένα γίνεται λόγος για την ασφάλεια της πληροφορίας και για την ασφάλεια των τεχνολογιών επικοινωνίας και πληροφορίας (ICT). Καθώς και για την κυβερνοασφάλεια (cybersecurity). Στη μελέτη τους οι vonSolms και vanNiekerk (2013) προσπάθησαν να αποσαφηνίσουν κάθε έννοια αλλά και να δείξουν πως οι όροι αυτοί σχετίζονται μεταξύ τους.

Σύμφωνα με την έρευνα αυτή η ασφάλεια σε επίπεδο πληροφορίας και επικοινωνίας περιλαμβάνει την προστασία της υποκείμενης τεχνολογίας, ενώ η ασφάλεια των πληροφοριακών συστημάτων, συμπεριλαμβάνει την ασφάλεια των συστημάτων.

Το επίπεδο ασφάλειας των πληροφοριών μέσα σε έναν οργανισμό εξαρτάται από τα εξής:

- τα αποδεκτά επίπεδα κινδύνου που έχουν καθοριστεί από τον οργανισμό
- την οργανωσιακή κουλτούρα της επιχείρησης
- Το σχέδιο που πρέπει να έχει την πλήρη υποστήριξη της διοίκησης και να βασίζεται στην ανάλυση κινδύνου της επιχείρησης.
- τη λειτουργικότητα του πληροφοριακού συστήματος
- το κόστος που προτίθεται ο οργανισμός να αναλάβει για την ασφάλεια.
- και να συμμορφωθεί με τις απαιτήσεις της κείμενης νομοθεσίας.

1.2.2. Πληροφοριακά συστήματα στις επιχειρήσεις

Η τεχνολογία της πληροφορίας αναφέρεται ως ένας γενικός όρος που αφορά σε όλες τις τεχνολογίες μέσω της χρήσης ενός ηλεκτρονικού υπολογιστή. Η τεχνολογία της πληροφορίας και της επικοινωνίας (Information and Communication Technology, ICT) παίζει σημαντικό ρόλο στην καθημερινότητα αλλά και στον τρόπο που αντιλαμβάνονται οι άνθρωποι και αλληλοεπιδρούν με το περιβάλλον τους. Τα πληροφοριακά συστήματα (Information Systems) είναι πλέον ζωτικής σημασίας για την εκτέλεση καθημερινών δραστηριοτήτων στο πλαίσιο ενός οργανισμού. Ως εκ τούτου η συνεχής εξέλιξη και ανάπτυξη των τεχνολογιών της πληροφορίας αναδεικνύει νέα πεδία εφαρμογής αυτών, ενώ υπάρχουν συνεχείς αλλαγές οι οποίες διαδίδονται με ταχύτατους ρυθμούς στις ανεπτυγμένες και αναπτυσσόμενες χώρες (Laudon 2012).Τα πληροφοριακά συστήματα του οργανισμού αποτελούν αναπόσπαστο μέρος του οργανισμού. Τα κύρια στοιχεία της οργάνωσης είναι οι άνθρωποι, η δομή, οι λειτουργικές διαδικασίες τους, οι πολιτικές τους και η κουλτούρα τους.

Η επιχείρηση λειτουργεί ως ένα κέντρο επιχειρηματικής οργάνωσης, το οποίο περιλαμβάνει τις πωλήσεις και τις αγορές, τη βιομηχανία, τις χρηματοπιστωτικές υπηρεσίες, τη λογιστική και τους ανθρώπινους πόρους. Περιλαμβάνει επίσης καθιερωμένες διαδικασίες για την εκτέλεση των καθηκόντων που διατυπώθηκαν και εκτελέστηκαν προκειμένου να ικανοποιηθούν οι επιθυμητές συνθήκες, όπως την πώληση προϊόντων και υπηρεσιών , την διοίκηση προϊόντων και υπηρεσιών (μετρητά, καταθέσεις ,τίτλοι κλπ.) και την τήρηση των οικονομικών καταστάσεων του οργανισμού (αποδείξεις, πληρωμές, επιταγές κλπ.). Αρχεία οικονομικών λογαριασμών του οργανισμού (αποδείξεις, πληρωμές, επιταγές κλπ.) ,προσωπικό από το γραφείο (εργαζόμενοι στον τομέα των δεδομένων) όπως γραμματείς και λογιστές, οι οποίοι διαχειρίζονται τη γραφειοκρατία του οργανισμού. Οι εργαζόμενοι που πραγματικά παράγουν τα προϊόντα ή τις υπηρεσίες της εταιρείας και τα ανώτερα διευθυντικά στελέχη , είναι εκείνα που καθοδηγούν την ιεραρχία και παίρνουν μακροπρόθεσμες αποφάσεις σε έναν οργανισμό. Οι μεσαίοι διαχειριστές είναι μέλη της διοίκησης που βρίσκονται στο κέντρο της ιεραρχίας του οργανισμού και είναι υπεύθυνοι για την υλοποίηση των σχεδίων και των στόχων της ανώτερης διοίκησης. Οι λειτουργικοί διαχειριστές είναι τα άτομα που είναι υπεύθυνα για την παρακολούθηση των καθημερινών δραστηριοτήτων του οργανισμού.

Τα πληροφοριακά συστήματα αποτελούν τον πυρήνα των σημερινών επιχειρήσεων καθώς επηρεάζουν σε ένα πολύ μεγάλο βαθμό τη δομή, τη διοίκηση και τις διαδικασίες τους. Πολύ μεγάλα χρηματικά ποσά διακινούνται καθημερινά μέσω συστημάτων που είναι αυτοματοποιημένα με πληροφοριακά συστήματα.

Σε διοικητικό επίπεδο η επιχείρηση οφείλει να συμμορφώνεται με τα Συστήματα Διαχείρισης Πληροφοριών (MIS) και τα Συστήματα Υποστήριξης Αποφάσεων (DSS). Τα συστήματα περιλαμβάνουν αναφορές παραγωγικότητας και απόδοσης που βασίζονται σε ιστορικά, διαχρονικά δεδομένα (π.χ. σωρευτικές πωλήσεις ενός προϊόντος τον προηγούμενο χρόνο). Η χρήση των πληροφοριακών συστημάτων μέσα στην επιχείρηση περιλαμβάνουν τον προγραμματισμό και την παρακολούθηση όλων των εταιρειών σε ένα περιβάλλον πλήρους εφαρμογής υπολογιστών. Τα μέλη του διοικητικού συμβουλίου σε μια μεγάλη εταιρεία μπορούν να παρακολουθούν, να ρυθμίζουν, να αξιολογούν μια κατάσταση και στη συνέχεια να λαμβάνουν μια απόφαση για συγκεκριμένες διοικητικές δραστηριότητες μέσω των εκθέσεων που παράγονται σε συγκεκριμένο, συνήθη ή πραγματικό χρόνο, ακολουθώντας ερωτήσεις στα βασικά δεδομένα. Ο Διευθυντής του τμήματος παραγωγής μπορεί, για παράδειγμα, να γνωρίζει με ακρίβεια ποσά, πρώτες ύλες και το σχετικό κόστος σε κάθε σημείο της παραγωγής, από το αποθεματικό μιας βιομηχανικής μονάδας και το σύστημα διαχείρισης της πρώτης ύλης και είναι πολύ πιο σημαντικό σε σύγκριση με κάποια άλλη χρονική περίοδο. Αυτή η κατηγορία συστημάτων καλύπτει τις άμεσες και κατανοητές απαιτήσεις πληροφόρησης των υπεύθυνων διαχείρισης, συμπεριλαμβανομένων των συνοπτικών αγορών δεδομένων, πωλήσεων και διανομής, ανά μονάδα, πελάτη και αντικείμενο.

1.3. Διαχείριση ασφάλειας πληροφοριακών συστημάτων

Η διαχείριση των πληροφοριών, δηλαδή η εισαγωγή και η διατήρηση, ενός ασφαλούς περιβάλλοντος πληροφορίας μέσα σε έναν οργανισμό απαιτεί συχνά ένα ολοκληρωμένο σύστημα ασφάλειας διαχείρισης πληροφοριών (VonSolms, 1998). Επιπλέον απαραίτητη είναι η συστηματική προσέγγιση για τον προσδιορισμό των απαιτήσεων για την υλοποίηση και τη διαχείριση της ασφάλειας των πληροφοριών μέσα σε έναν οργανισμό. Αυτή η διαδικασία ονομάζεται διαχείριση της ασφάλειας των πληροφοριών. Ο σχεδιασμός και η διαχείριση της τεχνολογίας πληροφορικής είναι η γενική διαδικασία δημιουργίας και συντήρησης ενός προγράμματος ασφάλειας πληροφοριών μέσα στον οργανισμό. Περιλαμβάνει ανθρώπους, διαδικασίες και πληροφοριακά συστήματα. Επειδή το είδος διαχείρισης, τα οργανωτικά μεγέθη και οι δομές διαφέρουν, αυτή η διαδικασία πρέπει να προσαρμόζεται στο περιβάλλον που χρησιμοποιείται. Ως εκ τούτου, είναι σημαντικό οι οργανισμοί να ακολουθούν μια δομημένη μεθοδολογία βασιζόμενη σε υγιείς αρχές και διαδικασίες διαχείρισης κατά την εφαρμογή και διατήρηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (διοίκησης πληροφοριακών συστημάτων).Ο ρόλος της τεχνολογίας των πληροφοριών έχει πολύ σημαντική επίδραση στις σημερινές επιχειρήσεις. Λόγω της μεγάλης διείσδυσης αυτών των τεχνολογιών η ασφάλεια πρέπει να αποτελεί βασικό στοιχείο του σύγχρονου επιχειρηματικού σχεδιασμού και της διαχείρισης πληροφοριών. Αυτή η περιχαράκωση γύρω από την έννοια της ασφάλειας αφορά επίσης στην ραγδαία ανάπτυξη των ηλεκτρονικών συναλλαγών και τροφοδοτείται εν μέρει από το διαδίκτυο καθώς το ηλεκτρονικό εμπόριο πολλαπλασιάζεται με την ανάπτυξη των δικτύων. Ο στόχος της ασφάλειας των πληροφοριών είναι να εξασφαλιστεί το περιεχόμενο της πληροφορίας αλλά και να διασφαλιστούν οι πόροι επεξεργασίας πληροφοριών (Ryan και Bordoloi, 1997; Chou κ.α.1999; Chang και Ho, 2006).

Η θεωρία της διοίκησης πληροφοριακών συστημάτων χρησιμοποιείται για την προστασία όλων των πολύτιμων περιουσιακών στοιχείων και των πληροφοριών. Έχει ως σκοπό την άμβλυνση των διαφόρων κίνδυνων ως προς τις πληροφορίες που προέρχονται από όλες τις πτυχές του περιβάλλοντος του οργανισμού μέσα από την εφαρμογή της τεχνολογικής ασφάλειας και της διαδικασίας διαχείρισης.

Σύμφωνα με μια ευρεία έρευνα που διεξήχθη από το περιοδικό Ασφάλειας Πληροφοριών (2002), τα πιο σημαντικά προβλήματα στην ασφάλεια των πληροφοριών, με βάση τα δεδομένα που συλλέχθηκαν από 2.196 επαγγελματίες ασφάλειας πληροφοριών, είναι ο κακόβουλος κώδικας, η εξασφάλιση εξουσιοδοτημένων χρηστών ,η ασφάλεια της πληροφορικής και τηλεπικοινωνιών , οι μη πιστοποιημένοι χρήστες και η οργανωσιακή διαχείριση. Το αποτέλεσμα της έρευνας δείχνει επίσης ότι τα πιο πολλά προβλήματα ασφάλειας πληροφοριών προκαλούνται από την αμέλεια των ανθρώπων, παρά από συμβάντα επίθεσης. Κατά συνέπεια, είναι σημαντικό να γίνετε η κατάλληλη εκπαίδευση στους ανθρώπους για την αποφυγή των λαθών.

Ένα αποδεκτό επίπεδο ασφάλειας πληροφοριών μπορεί να επιτευχθεί και να διατηρηθεί μόνο εάν το σωστό σύνολο ελέγχων ασφάλειας εντοπίζεται, υλοποιείται και συντηρείται. Ο εντοπισμός ενός εύλογου αποτελεσματικού συνόλου ελέγχων ασφάλειας μπορεί να είναι πολύ περίπλοκο σαν διαδικασία καθώς περιλαμβάνει την διαθεσιμότητα πολλών πόρων, η οποία απαιτεί ειδικούς, εργασία και εμπειρογνωμοσύνη που οι περισσότερες εταιρείες δεν διαθέτουν. Γι' αυτό υπάρχει επείγουσα ζήτηση για πρότυπα διοίκησης συστημάτων, τα οποία προσφέρουν κατευθυντήριες γραμμές στους οργανισμούς με τον εντοπισμό και την εισαγωγή ενός συνόλου των ελέγχων που συμβάλλουν σε ένα αποδεκτό επίπεδο προστασίας των πληροφοριακών πόρων.

Διαχρονικά έχουν αναπτυχθεί διάφορες τεχνολογικές λύσεις για την ασφάλεια των τεχνολογικών συστημάτων, ενώ πολλές άλλες βρίσκονται σε εξέλιξη. Ωστόσο η ασφάλεια πληροφορίας αποτελεί μια μεγάλη πρόκληση για τους περισσότερους οργανισμούς (Grant, Edgar, Sukumar, &Meyer, 2014). Οι υφιστάμενες τεχνολογικές λύσεις εξαρτώνται επίσης από την πολιτική ασφάλειας των πληροφοριών και τις οργανωτικές στρατηγικές, οπότε η διερεύνηση της διαχείρισης της ασφάλειας είναι ένα σημαντικό κομμάτι. Οι Ernst και Young (2012) αναφέρουν πως στα πλαίσια μιας επιχείρησης η ασφάλεια των πληροφοριών θα έπρεπε να διαχειρίζεται σε επίπεδο διοικητικό και όχι μόνο να αναφέρεται με τεχνικούς όρους . Στη βιβλιογραφία η ασφάλεια των πληροφοριακών συστημάτων εξετάστηκε από διάφορους συγγραφείς, δίνοντας όμως έμφαση στα τεχνικά χαρακτηριστικά τους (Singh κ.ά., 2013). (2007), Chang και Lin (2007), Ernst και Young (2012), Ezingeard και Bowen-Schrire (2007), Knapp, Marshall, Rainer Jr και Morrow (2006), Siponen κ.α. (2009, 2014). Ενώ οι Phillips (2013) και οι VonSolms και VonSolms (2004), προετοίμασαν το δρόμο για την εξέταση της ασφάλειας των πληροφοριακών συστημάτων από μια διαχειριστική σκοπιά.

Από μια ευρύτερη σκοπιά η διαχείριση της ασφάλειας έχει μια βασική ευθύνη των επιχειρησιακών θεμάτων, επομένως έχει ένα σημαντικό ρόλο σε κάθε μια από τις επιχειρηματικές δραστηριότητες. Η ασφάλεια των πληροφοριών είναι πρωτίστως ένα διοικητικό και επιχειρησιακό θέμα επομένως οι διαχειριστές και γενικότερα η ανώτατη διοίκηση πρέπει να είναι ενήμεροι για τη σημασία των πολιτικών ασφάλειας των πληροφοριακών συστημάτων αλλά και την εφαρμογή τους μέσα στα πλαίσια ενός οργανισμού. (Chang&Ho, 2006).

Υπάρχουν πολλοί παράγοντες που επηρεάζουν την πολιτική ασφάλειας των πληροφοριακών συστημάτων μέσα στα πλαίσια ενός οργανισμού. Πρώτα από όλα το είδος της επιχείρησης, το μέγεθος και η δομή της επηρεάζουν σημαντικά την εφαρμογή των πολιτικών ασφάλειας των πληροφοριακών συστημάτων. Οι μεγάλοι χρηματοπιστωτικοί οργανισμοί για παράδειγμα δέχονται μεγαλύτερη επίδραση από τις εφαρμογές ασφάλειας των πληροφοριακών συστημάτων κυρίως λόγω των μεγαλύτερων απειλών που δέχονται σε επίπεδο ασφάλειας. Εκτός από την ανάπτυξη της πολιτικής για την ασφάλεια των πληροφοριών, η υποστήριξη της διαχείρισης είναι επίσης σημαντική για την αποτελεσματική εφαρμογή της (Knappκ.α., 2006, Ma, Schmidt, &Pearson, 2009). Η οργανωσιακή δομή είναι επίσης εξαιρετικά σημαντική στη διαχείριση της ασφάλειας των πληροφοριών(Boss, Kirsch, Angermeier, Shingler, και Boss, 2009, Kayworth&Whitten, 2010). Οι Ma κ.α. (2009) αναφέρουν ότι η διαχείριση της ασφάλειας των πληροφοριών απαιτεί μια οργανωσιακή δομή που διευκολύνει την υποβολή εκθέσεων, την αποτελεσματική επικοινωνία, τη σαφή εξουσιοδότηση και τη γρήγορη ροή των πληροφοριών.

Η υφιστάμενη βιβλιογραφία υποστηρίζει μια επίσημη δομή για την καλύτερη διαχείριση της ασφάλειας πληροφοριών (Kayworth&Whitten, 2010). Ένα σύστημα αποκεντρωμένης απόφασης για την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριών όπως οι Pulkkinen, Naumenkoκαι Luostarinen (2007) προτείνουν είναι ότι εάν εφαρμοστούν αποφάσεις ασφάλειας σε όλα τα επίπεδα εντός των οργανισμών, θα υπάρχει ασφαλής αρχιτεκτονική πληροφόρηση για την ανταλλαγή εμπιστευτικών πληροφοριών στο επιχειρηματικό δίκτυο. Η ανάπτυξη συστημάτων ασφάλειας πληροφοριών έχει ως στόχο να αποτρέψει την παρέμβαση από τρίτους στις πληροφορίες.

Ένα αποτελεσματικό πρόγραμμα και πολιτική διακυβέρνησης για την ασφάλεια της πληροφόρησης, η ποιότητα της εκτελεστικής υποστήριξης διαχείρισης (Johnston&Hale, 2009), οι συνεχείς αξιολογήσεις και η ενσωμάτωση ορισμένων αλλαγών στην αντιμετώπιση νέων προκλήσεων αποτελούν βασικούς παράγοντες για την αποτελεσματικότητά τους (Ezingeard&Bowen-Schrire, 2007).

Όλες αυτές οι δραστηριότητες απαιτούν το ενδιαφέρον και την προσοχή της ανώτερης διαχείρισης, επομένως είναι προφανές πως ο ρόλος του διαχειριστή είναι σημαντικός για την αποτελεσματικότητα της διαχείρισης των συστημάτων ασφάλειας των πληροφοριών.

Στην μελέτη του ο Cortada (2010) υποστήριξε πως από τότε που εισήχθη η τεχνολογία πληροφορίας μέσα στις επιχειρήσεις υπάρχουν πολλές και διαφορετικές αντιδράσεις στον τρόπο με τον οποίο αντιδρούν οι οργανισμοί στους διάφορους κινδύνους που σχετίζονται με την ασφάλεια. Έτσι, λοιπόν, η σημασία στον τρόπο αντιμετώπισης των απειλών που έχει η ανώτερη διοίκηση καταδεικνύει την σημασία που έχουν οι αντιδράσεις της ανώτερης διοίκησης, τους χρηματικούς περιορισμούς και την απουσία των ικανών ανθρώπινων πόρων αλλά και την έλλειψη των κατάλληλων εργαλείων προκειμένου να αντιμετωπιστούν οι κίνδυνοι αυτοί, καθώς όπως έχει ήδη αναφερθεί η διοίκηση είναι αυτή που πρέπει να βρει τρόπους αντιμετώπισης των κινδύνων αυτών.

Η αποτελεσματικότητα των συστημάτων ασφάλειας πληροφοριών εξαρτάται από πολλούς παράγοντες. Συγκεκριμένα προκειμένου να είναι αποτελεσματικό το σύστημα πρέπει να περιλαμβάνει τα εξής:

- διαδικασίες διαχείρισης περιστατικών παραβίασης ασφάλειας,
- σχέδιο επιχειρησιακής συνέχειας και
- ένα σύστημα μέτρησης της ίδιας του της απόδοσης, ώστε να καθίσταται δυνατή η βελτίωσή του.

1.4. Στοιχεία της διαχείρισης ασφάλειας πληροφοριακών συστημάτων

Ένα από τα βασικά στοιχεία του σχεδιασμού μιας φιλοσοφίας για την διαχείριση των συστημάτων ασφάλειας των πληροφοριών είναι η ολοκλήρωση. Η ανάπτυξη μιας ολοκληρωμένης μεθοδολογίας μπορεί να επιτευχθεί μελετώντας τα στοιχεία που είναι απαραίτητα για την εισαγωγή ενός ολοκληρωμένου συστήματος διαχείρισης ασφάλειας των πληροφοριών.

Τα στοιχεία, λοιπόν, της διαχείρισης ασφάλειας των πληροφοριακών συστημάτων είναι τα εξής:

- Καθορισμός ενός πλαισίου

  Οι σωστές κατευθύνσεις της διοίκησης και η δέσμευση για την υλοποίηση τους είναι πολύ σημαντικές προϋποθέσεις για την ανάπτυξη ενός συστήματος ασφάλειας μέσα στα πλαίσια ενός οργανισμού. Οι κατευθύνσεις πρέπει να δίνονται στα πλαίσια γενικών οδηγιών και να περιλαμβάνουν: την πολιτική ασφάλειας της πληροφορίας που είναι η βάση για μια υπεύθυνη συμπεριφορά σχετικά με την συνολική ασφάλεια των στόχων της οργάνωσης. Καθώς επίσης και μια δήλωση σχετικά με την κατανομή των ευθυνών. Την στρατηγική ασφάλειας της πληροφορίας η οποία πρέπει να απεικονίζει πως θα επιτευχθούν οι στόχοι που έχουν τεθεί. Την οργάνωση του συστήματος και την κατάλληλη ανάθεση των διάφορων ρόλων που έχει ο καθένας μέσα στο σύστημα.

- Εκτίμηση του κινδύνου

  Οι επιχειρηματικοί κίνδυνοι πρέπει να μπορούν να εκτιμηθούν σωστά ώστε να ληφθεί ένα ανεκτό επίπεδο ασφάλειας. Συνεπώς, η διοίκηση έχει την ευθύνη να ορίσει και να παρέχει τα κατάλληλα εργαλεία αξιολόγησης των κινδύνων ώστε να αναγνωριστούν οι απειλές για τον οργανισμό και να εγκρίνει την λήψη των απαιτούμενων αντίμετρων που πρέπει να εφαρμοστούν. Η αξιολόγηση του κινδύνου πρέπει να συζητείται τακτικά από τη διευθύνουσα επιτροπή ως μέρος της συνολικής αξιολόγησης των διαδικασιών διαχείρισης της ασφάλειας συμπεριλαμβανομένων των σωστών οδηγιών και του τρόπου με τον οποίο τηρούνται.

- Σχεδιασμός:

  Στο στάδιο αυτό καθορίζονται και προγραμματίζονται τα έργα υλοποίησης, τα μέτρα ασφάλειας τα οποία θα πρέπει να σχεδιάζονται σύμφωνα με τις επιχειρηματικές ανάγκες που ορίζονται κατά τη διάρκεια της αξιολόγησης κινδύνου. Με βάση τους κινδύνους που έχουν εντοπιστεί είναι απαραίτητο να καθορίζεται το σύνολο αντιμέτρων. Για να είναι συνεκτικά και πλήρη τα μέτρα θα ήταν σωστό να οριστεί μια αρχιτεκτονική ασφάλειας της πληροφορίας.

- Εφαρμογή:

  Τα μέτρα ασφάλειας εφαρμόζονται με τη μορφή τεχνικών μηχανισμών και των διοικητικών διαδικασιών. Σύμφωνα με το πληροφοριακό σύστημα F (Φόρουμ Ασφάλειας Πληροφοριών)διεθνής ένωση περισσότερων από 240 ηγετικών οργανισμών που παρέχουν συγκεκριμένα πρότυπα στα μέλη της, πρέπει να καλύπτουν τουλάχιστον τους ακόλουθους τομείς: Διαχείριση Ασφάλειας, Κρίσιμες επιχειρηματικές εφαρμογές, Επεξεργασία πληροφορίας, Δίκτυα Επικοινωνιών και Ανάπτυξη Συστημάτων.

- Εκπαίδευση:

  Αυτό το στοιχείο δεν πρέπει να παραληφθεί επειδή το κομμάτι της ασφάλειας που αφορά τον ανθρώπινο παράγοντα είναι αποφασιστικής σημασίας για το αποτέλεσμα ενός συνολικού προγράμματος ασφάλειας της πληροφορίας. Είναι απαραίτητα τα προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης εργαζομένων προκειμένου να υπάρχει ενημέρωση αλλά και κατανόηση των προγραμμάτων που αφορούν στην ασφάλεια της πληροφορίας. Επιπλέον είναι σημαντική η διαθεσιμότητα σχετικής εξωτερικής κατάρτισης (σεμινάρια, σεμινάρια ή συνέδρια)για τους υπαλλήλους.

- Λειτουργία:

  Κατά το στάδιο της λειτουργίας εφαρμόζονται τα μέτρα και οι διαδικασίες που πρέπει να ακολουθούνται στις καθημερινές δραστηριότητες. Πρέπει να αντιμετωπίζονται τα περιστατικά και για τα αρχεία των δεδομένων να δημιουργούνται αντίγραφα ασφάλειας κατά τη διάρκεια των εργασιών.

  Επίσης, η διαδικασία διαχείρισης αλλαγών χρησιμοποιείται για τον εντοπισμό νέας ασφάλειας όταν μεταβάλλονται τα συστήματα της πληροφορίας.

- Παρακολούθηση:

  Στο πλαίσιο του κύκλου διαχείρισης της ασφάλειας της πληροφορίας, η διαχείριση πρέπει να είναι σε θέση να αποκτήσει σαφή αποτελέσματα των επιτευγμάτων σε σύγκριση με τους αρχικούς στόχους. Στο στάδιο της παρακολούθησης, γίνεται η επανεξέταση της εφαρμογής των μέτρων και των διαδικασιών που πρέπει να τηρούνται. Ανασκόπηση των αλλαγών στο περιβάλλον και στην τεχνική υποδομή προκειμένου να καταστήσει αποτελεσματικές τις αλλαγές ασφάλειας. Εγκατάσταση προγράμματος αυτοπαρακολούθησης. Ανεξάρτητες κριτικές τρίτων που τηρούν συγκεκριμένα πρότυπα.

- Αξιολόγηση:

  Πρέπει να αναφέρεται η διαδικασία παρακολούθησης και τα αποτελέσματα που προέκυψαν, ιδίως οι αποκλίσεις διαχείρισης σε τακτική βάση - και αξιολόγηση των επιτευχθέντων επιτευγμάτων. Ώστε να προσδιορίσουν εάν έχουν ικανοποιητικό χαρακτήρα ή εάν η πολιτική ασφάλειας IT χρειάζεται συντονισμό. Για την εφαρμογή αυτού η διοίκηση πρέπει να εξετάζει τις εκθέσεις αξιολόγησης αποφασίζει για τα κατάλληλα μέτρα που πρέπει να ληφθούν. Ως βάση για την αξιολόγηση αποκτάται μια επικαιροποιημένη εκτίμηση κινδύνου.

- Διόρθωση:

  Εάν από την διαδικασία της αξιολόγησης παρατηρηθούν σημεία που δεν ενσωματώθηκαν οι νέες δραστηριότητες, θα κριθούν αναγκαίες διορθώσεις. Έχουν προτεραιότητα και διατίθενται πόροι ώστε να ενημερωθούν, η πολιτική ασφάλειας IT ,

  η στρατηγική ασφάλειας IT, που αλλάζει σύμφωνα με νέες προτεραιότητες και ξεκινούν τα απαραίτητα έργα υλοποίησης.

1.5. Η διαχείριση της αλλαγής

Η διαχείριση της αλλαγής είναι μια έννοια που εδώ και πολλά χρόνια αποτελεί αντικείμενο συζήτησης στον κόσμο των επιχειρήσεων, με αποτέλεσμα να έχουν δοθεί πολλές ερμηνείες γύρω από αυτήν. Οι Moran και Brightman (2000) ορίζουν τη διαχείριση της αλλαγής μέσα στα πλαίσια ενός οργανισμού ως τη "διαδικασία της συνεχούς αλλαγής της κατεύθυνσης ενός οργανισμού, της δομής του αλλά και της ικανότητας του να είναι σε θέση να εξυπηρετεί τις διαρκείς ανάγκες της αγοράς των πελατών αλλά και των εργαζομένων" (Moran&Brightman, 2000, p. 73). Συμπληρωματικά ο Duck (1993) αναφέρεται στη διαχείριση της αλλαγής μέσα από τη σκοπιά αυτών που ηγούνται και αυτών που είναι σε θέση να εφαρμόσουν την αλλαγή μέσα από νέες στρατηγικές, διαχειριζόμενοι το οργανωτικό πλαίσιο ,στο οποίο λαμβάνει χώρα η αλλαγή». Η διαχείριση της αλλαγής περιλαμβάνει την εξέλιξη από την παρούσα κατάσταση στην πιο επιθυμητή κατάσταση (Galli, 2018) και ο σκοπός είναι να επιτευχθεί καλύτερη απόδοση για τον οργανισμό (Chou,2007). Σύμφωνα με τους Yilmaz, Ozgen, και Akyel (2013) η διαχείριση της αλλαγής στοχεύει είτε την αύξηση της απόδοσης του οργανισμού είτε να προσαρμοστεί σε νέες συνθήκες.

Οι Detert κ.α. (2000) προσδιόρισαν τη διαχείριση της αλλαγής ως μία από τις διαστάσεις της οργανωσιακής κουλτούρας. Δηλώνοντας πως "η βελτίωση δεν μπορεί να έρθει χωρίς αλλαγή". Επιπρόσθετα οι Ruighaveretaï. (2007) εφάρμοσαν το μοντέλο που προτείνεται από τους Detert κ.α. (2000) στην κουλτούρα ασφάλειας πληροφοριών ενός οργανισμού προκειμένου να ενσωματώσουν την εστίαση στην αλλαγή. Η διαχείριση αλλαγών απαιτείται σε έναν οργανισμό για τη βελτίωση της συμμόρφωσης των εργαζομένων με τις πολιτικές ασφάλειας πληροφοριών, τον τρόπο με τον οποίο προστατεύονται οι πληροφορίες και την ευαισθητοποίηση των εργαζομένων με σκοπό τη βελτίωση της κουλτούρας ασφάλειας πληροφοριών στον οργανισμό. Ο AlHogail (2015) υποστηρίζει ότι η αλλαγή της κουλτούρας ασφάλειας πληροφοριών σε έναν οργανισμό απαιτεί εισροή από τη διοίκηση που θα οδηγήσει σε μια τεράστια προσπάθεια να ανακατευθύνει τους υπαλλήλους προς την σωστή διαχείριση και αποφυγή λαθών.

Από όλα τα παραπάνω είναι εμφανές πως για να επιτευχθεί η οργανωσιακή αλλαγή ο οργανισμός πρέπει να εστιάσει στους ανθρώπους που είναι οι φορείς αυτής. Συνεπώς η ανώτερη διοίκηση και η ηγεσία διαδραματίζουν έναν εξαιρετικά σημαντικό ρόλο στη διαχείριση της αλλαγής.

Ο Rao (2015) ορίζει την ηγεσία ως τη διαδικασία που ουδετεροποιεί τις δυνάμεις εκείνες που δεν επιδιώκουν την αλλαγή και να πείσει τους ανθρώπους να συμμετάσχουν σε αυτή τη διαδικασία. Η ηγεσία είναι απαραίτητη προκειμένου να καλλιεργηθεί η κουλτούρα της αλλαγής σε έναν οργανισμό(Page και Schoder ,2018),καθώς επίσης και να παρακάμψει τα εμπόδια και τις δυσκολίες που προκύπτουν κατά τη διάρκεια της διαδικασίας της αλλαγής. Ένας ηγέτης που μπορεί να προωθήσει την οργανωσιακή αλλαγή δεν είναι τίποτα άλλο παρά κάποιος που μπορεί να καλλιεργήσει την ελπίδα και το όραμα της αλλαγής και κατέχει υψηλές επικοινωνιακές ιδιότητες.

1.6. Σκοπός της έρευνας

Ο σκοπός της παρούσας έρευνας είναι να διασφαλίσει το εάν και κατά πόσο η οργανωσιακή κουλτούρα επιδρά στην αλλαγή της διαχείρισης της ασφάλειας πληροφοριών. Υπό αυτό το πρίσμα είναι εξαιρετικά σημαντικό να διατυπωθούν οι ερευνητικές υποθέσεις που θα διασφαλίσουν την καλύτερη κατανόηση του θέματος και τη σύνδεση του με την υπάρχουσα βιβλιογραφία. Με λίγα λόγια η παρούσα εργασία έχει ως σκοπό να απαντήσει σε ερωτήματα που σχετίζονται με την συμμετοχή του ανθρώπινου παράγοντα και της κουλτούρας στην διαχείριση της ασφάλειας πληροφοριακών συστημάτων.

1.7. Ερευνητικές ερωτήσεις

Οι ερευνητικές ερωτήσεις είναι οι εξής:

1. Πως η ασφάλεια πληροφοριακών συστημάτων σχετίζεται με την οργανωσιακή κουλτούρα?
2. Πώς η διάχυση γνώσης σε έναν οργανισμό επηρεάζει ασφάλεια πληροφοριακών συστημάτων μέσα στην οργάνωση?
3. Πώς η εμπιστοσύνη επηρεάζει την ασφάλεια πληροφοριακών συστημάτων?
4. Πώς η αποτελεσματικότητα της οργάνωσης επηρεάζει την ασφάλεια πληροφοριακών συστημάτων?

1.8. Θεωρητικό μοντέλο

Λαμβάνοντας υπόψη την σχετική βιβλιογραφία το θεωρητικό μοντέλο της εργασίας θα αναπτυχθεί ως εξής :

1.9 Υποθέσεις έρευνας

<u>Η1. Υπάρχει σημαντικά στατιστική σχέση μεταξύ οργανωσιακής κουλτούρας και ISM.</u>

<u>Η2. Υπάρχουν σημαντικές σχέσεις μεταξύ οργανωσιακής κουλτούρας και εμπιστοσύνης</u>

<u>Η3. Υπάρχουν σημαντικές σχέσεις μεταξύ της οργανωσιακής κουλτούρας και της καινοτομίας</u>

<u>Η4. Υπάρχουν σημαντικές σχέσεις μεταξύ οργανωσιακής κουλτούρας και διάχυσης της γνώσης</u>

<u>Η5. Υπάρχουν σημαντικές σχέσεις μεταξύ αλλαγής οργανωσιακής κουλτούρας και αποτελεσματικότητας</u>

Κεφάλαιο 2: Βιβλιογραφική επισκόπηση

2.1. Η Οργανωσιακή κουλτούρα της ασφάλειας μέσω της διαχείρισης των αλλαγών.

Έχουν γίνει αρκετές προσπάθειες να διερευνηθεί η σημασία αλλά και το νόημα της οργανωσιακής κουλτούρας . Σε μια γενικότερη θεώρηση η οργανωσιακή κουλτούρα, μπορεί να οριστεί ως το σύνολο των πεποιθήσεων, των αξιών των κανόνων και των ηθών που διέπουν έναν οργανισμό (Stoyko, 2009). Εκτός αυτών, μπορεί να θεωρηθεί το συνολικό αποτέλεσμα των διεργασιών και των συζητήσεων που λαμβάνουν χώρα μέσα στα πλαίσια ενός οργανισμού. Μια άλλη έννοια που μπορεί να δοθεί στην οργανωσιακή κουλτούρα είναι ένα σύνολο παραδοχών, οι οποίες έχουν λειτουργήσει αποτελεσματικά στο παρελθόν και κατά συνέπεια μπορούν να θεωρηθούν έγκυρες και ωθούν τον οργανισμό προς μια δράση. Παρόλο που οι ορισμοί για την οργανωσιακή κουλτούρα ποικίλουν, είναι σαφές πως περιλαμβάνει ένα ενοποιημένο και κοινό σύστημα αξιών και ιδεολογιών. Μέσα από τη βιβλιογραφία φαίνεται πως η οργανωσιακή κουλτούρα αποκτά χαρακτηριστικά ενός ξεχωριστού οργανισμού, ο οποίος έχει δική του προσωπικότητα και αξίες. Παρομοιάζεται, λοιπόν, με την προσωπικότητα ενός ατόμου που έχει ξεχωριστή οντότητα. Η οργανωσιακή κουλτούρα περιλαμβάνει όλες εκείνες τις πεποιθήσεις, τις αξίες που δημιουργούν έναν κοινό κώδικα μέσα στον οποίο τα μέλη του οργανισμού συμπεριφέρονται με τέτοιο τρόπο προκειμένου να διασφαλιστεί η επιβίωση του μέσα σε ένα δυναμικό και διαρκώς μεταβαλλόμενο περιβάλλον (Den-on πληροφοριακό σύστημα, 1990; Schein, 1992). Στα πλαίσια του οργανισμού η κουλτούρα υποδεικνύει την εξιδανίκευση και ως εκ τούτου αποτελεί μέρος του συνόλου του οργανισμού που θα μπορούσε να προσομοιάζει σε μια μικρή κοινωνία. Συνεπώς υπάρχει μια αλληλεξάρτηση μεταξύ οργανισμού και κουλτούρας.

Η κατανόηση της οργανωσιακής κουλτούρας δεν είναι εύκολο έργο. Στην πράξη, μπορεί να αποδειχτεί ότι είναι ένα ρευστό, εξελισσόμενο φαινόμενο που επηρεάζεται τόσο από το περιβάλλον όσο και από άλλους οργανωτικούς παράγοντες, κάτι που καθιστά δύσκολη την κατανόηση του για τους εμπλεκόμενους και για τους τρίτους ,να το κατανοήσουν. Ένα μεγάλο μέρος της είναι άγνωστο στους ξένους και ταυτόχρονα αόρατο στους ίδιους τους συμμετέχοντες στην κουλτούρα του οργανισμού. Επιπλέον, είναι μια σημαντική επιρροή σκέψης και αντίληψης που είναι δύσκολο να διαφοροποιηθεί από τη δική τους φυσική κρίση και προσωπικότητα. Στην πραγματικότητα η οργανωσιακή κουλτούρα είναι ένα αόρατο πλαίσιο σκέψης που περιβάλλει το προσωπικό. Κάτι που αφομοιώνεται σταδιακά και ασυνείδητα , προς το συμφέρον τους αλλά και το συμφέρον του οργανισμού μέσα στον οποίο δρουν και εξελίσσονται (Da Veiga, 2016).

Η έννοια της οργανωσιακής κουλτούρας αντλείται από την ανθρωπολογία. Σχεδόν κάθε ερευνητής που έχει ασχοληθεί με το θέμα έχει διαφορετικές απόψεις και προσεγγίσεις για την έννοια της κουλτούρας . Οι ερευνητές δίνουν διαφορετικούς ορισμούς , για την έννοια της (Bali κ.ά., 1999). Ο Douglas (1985) επεσήμανε ότι η οργανωσιακή κουλτούρα αποτελεί το αναδυόμενο αποτέλεσμα των διαρκών διαπραγματεύσεων σε ότι αφορά τις αξίες, τις έννοιες και τις ιδιότητες μεταξύ των μελών του οργανισμού. Βασίζεται σε δύο βασικές κατηγοριοποιήσεις συμπεριλαμβανομένων των εσωτερικών / εξωτερικών προσανατολισμών και της ευελιξίας ελέγχου.

Οι Quinn και ο Spreitzer (1991) ανέπτυξαν μια τυπολογία για την αναγνώριση και την ταξινόμηση της οργανωσιακής κουλτούρα σε τέσσερις τύπους: α) ομαδική κουλτούρα, β) αναπτυξιακή κουλτούρα, γ) την ιεραρχική κουλτούρα δ) την ορθολογική κουλτούρα. Επιπλέον τόνισαν πως η οργανωσιακή κουλτούρα είναι πολύ πιθανόν να έχει χαρακτηριστικά αλλά και αξίες που να εμπεριέχουν και τα τέσσερα είδη οργανωσιακής κουλτούρας.

Με βάση την τυπολογία που ανέπτυξαν οι Quinn και Spreitzer για το πλαίσιο της οργανωσιακής κουλτούρας, ο Boggs (2004) ταξινόμησε την οργανωσιακή κουλτούρα σε τέσσερις διαφορετικούς τύπους. Δηλαδή, την κουλτούρα των κλώνων, την κουλτούρα ιεραρχίας, κουλτούρα adhocracy και κουλτούρα της αγοράς, για την εξέταση της εφαρμογής της συνολικής διαχείρισης της ποιότητας.

Επίσης ταξινόμησε την οργανωσιακή κουλτούρα σε τέσσερις τύπους βασισμένους σε τέσσερα πολιτιστικά χαρακτηριστικά(αποστολή, συνέπεια, προσαρμοστικότητα και συμμετοχή) που προέρχονται από αποτελεσματικές οργανώσεις. Υπάρχει μια γενική διαπίστωση, η οποία επισημαίνει πως η κουλτούρα μέσα στα πλαίσια της οργάνωσης είναι εξαιρετικά σημαντική και ευνοεί την αλλαγή και την ανάπτυξη μιας κουλτούρας ασφάλειας (Sizer και Clark 1989, Schwartzwalder 1999, Breidenbach 2000, vonSolms 2000, Andres και Fonseca 2000, Clark-Dickson 2001, Beynon 2001).Ωστόσο δεν υπάρχει ένας ξεκάθαρος ορισμός για το τι είναι η κουλτούρα της ασφάλειας.

Η κουλτούρα είναι ένας κρίσιμος παράγοντας για τις επιχειρήσεις ώστε να συνεχίσουν να ζουν, δεδομένου ότι οδηγεί την οργάνωση και τις ενέργειες της. Πολλά άρθρα εταιρικής ασφάλειας επισημαίνουν ότι η ασφάλεια είναι κατά κύριο λόγο ζήτημα διαχείρισης, αντί για τεχνολογικό, επειδή η τεχνολογία είναι ένα μέρος αυτής.Όμως, χωρίς μια βαθιά αλλαγή στην οργάνωσης της διαχείρισης της ασφάλειας που άμεσα επηρεάζει τις πρακτικές της, η αγορά προϊόντος για την επίτευξή της θα φέρει ελάχιστη ασφάλεια στην αντιμετώπιση των κινδύνων (vonSolms 2004). Εκτιμώντας πώς οι εργαζόμενοι σκέφτονται, ενεργούν και αισθάνονται, η κουλτούρα είναι σαν το "λειτουργικό σύστημα" του οργανισμού (Hagberg και Heifetz, 1997).Καταλήγοντας στο συμπέρασμα ότι το παράδειγμα της κουλτούρας είναι άρρηκτα συνδεδεμένο με τις υπάρχουσες πρακτικές και τους ρόλους σε έναν οργανισμό (Allenκαι Fifield, 1999). Πρωτοβουλίες για την υιοθέτηση νέων πρακτικών για την τεχνολογία των πληροφοριών, τη διεξαγωγή αναδιοργάνωσης των επιχειρηματικών διαδικασιών και την εφαρμογή οργανωτικών ή διαχειριστικών αλλαγών που συχνά εξαντλείται, γιατί οι άνθρωποι δεν θέλουν να αλλάξουν αυτό που έχουν συνηθίσει και υπάρχει έλλειψη κινήτρων για να αλλάξουν τις συνήθειες τους (Cooper, 1994, Allen και Fifield, 1999, Cooper, 2000; Melton κ.ά., 2006). Δεδομένου ότι οι νέες πολιτικές ασφάλειας συχνά έρχονται σε αντίθεση με τον τρόπο με τον οποίο οι εργαζόμενοι έχουν συνηθίσει να εργάζονται εδώ και χρόνια, η υλοποίηση για το σχέδιο με βάση τις πολιτικές ασφάλειας είναι εξαιρετικά δύσκολη. Συνεπώς, διερευνώντας διάφορα χαρακτηριστικά της οργανωσιακής κουλτούρας για τη διευκόλυνση των επιχειρήσεων στην υλοποίηση διοίκησης πληροφοριακών συστημάτων, για την οικοδόμηση κοινών αξιών, πεποιθήσεων και τα πρότυπα για τη διοίκησης πληροφοριακών συστημάτων με βάση την έννοια της οργανωσιακής νοοτροπίας, είναι εξαιρετικά σημαντικά για τους ερευνητές και τους επαγγελματίες.

Δεδομένου ότι υπάρχει ελλιπής έρευνα που ασχολείται με τη σχέση μεταξύ οργανωσιακής κουλτούρας και διοίκησης πληροφοριακών συστημάτων, η μελέτη μας προσπάθησε να γεμίσει το χάσμα για να ανακαλύψει μια τέτοια σχέση διερευνώντας πόσο οι διαφορετικοί τύποι οργανωσιακής νοοτροπίας επηρεάζουν την αποτελεσματικότητα της πρακτικής εφαρμογής διοίκησης πληροφοριακών συστημάτων.

Στην ασφάλεια υπάρχει συχνά η τάση να ευνοείται η σταθερότητα έναντι των αλλαγών. Η αλλαγή συχνά θεωρείται ως κάτι επιβλαβές ή ακόμα και ως κάτι απειλητικό, καθώς μπορεί να οδηγήσει στην εισαγωγή νέων κινδύνων ή στην ακύρωση, είτε στην παράκαμψη των ελέγχων σε υφιστάμενους κινδύνους. Ενώ η διαχείριση κινδύνων αποτελεί σημαντική πτυχή της ασφάλειας των πληροφοριών (Webb 2000), η καλή ασφάλεια είναι κάτι περισσότερο από έναν απλό μετριασμό των κινδύνων. Παρόλο που η αλλαγή θα πρέπει να γίνεται προσεκτικά, η ασφάλεια δεν είναι ποτέ απόλυτη και οι οργανισμοί πρέπει να διασφαλίσουν ότι η στάση της ασφάλειας τους δεν είναι στατική (Shinn 2000). Επιπλέον οι οργανισμοί πρέπει να συνειδητοποιήσουν ότι οι διαδικασίες και οι πρακτικές ασφάλειας πρέπει να βελτιώνονται και να γίνονται συνεχώς βήματα για τον εμπλουτισμό της οργανωσιακής ασφάλειας. Ένα άλλο κοινό πρόβλημα στους οργανισμούς είναι ότι πολλοί είναι έτοιμοι να αγνοήσουν ορισμένους από τους δευτερεύοντες κινδύνους για την ασφάλεια. Λίγοι οργανισμοί αντιμετωπίζουν τους κινδύνους αυτούς . Ως εκ τούτου, είναι προτιμότερη η πρόληψη, παρά η αντίδραση στις παραβιάσεις της ασφάλειας. Όπως ήδη αναφέρθηκε η αλλαγή της κουλτούρας στη διαχείριση, οι αλλαγές μια τυπικής οργάνωσης αναμένεται συχνά να επιφέρουν μια απροθυμία για την αλλαγή. Συχνά η αλλαγή επιφέρει αντίσταση καθώς υπάρχει προσκόλληση στην οργανωσιακή κουλτούρα και μια γενικότερη αντίσταση στην αλλαγή. Πολλοί από τους διαχειριστές των οργανισμών και ειδικότερα αυτοί που ασχολούνται με την ασφάλεια θα επιθυμούσαν να εισαγάγουν μια καλύτερη "κουλτούρα ασφάλειας". Στην πράξη, η δημιουργία μιας κουλτούρας ασφάλειας σημαίνει πολλά και διαφορετικά πράγματα, για παράδειγμα για κάποιους η δημιουργία της μπορεί να συνεπάγεται την πειθαρχία στην εφαρμογή των ελέγχων ασφάλειας ενώ για άλλους μπορεί απλώς να συνεπάγεται μία προσεκτική διαχείριση των πληροφοριών. Ωστόσο πρέπει να γίνει κοινά αποδεκτό πως η κουλτούρα της ασφάλειας αποτελεί ένα ευρύ φάσμα δυνατοτήτων. Ο σχεδιασμός της κουλτούρας ασφάλειας μπορεί να εστιάζει στην ενδυνάμωση και την εμπιστοσύνη γύρω από ένα κλίμα φόβου. Έτσι, η ανάπτυξη μιας κουλτούρας ασφάλειας συνεπάγεται τη δημιουργία εμπιστοσύνης και την έμπνευση μέσα στα πλαίσια του οργανισμού.

2.2 Συσχέτιση μεταξύ οργανωσιακής κουλτούρας και κουλτούρας ασφάλειας της πληροφορίας

Εδώ και χρόνια υπάρχει ένας συνεχής διάλογος σχετικά με την κουλτούρα διαχείρισης της πληροφορίας, καθώς αποτελεί ένα από τα πιο αμφιλεγόμενα θέματα στον ακαδημαϊκό κλάδο αλλά και στον κόσμο των επιχειρήσεων. Η έκταση που έχουν λάβει οι προβληματισμοί για την ανάπτυξη της κουλτούρας της πληροφορίας είναι εμφανής και από το γεγονός πως ο Οργανισμός για την Οικονομική Σταθερότητα και Συνεργασία (OECD) έχει εκδώσει ειδικές κατευθυντήριες γραμμές για τη δημιουργία κουλτούρας ασφάλειας της πληροφορίας (OECD, 2002, 2003, 2005). Πολλοί ερευνητές (όπως έχει ήδη αναφερθεί) υποστηρίζουν πως η κουλτούρα της ασφάλειας δεν μπορεί να νοηθεί ξεχωριστά από την οργανωσιακή κουλτούρα. (VonSolms, 2000; Schlienger, T.&Teufel, 2002, 2003b). Το ιδανικό σενάριο θα ήταν οι εργαζόμενοι να είναι σε θέση να ακολουθούν τις κατευθύνσεις που ορίζονται στην κουλτούρα ασφάλειας εθελοντικά χωρίς να υπάρχει παρέμβαση της διοίκησης και να την αντιμετωπίζουν σαν μέρος της οργανωσιακής κουλτούρας(Vroom & vonSolms, 2004; Thomson & vonSolms, 2005; Thomsonκ.α., 2006).

Ωστόσο είναι βέβαιο πως η πραγματικότητα απέχει σημαντικά από αυτό το ιδανικό σενάριο. Στην πραγματικότητα η κουλτούρα ασφάλειας μπορεί να συνδέεται με την οργανωσιακή κουλτούρα με διαφόρους τρόπους. Καταρχάς μπορεί να είναι εντελώς ξεχωριστή από αυτήν. Επιπλέον μπορεί να αποτελεί είτε μια υποκουλτούρα της είτε να είναι αναπόσπαστο κομμάτι αυτής, ή απλώς να περιέχεται μέσα σε αυτήν. Στην πρώτη περίπτωση η κουλτούρα ασφάλειας δεν αποτελεί ένα ζωτικό κομμάτι της οργανωσιακής κουλτούρας (Chiaκ.α., 2002; Knapp, Marshall, Rainer κ.α., 2004). Συχνά, οι οργανώσεις και τα μέλη συστημάτων ISM δεν εμπλέκονται, αλλά αν εμπλέκονται είναι στο ελάχιστο επίπεδο της εφαρμογής ασφάλειας σε οργανισμούς (Chia κ.α., 2002; Kohκ.α., 2005). Τα μέλη των οργανώσεων έχουν πολύ λίγη γνώση και δεν πιστεύουν ότι είναι δική τους αρμοδιότητα να εμπλέκονται με θέματα ασφάλειας. Αντίθετα θεωρούν πως είναι ευθύνη τους σε περιπτώσεις που προκύπτουν προβλήματα ασφάλειας. Οι οργανισμοί τείνουν συχνά να βλέπουν τις δαπάνες ασφάλειας ως κόστος και συχνά αγωνίζονται να κερδίσουν χρηματοδότηση για πρωτοβουλίες ασφάλειας (Shedden κ.α., 2006). Η φύση της σχέσης του πληροφοριακού συστήματος είναι η κατάσταση όπου το σύστημα ISM διαχωρίζεται εντελώς από την οργανωσιακή κουλτούρα.

Η ευαισθητοποίηση σχετικά με την ασφάλεια των οργανισμών είναι χαμηλή. Για να προχωρήσει το σύστημα, η κατάσταση στην οποία η δραστηριότητα ασφάλειας πληροφοριών χρειάζεται να φροντίζεται είναι μόνο από το τμήμα πληροφορικής και ασφάλειας, πάντα σε σχέση με τις αρχές πληροφοριακής ασφάλειας. Διάφορες μελέτες έχουν δείξει ότι η καθιέρωση μιας κουλτούρας ασφάλειας στον οργανισμό είναι απαραίτητη για την αποτελεσματικότητα σε ότι αφορά την ασφάλεια των πληροφοριών (Eloff και Solms, 2000). Ωστόσο, η κουλτούρα ασφάλειας δεν μπορεί να αξιολογηθεί μεμονωμένα από τη συνολική εταιρική κουλτούρα. Η κουλτούρα μπορεί να μην είναι ομοιόμορφη σε έναν οργανισμό, αλλά μπορεί να χωριστεί σε υποκουλτούρες. Οι υποκουλτούρες μπορούν να παρατηρηθούν σε διαφορετικά επίπεδα εργασίας, λειτουργίες και ρόλους μέσα σε έναν οργανισμό με αποτέλεσμα να υπάρχουν διαφορές στις στάσεις, τις πεποιθήσεις και τις αξίες μεταξύ των μελών ενός οργανισμού. Οι διαφορετικές υποκουλτούρες μπορεί να ευθυγραμμιστούν πλήρως ή μερικώς με την εταιρική κουλτούρα ή να είναι εντελώς ασυμβίβαστες με αυτήν. Επιπλέον, οι υποκουλτούρες μέσα σε έναν οργανισμό μπορεί να είναι προβληματικές και να επηρεάσουν αρνητικά την απόδοση όταν υπάρχουν για αυτές διαφορετικές προτεραιότητες και ατζέντες.

Η σχέση μεταξύ των διαχειριστών της ασφάλειας των πληροφοριών και άλλων εργαζομένων θα μπορούσε να θεωρηθεί σχέση μεταξύ των ηγετών και των υφισταμένων τους. Για να συνεχίσουν οι εργαζόμενοι σε έναν οργανισμό να συμμορφώνονται με τα συστήματα πληροφοριακής ασφάλειας, οι διαχειριστές ασφάλειας πληροφοριών προσπαθούν να τους πείσουν, να τους εμπνεύσουν και να τους παρακινήσουν. Ενώ οι διαχειριστές ασφάλειας πληροφοριών δεν έχουν άμεσα δικαιώματα να δίνουν διαταγές, να παρακολουθούν και να επιπλήττουν άλλους υπαλλήλους, πρέπει να επιβάλλουν έναν κοινό κώδικα ασφάλειας.

Προτάθηκε η ανάγκη μετατόπισης από την συναλλακτική ηγεσία στην μετασχηματιστική ηγεσία. Η μετασχηματιστική ηγεσία έχει αναζωογονήσει τις αξίες υψηλότερης τάξης και έχει αυξήσει τις προσδοκίες των μελών, έτσι ώστε να προσδιορίσουν την αποστολή/το όραμά τους, να είναι καλύτεροι ώστε να εργαστούν για να αποδώσουν στο μέγιστο το έργο τους πέρα από τις βασικές προσδοκίες και τις απλές συναλλαγές. Η μετασχηματιστική ηγεσία απευθύνει έκκληση στις ηθικές αξίες των μελών σε μια προσπάθεια να αυξήσουν τη συνείδησή τους για ηθικά ζητήματα και να κινητοποιήσουν την ενέργεια και τους πόρους τους για τη μεταρρύθμιση των θεσμών.

Η μετασχηματιστική ηγεσία έχει θετική σχέση με την αποτελεσματικότητα της ηγεσίας και τα οργανωτικά αποτελέσματα σε διάφορους τύπους οργανισμών, καταστάσεων και πολιτισμών. Οι επιπτώσεις της μετασχηματιστικής ηγεσίας πραγματοποιούνται σε σχέση με τα αποτελέσματα των επιδόσεων. Οι ερευνητές αναφέρουν ότι η συμπεριφορά της μετασχηματιστικής ηγεσίας αποτελείται από τα εξής τέσσερα χαρακτηριστικά, το εμπνευσμένο κίνητρο, την εξιδανικευμένη επιρροή, την εξατομικευμένη εξέταση και την πνευματική διέγερση. Το εμπνευσμένο κίνητρο σημαίνει την παρουσίαση και τη δημιουργία συμβόλων και συναισθηματικών επιχειρημάτων, την επίδειξη αισιοδοξίας και ενθουσιασμού και ακόμη ένα ελκυστικό όραμα. Η εξιδανικευμένη επιρροή περιλαμβάνει συμπεριφορές όπως η επίδειξη ηθικών προτύπων, η αυτοθυσία για την ομάδα και το σύνολο ενός προσωπικού μοντέλου. Εξατομικευμένη εξέταση παρέχει άτομα με προπόνηση, ενθάρρυνση, και υποστήριξη. Η πνευματική διέγερση περιέχει συμπεριφορά που δίνει μια πρόκληση στα άτομα να εξετάσουν τα προβλήματα με μια νέα προοπτική. Προηγούμενες έρευνες υποδεικνύουν ότι η μετασχηματιστική ηγεσία έχει συσχετιστεί θετικά με την υψηλή απόδοση των εργαζομένων και την αποτελεσματικότητα της ηγεσίας.

Η έννοια της οργανωσιακής κουλτούρας ορίστηκε διαφορετικά από πολλούς μελετητές. Η κουλτούρα της οργάνωσης είναι άμεσο προϊόν των συνεχιζόμενων αλληλεπιδράσεων σχετικά με τις έννοιες, τις αξίες και τις ιδιότητες μεταξύ των μελών ενός οργανισμού. Με βάση δύο άξονες ταξινόμησης, όπως ο προσανατολισμός του εσωτερικού/εξωτερικού περιβάλλοντος και ο προσανατολισμός ευελιξίας/ελέγχου, δημιουργείται ένα μοντέλο που προσδιορίζει και ταξινομεί την οργανωσιακή κουλτούρα σε τέσσερις τύπους: την ομαδική κουλτούρα, την αναπτυξιακή κουλτούρα, την ιεραρχική κουλτούρα και την ορθολογική κουλτούρα. Κατευθύνοντας τον τρόπο με τον οποίο τα μέλη της οργάνωσης σκέφτονται και ενεργούν. Η κουλτούρα είναι από τα θεμελιώδη συστήματα της οργάνωσης και είναι στενά συνδεδεμένη με τους υπάρχοντες ρόλους και πρακτικές σε έναν οργανισμό.

2.3. Η ασφάλεια των πληροφοριών και η οργανωσιακή απόδοση

Όπως έχει ήδη αναφερθεί η ανάπτυξη των δικτύων και η ευρεία χρήση του διαδικτύου αυξάνει τον όγκο των υπηρεσιών του οργανισμού που βασίζονται σε αυτό. Μια τέτοια αλλαγή στον τρόπο που διεξάγονται πλέον οι δραστηριότητες στα πλαίσια του οργανισμού συνεπάγεται και μια αύξηση της σημασίας των δραστηριοτήτων ασφάλειας πληροφοριών. Επιπλέον, οι οργανισμοί- συμπεριλαμβανομένων των δημόσιων οργανισμών και εταιριών- υιοθετούν ποικίλες λύσεις προστασίας της πληροφορίας και σχεδιάζουν συστηματικά μέτρα για την προστασία των πληροφοριακών τους περιουσιακών στοιχείων από απειλές και κινδύνους, σε μια προσπάθεια να επενδύσουν στις δραστηριότητές τους για την ασφάλεια των πληροφοριών. Αυτό υποδηλώνει ότι οι επενδύσεις στην ασφάλεια των πληροφοριών από εταιρείες και άλλους οργανισμούς έχουν πλέον εδραιωθεί ως κλειδί για την επιτυχία των δραστηριοτήτων τους. Αυτό οφείλεται στο γεγονός ότι, ένας οργανισμός θεωρεί τις δραστηριότητες ασφάλειας πληροφοριών όχι ως επένδυση αλλά ως κόστος, το οποίο αποτελεί τον μεγαλύτερο φραγμό στην αποτελεσματικότητα της ασφάλειας των πληροφοριών. Τα μέλη ενός οργανισμού δεν έχουν ούτε την κατάλληλη συνειδητοποίηση ούτε μοιράζονται την αναγκαιότητα δραστηριοτήτων ενημέρωσης για την ασφάλεια των πληροφοριών, αλλά ασχολούνται με τις δραστηριότητες ασφάλειας ως κάτι περισσότερο από ενοχλητικές και ακατάλληλες διαδικασίες, παραλείποντας έτσι να παρακινηθούν να διεξάγουν δραστηριότητες προστασίας των πληροφοριών.

Όσον αφορά το στόχο και την αναγκαιότητα υιοθέτησης και διαχείρισης των τεχνολογιών της πληροφορίας, τα μέλη μιας οργάνωσης έχουν μεγάλη επίγνωση της ανάγκης και των επιδόσεων, αλλά έχουν χαμηλή επίγνωση της αναγκαιότητας της αντίστοιχης επένδυσης. Έτσι δεν διευκολύνουν τέτοιες δραστηριότητες ασφάλειας πληροφοριών και καταλήγουν να θεωρούνται εμπόδιο.

Στον χρηματοπιστωτικό κλάδο, συμπεριλαμβανομένων των κινητών αξιών και των τραπεζών, οι δραστηριότητες για την ασφάλεια των πληροφοριών καθίστανται όλο και πιο σημαντικές. Στις χρηματοπιστωτικές επιχειρήσεις, οι οποίες λειτουργούν με βάση τα συστήματα πληροφοριών, οι δραστηριότητες ασφάλειας των πληροφοριών είναι απαραίτητες για τη διαχείριση των συναλλαγών και τη διαιώνιση των επιχειρήσεων. Συγκεκριμένα, στον τομέα της διαχείρισης των συναλλαγών των υπηρεσιών πρέπει να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα της ασφάλειας των πληροφοριών.

Η ασφάλεια αναφέρεται στη διαδικασία με την οποία προστατεύονται όλα τα περιουσιακά στοιχεία από κινδύνους ή απώλειες. Συγκεκριμένα, η ασφάλεια πληροφοριών αφορά τη διαδικασία με την οποία προστατεύονται οι πληροφορίες από εσωτερικές ή εξωτερικές απειλές ή κινδύνους. Έτσι, συνεχίζει να αναπτύσσεται η ασφάλεια των πληροφοριών. Οι στόχοι της ασφάλειας των πληροφοριών περιλαμβάνουν όχι μόνο τις διαδικασίες και τις πληροφορίες αλλά και τις τεχνολογίες που χρησιμοποιούνται για την επεξεργασία και την αποθήκευση πληροφοριών. Τις οργανωτικές δομές και τους ανθρώπινους πόρους που ασχολούνται με την επεξεργασία, διατήρηση, διαχείριση και τις δραστηριότητες επεξεργασίας πληροφοριών. Συγκεκριμένα, οι χρηματοπιστωτικές επιχειρήσεις αντιμετωπίζουν πολλές εισβολές και ατυχήματα λόγω της κακής διαχείρισης προσωπικών πληροφοριών και των πληροφοριών σχετικά με την επεξεργασία συναλλαγών και την εργασία. Δεδομένης της ιδιαιτερότητας των χρηματοπιστωτικών επιχειρήσεων, η οποία συνδέεται στενά με τα προσωπικά περιουσιακά στοιχεία, ο βαθμός συνειδητοποίησης και διαχείρισης αυτής της ασφάλειας πληροφοριών έχει τεράστιο αντίκτυπο στην εμπιστοσύνη των πελατών.

2.4. Προσεγγίσεις και θεωρίες στη διαχείριση αλλαγής

Η οργανωσιακή κουλτούρα όπως ήδη αναφέρθηκε μπορεί να αποτελέσει το " πρίσμα μέσω του οποίου οι εργαζόμενοι ενός οργανισμού μαθαίνουν να ερμηνεύουν το περιβάλλον" (Jex και Britt, 2008). Αποτελεί τον πυρήνα για την καθοδήγηση της συμπεριφοράς των εργαζομένων, για παράδειγμα, να διασφαλίσει ότι όλα τα αιτήματα πρόσβασης εγκρίνονται και τεκμηριώνονται ή ότι όλα τα εργασιακά τους εργαλεία προστατεύονται με κωδικό πρόσβασης. Μια οργανωσιακή κουλτούρα που έχει αναπτυχθεί με την πάροδο του χρόνου είναι πια παγιωμένη και θεωρείται πως είναι δύσκολο να αλλάξει. Αυτό όμως εξαρτάται από τις αντιλήψεις των εργαζομένων που μπορεί να χρειαστεί να αλλάξουν (Jex και Britt, 2008). Ο Lewin (1947) εισήγαγε την έννοια της προγραμματισμένης αλλαγής (Bojeetal., 2012). Εισήγαγε μια προσέγγιση τριών βημάτων που ονομάζεται "θεωρία αλλαγής"(Leban και Stone, 2008), όπου το βήμα "ξεπάγωμα" χρησιμοποιείται για να ξεπαγώσει την υπάρχουσα συμπεριφορά μέσω επίδειξης ή αποσαφήνισης του προβλήματος. Αυτό ακολουθείται από τη δημιουργία μιας επιθυμίας αλλαγής μέσω των κινητήριων δυνάμεων και έτσι να "μετακινηθεί ή να αλλάξει" στην επιθυμητή συμπεριφορά, η οποία πρέπει να "παγώσει" ξανά. Η έκθεση ευαισθητοποίησης για την ασφάλεια των πληροφοριών που δημοσιεύθηκε από το φόρουμ Ασφάλειας Πληροφοριών (ISF) (2002) απαριθμεί μια σειρά κινητήριων δυνάμεων και λόγων αντίστασης που μπορούν να διαδραματίσουν ρόλο σε αυτή τη διαδικασία. Το ISF εξηγεί τη διαδικασία χρησιμοποιώντας το παράδειγμα μιας νέας πολιτικής που απαιτεί από τους υπαλλήλους να διατηρούν τα δελτία ταυτότητάς μαζί τους για να εισέρχονται και να εξέρχονται από διάφορες περιοχές σε ένα κτίριο. Ένας τέτοιος κανόνας μπορεί να αποτελέσει λόγος σύγκρουσης από υπαλλήλους που αντιτίθενται σε αυτό. Με την εισαγωγή θετικών κινητήριων δυνάμεων, όπως θα μπορούσε να είναι για παράδειγμα, οι εκπτώσεις κυλικείων για τους κατόχους καρτών, οι εργαζόμενοι μπορεί να συνειδητοποιήσουν ότι θα επωφεληθούν από την τήρηση της πολιτικής και θα αρχίσουν να κινούνται προς την επιθυμητή συμπεριφορά. Πρόκειται για μια αποτελεσματική προσέγγιση στο πλαίσιο της ασφάλειας των πληροφοριών, όπου οι εργαζόμενοι πρέπει συνεχώς να προσαρμόζονται στις τεχνολογικές αλλαγές και όπου πρέπει να καλλιεργούνται ασφαλείς συνήθειες (Karlsson, κ.α., 2018).

Η αντίσταση των εργαζομένων, η οποία υπογραμμίζεται από την οργανωσιακή κουλτούρα, πρέπει να αλλάξει σε θετική αποδοχή της αλλαγής μέσω της χρήσης προγραμματισμένων κινητήριων δυνάμεων που υλοποιούνται προληπτικά από τη διοίκηση [φόρουμ Ασφάλειας Πληροφοριών (ISF), 2002].

Έχοντας ως εφαλτήριο την προσέγγιση του Lewin (1951), έχουν αναπτυχθεί διάφορες θεωρητικές προσεγγίσεις καθώς και μοντέλα διαχείρισης της αλλαγής. Το μοντέλο συσχέτισης του Nadler και του Tushman (1980) ενσωματώνει την εστίαση στην οργανωσιακή απόδοση και τον ρόλο που διαδραματίζει η ηγεσία στη διαδικασία. Υποστηρίζουν ότι οι οργανισμοί είναι παρόμοιοι με τα συστήματα που πρέπει να είναι σε συμφωνία για να εξασφαλίσουν τη βέλτιστη απόδοση. Προς υποστήριξη του μοντέλου συσχέτισης, οι Nadler και Tushman (1980) προτείνουν μια διαδικασία που περιλαμβάνει πέντε στάδια, δηλαδή τη διάγνωση (Στάδιο 1), την προετοιμασία (Στάδιο 2), την εφαρμογή της Αλλαγής (Στάδιο 3), την εδραίωση της Αλλαγής (Στάδιο 4) και τη διατήρηση της Αλλαγής (Στάδιο 5) (Leban και Stone, 2008). Αν και το μοντέλο τους παρουσιάζει μια δομημένη προσέγγιση, μπορεί να περιλαμβάνει μια μακρά και δαπανηρή διαδικασία για την εφαρμογή (Basu, 2018).

Στη συνέχεια, έρχεται η ανάπτυξη του πολύ σημαντικού ερευνητικού έργου του Kotter (1996, 2006) περιγράφοντας ένα μοντέλο διαχείρισης αλλαγών οκτώ σταδίων που επικεντρώνεται στις διαδικασίες που πρέπει να ακολουθήσουν για την πραγματοποίηση της αλλαγής:

- Δημιουργία μεγαλύτερης αίσθησης επείγουσας ανάγκης
- Σχηματισμός μιας καθοδηγητικής συνέργειας
- ανάπτυξη ενός οράματος μετασχηματισμού
- επικοινωνία του οράματος μετασχηματισμού
- ενθάρρυνση των εργαζόμενων να δράσουν
- δημιουργία βραχυπρόθεσμων στόχων
- εδραίωση βελτιώσεων και δημιουργία περισσότερων αλλαγών
- θεσμοθέτηση νέων προσεγγίσεων στην κουλτούρα (Kotter, 2006, Leban και Stone, 2008).

Το μοντέλο του Kotter (2006) έχει σχεδιαστεί έχοντας κατά νου μια στρατηγική άποψη και είναι ένα από τα πιο ευρέως χρησιμοποιούμενα μοντέλα, παρόλο που δεν έχει τακτική εστίαση (Leban και Stone, 2008). Μια κριτική του μοντέλου του Kotter είναι η έλλειψη ολοκλήρωσης της διαχείρισης έργων (Kazmi και Naarananoja, 2014).

Υπάρχουν πολλά άλλα μοντέλα για τη διαχείριση της αλλαγής που έχουν προκύψει, όπως για παράδειγμα, η θεωρία των περιορισμών του Goldratt (1999) (TOC) (Kazmi και Naarananoja, 2014) και το μοντέλο Kaizen (Plan – Do – Check – Act) (Plunkett και Attner, 1994). Τα επιχειρήματα , βάσει αυτών των μοντέλων, είναι ότι εφαρμόζονται σε μεγαλύτερες περιόδους και έχουν μεγαλύτερο χρονικό πλαίσιο επιπτώσεων (Kazmi και Naarananoja, 2014). Αυτή η κριτική πρέπει να εξεταστεί υπό το πρίσμα του έργου του Kotter, το οποίο τονίζει ότι η αλλαγή απαιτεί σημαντικό χρονικό διάστημα, ειδικά όταν κάποιος στοχεύει να την ενσωματώσει στην κουλτούρα ενός οργανισμού (Kotter, 2006). Άλλα μοντέλα διαχείρισης αλλαγών που πρέπει να ληφθούν υπόψη είναι αυτά των Kanter, Stein και Jick (1992) και Luecke (2003). Αυτά τα δύο μοντέλα ενσωματώνουν μια έμφαση στην ηγεσία και τον εντοπισμό της ανάγκης για αλλαγή (Abdulkadhimetal., 2015). Ο Todnem (2005) εξέτασε κριτικά τα μοντέλα διαχείρισης αλλαγών το 2005. Έκανε μια ολοκληρωμένη σύγκριση του έργου του Kanter, Kotter και Luecke εξετάζοντας τα ως αναδυόμενα μοντέλα, με αντίθετες απόψεις από τους ερευνητές. Από τότε έχουν προκύψει νέες προοπτικές και μοντέλα για τη διαχείριση της αλλαγής. Ο ιστότοπος ενεργοποίησης αλλαγών απαριθμεί τουλάχιστον 16 διαφορετικά μοντέλα ή προσεγγίσεις διαχείρισης αλλαγών για τα οποία υπάρχουν διαθέσιμα εργαλεία (Ενεργοποίηση αλλαγής, 2018). Τρεις από τις προσεγγίσεις σχετίζονται με το έργο του Prosci, το οποίο δεν είχε ακόμη αναπτυχθεί όταν ο Todnem έκανε την αναθεώρησή του για τη διαχείριση της αλλαγής.

Το μοντέλο ADKAR (Εικόνα 2)που αναπτύχθηκε από την Prosci δημοσιεύθηκε με τη μορφή εγχειριδίου το 2006 (Hiatt, 2006). Σύμφωνα με το μοντέλο, ο Prosci ανέπτυξε μια προσέγγιση διαχείρισης αλλαγών που αποτελείται από τρεις φάσεις, δηλαδή την προετοιμασία για αλλαγή, τη διαχείριση της αλλαγής και την μετά-παρέμβαση. Αυτές οι τρεις φάσεις αντιστοιχούν στη θεωρία του Lewin (1951), αλλά επιπλέον, ενσωματώνονται λεπτομερέστερα βήματα σε κάθε φάση. Κατά τη διάρκεια της Φάσης Ι, ορίζεται η στρατηγική διαχείρισης αλλαγής, προετοιμάζεται η ομάδα και αναπτύσσεται το μοντέλο χορηγίας. Στη φάση ΙΙ, η διαχείριση αλλαγής προκύπτει μέσω σχεδίων οργάνωσης και υλοποίησης.

Το μοντέλο ADKAR, το οποίο χρησιμεύει ως μοντέλο διαχείρισης αλλαγών προσανατολισμένο στο στόχο που μπορεί να εφαρμοστεί σε προσωπικό ή οργανωτικό πλαίσιο, ενσωματώνεται σε αυτή τη φάση. Επικεντρώνεται στους πέντε βασικούς τομείς που συνθέτουν το ακρωνύμιο ADKAR, δηλαδή την ευαισθητοποίηση (της ανάγκης για αλλαγή), την επιθυμία (για υποστήριξη και συμμετοχή στην αλλαγή), τη γνώση (για τον τρόπο αλλαγής), την ικανότητα (για την εφαρμογή της αλλαγής) και την ενίσχυση (για τη διατήρηση της αλλαγής). Η τελευταία φάση επικεντρώνεται στην μετα-παρέμβαση. Σε αυτή τη φάση, συλλέγονται και αναλύονται ανατροφοδοτήσεις, διαγιγνώσκονται κενά και εφαρμόζονται διορθωτικές ενέργειες.

Εικόνα 1: Μοντέλο αλλαγής ADKAR

Η σημερινή κατάσταση, η οποία πρέπει να αλλάξει (δηλαδή να "αποψυχθεί" όπως αναφέρεται) σύμφωνα με τη θεωρία του Lewin (1951), αντιστοιχεί στις φάσεις συνειδητοποίησης και επιθυμίας του Prosci. Οι φάσεις της γνώσης και της ευαισθητοποίησης αντιστοιχούν στην μετάβαση της "κίνησης ή αλλαγής", όπως αναφέρεται σε αυτήν ο Lewin. Η φάση ενίσχυσης βοηθά στη συμπεριφορά "επαναψύξης". Αυτά τα βήματα είναι εύκολο να μετατραπούν σε σχέδια διαχείρισης έργων και να επικεντρωθούν έντονα στους υπαλλήλους και να αλλάξουν τη συμπεριφορά τους. Η προσέγγιση μπορεί να εφαρμοστεί σε μια ευρεία ποικιλία αλλαγών, συμπεριλαμβανομένης μιας αλλαγής νοοτροπίας ασφάλειας πληροφοριών. Από την άποψη της οργανωσιακής αλλαγής, η Prosci (2013) διαπιστώνει ότι οκτώ στα δέκα έργα ακολουθούν μια δομημένη προσέγγιση στη διαχείριση των αλλαγών, η οποία τους βοηθά με προγραμματισμένες παρεμβάσεις να αποκομίσουν βιώσιμες αλλαγές στη συμπεριφορά. Ως εκ τούτου, είναι αναγκαίο, από την άποψη της ασφάλειας των πληροφοριών, να ακολουθηθεί μια δομημένη προσέγγιση για την αλλαγή μιας νοοτροπίας ασφάλειας των πληροφοριών, ώστε να ελαχιστοποιηθεί ο κίνδυνος που θα μπορούσε να θέσει η ανθρώπινη συμπεριφορά (δηλαδή σφάλμα ή αμέλεια) στην προστασία των πληροφοριών.

Το μοντέλο ADKAR μπορεί να χρησιμοποιηθεί αποτελεσματικά για να διαπιστωθεί εάν οι εργαζόμενοι είναι έτοιμοι να αλλάξουν. Το μοντέλο μπορεί επίσης να χρησιμοποιηθεί για τον καθορισμό αντίστοιχων σχεδίων δράσης. Οι Kazmi και Naarananoja (2014) χρησιμοποίησαν το μοντέλο ADKAR ως το προτιμώμενο μοντέλο στην έρευνά τους για ένα έργο υγειονομικής περίθαλψης στη Φινλανδία. Το βρήκαν αποτελεσματικό στον εντοπισμό προβληματικών περιοχών και το προσάρμοσαν ανάλογα για να εφαρμόσουν την αλλαγή αποτελεσματικά και αποδοτικά. Το μοντέλο ADKAR έχει επίσης εφαρμοστεί με επιτυχία σε άλλα σενάρια, για παράδειγμα αλλαγές στις δομές διακυβέρνησης σε νοσοκομειακό περιβάλλον του Τέξας (Sheperdetal., 2014) και ανάλυση των ικανοτήτων διαχείρισης αλλαγών των διευθυντών σχολείων στο Πακιστάν (Kiani και Shah, 2014).

Οι πτυχές που λείπουν από την προσέγγιση και το μοντέλο Prosci είναι πώς πρέπει να γίνει κατανοητή η αλλαγή από την σκοπιά της κουλτούρας ασφάλειας πληροφοριών. Δηλαδή, τι είδους αλλαγή απαιτείται και ποιες πληροφορίες πρέπει να συγκεντρωθούν πριν από την πρώτη φάση (προετοιμασία για αλλαγή).

Οι πληροφορίες για όλες αυτές τις πτυχές απαιτούνται για τον καθορισμό της στρατηγικής, για τον προσδιορισμό του ποιος πρέπει να συμμετάσχει στην αλλαγή, για την κατανόηση του επείγοντος χαρακτήρα της αλλαγής και για την ανάπτυξη των πτυχών που απαιτούνται για την αντιμετώπιση των πέντε τομέων του ADKAR. Η έννοια της οργανωσιακής ανάπτυξης (OD) μπορεί να ενσωματωθεί για την αντιμετώπιση αυτού του περιορισμού, καθώς ακολουθεί ένα σχέδιο έρευνας δράσης στο οποίο χρησιμοποιείται ένας κύκλος εκτιμήσεων και αξιολογήσεων για την επίλυση ενός προβλήματος (Bojeetal , 2012; Berry και Houston, 1993; Coghlan και Brydon-Miller, 2014). Μπορεί να εφαρμοστεί για να γίνει κατανοητό το περιβάλλον όπως είναι ,από την άποψη της κουλτούρας ασφάλειας πληροφοριών και να αξιολογήσει τις επιπτώσεις της αλλαγής επαναλαμβάνοντας τη διάγνωση, συγκρίνοντας τα αποτελέσματα για την παρακολούθηση της βελτίωσης διαχειρίζοντας και κατευθύνοντας την αλλαγή με συνέπεια. Αυτό αντιστοιχεί με την προσέγγιση του μοντέλου Kaizen, όπου διεξάγεται επίσης αξιολόγηση ως μέρος της φάσης ελέγχου για να εξασφαλιστεί η συνεχής βελτίωση.

Η επόμενη ενότητα περιγράφει την προτεινόμενη προσέγγιση αλλαγής νοοτροπίας ασφάλειας πληροφοριών υπό το πρίσμα της παραπάνω συζήτησης.

2.5. Η αλλαγή της κουλτούρας της ασφάλειας πληροφοριών

Μια προσέγγιση διαχείρισης της αλλαγής σε μια κουλτούρα ασφάλειας πληροφοριών είναι σημαντικό να βασίζεται σε υπάρχοντα μοντέλα ή προσεγγίσεις διαχείρισης αλλαγών, καθώς αυτά τα μοντέλα έχουν ήδη χρησιμοποιηθεί με επιτυχία στις κοινωνικές επιστήμες. Είναι επίσης σημαντικό, να γίνει κατανοητή η υπάρχουσα κουλτούρα ασφάλειας των πληροφοριών σε έναν οργανισμό πριν από την εισαγωγή οποιωνδήποτε αλλαγών. Επομένως, πρέπει να διεξαχθεί αξιολόγηση για να κατανοηθεί το περιβάλλον όπως είναι και να προσδιοριστούν οι συμπεριφορές που πρέπει να αλλάξουν. Μόλις γίνει κατανοητό, είναι σημαντικό να χρησιμοποιηθούν προγραμματισμένες παρεμβάσεις για την αλλαγή της κουλτούρας. Αυτό απαιτεί συγκεκριμένες ενέργειες που μπορεί να υλοποιήσει ο οργανισμός για να οδηγήσει επιτυχώς την αλλαγή. Τέλος, μετά τις παρεμβάσεις, ο οργανισμός πρέπει να επανεξετάσει εάν οι ενέργειες είχαν το επιθυμητό αντίκτυπο και εάν είχαν ως αποτέλεσμα μια θετική εξέλιξη για τον οργανισμό. Η προσέγγιση της διαχείρισης αλλαγής της ασφάλειας πληροφοριών κατασκευάζεται ενσωματώνοντας τις ακόλουθες πτυχές από τις υφιστάμενες προσεγγίσεις διαχείρισης αλλαγών που εξετάζονται στην ενότητα 3. Την θεωρία του Lewin σχετικά με τη «δέσμευση», τη «μετακίνηση» και την «αναζωογόνηση» συμπεριφοράς (που αντιστοιχεί στο ADKAR). Το μοντέλο ADKAR, έτσι ώστε η πρακτική εφαρμογή της θεωρίας του Lewin να μπορεί να παρακολουθείται μέσω λεπτομερών τακτικών και επιχειρησιακών δραστηριοτήτων. Την προσέγγιση της Prosci για τη διαχείριση αλλαγών, ώστε οι φάσεις της διαχείρισης της αλλαγής να μπορούν να διαρθρωθούν σε ένα πρόγραμμα διαχείρισης οργανωσιακής αλλαγής. Τη διαδικασία ΟΕ, έτσι ώστε να μπορεί να διεξαχθεί μια αξιολόγηση ως προς την ταυτοποίηση των κενών και να καθοριστεί το σκεπτικό της αλλαγής που μπορεί να τροφοδοτήσει τη στρατηγική διαχείρισης αλλαγής. Επιπλέον, να μπορεί να παρακολουθείται συνεχώς η αλλαγή, ώστε να κατευθύνεται και να διατηρείται. Η προσέγγιση διαχείρισης αλλαγής της ασφάλειας πληροφοριών, επικεντρώνεται στη μετάβαση σε μια θετική ή επιθυμητή νοοτροπία ασφάλειας των πληροφοριών σε έναν οργανισμό για να βοηθήσει στην άμβλυνση των κινδύνων που ενέχει το ανθρώπινο στοιχείο για την προστασία τους.

2.5.1. Ανταλλαγή γνώσεων

Η ανταλλαγή γνώσεων μπορεί να είναι πολύ επωφελής για τους οργανισμούς. Ένα παράδειγμα είναι η περίπτωση της Toyota. Ο έμπορος αυτοκινήτων σημείωσε επιτυχία μέσω της ανταλλαγής γνώσεων με άλλους οργανισμούς στην αλυσίδα εφοδιασμού της (Dyer&Nobeoka, 2000, σελ. 316). Η Toyota μοιράστηκε γνώσεις σχετικά με τις λιτές τεχνικές παραγωγής στην αλυσίδα εφοδιασμού της, με αποτέλεσμα ανώτερη παραγωγικότητα (Dyer&Nobeoka, 2000). Ως αποτέλεσμα αυτής της ανταλλαγής γνώσεων, η Toyota παρουσίασε σταθερή ανάπτυξη από το 1965 έως το 1990 (Dyer&Nobeoka, 2000). Οι Bijetal, Song και Weggeman (2003) μελέτησαν παράγοντες που επηρεάζουν την ανταλλαγή γνώσεων σε στρατηγικές επιχειρηματικές μονάδες (SBUs). Οι Bijetal, Song και Weggeman (2003) δοκίμασαν 10 παράγοντες στη μελέτη τους, συμπεριλαμβανομένης της ατομικής δέσμευσης και της συμπεριφοράς ανάληψης κινδύνων, σε 277 SBUs εταιρειών τεχνολογίας με έδρα τις ΗΠΑ για να προσδιορίσουν ποιοι παράγοντες (εάν υπάρχουν) είχαν επίδραση στην ανταλλαγή γνώσεων. Τα ευρήματα της μελέτης έδειξαν ότι με την εξαίρεση δύο παραγόντων (χρήση της τεχνολογίας των πληροφοριών και οργανωσιακή απόλυση), υπήρχε εμπειρική υποστήριξη ότι καθένας από τους παράγοντες συσχετίστηκε θετικά με την ανταλλαγή γνώσεων. Κάθε οργανισμός έχει τη δική του μοναδική κουλτούρα που αποτελεί τη βάση για την κατανόηση της πραγματικότητας, τη λήψη αποφάσεων και την επιλογή του καλύτερου τρόπου δράσης στον οργανισμό. Αυτή η κουλτούρα μπορεί είτε να διευκολύνει τη μεταφορά γνώσης είτε να την εμποδίσει, ανάλογα με τις βασικές αξίες στις οποίες βασίζεται. Δεν υπάρχει κανένα μοντέλο κουλτούρας που να είναι ιδανικό για την υποστήριξη της μεταφοράς γνώσης. Το πιο σημαντικό, είναι πως ορισμένα χαρακτηριστικά του πολιτισμού εξαρτώνται από τη στρατηγική που επιλέγει ένας οργανισμός για τη διαχείριση της γνώσης. Σύμφωνα με τους Hansen, Nohria, &Tierney (1999), υπάρχουν δύο βασικές προσεγγίσεις για την ανταλλαγή πολύτιμων γνώσεων σε έναν οργανισμό, η στρατηγική κωδικοποίησης και η στρατηγική εξατομίκευσης. Το πρώτο συνδέεται στενά με την επαναχρησιμοποίηση ρητής γνώσης που κωδικοποιείται από υπαλλήλους και αποθηκεύεται σε ηλεκτρονικές βάσεις δεδομένων. Απαιτεί μια τεράστια επένδυση σε τεχνολογίες πληροφορικής που παρέχουν αποτελεσματικά εργαλεία για τη συσσώρευση οργανωτικών γνώσεων και για να καταστήσουν τους προσβάσιμους πόρους, για κάθε μέλος του οργανισμού, ακόμη και χωρίς την επαφή με ένα άτομο που την κωδικοποίησε (Hansenetal, 1999; Hansen & Nørbjerg, 2005).

Η πιο σημαντική πτυχή της στρατηγικής εξατομίκευσης είναι οι σχέσεις μεταξύ υπαλλήλων που μοιράζονται τη σιωπηρή τους γνώση με άλλους προκειμένου να δημιουργήσουν την καταλληλότερη λύση των αναδυόμενων προβλημάτων. Ο ρόλος της πληροφορικής και της ασφάλειας των πληροφοριακών συστημάτων είναι εντελώς διαφορετικός εδώ, καθώς χρησιμοποιείται για τον εντοπισμό εμπειρογνωμόνων σε ένα συγκεκριμένο πεδίο γνώσης που είναι σε θέση να βοηθήσουν στην αναλυθείσα κατάσταση (Hansenetal., 1999; Venkitachalam, Scheepers, &Gibbs, 2004). Αυτές οι στρατηγικές είναι συμπληρωματικές και η επιλογή μίας δεν αποκλείει κάποια άλλη. Οι διαχειριστές, όμως πρέπει να αποφασίσουν μια κυρίαρχη στρατηγική και να την ενσωματώσουν με τη δεύτερη σε αναλογία 80/20. Η έμφαση στη λανθασμένη στρατηγική ή η χρήση και των δύο στο ίδιο επίπεδο σημασίας μπορεί να «υπονομεύσει γρήγορα μια επιχείρηση» (Hansenetal., 1999). Η στρατηγική κωδικοποίησης και εξατομίκευσης εστιάζει σε διαφορετικές πτυχές της ανταλλαγής γνώσεων, πράγμα που σημαίνει ότι χρειάζονται διαφορετικές συνθήκες και εργαλεία για τη μεταφορά της. Αυτό απαιτεί ορισμένα συγκεκριμένα χαρακτηριστικά μιας οργανωσιακής κουλτούρας. Λαμβάνοντας υπόψη το ανταγωνιστικό πλαίσιο αξιών (Cameron & Quinn, 2011), μπορεί κανείς να πιστεύει ότι οι καλύτερες προϋποθέσεις για τη στρατηγική κωδικοποίησης παρέχονται από τη γραφειοκρατική κουλτούρα και ότι η στρατηγική εξατομίκευσης μπορεί να αναπτυχθεί σε οργανισμούς που μοιάζουν με φατρίες. Αυτή η άποψη είναι μια απλοποίηση. Γενικά, η κουλτούρα της γνώσης πρέπει να βασίζεται στην εμπιστοσύνη ,η οποία επιτρέπει τη συνεργασία, ώστε να προωθήσει μια θετική προοπτική για τη γνώση που απαιτεί την καθοδήγηση μέσω παραδείγματος αντί για λεκτικά κίνητρα. Ακόμη υποστηρίζει την καινοτομία και το άνοιγμα υπό την ευρεία της έννοια . Ένα πολύ σημαντικό πλεονέκτημα της εφαρμογής της κουλτούρας σε επίπεδο ασφάλειας συστημάτων είναι πως άρει όλα τα εμπόδια που αναστέλλουν τη ροή της γνώσης (Davenport & Prusak, 1998; Sveiby & Simons, 2002;). Αυτά τα χαρακτηριστικά, ωστόσο, έχουν διαφορετική σημασία σε οργανισμούς με διαφορετικές στρατηγικές γνώσης. Η ίδια η οργανωσιακή κουλτούρα, ως τρόπος κατανόησης της πραγματικότητας μέσα στον οργανισμό, είναι πραγματικά σημαντική εάν η κορυφαία στρατηγική είναι η κωδικοποίηση. Μέσω αυτής της στρατηγικής, η οποία γίνεται αντιληπτή ως προσέγγιση «από άτομο σε έγγραφο», σημαίνει πως η γνώση «εξάγεται από το άτομο που την ανέπτυξε, ανεξαρτητοποιήθηκε από αυτό το άτομο και επαναχρησιμοποιήθηκε για διάφορους σκοπούς» (Hansenetal., 1999). Επίσης, χρησιμοποιείται για την κοινή χρήση ρητής γνώσης και απαιτεί την ανάκτησή της που αποτελείται από διαδικασίες αναζήτησης και αποκωδικοποίησης.

Οι συσκευές πληροφορικής επιτρέπουν σε κάποιον να βρει τις απαραίτητες πληροφορίες, αλλά η αποκρυπτογράφηση των πληροφοριών και η απόκτηση της σημασίας της σε συγκεκριμένο πλαίσιο είναι πολύ πιο δύσκολη (Gammelgaard&Ritter, 2005).

2.5.2. Εμπιστοσύνη

Η εμπιστοσύνη μεταξύ των εργαζομένων είναι ουσιαστικό στοιχείο της επιτυχούς ανταλλαγής γνώσεων σε έναν καινοτόμο οργανισμό. Οι Olander, Vanhala, Hurmelinna-Laukkanen και Blomqvist (2015) δηλώνουν ότι οι γνώσεις είναι ενσωματωμένες στο προσωπικό και εάν το προσωπικό χειρίζεται τέτοιες γνώσεις απρόσεκτα ή αφήνει να πάρει τη γνώση μαζί του, όχι μόνο ανοίγεται η πόρτα σε επιβλαβείς ανταγωνιστικές απομιμήσεις (McEvily&Chakravarthy, 2002) ,αλλά αυξάνεται επίσης η πιθανότητα διακοπής της καινοτόμου δραστηριότητας. Αυτή η δήλωση μπορεί να εφαρμοστεί τόσο στην ανταλλαγή γνώσεων μεταξύ του προσωπικού, εντός ενός οργανισμού, όσο και στην ανταλλαγή γνώσεων από τους εργαζόμενους μεταξύ ξεχωριστών οργανισμών. Ο landeretaï (2015) δήλωσε, ότι η ασφάλεια πληροφοριών θεωρείται μερικές φορές εμπόδιο στην «καινοτόμο συμπεριφορά ανταλλαγής γνώσεων». Οι διευθυντές πρέπει να συνεργάζονται με υφισταμένους για τη δημιουργία ισορροπίας εμπιστοσύνης και ασφάλειας γνώσης καθώς υπάρχει κίνδυνος εμπιστοσύνης προσωπικού με δυνητικά σημαντικές γνώσεις. Η πολιτιστική ιδέα συμβάλλει στην αύξηση της εμπιστοσύνης μεταξύ των διαφόρων παραγόντων σχετικά με την ασφάλεια των πληροφοριών εντός ενός οργανισμού.

Η κουλτούρα ασφάλειας περιλαμβάνει όλα τα κοινωνικοπολιτιστικά μέτρα που υποστηρίζουν τα τεχνικά μέτρα ασφάλειας, έτσι ώστε η ασφάλεια των πληροφοριών να γίνει μια φυσική πτυχή στις καθημερινές δραστηριότητες κάθε εργαζομένου. Η κουλτούρα ασφάλειας σαν ιδέα συμβάλλει στην αύξηση της εμπιστοσύνης μεταξύ των διαφόρων παραγόντων σχετικά με την ασφάλεια των πληροφοριών εντός ενός οργανισμού και γι’ αυτό ξεκινάμε με την εξήγηση της «έννοιας της οργανωσιακής κουλτούρας», ρωτώντας πώς μπορεί να χρησιμοποιηθεί για την εφαρμογή της κουλτούρας ασφάλειας πληροφοριών.

2 5.3. Εκπαίδευση

Η έρευνα δείχνει ότι η εκπαίδευση είναι ένα άλλο σημαντικό στοιχείο της επιτυχούς ανταλλαγής γνώσεων σε καινοτόμους οργανισμούς. Προκειμένου να προωθηθεί η καινοτομία, είναι σημαντικό να κατανοήσουμε τις γνώσεις σχετικά με το αντικείμενο της καινοτομίας (π.χ. καινοτομίες προϊόντων τεχνολογίας ή βελτιώσεις διεργασιών). Σύμφωνα με τους Neirotti και Paolucci (2013), «η εκπαίδευση σε όλα τα επίπεδα οργάνωσης μπορεί να διευκολύνει την έκθεση των εργαζομένων σε μια ποικιλία γνώσεων και να ενθαρρύνει το άνοιγμα σε νέες ιδέες που είναι πιθανό να αποτελούν πηγή τεχνολογικών και οργανωτικών καινοτομιών». Το προσωπικό πρέπει να είναι σε θέση να κατανοήσει την χρησιμότητα των γνώσεων που διαθέτει και τα πιθανά αποτελέσματα αυτών μέσω της εφαρμογή τους ,πριν τις αξιοποιήσουν στα είδη των καινοτομιών. Οι Neirotti και Paolucci επισημαίνουν επίσης ότι «η κατάρτιση είναι επομένως μια από τις πρακτικές που μπορεί να παραμείνουν στη βάση των απορροφητικών ικανοτήτων των επιχειρήσεων». Η εκπαίδευση είναι σημαντική για τη συλλογή γνώσεων προκειμένου να κατανοήσουμε και να αναλύσουμε τη γνώση.

2.5.4. Διαχείριση καινοτομίας

Η καινοτομία είναι προϊόν μιας διαδικασίας πολλαπλών βημάτων που περιλαμβάνει ανάπτυξη, προσαρμογή και παράδοση των προϊόντων στους τελικούς χρήστες (Bakir, 2016). Οι Murphy, Perera και Heaney (2015) ορίζουν μια καινοτομία ως «ιδέα που αναπτύχθηκε και υλοποιήθηκε στο εμπόριο σε ένα ίδρυμα, βιομηχανία, επιχείρηση ή έργο». Έτσι, η διαχείριση της καινοτομίας είναι το «σύνολο κριτικών ικανοτήτων διευθυντή ή ηγέτη οποιουδήποτε οργανισμού, επειδή επιτρέπει στον διαχειριστή να δημιουργήσει οργανωσιακή ανάπτυξη και κερδοφορία» (Yasini, 2016). Υπάρχουν δύο τύποι καινοτομιών, οι καινοτομίες προϊόντων και διεργασιών. Οι καινοτομίες προϊόντων είναι εκείνες όπου το αποτέλεσμα είναι ένα «ποιοτικά ανώτερο προϊόν από μια δεδομένη ποσότητα πόρων» (Murphyetal., 2015). Οι καινοτομίες της διαδικασίας ορίζονται ως «εισαγωγές προηγμένων τεχνικών διαχείρισης» (Murphyetal., 2015). Και οι δύο τύποι καινοτομιών συνεχίζουν να καθορίζουν τους οργανισμούς στη σημερινή επιχειρηματική σκηνή.

Οι καινοτομίες αναπτύσσονται διαρκώς με την πάροδο του χρόνου, αλλά το ραγδαίο ενδιαφέρον για την καινοτομία έχει αυξηθεί από το 1990 (Walecka-Jankowska, 2015). Ο Έβερετ Ρότζερς δημιούργησε ένα βιβλίο το 2003, Diffusion of Innovations, σχετικά με το πώς οι ιδέες εξαπλώθηκαν σε οργανισμούς (Valente, Dyal, Chu, Wipfli, &Fujimoto, 2015). Ένας από τους κύριους ισχυρισμούς του κειμένου Rogers είναι ότι, «νέες ιδέες και πρακτικές συχνά εξαπλώνονται μέσω διαπροσωπικών επαφών σε μεγάλο βαθμό μέσω διαπροσωπικής επικοινωνίας» (Valenteetal., 2015). Ως εκ τούτου, η διαπροσωπική επικοινωνία είναι μια οντότητα στη διαδικασία καινοτομίας που οι διευθυντές και οι ηγέτες των ομάδων καινοτομίας πρέπει να διαχειριστούν κατάλληλα και να αξιοποιήσουν για να μεγιστοποιήσουν την επιτυχία της ομάδας και της οργάνωσης.

Υποθέσεις έρευνας

Η οργάνωση της κουλτούρας μπορεί να θεωρηθεί ως πρότυπο πεποιθήσεων και προσδοκιών που μοιράζονται μέλη του οργανισμού, και αυτές οι πεποιθήσεις και προσδοκίες παράγουν κανόνες που διαμορφώνουν έντονα τη συμπεριφορά ατόμων, ομάδων ή οργανισμών (Schwartz,1981). Η οργανωσιακή κουλτούρα μπορεί επίσης να περιλαμβάνει τις ιδέες που μοιράζονται οι άνθρωποι της οργάνωσης και επικοινωνούν μεταξύ τους (Szilagyiand Wallace, 1987). Η οργανωσιακή κουλτούρα δεν αποτελεί μόνο έναν κρίσιμο παράγοντα για να μπορέσει ένας οργανισμός να συνεχίσει να ζει αλλά καθοδηγεί τις διαδικασίες και τις ενέργειές του, συμπεριλαμβανομένων ιδίως της πρακτικής της προστασίας των πόρων πληροφόρησης αλλά κι επιπλέον συντελεί σημαντικά στην αλλαγή της ασφάλειας. Συνεπώς, με βάση τη σημαντικότητα της οργανωσιακής κουλτούρας και των χαρακτηριστικών της προκύπτουν και οι υποθέσεις της έρευνας όπως έχουν ήδη αναφερθεί στην παράγραφο **1.9**.

.

Κεφάλαιο 3: Μεθοδολογία έρευνας

3.1. Φιλοσοφία Έρευνας

Η πρώτη φάση χαρτογράφησης του θεωρητικού πλαισίου της έρευνας είναι η διαμόρφωση της πνευματικής προοπτικής ή στάσης των ερευνητών. Η ερευνητική φιλοσοφία είναι ο εξωτερικός φλοιός αυτού που ονομάζεται "κρεμμύδι της έρευνας" (Saundersetal, 2007) ,(Εικόνα 3). Ένας σχηματισμός που μέσα από διαφορετικά στρώματα έρευνας σχεδιασμού (φιλοσοφία, προσέγγιση, στρατηγική, μέθοδοι, χρονοδιαγράμματα, τεχνικές), βοηθά στην στρωματοποίηση ενός σχεδιασμού έρευνας έτσι ώστε τελικά να αντικατοπτρίζει τους καλύτερους σκοπούς του ερευνητή.

Μια από τις πλέον σημαντικές φάσεις της έρευνας είναι ο σχεδιασμός της αλλά και ο καθορισμός των βασικών αρχών της. Επομένως, είναι σημαντικό να εκτιμηθεί πρωτίστως η φιλοσοφία και οι αξίες πίσω από την έρευνα, οι οποίες επιβεβαιώνουν το εννοιολογικό πλαίσιο στο οποίο αναλύονται τα ερευνητικά ερωτήματα και ερμηνεύονται τα αποτελέσματα, που επιβεβαιώνονται από την υποκείμενη θεωρία και την έρευνα. Στην τρέχουσα έρευνα, το βασικό ερώτημα είναι πως «η οργανωσιακή κουλτούρα μπορεί να επηρεάσει την αλλαγή στην ασφάλεια των πληροφοριακών συστημάτων» και να παράσχει τα σχετικά ευρήματα που να συνάδουν με την θεωρία (Bryman & Bell, 2007). Η βασική ερευνητική προσέγγιση που θα χρησιμοποιηθεί βασίζεται στη θετικιστική προσέγγιση.

Ο θετικισμός είναι μία από τις πιο δημοφιλείς και αναγνωρισμένες φιλοσοφικές προσεγγίσεις της έρευνας σήμερα. Η ανάπτυξη υποθέσεων καθοδηγείται από την ανάλυση δεδομένων από κατάλληλες πηγές γνώσης. Αυτό βασίζεται σε ακριβή και επαναλαμβανόμενα αποτελέσματα, μέσω ποσοτικής ή ποσοτικοποιημένης στατιστικής ανάλυσης.

Οι Mitra και Lankford (1999), στη δική τους μελέτη, υπογραμμίζουν τη σημασία της εγκυρότητας των διαδικασιών. Στο πλαίσιο αυτό, η «καταλληλόλητα, η ακρίβεια και η αξιοπιστία των ευρημάτων επικυρώνονται μέσω αξιόπιστων και έγκυρων διαδικασιών». Λαμβάνοντας υπόψη όλα τα παραπάνω, είναι σημαντικό να υπογραμμιστεί η χρήση ενός μέσου έρευνας το οποίο εγγυάται ότι οι συμμετέχοντες θα εμπλακούν στη διαδικασία έρευνας έτσι ώστε να μπορέσουν να αποκομίσουν ακριβή και συνεπή αποτελέσματα.

Η συμπερασματική προσέγγιση (deductive research) αφορά την ύπαρξη συγκεκριμένων ερωτήσεων, υποθέσεων ή αποφάσεων που καλούνται να απαντηθούν και να είναι έγκυρες. Στόχος αυτής της προσέγγισης είναι να εξαχθούν συμπεράσματα τόσο εύκολα ώστε να απαντηθούν θετικά η αρνητικά οι θεωρητικές προτάσεις που ήδη υπάρχουν.

Πρακτικά, ένα θεωρητικό πλαίσιο κατασκευάζεται ανάλογα με την πρόθεσή του ερευνητή στην οποία αντλούνται σαφείς υποθέσεις, οι οποίες πρέπει να επικυρωθούν ή να απορριφθούν από τη μελέτη. Το έργο είναι το αποτέλεσμα της μελέτης που πραγματοποίησε ο ερευνητής και αυτή η θεωρητική ανάλυση εξετάζει την ακρίβεια και την εγκυρότητα των αποτελεσμάτων του.

Ο στόχος αυτής της μελέτης είναι, φυσικά, να ενισχυθεί η αλήθεια για το θεωρητικό πλαίσιο, μέσω της θεωρητικής έρευνας, της ανάλυσης των προηγούμενων έρευνών , ως απάντηση στις υποθέσεις που τέθηκαν κατά την ερευνητική διαδικασία.

Η συμπερασματική ή αλλιώς παραγωγική προσέγγιση της έρευνας περιλαμβάνει μια σειρά βασικών μέτρων, όπως Α) συλλογή δευτερογενών στοιχείων , Β) διατύπωση υποθέσεων (Γ) συλλογή δεδομένων (Δ) αποτελέσματα. Η λύση που βασίζεται σε αυτά τα μέτρα εξηγείται ως εξής (Wilson, 2010):

1. Η παρούσα θεωρία αντλεί πληροφορίες από άλλες θεωρίες του παρελθόντος .

2. Οι υποθέσεις κατασκευάζονται συστηματικά και δύο μοναδικές μεταβλητές υποδηλώνουν τις σχέσεις.

3. Οι υποθέσεις ελέγχονται χρησιμοποιώντας τις κατάλληλες μεθόδους.

4. Η συνέπεια της δοκιμασίας υποθέσεων λαμβάνεται υπόψη και έτσι ο ερευνητής μπορεί να αποδεχθεί ή να απορρίψει τις υποθέσεις.

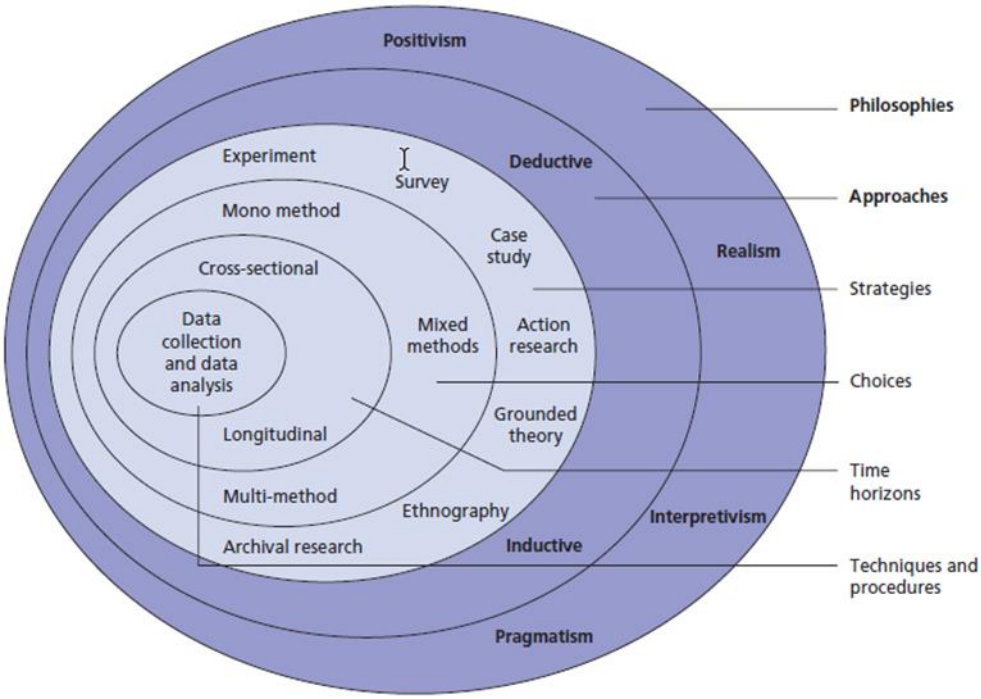
5. Σε περιπτώσεις όπου οι θεωρίες απορρίπτονται, η θεωρία ενημερώνεται.

Η μέθοδος αυτή ακολουθείται στην παρούσα έρευνα και στη συνολική ανάλυση, καθώς το θεωρητικό υλικό είναι αρκετό, γεγονός που αποτελεί βασικό δείκτη ότι μια συμπερασματική προσέγγιση είναι η σωστή (Bruno & Borgolia, 2009).

Το κύριο μέσο της έρευνας είναι η ερευνητική στρατηγική και η βιβλιογραφική ανασκόπηση στο δεύτερο κεφάλαιο που χρησιμοποιήθηκε ήδη ως το μέσο της έρευνας συμβάλοντας σε αυτήν και οι περιπτωσιολογικές μελέτες στο ίδιο κεφάλαιο ,με τη μορφή της υπάρχουσας έρευνας.

Ως εκ τούτου, η βασική ανάλυση παρατίθεται στη λεγόμενη έρευνα πεδίου, όπου συλλέγονται μεγάλοι αριθμοί στατιστικών στοιχείων, τα οποία στη συνέχεια αναλύονται με τρόπο ώστε να δοκιμάζονται οι υποθέσεις μιας παραγωγικής μεθόδου. Αυτή η επιλογή προτιμάται επειδή είναι ο καλύτερος τρόπος εξεύρεσης ,οποιωνδήποτε σχέσεων μεταξύ της οργανωσιακής κουλτούρας και της αλλαγής των πληροφοριακών συστημάτων ασφάλειας.

Εικόνα 3: Το«κρεμμύδι της έρευνας»



3.2. Σχεδιασμός Έρευνας

Προκειμένου να διαμορφωθεί ο σχεδιασμός της έρευνας, είναι επιτακτική ανάγκη ο ερευνητής να έχει πλήρη επίγνωση των ερευνητικών στόχων καθώς και των ερευνητικών ερωτημάτων (Christensen κ.α. 2001), δεδομένου ότι ο σχεδιασμός της παρέχει πληροφορίες για το σχέδιο του ερευνητή.
Ο Yin (1994), επιβεβαιώνει ότι το ερευνητικό στυλ και το σχέδιο έχει εξαιρετική θέση στην έρευνα, καθώς αντικατοπτρίζει τη σχέση μεταξύ των πληροφοριών που συλλέγονται κατά τη διάρκεια της διαδικασίας και των ερευνητικών στόχων.

Απεναντίας, οι Saunders κ.α. (2012) τονίζουν τη σημασία της κατάρτισης ενός συγκεκριμένου σχεδίου που να ανταποκρίνεται σε όλες τις ερευνητικές ερωτήσεις. Ως εκ τούτου, ο σχεδιασμός της έρευνας αντανακλά την κατεύθυνση που πρέπει να κάνει ο ερευνητής για να επιτύχει την υλοποίηση της έρευνας. Επομένως, είναι εύκολο να υποστηριχθεί ότι ο σχεδιασμός της έρευνας ασκεί εξέχοντα ρόλο και έχει μεγάλη σημασία για την πραγματοποίησή της.

Στην πραγματικότητα, ο σχεδιασμός της έρευνας βοηθά τους σκοπούς και τους στόχους της μελέτης, αλλά βοηθά επίσης τον ερευνητή να ανταποκριθεί στα ερευνητικά ερωτήματα και τις ερευνητικές υποθέσεις, καθώς διαμορφώνονται στη διαδικασία. Στην παρούσα μελέτη, είναι προφανές ότι η πιο κατάλληλη διαδικασία είναι να χρησιμοποιηθεί μια περιγραφική έρευνα. Η χρήση περιγραφικής έρευνας διεξάγεται προκειμένου να "προσδιοριστούν ή να εξαχθούν πρότυπα συμπεριφοράς σε τομείς δραστηριότητας". Κατά συνέπεια, η περιγραφική έρευνα επιδιώκει ακριβείς, ορθολογικές και συγκεκριμένες απαντήσεις στα ερευνητικά ερωτήματα. Εκτός αυτού, η περιγραφική έρευνα προσφέρει μια διεξοδική ερμηνεία ενός φαινομένου (Newman, 2006), χρησιμοποιώντας το περιγραφικό ερευνητικό σχέδιο του ερευνητή για να αναγνωρίσει και να ανακαλύψει τις ενώσεις που διαμορφώνονται στο πλαίσιο του φαινομένου. Ως εκ τούτου, η επιλογή ενός κατάλληλου ερευνητικού σχεδίου μπορεί να είναι εξίσου ζωτικής σημασίας όπως η εύρεση της σωστής διαδικασίας για την έρευνα, η οποία θα είναι κατάλληλη να αποδώσει τα σχετικά στοιχεία.

3.3. Ο πληθυσμός της μελέτης και η διαδικασία δειγματοληψίας

Μια από τις διαδικασίες που μπορούν να καθορίσουν την επιτυχία και την έκβαση της έρευνας είναι ο προσδιορισμός του πληθυσμού της. Είναι μια σημαντική διαδικασία που θα μπορούσε να έχει πιθανή επίδραση στην επίτευξη των ερευνητικών στόχων. Κυρίως, η διαδικασία της δειγματοληψίας είναι μια σημαντική διαδικασία, ενώ το δείγμα ιδανικά, θα πρέπει να είναι αντιπροσωπευτικό του πληθυσμού της μελέτης. Όπως έχει ήδη ειπωθεί , το δείγμα της έρευνας πρέπει να μπορεί να έχει ως αποτέλεσμα την ορθότητα και την αξιοπιστία των ευρημάτων. Αν και εκτός αυτού, η κατάλληλη επιλογή δείγματος θα μπορούσε να αποφέρει πρόσθετα οφέλη στην έρευνα, καθώς είναι διαδικασία εξοικονόμησης κόστους, κυρίως όταν πρόκειται για μεγάλες έρευνες που περιλαμβάνουν μεγάλο αριθμό συμμετεχόντων. Όπως διευκρινίστηκε, ο πληθυσμός της μελέτης αυτής αποτελείται από 108 ενήλικα άτομα, κατοίκους της Ελλάδας που εργάζονται σε επιχειρήσεις στην Αθήνα όπου χρησιμοποιούνται πληροφοριακά συστήματα. Καμία άλλη απαίτηση δεν εφαρμόστηκε στο δείγμα αυτής της μελέτης, εκτός από την προϋπόθεση ότι οι συμμετέχοντες σε αυτήν την έρευνα θα πρέπει να είναι υπάλληλοι με έδρα την Αττική.

Ο κύριος λόγος για τον οποίο η έρευνα δεν εφάρμοσε περαιτέρω περιορισμούς στη συλλογή του δείγματος έχει να κάνει με την προσπάθεια να επιτευχθεί απλότητα αλλά και προσβασιμότητα στο δείγμα. Επιπλέον, εμπλέκεται στη μελέτη, η μέθοδος της δειγματοληψίας μη-πιθανότητας. Η τρέχουσα έρευνα χρησιμοποιεί δειγματοληψία ευκολίας (Etikan κ.α.., 2015). Γενικά, το δείγμα ευκολίας είναι ένας τύπος δειγματοληψίας μη-πιθανότητας και χρησιμοποιείται όταν ο ερευνητής προσπαθεί να στοχεύσει στην εγγύτητα, την προσβασιμότητα και τη διαθεσιμότητα του δείγματος σε δεδομένη στιγμή (Dörnye, 2007). Πέρα από αυτό, ο τρόπος δειγματοληψίας καθιστά τη διαδικασία συλλογής δεδομένων πολύ ευκολότερη, καθώς επιτρέπει την απρόσκοπτη πρόσβαση του ερευνητή στους συμμετέχοντες. Παρ 'όλα αυτά, η δειγματοληψία με δείγμα ευκολίας έχει ορισμένους περιορισμούς. Συγκεκριμένα , υπάρχουν πολλές ενστάσεις σχετικά με το κατά πόσο οι μέθοδοι δειγματοληψίας ευκολίας μπορούν να προσφέρουν ακριβή στοιχεία που θα είναι αντιπροσωπευτικά για τον πληθυσμό (Jennings, 2001).

Αυτό θα μπορούσε να αποτελέσει σημαντικό εμπόδιο για την όλη διαδικασία, καθώς αυτή η μέθοδος δειγματοληψίας μπορεί να διαταράξει την ικανότητα του ερευνητή να επιτύχει ορισμένες αξιόπιστες και ακριβείς παραδοχές όσον αφορά τον πληθυσμό της μελέτης (Battaglia M, 2008).

Αν και το δείγμα ευκολίας χρησιμοποιείται πολύ συχνά στις κοινωνικές έρευνες, δεδομένου ότι η διαδικασία αυτή παρέχει ευρείες πληροφορίες (Jennings, 2001),ωστόσο είναι μια μέθοδος που δεν ενδείκνυται όταν τα χρονικά περιθώρια είναι στενά.

3.4. Το εργαλείο της έρευνας - Ερωτηματολόγιο

Το ερωτηματολόγιο (βλ. Παράρτημα 1), είναι το εργαλείο της έρευνας που αφορά σε ερωτήσεις ιστορικού ασφάλειας πληροφοριών, οι οποίες απαντώνται κυρίως χρησιμοποιώντας μια κλίμακα ναι / όχι. Η πρώτη ενότητα αποτελείται από τις ερωτήσεις που δόθηκαν στο δείγμα της έρευνας που αναπτύσσεται με τον οργανισμό που συμμετέχει στη μελέτη για να θέσει ερωτήματα σχετικά με τις υπάρχουσες πολιτικές και δραστηριότητες ευαισθητοποίησης για σκοπούς υποβάθρου.

Η δεύτερη ενότητα περιλαμβάνει δέκα διαστάσεις με συνολικά 20 μεταβλητές που μετρούν την κουλτούρα ασφάλειας πληροφοριών σε κλίμακα Likert πέντε σημείων (διαφωνώ έντονα, διαφωνώ, δεν είμαι σίγουρος, συμφωνώ, συμφωνώ απόλυτα)

Στην Τρίτη ενότητα οι συμμετέχοντες καλούνται να απαντήσουν σε δημογραφικές ερωτήσεις για να χωρίσουν τα δεδομένα σε ομάδες υπαλλήλων, όπως τοποθεσία γραφείου, ομάδα παραγωγής, φύλο, επιχειρηματική μονάδα ή / και επίπεδο εργασίας.

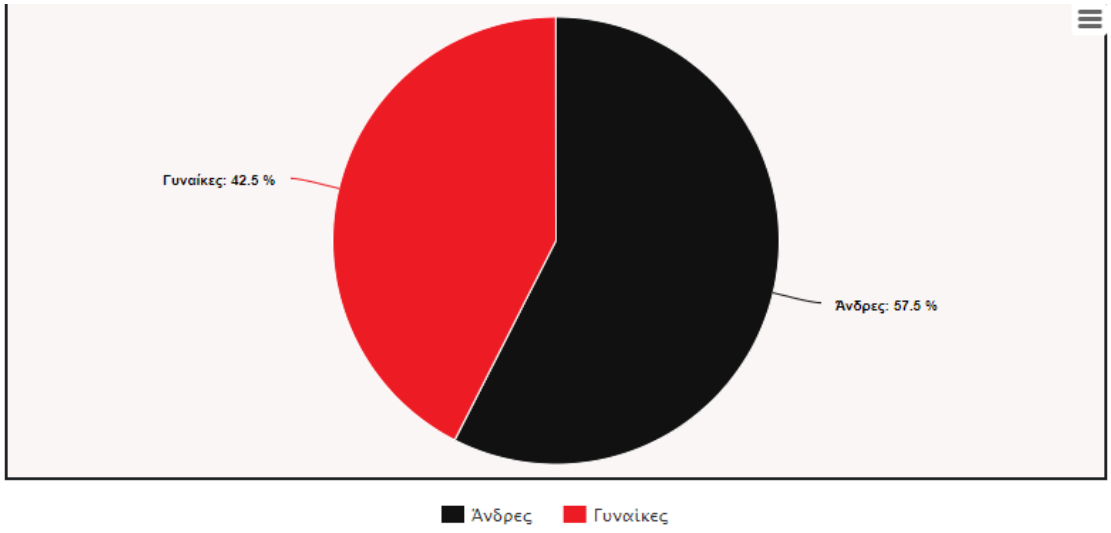
Κεφάλαιο 4: Ανάλυση ευρημάτων

4.1. Ευρήματα έρευνας

Αφού συγκεντρώθηκαν συνολικά 108 ερωτηθέντες, τα αποτελέσματα των ερευνών που προέκυψαν και ήταν είτε άκυρα είτε ατελή ,απορρίφθηκαν.

Συνολικά, συγκεντρώθηκαν 87 χρήσιμα αντίγραφα του ερωτηματολογίου και χρησιμοποιήθηκαν για την ανάλυση. Μεταξύ 87 χρηστών που απάντησαν, το 57,5% ήταν άνδρες και το 42,5% ήταν γυναίκες (Σχήμα 1).

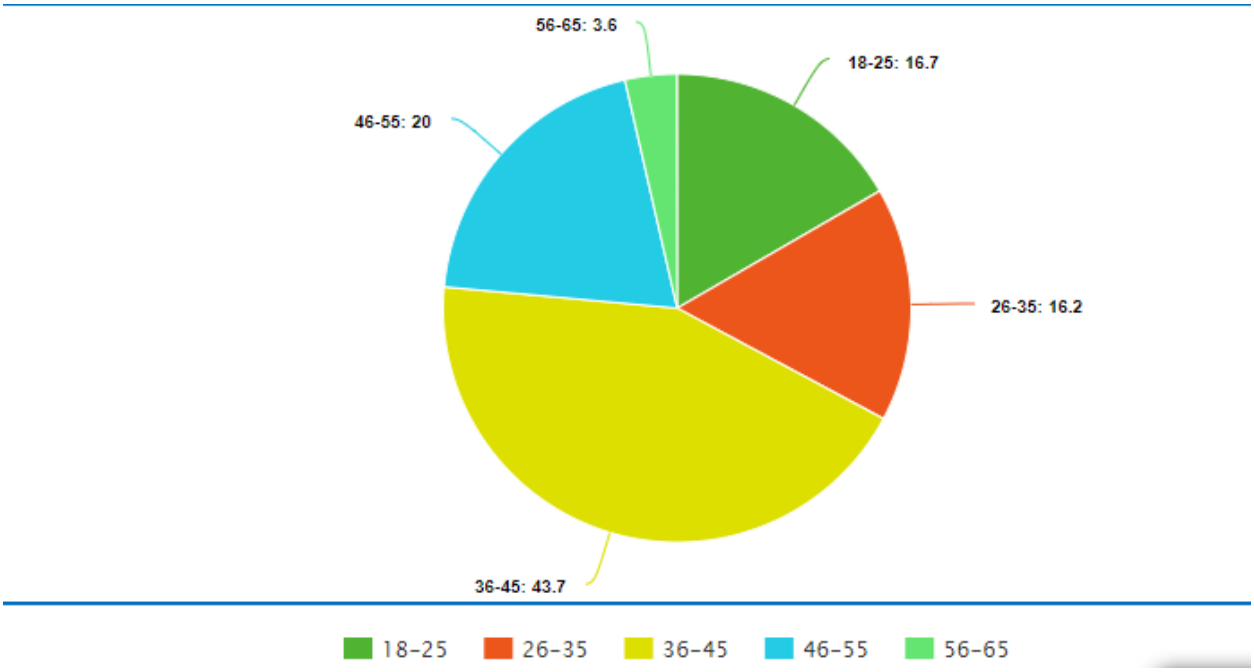
Σχήμα 1 Δημογραφικά στοιχεία : Άνδρες -γυναίκες



Πηγή : ευρήματα έρευνας

Σε ότι αφορά την ηλικία η πλειοψηφία των συμμετεχόντων ανήκαν στο ηλικιακό γκρουπ 36-45 (43,7%),ενώ το 20 % ανήκαν στην ηλικιακή ομάδα 46-55(Σχήμα 2).

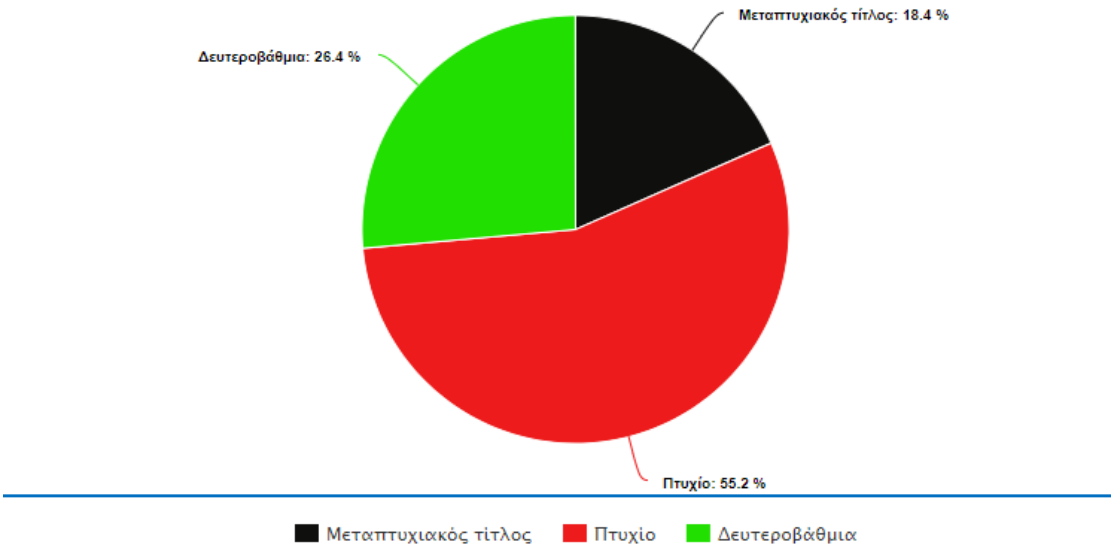
Σχήμα 2 : Ηλικιακά γκρούπ



Πηγή: Ευρήματα έρευνας

Σχετικά με το επίπεδο εκπαίδευσης, από το δείγμα μας προκύπτει πως το 18,4% ήταν κάτοχος μεταπτυχιακού τίτλου σπουδών ή άνω, το 55,2% ήταν κάτοχοι τίτλου πτυχίου και το 26,4% δεν είχε πτυχίο ανώτερης ή ανώτατης εκπαίδευσης (Σχήμα 3).

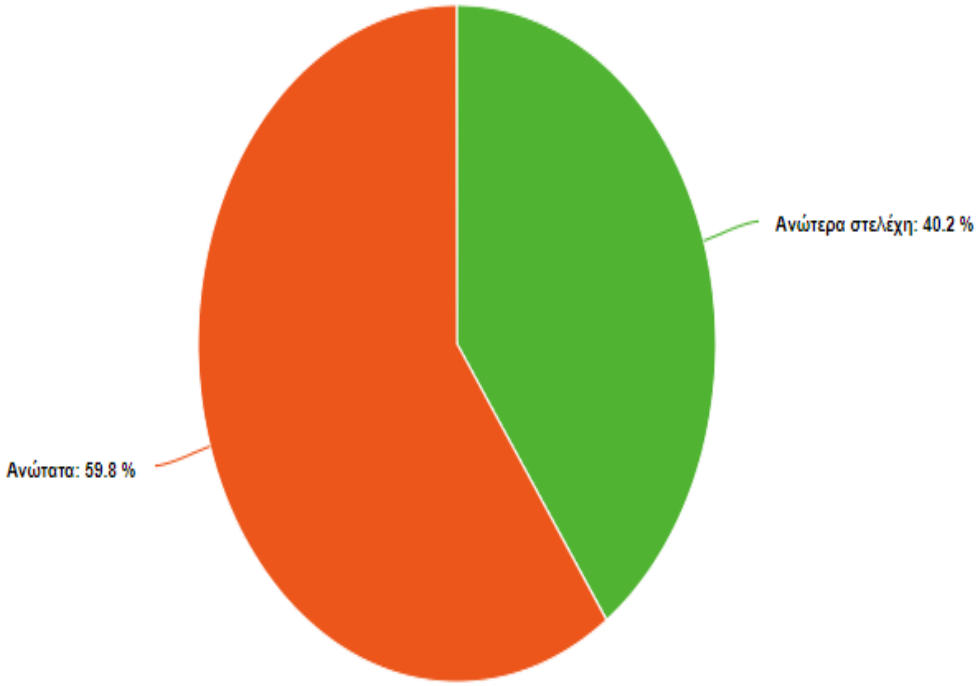
Σχήμα 3: Δημογραφικά στοιχεία: Εκπαίδευση



Πηγή: Ευρήματα έρευνας

Περίπου το 40,2% από τα συμπληρωμένα ερωτηματολόγια προέρχονταν από ανώτερα στελέχη και διευθυντές και το 59,8% από ανώτατα στελέχη με γνώση στην τεχνολογία πληροφορικής (Σχήμα 4).

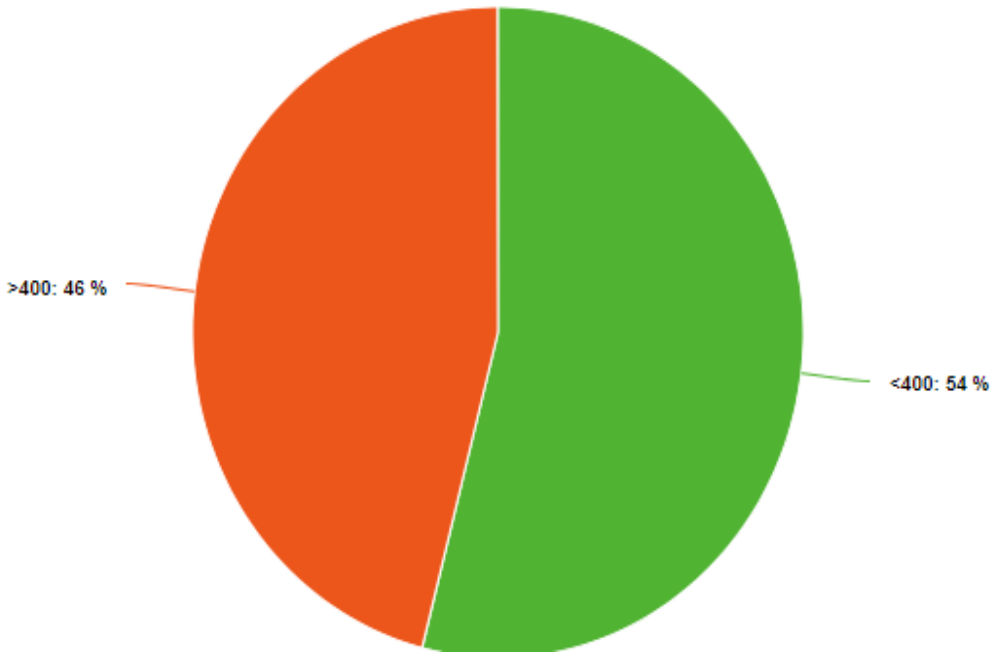
Σχήμα 4: Θέση εργασίας



Πηγή: Ευρήματα έρευνας

Περίπου το 54% των ερωτηθέντων εργάστηκε για εταιρείες που απασχολούσαν λιγότερο από 400 εργαζομένους , ενώ το υπόλοιπο 46% απασχολούσε περισσότερο από 400 εργαζομένους (Σχήμα 5).

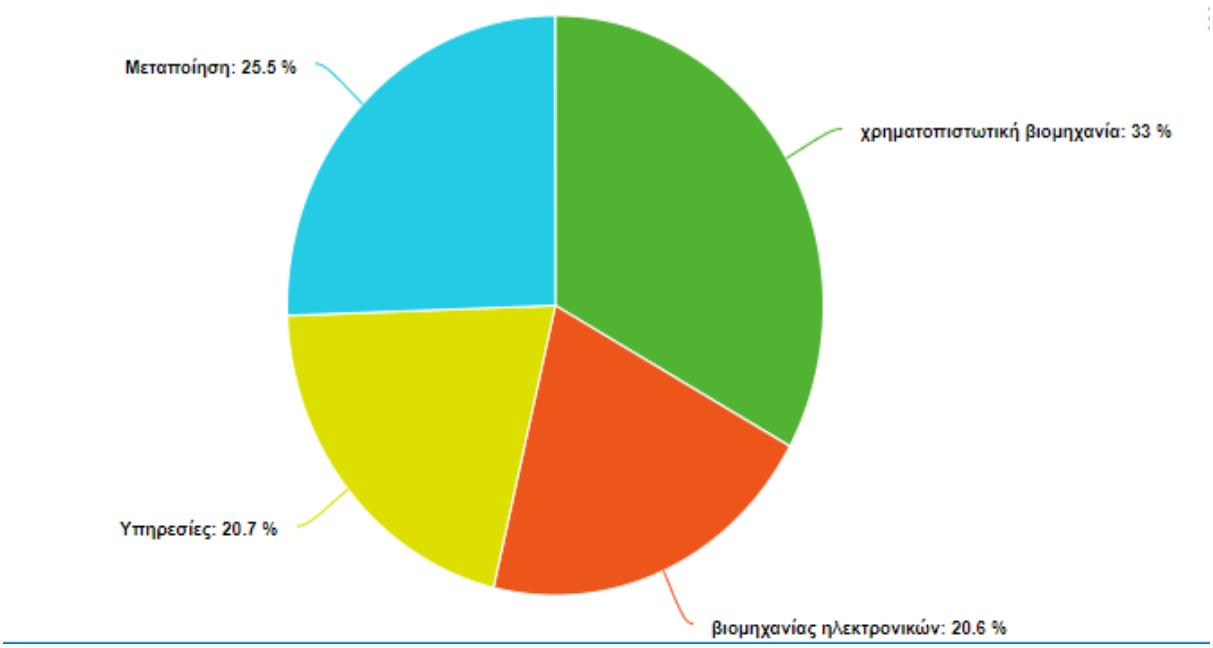
Σχήμα 5: Αριθμός εργαζομένων



Πηγή: Ευρήματα έρευνας

Από τους ερωτηθέντες, το 33,3% εργάστηκε για εταιρείες στη χρηματοπιστωτική βιομηχανία, το 20,6% στη βιομηχανία ηλεκτρονικών / ηλεκτρικών ή ηλεκτρονικών υπολογιστών, το 20,7% στους τομείς των υπηρεσιών και το 25,5% σε άλλους τομείς όπως η μεταποιητική βιομηχανία, η υγειονομική περίθαλψη, η βιομηχανία τροφίμων κ.λπ. (Σχήμα 6).

Σχήμα 6 Κλάδος



Πηγή: Ευρήματα έρευνας

4.2. Συσχέτιση μεταξύ των μεταβλητών

Με σκοπό την ανάλυση των υποθέσεων της έρευνας πρώτα πραγματοποιείται η συσχέτιση μεταξύ των μεταβλητών. Για να μπορέσει να υπάρξει συσχέτιση μεταξύ των μεταβλητών, ο συντελεστής συσχέτισης που χρησιμοποιείται, Pearson(r) πρέπει να ξεπερνά το r= ±0.3. Οι μεταβλητές που θα συσχετιστούν είναι η οργανωσιακή κουλτούρα και τα χαρακτηριστικά που επηρεάζουν στην εφαρμογή της από τις υποθέσεις της έρευνας. Η δημιουργία των μεταβλητών προκύπτει από τα στοιχεία του ερωτηματολογίου της έρευνας. Η συσχέτιση των μεταβλητών δείχνει το κατά πόσο επιδρούν και επηρεάζονται μεταξύ τους. Με τη χρήση του στατιστικού προγράμματος SPSS 23.00 εξάγονται τα στοιχεία για τα συμπεράσματα σχετικά με τα ευρήματα της έρευνας.

Αρχικά οι μεταβλητές που θα συσχετιστούν είναι η οργανωσιακή κουλτούρα και η ασφάλεια των πληροφοριακών συστημάτων προκειμένου να γίνει εμφανές πως επιδρούν οι δύο αυτές μεταβλητές.

Πίνακας 1: Συσχέτιση μεταξύ ασφάλειας πληροφοριακών συστημάτων και οργανωσιακής κουλτούρας.

	Οργανωσιακή κουλτούρα
Ασφάλεια πληροφοριακών συστημάτων	**,334****

****. Correlation is significant at the 0.01 level (2-tailed)**

Με βάση την ανάλυση της συσχέτισης μεταξύ δύο μεταβλητών πρέπει να αναφερθούν τα εξής. Ο συντελεστής Pearson είναι (r=,334) και δείχνει μια θετική συσχέτιση. Αυτό σημαίνει πως η αλλαγή της οργανωσιακής κουλτούρας επηρεάζει σημαντικά την ασφάλεια πληροφοριακών συστημάτων διοίκησης.

Πίνακας 2: Συσχέτιση μεταξύ εμπιστοσύνης και οργανωσιακής κουλτούρας.

	Οργανωσιακή κουλτούρα
Εμπιστοσύνη	,725**

****. Correlation is significant at the 0.01 level (2-tailed).**

Ο συντελεστής Pearson (r=,725), δείχνει πως υπάρχει ισχυρή θετική συσχέτιση μεταξύ οργανωσιακής κουλτούρας και εμπιστοσύνης. Συνεπώς, για τη σχέση των μεταβλητών φαίνεται πως η εμπιστοσύνη αυξάνεται καθώς βελτιώνεται η οργανωσιακή κουλτούρα.

Πίνακας 3: Συσχέτιση μεταξύ καινοτομίας και οργανωσιακής κουλτούρας.

	Οργανωσιακής κουλτούρας
Καινοτομίας	,493**

****. Correlation is significant at the 0.01 level (2-tailed).**

Ο συντελεστής Pearson (r=,493), δείχνει πως υπάρχει ισχυρή θετική συσχέτιση μεταξύ οργανωσιακής κουλτούρας και καινοτομίας . Αυτό σημαίνει πως η επιθυμία για καινοτομία αυξάνεται καθώς βελτιώνεται η οργανωσιακή κουλτούρα.

Πίνακας 4: Συσχέτιση μεταξύ διάχυσης γνώσης και οργανωσιακής κουλτούρας.

	Οργανωσιακή κουλτούρα
Διάχυση γνώσης	**,561****

****. Correlation is significant at the 0.01 level (2-tailed).**

Ο συντελεστής Pearson (r=,561), δείχνει πως υπάρχει ισχυρή θετική συσχέτιση μεταξύ οργανωσιακής κουλτούρας και διάχυσης της γνώσης. Αυτό σημαίνει πως καθώς βελτιώνεται η οργανωσιακή κουλτούρα αυξάνεται και η διαδικασία διάχυσης της γνώσης.

Πίνακας 5: Συσχέτιση μεταξύ αποτελεσματικότητας και οργανωσιακής κουλτούρας.

	Οργανωσιακή κουλτούρα
Αποτελεσματικότητα	**,463****

****. Correlation is significant at the 0.01 level (2-tailed).**

Ο συντελεστής Pearson (r=,463), δείχνει πως υπάρχει επίσης, ισχυρή θετική συσχέτιση μεταξύ της οργανωσιακής κουλτούρας και της αποτελεσματικότητας. Το μέγεθος της συσχέτισης σημαίνει πως η αποτελεσματικότητα αυξάνεται και επιτυγχάνεται καθώς βελτιώνεται η οργανωσιακή κουλτούρα.

4.3. Ανάλυση υποθέσεων

Για την ανάλυση των υποθέσεων που έχουν δημιουργηθεί χρησιμοποιήθηκε το στατιστικό πρόγραμμα SPSS 23.00 και η μέθοδος Anova.

<u>H1. Υπάρχει σημαντική στατιστική σχέση μεταξύ οργανωσιακής κουλτούρας και αλλαγής του ISM.</u>

Για την υπόθεση 1 θα πραγματοποιηθεί γραμμική παλινδρόμηση προκειμένου να προσδιοριστεί ο τρόπος, με τον οποίο η σχέση μεταξύ οργανωσιακής κουλτούρας και αλλαγής του ISM, θεωρείται στατιστικά σημαντική. Αρχικά, Θα απορρίψουμε την μηδενική υπόθεση εάν οι δύο μεταβλητές έχουν σημαντική σχέση μεταξύ τους και συνεπώς η κλίση της παλινδρόμησης δεν θα ισούται με το μηδέν για να μπορέσει να υπάρξει η μηδενική υπόθεση.

Ho =>bp = 0, Χα =>bp ≠ 0

Στην υπόθεση 1 η συσχέτιση του Pearson δείχνει ότι υπάρχει μια στατιστικά σημαντική σχέση μεταξύ των δύο μεταβλητών. Στο μοντέλο που χρησιμοποιείται και απεικονίζεται στον Πίνακα 6 η «οργανωσιακή κουλτούρα» είναι η εξαρτημένη μεταβλητή. Από το τεστ ANOVA προκύπτει, ότι η υπόθεση ισχύει, αφού η τιμή του συντελεστή p = 0,001, (p<0,05) και η επίδραση των μεταβλητών είναι σημαντική καθώς το F=16,984, (F>1).

Πίνακας 6 : Υπόθεση 1

Μεταβλητές	β	t-value	F	Significance
Constant		26,311		,000
Οργανωσιακή κουλτούρα	,384	4,122	16,984	,0001

Η2. Υπάρχουν σημαντικές σχέσεις μεταξύ οργανωσιακής κουλτούρας και εμπιστοσύνης

Η υπόθεση 2 θα ελεγχθεί για να προσδιοριστεί εάν υπάρχει στατιστικά σημαντική σχέση μεταξύ των μεταβλητών «οργανωσιακής κουλτούρας» και «εμπιστοσύνης». Σε αυτό το μοντέλο η «οργανωσιακής κουλτούρας» είναι η εξαρτημένη μεταβλητή. Σύμφωνα με το Anova Test, η σχέση μεταξύ εξαρτημένης και ανεξάρτητης μεταβλητής είναι σημαντική σε επίπεδο 0,01. Η τιμή του συντελεστή F είναι μεγάλη 6,178 και αυτό δείχνει ότι το μοντέλο ταιριάζει καλά και ότι η γραμμική παλινδρόμηση είναι στατιστικά σημαντική μεταξύ τους. Με βάση τα παραπάνω και επίσης λαμβάνοντας υπόψη ότι και p = 0, 01, ($p<0,05$) μπορούμε να απορρίψουμε την μηδενική υπόθεση και να δεχτούμε την υπόθεση Η2.

Πίνακας 7 : Υπόθεση 2

Variables	B	t-value	F	Significance
Constant		2,63		,001
Αποτελεσματικότητα οργάνωσης	,423	2,87	6,918	,001

Η3. Υπάρχουν σημαντικές σχέσεις μεταξύ της οργανωσιακής κουλτούρας και της καινοτομίας

Το Η3 αναφέρεται στον έλεγχο της σχέσης μεταξύ της οργανωσιακής κουλτούρας και της καινοτομίας. Η εξαρτημένη μεταβλητή σε αυτό το μοντέλο είναι η οργανωσιακή κουλτούρα. Έχοντας, F = 12,353 και p=0,01, δείχνει ότι η παλινδρόμηση είναι αρκετά σημαντική (F>1), συνεπώς και η επίδραση μεταξύ των μεταβλητών. Ακόμη από την τιμή του p<0,05, η Η3 είναι αποδεκτή.

Πίνακας 8: Υπόθεση 3

Variables	B	t-value	F	Significance
Constant		3,300		,001
Οργανωσιακή κουλτούρα	,335	3,515	12,353	,001

Η4. Υπάρχουν σημαντικές σχέσεις μεταξύ οργανωσιακής κουλτούρας και διάχυσης της γνώσης

Προκειμένου να ελέγξουμε τη σχέση μεταξύ οργανωσιακής κουλτούρας και διάχυσης της γνώσης ορίζουμε την οργανωσιακή κουλτούρα ως εξαρτημένη μεταβλητή. Επίσης και σε αυτή την περίπτωση η επίδραση μεταξύ των μεταβλητών είναι αρκετά σημαντική αφού F = 29.883, (F>1) και p=0,000, (p<0,05) που δείχνει μια καλή εφαρμογή για το μοντέλο και επομένως η υπόθεση Η4 ισχύει.

Πίνακας 9: Υπόθεση 4

Variables	β	t-value	F	Significance
Constant		4,119		,000
Οργανωσιακή κουλτούρα	,483	5,467	29.883	,000

<u>Η5. Υπάρχουν σημαντικές σχέσεις μεταξύ αλλαγής οργανωσιακής κουλτούρας και αποτελεσματικότητας της οργάνωσης</u>

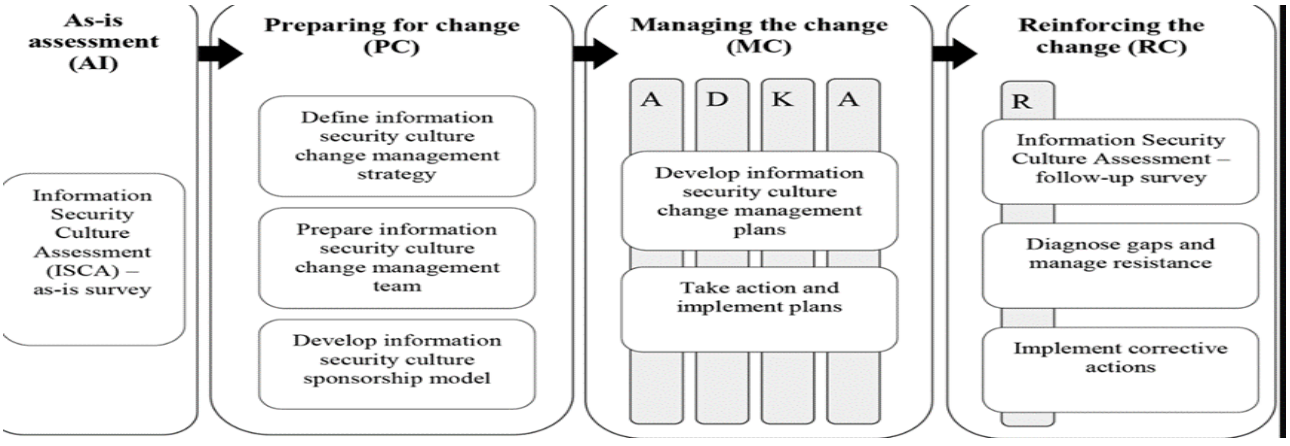
Ο έλεγχος της υπόθεσης 5 θα γίνει μεταξύ των μεταβλητών της οργανωσιακής κουλτούρας και αποτελεσματικότητας. Η αποτελεσματικότητα στην οργάνωση είναι η εξαρτημένη μεταβλητή. Σύμφωνα με το Anova Test, η σχέση μεταξύ εξαρτημένων και ανεξάρτητων μεταβλητών είναι σημαντική σε επίπεδο 0,01, $p<0,05$. Επομένως η υπόθεσή μας ισχύει και η τιμή $F=6,918$ εκφράζει μία αρκετά σημαντική σχέση των μεταβλητών και αυτό δείχνει ότι το μοντέλο ταιριάζει καλά. Συνεπώς, η αποτελεσματικότητα επηρεάζεται άμεσα από την καλή εφαρμογή της οργανωσιακής κουλτούρας.

Πίνακας 10: Υπόθεση 5

Variables	B	t-value	F	Significance
Constant		30,734		,000
Αποτελεσματικότητα οργάνωσης	,257	2,856	6,918	,010

4.4. Περιορισμοί έρευνας

Η συζήτηση της προσέγγισης διαχείρισης αλλαγής ασφάλειας πληροφοριών σε αυτή τη μελέτη περιλαμβάνει μια ποσοτική αξιολόγηση χρησιμοποιώντας το όργανο ISCA, για την έρευνα as-is, στη φάση AI μετά από μια ποσοτική προσέγγιση. Δεν χρησιμοποιήθηκαν άλλα οργανωτικά δεδομένα ή εκθέσεις και ποιοτικά δεδομένα, αλλά θα μπορούσαν να ενσωματωθούν για να επικυρώσουν και να συμπληρώσουν τα αποτελέσματα της έρευνας as-is ,της φάσης AI. Αλλά και τα αποτελέσματα της έρευνας παρακολούθησης της φάσης RC. Αυτή η προσέγγιση διαχείρισης αλλαγής ασφάλειας πληροφοριών που ενσωματώνει το διαγνωστικό όργανο ISCA έχει εφαρμοστεί μόνο σε έναν οργανισμό. Μπορεί να επεκταθεί σε περισσότερους οργανισμούς, σε όλες τις βιομηχανίες για να συγκρίνει τα αποτελέσματα σχετικά με την αλλαγή του πολιτισμού και το αντίκτυπο του μετασχηματισμού. Υπάρχει περιορισμένη εργασία που επικεντρώνεται στις επίσημες προσεγγίσεις αλλαγής κουλτούρας ασφάλειας πληροφοριών για τη μετατροπή της κουλτούρας ασφάλειας πληροφοριών των οργανισμών στην επιθυμητή κατάσταση. Σε αυτή την έρευνα, το έργο του Prosci σχετικά με το μοντέλο ADKAR ενσωματώθηκε με το διαγνωστικό όργανο ISCA για να προτείνει μια προσέγγιση διαχείρισης αλλαγής ασφάλειας πληροφοριών. Οι δηλώσεις του διαγνωστικού οργάνου ISCA συμπεριλήφθηκαν ειδικά για να ενημερώσουν τη μελλοντική έρευνα με στόχο την εφαρμογή και τη βελτίωση της προσέγγισης. Η εφαρμογή αυτής της προσέγγισης απεικονίστηκε μέσω μιας εμπειρικής μελέτης που διεξήχθη σε έναν οικονομικό οργανισμό.



Κεφάλαιο 5: Συμπεράσματα

Η παλινδρόμηση που εξετάστηκε έδειξε πως η ασφάλεια πληροφοριακών συστημάτων σχετίζεται άμεσα και με την οργανωσιακή κουλτούρα , ενώ με τη σειρά της η οργανωσιακή κουλτούρα σχετίζεται με την εμπιστοσύνη στην ηγεσία, με την καινοτομία και την διάχυση της γνώσης, καθώς ο έλεγχος υποθέσεων έδειξε μια σημαντική στατιστική σχέση και για τις πέντε υποθέσεις.

Η ασφάλεια αποτελεί μείζον μέλημα των οργανώσεων γενικότερα. Ειδικά, για εταιρείες που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο. Το επίπεδο της αντιληπτής ασφάλειας οδηγεί σε μεγαλύτερη ικανοποίηση και εμπιστοσύνη των πελατών αλλά και των εργαζομένων μέσα στον οργανισμό (Huangetal ,2004;). Ένα υψηλότερο επίπεδο ικανοποίησης μεταξύ των εργαζομένων μπορεί τελικά να δημιουργεί περισσότερες ευκαιρίες συναλλαγών και να ωφελούνται οι επιχειρήσεις (Sudaporn και Ogenyi, 2004). Οι επιχειρήσεις επενδύουν όλο και περισσότερο στο σύστημα ασφάλειας πληροφοριών, λόγω του γεγονότος ότι οι ιοί και οι επιθέσεις έχουν γίνει η τάση στο διαδίκτυο τα τελευταία χρόνια. Ωστόσο, αυτή η άνοδος επιβραδύνθηκε το 2005. Εν μέρει επειδή το κόστος του συστήματος ασφάλειας πληροφοριών είναι πολύ ακριβό και είναι δύσκολο για τις επιχειρήσεις να συμβαδίσουν με την τεράστια αυξανόμενη δαπάνη που απαιτείται. Ενώ, η ασφάλεια των πληροφοριών στα συστήματα είναι ακόμη ουσιαστικά σημαντική, έχει γίνει όλο και πιο σημαντικό για τις επιχειρήσεις να δώσουν προσοχή στη διαχείριση της ασφάλειας πληροφοριών, η οποία έχει ως απώτερο στόχο τον σχεδιασμό και την εφαρμογή στρατηγικών ασφάλειας σε έναν αποτελεσματικό τρόπο. (Ezingeard και Bowen-Schrire, 2007).

Δεδομένου ότι, όλα τα προϊόντα τεχνικής ασφάλειας πρέπει να λειτουργούν και να διαχειρίζονται από άτομα, μια λύση τεχνικής ασφάλειας από μόνη της δεν μπορεί να προστατεύσει έναν οργανισμό χωρίς μια καλή πολιτική και πρακτική διαχείρισης ασφάλειας. Μπορούν να υποστηριχθούν στρατηγικές μεταξύ εταίρων εντός της οργάνωσης και να διευκολύνεται από συστήματα και τεχνολογίες ασφάλειας πληροφοριών. Όμως, δεν είναι εξασφαλισμένο από αυτούς. Η τεχνολογία ασφάλειας πληροφοριών είναι απαραίτητη αλλά δεν επαρκεί για την επιτυχία ενός συστήματος είτε σε ενδοοργανωτικό επίπεδο είτε σε δια-οργανωτικούς εταίρους. Επομένως, οι επιχειρήσεις πρέπει να υιοθετήσουν μια ολοκληρωμένη στρατηγική που θα συνδυάζει και τα δύο.

Πρώτα την ασφάλεια πληροφοριών αλλά και τις πτυχές της οργάνωσης, εστιάζοντας όχι μόνο στα «εξωτερικά» αντικείμενα και μοτίβα συμπεριφοράς που είναι ορατά και ακούγονται, αλλά και στα «εσωτερικά», την ανθρώπινη φύση, την δραστηριότητα και τις σχέσεις που είναι κρυμμένες και κυρίως μη αισθητές. Επιτυγχάνοντας, έτσι την αποτελεσματικότητα της «εξωτερικής» πλευράς των πληροφοριών.

Η ασφάλεια απαιτεί την «εσωτερική» πτυχή μιας οργανωσιακής κουλτούρας που είναι ενσωματωμένη στις αξίες και τις πεποιθήσεις της ασφάλειας πληροφοριών που μοιράζονται όλες οι μονάδες, σε όλα τα επίπεδα μίας οργάνωσης. Ως κοινή πίστη και πρακτική κάθε μέλους σε έναν οργανισμό, η εφαρμογή μιας ολοκληρωμένης πρακτικής και οργανωσιακής ασφάλειας πληροφοριών, η κουλτούρα, θα μείωνε τελικά τη ζημία σημαντικών γεγονότων ασφάλειας πληροφοριών (Bodin k.a., 2008).

Η προσέγγιση διαχείρισης αλλαγής της ασφάλειας πληροφοριών, εφαρμόστηκε για να απεικονίσει τον τρόπο με τον οποίο αναπτύσσονται οι παρεμβάσεις λαμβάνοντας υπόψη τα δεδομένα που συλλέγονται από το διαγνωστικό μέσο ISCA. Αυτό έχει ως στόχο να δημιουργηθεί στους εργαζομένους η επιθυμία της αλλαγής και να ενισχυθεί, με μια έρευνα παρακολούθησης της εφαρμογής της αλλαγής μετά την υλοποίηση των προσδιορισμένων ενεργειών. Συζητήθηκαν οι γενικές φάσεις της διαχείρισης αλλαγής ασφάλειας πληροφοριών, δηλαδή η καθιέρωση της τρέχουσας κατάστασης, η μετάβαση, η μελλοντική κατάσταση, καθώς και οι δραστηριότητες στις φάσεις ADKAR.

Τα δεδομένα της έρευνας κατακερματίστηκαν για να εντοπίσουν και να δώσουν προτεραιότητα σε δημογραφικές ομάδες υψηλού κινδύνου για παρεμβάσεις για την ενημέρωση των σχεδίων δράσης στις φάσεις ADKAR.

Ορισμένα γραφεία του συμμετέχοντος οργανισμού προσδιορίστηκαν ως περιοχές υψηλού κινδύνου με βάση τη χαμηλή μέση βαθμολογία σε επίπεδα διαστάσεων και μεμονωμένων δηλώσεων. Ο συνολικός μέσος όρος της κουλτούρας ασφάλειας πληροφοριών βελτιώθηκε από τη μία έρευνα στην άλλη, με σημαντικές βελτιώσεις σε ατομικό επίπεδο δήλωσης και για τα γραφεία.

Η προσέγγιση διαχείρισης αλλαγής της πληροφοριακής ασφάλειας χρησιμεύει ως μια δομημένη προσέγγιση που συνδυάζει στοιχεία του ADKAR και του ISCA για να κατευθύνει τις προσπάθειες αλλαγής της κουλτούρας ασφάλειας πληροφοριών σε έναν οργανισμό για να ελαχιστοποιήσει τα περιστατικά που σχετίζονται με ανθρώπινο λάθος ή αμέλεια όταν οι εργαζόμενοι επεξεργάζονται πληροφορίες. Αυτό βοηθά τη διοίκηση, για παράδειγμα, στην ανάπτυξη προγραμμάτων κατάρτισης και ευαισθητοποίησης για την ασφάλεια των πληροφοριών που δεν βασίζονται σε ξεπερασμένες υποθέσεις, αλλά στην κατάσταση ως έχουν. Επιτρέπει στη διοίκηση να κατανέμει αποτελεσματικά τους πόρους, να δίνει προτεραιότητα σε επιχειρηματικούς τομείς υψηλού κινδύνου και να παρακολουθεί την επιτυχία και τον αντίκτυπο των παρεμβάσεων. Βοηθά τη διοίκηση να υλοποιήσει πρωτοβουλίες σκόπιμα από μια ευρύτερη προοπτική, προκειμένου να δημιουργήσει μια φιλοδοξία για αλλαγή και να ενισχύσει τις αλλαγές συνεχώς μέσα από μια ποικιλία προσπαθειών.

Για την κατανόηση και τη βελτίωση της συμπεριφοράς της οργάνωσης σε κάθε επίπεδο, σε ότι αφορά την ασφάλεια των πληροφοριών, οι επιχειρήσεις μπορούν να εξετάζουν την οργανωσιακή κουλτούρα και τον τρόπο που επηρεάζει την πρακτική ασφάλειας πληροφοριών. Το πρώτο βήμα για την επίτευξη του στόχου της ασφάλειας πληροφοριών είναι η αξιολόγηση των προϋποθέσεων της οργανωσιακής κουλτούρας για τον ISM.

Για παράδειγμα, διαφορετικές υποομάδες εντός ενός οργανισμού μπορεί να έχουν ορισμένα κοινά χαρακτηριστικά οργανωσιακής κουλτούρας, αλλά και βιώνουν μια μοναδική υπό-κουλτούρα σε κάποια συγκεκριμένη υποομάδα. Μια τέτοια παραλλαγή της οργανωσιακής κουλτούρας σε υποομάδες μπορεί τελικά να επηρεάσει την οργανωσιακή κουλτούρα στο σύνολό της. Η έρευνά μας συμβάλλει στην καλύτερη κατανόηση των σχέσεων μεταξύ της οργανωσιακής κουλτούρας , των χαρακτηριστικών και της αποτελεσματικότητας της εφαρμογής ISM (όπως αναλύεται σε προηγούμενες ενότητες ενώ καλύπτει εμπειρικά ευρήματα και επιπτώσεις). Μια καλύτερη κατανόηση αυτού του είδους μπορούν να προσφέρουν οι σχέσεις καθώς μπορούν να παρέχουν μια καλύτερη εικόνα για το πώς να διασφαλιστεί η ασφάλεια των πληροφοριών.

Η εφαρμογή της προσέγγισης αλλαγής της πληροφοριακής ασφάλειας μπορεί να έχει θετικό αντίκτυπο στην κουλτούρα ασφάλειας πληροφοριών σε έναν οργανισμό και μπορεί να έχει επιτυχή αποτελέσματα αλλαγής.

Η προσέγγιση της διαχείρισης αλλαγής της πληροφοριακής ασφάλειας αντιμετωπίζει ορισμένους περιορισμούς των υφιστάμενων προσεγγίσεων διαχείρισης αλλαγών, καθώς ενσωματώνει τακτική και επιχειρησιακή εστίαση κατά την εφαρμογή του σχεδίου και είναι οικονομικά αποδοτική επειδή βασίζεται σε έρευνα. Η ενσωμάτωση της έρευνας ISCA καθιστά την διαχείρισης αλλαγής ασφάλειας πληροφοριών, σχετικά με την ασφάλεια των πληροφοριών, διότι οι αντιλήψεις για την ασφάλεια των πληροφοριών των εργαζομένων αξιολογούνται με στόχο τη μετατροπή της κουλτούρας.

5.1. πρακτική εφαρμογή έρευνας

Η προσέγγιση διαχείρισης αλλαγής πληροφοριακής ασφάλειας μπορεί να βελτιωθεί με την ενσωμάτωση μεθόδων ποιοτικής αξιολόγησης για τον εντοπισμό ζητημάτων σε ένα συγκεκριμένο πλαίσιο. Περαιτέρω έρευνα μπορεί να επικεντρωθεί στην εφαρμογή της προσέγγισης της αλλαγής της πληροφοριακής ασφάλειας σε άλλες βιομηχανίες και στη δοκιμή της αποτελεσματικότητας της προσέγγισης με την πάροδο του χρόνου. Η αλλαγή μιας κουλτούρας θα μπορούσε να διαρκέσει πολλά χρόνια, αλλά εφαρμόζοντας μια δομημένη προσέγγιση όπως της διαχείρισης αλλαγής της ασφάλειας πληροφοριών, οι οργανισμοί μπορούν να μετατρέψουν σκόπιμα την κουλτούρα ασφάλειας των πληροφοριών σε μια επιθυμητή κατάσταση όπου η συμπεριφορά των εργαζομένων είναι σύμφωνη με τις οργανωτικές πολιτικές και τις απαιτήσεις για την προστασία των πληροφοριών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική βιβλιογραφία

1. Βασιλακόπουλος, Γ. και Χρυσικόπουλος Β. (1990)Πληροφοριακά συστήματα διοίκησης, Εκδόσεις Πειραιάς .
2. Φωλίνας Δ. (2006). Ολοκληρωμένα πληροφοριακά συστήματα διαχείρισης επιχειρηματικών πόρων, Αθήνα, Εκδόσεις Ανίκουλα.
3. Τασόπουλος Α. (2005). Πληροφοριακά συστήματα. Οργάνωση, μεθοδολογία, εφαρμογές, Αθήνα, Εκδόσεις Σταμούλη Α.Ε. ο

Ξενόγλωσση

4. Allen, D.K. and Fifield, N. (1999), "Re-engineering change in higher education", Information Research, Vol. 4 No. 3, available at: http://informationr.net/ir/4-3/paper56.html
5. Bali, R., Cockerham, G. and Bloor, C. (1999), "MISCO: a conceptual model for MIS implementation in SMEs", Information Research, Vol. 4 No. 4, available at: http://informationr.net/ir/4-4/paper61.html
6. Bishop, M. (2003), "What is computer security?", IEEE Security and Privacy, Vol. 1 No. 1, pp. 67-9.
7. Boggs, W.B. (2004), "TQM and organizational culture: a case study", The Quality Management Journal, Vol. 11 No. 2, pp. 42-52.
8. Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. Communications of the ACM, 51(4), 64–68.
9. Borglund, E. (2005), "Operational use of electronic records in police work", Information Research, Vol. 10 No. 4, available at: http://InformationR.net/ir/10-4/paper236.html
10. Cameron, K.S. (1991), "Culture congruence strength and type: relationship to effectiveness", Research in Organizational Change and Development, Vol. 5, pp. 23-58.
11. Connolly, L.Y., Lang, M., Gathegi, J. and Tygar, D.J. (2017), "Organisational culture, procedural countermeasures, and employee security behavior: a qualitative study", Information and Computer Security, Vol. 25 No. 2, pp. 118-136.

12. Davenport, T. H.& Prusak, L. (1998). What do we talk about when we talk about knowledge Working knowledge: How organizations manage what they know
13. Da Veiga, A. (2016), "Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study", Information and Computer Security, 24 (2). 139-151.
14. Ezingeard, J., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. Journal of General Management, 32(4), 53–72.
15. Gammelgaard, J., & Ritter, T. (2005). The knowledge retrieval matrix: codification and personification as separate strategies. Journal of Knowledge Management, 9(4), 133-143.
16. Karlsson, M., Denk, T. και Åström, J. (2018), "Perceptions of organizational culture and value conflicts in information security management", Information and Computer Security, 26(2) 213-229.
17. Kotulic, A.G. and Clark, J.G. (2004), “Why there aren’t more information security research studies”, Information & Management, Vol. 41 No. 5, pp. 597-607.
18. Laudon K., Laudon J. (2012). Management Information Systems: Managing the Digital Firm, 12th edition, Prentice Hall.
19. Kotulic, A.G. and Clark, J.G. (2004), “Why there aren’t more information security research
20. studies”, Information & Management, Vol. 41 No. 5, pp. 597-607.
21. Melton, C.E., Chen, J.C.H. and Lin, B. (2006), “Organisational knowledge and learning: leveraging it to accelerate the creation of competitive advantages”, International Journal of Innovation and Learning, Vol. 3 No. 3, pp. 254-66.
22. Nunnally, J.C. and Bernstein, I.H. (1994), Psychometric Theory, McGraw-Hill, New York, NY. Owens I., Wilson, T.D. and Abell, A. (1995), “Information and business performance: a study of information systems and services in high-performing companies”, Information Research,
23. Vol. 1 No. 2, available at: http://informationr.net/ir/1-2/paper5.html
24. Quinn, R.E. and Spreitzer, G.M. (1991), “The psychometrics of the competing values culture
25. instrument and an analysis of the impact of organization culture on quality of life”, Research in Organizational Change and Development, Vol. 5, pp. 115-42.

26. Sanderson, E. and Forcht, K.A. (1996), “Information security in business environment”, Information Management & Computer Security, Vol. 4 No. 1, pp. 32-7.
27. Schein, E. (1985), “Coming to a new awareness of organizational culture”, Sloan Management Review, Vol. 25 No. 2, pp. 3-16.
28. Sveiby, K. E., & Simons, R. (2002). Collaborative climate and effectiveness of knowledge work-an empirical study. Journal of Knowledge Management, 6(5), 420-433
29. Owens, I., Wilson, T.D. and Abell, A. (1995), “Information and business performance: a study of information systems and services in high-performing companies”, Information Research, Vol. 1 No. 2, available at: http://informationr.net/ir/1-2/paper5.html.
30. Quinn, R.E. and Spreitzer, G.M. (1991), “The psychometrics of the competing values culture instrument and an analysis of the impact of organization culture on quality of life”, Research in Organizational Change and Development, Vol. 5, pp. 115-42.
31. Ryan, S.D. and Bordoloi, B. (1997), “Evaluating security threats in mainframe and client/server environments”, Information & Management, Vol. 32 No. 3, pp. 137-46.
32. Sanderson, E. and Forcht, K.A. (1996), “Information security in business environment”, Information Management & Computer Security, Vol. 4 No. 1, pp. 32-7.
33. Schein, E. (1985), “Coming to a new awareness of organizational culture”, Sloan Management Review, Vol. 25 No. 2, pp. 3-16.
34. Schwartz, B. (1981), Vertical Classification: A Study in Structuralism and the Sociology of Knowledge, University Chicago Press, Chicago, IL.
35. Shih, D-H., Sun, P-L. and Lin, B. (2005), “Securing industry-wide EPC global network with WS-security”, Industrial Management & Data Systems, Vol. 105 No. 7, pp. 972-96.
36. Sudaporn, S. and Ogenyi, O. (2004), “The store loyalty of the UK's retail consumers”, The Journal of American Academy of Business, Cambridge, Vol. 5 Nos 1/2, pp. 503-9.
37. Szilagyi, A.D. and Wallace, M.J. (1987), Organizational Behavior and Performance, 5th ed., Scott, Foresman and Company, Glenview, IL.
38. Vroom, C. και von Solms, R. (2004), “Towards information security behavioral compliance”, Computers & Security, Vol. 23 No. 3, pp. 191-8.
39. Yeh, Y-J., Lai, S-Q. καιHo, C-T. (2006), “Knowledge management enablers: a case study”, Industrial Management & Data Systems, Vol. 106 No. 6, pp. 793-810.

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα Ι

Ερωτηματολόγιο

1. Παρακαλώ επιλέξτε το φύλο σας
   Άνδρας Γυναίκα

2. Παρακαλώ επιλέξτε την ηλικία σας
   18-25
   26-35
   36-45
   46-55
   55-64
   65+

3. Ποια είναι η θέση σας στην εταιρεία
   Ανώτατο στέλεχος
   Ανώτερο στέλεχος

4. Πόσα άτομα απασχολεί η επιχείρηση σας
   Κάτω από 400
   Πάνω από 400

5. Σε ποιόν κλάδο δραστηριοποιείται η επιχείρηση σας.
   Μεταποίηση
   Χρηματοπιστωτικές υπηρεσίες
   Υπηρεσίες γενικότερα
   Βιομηχανίες ηλεκτρονικών ειδών

6. Έχει η επιχείρηση σας κάποιο σύστημα διαχείρισης της ασφάλειας
   Ναι Όχι

7. Σημειώστε την σωστή απάντηση ανάλογα με το κατά πόσο συμφωνείτε με τις παρακάτω προτάσεις.

	Διαφωνώ απόλυτα	Διαφωνώ	Ούτε συμφωνώ ούτε διαφωνώ	Συμφωνώ	Συμφωνώ απόλυτα
Μεταβλητή: Εμπιστοσύνη					
➢ Οι διαχειριστές εμψυχώνουν το προσωπικό ➢ Οι διαχειριστές συμπεριφέρονται στο προσωπικό σαν να είναι μέλη της οικογένειάς τους ➢ οι υπάλληλοι στην εταιρεία είναι έμπιστοι και εμπιστεύονται ο ένας τον άλλον ➢ Η επιχείρηση ενθαρρύνει τους υπαλλήλους να συμμετέχουν σε όλες τις δραστηριότητες της εταιρείας ➢ Οι υπάλληλοι είναι αφοσιωμένοι στο να προστατεύσουν τον οργανισμό ➢ οι υπάλληλοι νιώθουν πως οι διαχειριστές τους εμπιστεύονται και μπορούν να συμμετέχουν στην διαδικασία διαμόρφωσης μιας απόφασης					
Μεταβλητή : Καινοτομία					
➢ Οι διαχειριστές καθοδηγούν το προσωπικό ώστε να αναπτυχθεί και να προάγει την καινοτομία ➢ Οι διαχειριστές έχουν ένα όραμα για να δημιουργήσουν νέες ευκαιρίες μέσα στον οργανισμό					

➢ Οι εργαζόμενοι αντιμετωπίζουν τις προκλήσεις και μαθαίνουν να εξελίσσονται μέσα από αυτές ➢ Οι διαχειριστές ενθαρρύνουν την καινοτομία και την ανάληψη ρίσκου					
Μεταβλητή : Αποτελεσματικότητα					
➢ Η επιχείρηση δίνει μεγάλη σημασία στο να εργάζεται αποτελεσματικά κάθε τμήμα και κάθε εργαζόμενος πρέπει να συνεργάζεται με τους άλλους ➢ Για καλύτερη αποτελεσματικότητα η επιχείρηση δίνει μεγάλη σημασία στη διατήρηση των συγκριτικών πλεονεκτημάτων ➢ Η επιχείρηση προωθεί την αύξηση της αποτελεσματικότητας μέσω των εργαζομένων					
Μεταβλητή : διάχυση γνώσης					
➢ Πιστεύω πως αυτοί που συνεργάζονται μέσα στην εταιρεία δεν πρέπει να μοιράζονται τις πληροφορίες ➢ Οι συνάδελφοι μέσα στην εταιρεία από κοινού ανταλλάσσουν τις γνώσεις και την εμπειρία τους ενώ δουλεύουν πάνω σε κάποιο πρόβλημα μέσα στην εταιρεία ➢ Δεν υπάρχει το φαινόμενο κάποιοι από τους εργαζόμενους να κρατάνε τις πληροφορίες και τις γνώσεις που έχουν για τον εαυτό τους					

➢ υπάρχουν συγκεκριμένοι κανόνες μέσα στην εταιρεία που προστατεύουν κάποιον εργαζόμενο από κακές προθέσεις των άλλων όταν αυτός μοιράζεται πληροφορίες και γνώσεις πάνω σε κάποιο αντικείμενο ➢ Στο παρελθόν με έχουν βλάψει όταν επιχείρησα να μοιραστώ τη γνώση και την εμπειρία μου με τους συναδέλφους μου ➢ Πιστεύω ότι οι άνθρωποι μέσα στην εταιρεία θα διστάσουν να εκμεταλλευτούν τις πληροφορίες τις γνώσεις και την εμπειρία που διαχέεται από άλλους για προσωπικούς σκοπούς ➢ Η διάχυση της γνώσης μέσα στην εταιρεία ανταμείβεται και δίνονται κίνητρα προκειμένου να παρακινούνται οι εργαζόμενοι να μοιραστούν τις γνώσεις τους					
Μεταβλητή: Ασφάλεια συστημάτων-Αλλαγή ασφάλειας πληροφοριακών συστημάτων					
➢ Η επιχείρηση πραγματοποιεί ελέγχους ασφάλειας προκειμένου να διασφαλίσει την προστασία των ευαίσθητων πληροφοριών και των μυστικών της επιχείρησης ➢ οι υπάλληλοι χωρίς δικαιοδοσία δεν επιτρέπεται να έχουν πρόσβαση στις πηγές πληροφορίας της επιχείρησης					

➢ Οι υπάλληλοι πρέπει να ακολουθούν τις πολιτικές της εταιρείας και τους κανονισμούς όταν μεταδίδουν πληροφορίες μεταφέρουν πληροφορίες ➢ τα μέτρα ασφάλειες πληροφοριών εφαρμόζονται από την επιχείρηση για να για να προστατεύσουν τις ευαίσθητες πληροφορίες από διάχυση τους σε άτομα που δεν έχουν πρόσβαση ή δικαιοδοσία να τις γνωρίζουν ➢ η εταιρεία συχνά ανανεώνει τις πληροφορίες και δημιουργεί back up για να τις διασφαλίσει ➢ η επιχείρηση πολύ συχνά πραγματοποιεί ελέγχους και αξιολογήσεις σχετικά με το επίπεδο κινδύνου και ανανεώνει τα σχέδια ασφάλειας ➢ Με σκοπό να μειώσει την πιθανότητα απώλειας πληροφοριών η επιχείρηση έχει ελέγχους ασφάλειας όπως π.χ. διαδικασίες αλλαγής, διαχείρισης προκειμένου να αποτρέψει αλλαγές στις πληροφορίες χωρίς δικαιοδοσία ➢ οι βάσεις δεδομένων περιοδικά ανανεώνονται και διατηρούνται με σκοπό να υπάρχει ακρίβεια και αξιοπιστία των πληροφοριών ➢ Μέσα στα πλαίσια της αλλαγής της Ασφάλειας Πληροφοριακών Συστημάτων η εταιρεία προσπαθεί					

να μειώσει την πιθανότητα μιας διαρροής του συστήματος για να προστατεύσει τα δεδομένα της.					
Μεταβλητή : Εκπαίδευση εργαζομένων					
➢ Η επιχείρηση παρέχει επαρκή και ικανοποιητική εκπαίδευση για τους υπαλλήλους της πάνω στην ασφάλεια πληροφοριακών συστημάτων ➢ στα πλαίσια της εκπαίδευσης η επιχείρηση τοποθετεί ετικέτες και προειδοποιητικά σήματα τα οποία σχετίζονται με την ασφάλεια πληροφοριών.					
Μεταβλητή : Οργανωσιακή κουλτούρα					
➢ Οι μάνατζερ είναι σε θέση να θέσουν ξεκάθαρους στόχους σχετικά με την ασφάλεια των πληροφορικών συστημάτων ➢ η επιχείρηση έχει ξεκάθαρους κανόνες για τους εργαζόμενους σε ότι αφορά την ασφάλεια των πληροφοριακών συστημάτων ➢ η λειτουργία της επιχείρησης δίνει έμφαση στη σταθερότητα και τη διατήρηση της οργανωσιακής κουλτούρας					