Πρόγραμμα Μεταπτυχιακών Σπουδών στη
Φορολογική & Χρηματοοικονομική Διοίκηση
Στρατηγικών Αποφάσεων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

Διπλωματική εργασία

«ΣΥΝΕΙΣΦΟΡΑ ΕΣΩΤΕΡΙΚΟΥ ΕΛΕΓΧΟΥ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ»

της

ΑΝΑΣΤΑΣΙΑΣ ΓΩΓΟΥ

Επιβλέπων Καθηγητής: Δρογαλάς Γεώργιος

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του μεταπτυχιακού διπλώματος ειδίκευσης στη Φορολογική και Χρηματοοικονομική Διοίκηση Στρατηγικών Αποφάσεων

Θεσσαλονίκη,

Φεβρουάριος 2019

Πίνακας περιεχομένων

Περίληψη **4**

Abstract **5**

Ευχαριστίες **8**

Κεφάλαιο 1: Εισαγωγή **10**

1.1 Εισαγωγικές παρατηρήσεις 10

1.2 Αναγκαιότητα - Συνεισφορά Διπλωματικής Εργασίας 10

1.3 Σκοπός διπλωματικής εργασίας 11

1.4 Διάρθρωση Διπλωματικής Εργασίας 12

Κεφάλαιο 2: Θεωρητικό Πλαίσιο **13**

2.1 Εισαγωγή 13

2.2 Εννοιολογικό πλαίσιο εσωτερικού ελέγχου 13

2.3 Εννοιολογικό πλαίσιο της ασφάλειας των ηλεκτρονικών υπηρεσιών 14

Κεφάλαιο 3: Επισκόπηση ερευνών **16**

3.1 Εισαγωγή 16

3.2 Ρόλος εσωτερικού ελέγχου στην ασφάλεια ηλεκτρονικών υπηρεσιών 16

3.3 Εσωτερικός έλεγχος, ασφάλεια και εξειδίκευση γνώσεων 19

3.4 Εσωτερικός έλεγχος, ασφάλεια και πολιτικές-πλαίσια 20

3.5 Εσωτερικός έλεγχος, ασφάλεια και ανθρώπινος παράγοντας 22

Κεφάλαιο 4: Μεθοδολογία έρευνας **24**

4.1 Εισαγωγή 24

4.2 Πληθυσμός - Δείγμα 24

4.3 Ερωτηματολόγιο έρευνας 24

4.4 Μεθοδολογία Στατιστικής Ανάλυσης 26

Κεφάλαιο 5: Αποτελέσματα Έρευνας **27**

5.1 Εισαγωγή 27

5.2 Παρουσίαση Αποτελεσμάτων Περιγραφικής Στατιστικής 27

5.2.1 Δημογραφικά στοιχεία 27

5.2.2 Συμβουλευτικός ρόλος των εσωτερικών ελεγκτών 34

5.2.3 Σχέση μεταξύ εσωτερικών ελεγκτών και ειδικών της τεχνολογίας πληροφοριών 37

5.2.4 Εξειδικευμένες τεχνολογικές γνώσεις 41

5.2.5 Πολιτικές- πρότυπα ασφαλείας 46

5.2.6 Ενημέρωση-εκπαίδευση των εργαζομένων σε θέματα ασφαλείας 53

5.3 Παρουσίαση Αποτελεσμάτων Ανάλυσης Παλινδρόμησης....59
5.3.1 Εισαγωγικά- Ανάλυση Αξιοπιστίας....59
5.3.2 Πίνακας Συσχετίσεων....60
5.3.3 Ανάλυση πολλαπλής γραμμικής παλινδρόμησης....61
Κεφάλαιο 6: Συμπεράσματα, Περιορισμοί και Προτάσεις για Μελλοντική Έρευνα....68
6.1 Εισαγωγή....68
6.2 Συμπεράσματα....68
6.3 Περιορισμοί....70
6.4 Προτάσεις για Μελλοντική Έρευνα....71
Βιβλιογραφία....72
Ξενόγλωσση Βιβλιογραφία....72
Ελληνική Βιβλιογραφία....77
ΠΑΡΑΡΤΗΜΑ: ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΡΕΥΝΑΣ....78

Περίληψη

Οι επιχειρήσεις λειτουργούν σε ένα δυναμικό περιβάλλον, το οποίο μεταβάλλεται συνεχώς και ελλοχεύει διάφορους κινδύνους. Πιο συγκεκριμένα, οι επιχειρήσεις καλούνται να αντιμετωπίσουν ζητήματα που αφορούν την ασφάλεια των ηλεκτρονικών υπηρεσιών και των πληροφοριακών συστημάτων. Οι εσωτερικοί ελεγκτές, μέσω του πολύπλευρου ρόλου τους, μπορούν να συμβάλλουν στην άμβλυνση των περιστατικών παραβίασης των πληροφοριακών συστημάτων. Παρ' όλα αυτά, παρατηρείται περιορισμένος αριθμός ξένων ερευνών σχετικά με τη σύνδεση του εσωτερικού ελέγχου με την ασφάλεια των ηλεκτρονικών υπηρεσιών παγκοσμίως, όπως και πλήρη απουσία ελληνικών ερευνών. Υπό αυτό το πρίσμα, σκοπός της παρούσας διπλωματικής εργασίας είναι η εξέταση των παραγόντων που επιδρούν στην ασφάλεια των ηλεκτρονικών υπηρεσιών και ταυτόχρονα σχετίζονται με τον εσωτερικό έλεγχο. Για τους σκοπούς της έρευνας συντάχθηκε ερωτηματολόγιο μέσω των φορμών της Google, το οποίο στάλθηκε στις επιχειρήσεις που είναι εισηγμένες στο Χρηματιστήριο Αθηνών και είχε ως αποδέκτη τους εσωτερικούς ελεγκτές τους. Από τα συμπεράσματα της έρευνας προέκυψε πως ορισμένοι από τους παράγοντες που χρησιμοποιήθηκαν στην παλινδρόμηση επιδρούν στην ασφάλεια, ενώ κάποιοι άλλοι όχι, όμως απαιτείται περαιτέρω έρευνα, καθώς η παρούσα αποτελεί ένα πρώτο εγχείρημα προσέγγισης του συγκεκριμένου θέματος.

Λέξεις- Κλειδιά: ασφάλεια ηλεκτρονικών υπηρεσιών, πληροφοριακά συστήματα, εσωτερικός έλεγχος, παράγοντες, έρευνα.

Abstract

Businesses operate in a dynamic environment that is constantly changing and undermine various risks. In particular, businesses are asked to deal with issues that concern cyber security. Internal auditors, through their multifaceted role, can contribute to the reduction of the information systems' violation. Nevertheless, there is a limited number of foreign surveys on the connection between internal audit and cyber security worldwide, as well as there is complete absence of Greek surveys. Thus, the purpose of this thesis is to examine the factors that influence cyber security and at the same time are related to internal audit.
For the purposes of the survey, a questionnaire was created using Google forms, was sent to the companies listed on the Athens Stock Exchange and addressed to their internal auditors. The findings of the survey revealed that some of the factors that were used in the regression have an impact on cyber security, while others do not, but further research is needed as this is a first approach on this issue.

Keywords: cyber security, internal audit, factors, survey.

Κατάλογος Πινάκων

Πίνακας 1- Περιγραφικά στατιστικά ερώτησης 1 27
Πίνακας 2- Περιγραφικά στατιστικά ερώτησης 2 29
Πίνακας 3- Περιγραφικά στατιστικά ερώτησης 3 30
Πίνακας 4 -Περιγραφικά στατιστικά ερώτησης 4 31
Πίνακας 5 -Περιγραφικά στατιστικά ερώτησης 5 32
Πίνακας 6 -Περιγραφικά στατιστικά ερώτησης 6 33
Πίνακας 7 -Περιγραφικά στατιστικά ερώτησης 7 34
Πίνακας 8 -Περιγραφικά στατιστικά ερώτησης 8 35
Πίνακας 9 -Περιγραφικά στατιστικά ερώτησης 9 36
Πίνακας 10 -Περιγραφικά στατιστικά ερώτησης 10 38
Πίνακας 11 -Περιγραφικά στατιστικά ερώτησης 11 39
Πίνακας 12 -Περιγραφικά στατιστικά ερώτησης 12 40
Πίνακας 13 -Περιγραφικά στατιστικά ερώτησης 13 42
Πίνακας 14 -Περιγραφικά στατιστικά ερώτησης 14 43
Πίνακας 15 -Περιγραφικά στατιστικά ερώτησης 15 44
Πίνακας 16 -Περιγραφικά στατιστικά ερώτησης 16 46
Πίνακας 17 -Περιγραφικά στατιστικά ερώτησης 17 47
Πίνακας 18 -Περιγραφικά στατιστικά ερώτησης 18 48
Πίνακας 19 -Περιγραφικά στατιστικά ερώτησης 19 49
Πίνακας 20 -Περιγραφικά στατιστικά ερώτησης 20 51
Πίνακας 21 -Περιγραφικά στατιστικά ερώτησης 21 52
Πίνακας 22 -Περιγραφικά στατιστικά ερώτησης 22 53
Πίνακας 23 -Περιγραφικά στατιστικά ερώτησης 23 55
Πίνακας 24 -Περιγραφικά στατιστικά ερώτησης 24 56
Πίνακας 25 -Περιγραφικά στατιστικά ερώτησης 25 58
Πίνακας 26- Πίνακας αξιοπιστίας 60
Πίνακας 27- Συσχετίσεις εξαρτημένης μεταβλητής με τις ανεξάρτητες 60
Πίνακας 28- Συσχετίσεις μεταξύ των ανεξάρτητων μεταβλητών 61
Πίνακας 29- Σύνοψη μοντέλου 62
Πίνακας 30- Πίνακας ANOVA 63
Πίνακας 31- Πίνακας Coefficients 64
Πίνακας 32 – Ερευνητικές υποθέσεις 66

Πίνακας 33- Έλεγχος πολυσυγγραμικότητας 67
Πίνακας 34- Διαγνωστικός έλεγχος πολυσυγγραμικότητας.....67

Κατάλογος Εικόνων

Εικόνα 1-Διάγραμμα ράβδων ερώτησης 1 28
Εικόνα 2-Διάγραμμα ράβδων ερώτησης 2 29
Εικόνα 3-Διάγραμμα ράβδων ερώτησης 3 30
Εικόνα 4-Διάγραμμα ράβδων ερώτησης 4 31
Εικόνα 5-Διάγραμμα ράβδων ερώτησης 5 32
Εικόνα 6-Διάγραμμα ράβδων ερώτησης 6 33
Εικόνα 7-Διάγραμμα ράβδων ερώτησης 7 35
Εικόνα 8-Διάγραμμα ράβδων ερώτησης 8 36
Εικόνα 9-Διάγραμμα ράβδων ερώτησης 9 37
Εικόνα 10-Διάγραμμα ράβδων ερώτησης 10 38
Εικόνα 11-Διάγραμμα ράβδων ερώτησης 11 40
Εικόνα 12-Διάγραμμα ράβδων ερώτησης 12 41
Εικόνα 13-Διάγραμμα ράβδων ερώτησης 13 43
Εικόνα 14-Διάγραμμα ράβδων ερώτησης 14 44
Εικόνα 15-Διάγραμμα ράβδων ερώτησης 15 45
Εικόνα 16-Διάγραμμα ράβδων ερώτησης 16 46
Εικόνα 17-Διάγραμμα ράβδων ερώτησης 17 48
Εικόνα 18-Διάγραμμα ράβδων ερώτησης 18 49
Εικόνα 19-Διάγραμμα ράβδων ερώτησης 19 50
Εικόνα 20-Διάγραμμα ράβδων ερώτησης 20 51
Εικόνα 21-Διάγραμμα ράβδων ερώτησης 21 53
Εικόνα 22-Διάγραμμα ράβδων ερώτησης 22 54
Εικόνα 23-Διάγραμμα ράβδων ερώτησης 23 56
Εικόνα 24-Διάγραμμα ράβδων ερώτησης 24 57
Εικόνα 25-Διάγραμμα ράβδων ερώτησης 25 58

Ευχαριστίες

Παρ' όλο που η εκπόνηση της διπλωματικής εργασίας απαιτεί, κατά κοινή παραδοχή, προσωπική προσπάθεια, δεν θα μπορούσε να παραλειφθεί η σημαντική συμβολή του επιβλέποντα καθηγητή κ. Γεώργιου Δρογαλά, ο οποίος με τις πολύτιμες συμβουλές και την καθοδήγησή του συνέβαλε στην ταχύτερη εκπόνηση της διπλωματικής εργασίας. Επίσης, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς το διευθυντή του Μεταπτυχιακού Προγράμματος κ. Θεοφάνη Καραγιώργο, αλλά και στο διδακτικό προσωπικό συνολικά, για τη μεταλαμπάδευση των γνώσεων καθ' όλη τη διάρκεια των μαθημάτων.

Περαιτέρω, θα ήθελα να ευχαριστήσω την οικογένειά μου για την αμέριστη συμπαράσταση και υποστήριξη, ηθική και υλική, που μου παρείχε σε όλη τη διάρκεια του προγράμματος, καθώς και όλους τους συμμετέχοντες στην έρευνα, οι οποίοι με τις απαντήσεις τους συνέβαλαν στο τελικό αποτέλεσμα.

Κεφάλαιο 1: Εισαγωγή

1.1 Εισαγωγικές παρατηρήσεις

Τα τελευταία χρόνια, έχει αλλάξει ο τρόπος με τον οποίο λειτουργούν οι επιχειρήσεις, καθώς οι συνεχείς αλλαγές που προκύπτουν σε οικονομικό, τεχνολογικό ή οποιοδήποτε άλλο επίπεδο, καθιστούν επιτακτική την ανάγκη για ύπαρξη εσωτερικού ελέγχου (Drogalas et al., 2015; Siouziou et al., 2017). Σε ένα περιβάλλον αβέβαιο, οι επιχειρήσεις θα πρέπει να ανταποκρίνονται στην αβεβαιότητα και στους κινδύνους που ελλοχεύουν, με τη συμβολή του εσωτερικού ελέγχου να είναι καίριας σημασίας (Drogalas et al., 2016; Drogalas et al., 2015).

Ένας από τους πιο βασικούς, αλλά και ταυτόχρονα σύγχρονους κινδύνους, είναι αυτός που αφορά τη διατήρηση της ασφάλειας των ηλεκτρονικών υπηρεσιών (cybersecurity assurance). Αυτός ο κίνδυνος προέρχεται από την ψηφιοποίηση που επήλθε τα τελευταία χρόνια μέσω των πληροφοριακών συστημάτων που χρησιμοποιούν οι επιχειρήσεις. Η χρήση, όμως, αυτών των συστημάτων μπορεί να επιφέρει αρνητικές συνέπειες σε περίπτωση παραβίασής τους (Da Veiga & Eloff, 2007).

Οι παραβιάσεις στα συστήματα των επιχειρήσεων γίνονται όλο και πιο συχνές, με αποτέλεσμα οι απώλειες που υφίστανται οι επιχειρήσεις να είναι σημαντικές (Clark & Harrell, 2013). Γι’ αυτό, ο εσωτερικός έλεγχος, ο ρόλος του οποίου έχει διευρυνθεί εξαιτίας των σύγχρονων μεταβολών, πρέπει να συμβάλλει ενεργά στη διαφύλαξη της ασφάλειας των ηλεκτρονικών υπηρεσιών και διαδικασιών μιας επιχείρησης (Abu-Musa, 2008).

1.2 Αναγκαιότητα - Συνεισφορά Διπλωματικής Εργασίας

Τα συνεχώς αυξανόμενα περιστατικά παραβιάσεων στα πληροφοριακά συστήματα των επιχειρήσεων έχουν εφιστήσει την προσοχή των επιχειρήσεων στις μεθόδους που πρέπει να εφαρμόσουν, ώστε να περιοριστούν αυτά τα περιστατικά (Gordon et al., 2003). Η οικονομική κρίση δεν τα περιόρισε, αλλά τα επέτεινε, καθώς δημιούργησε μια γενικευμένη δυσαρέσκεια, ενισχύοντας τις παραβατικές συμπεριφορές (Broom, 2009). Η πλήρης εξάλειψή τους θεωρείται μη εφικτή σε μια εποχή, όπου το διαδίκτυο και οι εξελίξεις στον τεχνολογικό τομέα καλπάζουν, αλλά μπορεί να υπάρξει σωστή διαχείριση και προστασία (Kahyaoglu & Caliyurt, 2018).

Όμως, οι μέθοδοι που προτείνονται από τους ειδικούς της πληροφορικής δεν επαρκούν. Για να εξασφαλιστεί η ασφάλεια των πληροφοριακών συστημάτων που περιέχουν ευαίσθητες πληροφορίες, εκτός από τους ειδικούς στον τομέα πληροφορικής που μπορεί να έχει μια επιχείρηση, κρίνεται αναγκαία η συμβολή του εσωτερικού ελέγχου. (Eling & Schnell, 2016; Steinbart et al., 2018). Ο εσωτερικός

έλεγχος, μέσω του ευρέος φάσματος των προσφερόμενων υπηρεσιών του μπορεί να αποτελέσει τον ακρογωνιαίο λίθο στην άμβλυνση των περιστατικών παράβασης.

Παρά τη θετική επίδραση που μπορεί να έχει ο εσωτερικός έλεγχος στην ασφάλεια των ηλεκτρονικών υπηρεσιών, ελάχιστος αριθμός ερευνών προσεγγίζει το συγκεκριμένο θέμα (Steinbart et al., 2018). Η ασφάλεια των ηλεκτρονικών υπηρεσιών έχει μελετηθεί αρκετά από τους ειδικούς της πληροφορικής, όμως σε επιχειρηματικό επίπεδο παρουσιάζεται έλλειψη ερευνών (Eling & Schnell, 2016).

Για παράδειγμα, ο Fielden (2011) πρότεινε ένα ολιστικό πλαίσιο για την ασφάλεια πληροφοριών, συμπεριλαμβάνοντας κοινωνικούς και τεχνολογικούς παράγοντες. Κάποιες έρευνες, όπως των Clark and Harrell (2013), εστίασαν στη συμβολή των Διοικητικών Συμβουλίων των επιχειρήσεων στην ασφάλεια, υποστηρίζοντας ότι η επιχείρηση σαν σύνολο πρέπει να επενδύει στην ασφάλεια.

Από την άλλη, οι Sarens and De Beelde (2006) ερεύνησαν τη συμβολή του εσωτερικού ελέγχου στη διαχείριση κινδύνων και στην εταιρική διακυβέρνηση συγκρίνοντας αμερικάνικες και βέλγικες επιχειρήσεις. Επιπλέον, ο Thompson (1997) ασχολήθηκε με τα ηλεκτρονικά εγκλήματα στην Αυστραλία, δίνοντας έμφαση στις ηλεκτρονικές απειλές, αλλά και στη συμβολή των κρατικών οργάνων επιβολής νόμων στην ασφάλεια.

Υπό αυτό το πρίσμα, προκύπτει ερευνητικό ενδιαφέρον για τη διενέργεια θεωρητικής, αλλά και εμπειρικής έρευνας στην Ελλάδα στο ζήτημα των παραγόντων που σχετίζονται με τον εσωτερικό έλεγχο και επιδρούν στην ασφάλεια των πληροφοριακών συστημάτων με σκοπό τον εμπλουτισμό της διεθνούς βιβλιογραφίας και του ρόλου του εσωτερικού ελέγχου.

1.3 Σκοπός διπλωματικής εργασίας

Σκοπός της παρούσας διπλωματικής εργασίας είναι η εξέταση των παραγόντων που επιδρούν στην ασφάλεια των ηλεκτρονικών διαδικασιών και ταυτόχρονα σχετίζονται με τον εσωτερικό έλεγχο. Η εν λόγω εξέταση διεξάγεται μέσω θεωρητικής διερεύνησης, αλλά και μέσω ανάλυσης εμπειρικών δεδομένων που προκύπτουν μετά από έρευνα. Παράλληλα με αυτό το σκοπό, εξετάζονται και πέντε ερευνητικές υποθέσεις, οι οποίες διατυπώνονται σε επόμενο κεφάλαιο και έχουν ως στόχο την πληρέστερη ανάλυση του κύριου σκοπού της έρευνας.

1.4 Διάρθρωση Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία απαρτίζεται από έξι (6) κεφάλαια. Στο πρώτο κεφάλαιο, αρχικά, επισημαίνονται κάποιες εισαγωγικές παρατήσεις σχετικές με το θέμα της διπλωματικής εργασίας. Στη συνέχεια, τονίζονται η αναγκαιότητα-συνεισφορά της συγκεκριμένης διπλωματικής εργασίας, καθώς και ο σκοπός αυτής. Στο τέλος του πρώτου κεφαλαίου παρουσιάζεται η διάρθρωση των κεφαλαίων της διπλωματικής εργασίας.

Στο δεύτερο κεφάλαιο, αναλύεται το θεωρητικό πλαίσιο της διπλωματικής εργασίας. Πιο συγκεκριμένα, στην αρχή του κεφαλαίου, παρουσιάζεται το εννοιολογικό πλαίσιο του εσωτερικού ελέγχου, ενώ στη συνέχεια επισημαίνεται το εννοιολογικό πλαίσιο της ασφάλειας των ηλεκτρονικών υπηρεσιών.

Στο τρίτο κεφάλαιο, παρατίθενται κάποιες βασικές ερευνητικές προσεγγίσεις αναφορικά με το θέμα της εν λόγω διπλωματικής εργασίας. Αρχικά, παρουσιάζονται έρευνες σχετικά με το ρόλο και συμβολή του εσωτερικού ελέγχου στην ασφάλεια των ηλεκτρονικών διαδικασιών. Στη συνέχεια του κεφαλαίου, αναλύονται έρευνες που αφορούν την αναγκαιότητα ύπαρξης εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών και έρευνες σχετικά με το ρόλο του ανθρώπινου παράγοντα στην ασφάλεια. Τέλος, το κεφάλαιο ολοκληρώνεται με την παράθεση ερευνών που αφορούν τα πλαίσια και τις πολιτικές ασφαλείας.

Από το τέταρτο κεφάλαιο αρχίζει το εμπειρικό μέρος της διπλωματικής εργασίας. Πιο συγκεκριμένα, αρχικά παρουσιάζεται ο πληθυσμός και το δείγμα της εμπειρικής έρευνας, ενώ στη συνέχεια παρουσιάζεται ενδελεχώς το περιεχόμενο του ερωτηματολογίου της έρευνας. Τέλος, το τέταρτο κεφάλαιο ολοκληρώνεται με την παράθεση της μεθοδολογίας της στατιστικής ανάλυσης.

Στο πέμπτο κεφάλαιο ακολουθεί η παρουσίαση των αποτελεσμάτων που προέκυψαν από την επεξεργασία των ερωτηματολογίων. Πιο συγκεκριμένα, παρουσιάζονται τα αποτελέσματα από την περιγραφική στατιστική, όπου για κάθε ερώτηση προκύπτουν κάποιοι πίνακες και διαγράμματα που αφορούν συχνότητες και ποσοστά. Επιπλέον, γίνεται παρουσίαση των αποτελεσμάτων που προκύπτουν από την ανάλυση παλινδρόμησης.

Στο έκτο και τελευταίο κεφάλαιο καταγράφονται τα βασικά συμπεράσματα που προκύπτουν από τη διπλωματική εργασία, καθώς επίσης και γίνεται σύγκριση των αποτελεσμάτων της παρούσας έρευνας με άλλες έρευνες από τη βιβλιογραφία. Τέλος, το κεφάλαιο ολοκληρώνεται με την παρουσίαση των περιορισμών που προέκυψαν κατά τη διεξαγωγή της έρευνας και με την παράθεση προτάσεων για μελλοντική έρευνα.

Κεφάλαιο 2: Θεωρητικό Πλαίσιο

2.1 Εισαγωγή

Στο δεύτερο κεφάλαιο αναλύεται το θεωρητικό πλαίσιο της εργασίας. Πιο συγκεκριμένα, στην αρχή του κεφαλαίου παρουσιάζεται το εννοιολογικό πλαίσιο του εσωτερικού ελέγχου, ενώ μετέπειτα, αναλύεται το εννοιολογικό πλαίσιο αναφορικά με την ασφάλεια των ηλεκτρονικών υπηρεσιών.

2.2 Εννοιολογικό πλαίσιο εσωτερικού ελέγχου

Ο εσωτερικός έλεγχος άρχισε να εμφανίζεται τη δεκαετία του 1940 και αποτελεί, πλέον, αναπόσπαστο κομμάτι των επιχειρήσεων (Dittenhofer, 2001). Με την πάροδο των χρόνων, η σημασία του εσωτερικού ελέγχου ξεπέρασε τα στενά οικονομικά όρια και πλέον διαδραματίζει καθοριστικό ρόλο στη διαχείριση κάθε οντότητας (Drogalas et al., 2016; Siouziou et al., 2017).

Οι επιχειρήσεις, παρακολουθώντας τις εξελίξεις στην αγορά, πραγματοποιούν αλλαγές, ώστε η επιχείρησή τους να συμβαδίζει με τις νέες εξελίξεις. Σε αυτό το σημείο κρίνεται απαραίτητος ο εσωτερικός έλεγχος, αφού θα λειτουργήσει συμβουλευτικά προς τη διοίκηση και θα της παρέχει την απαραίτητη πληροφόρηση που απαιτείται για να λάβει αποφάσεις (Bou-Raad, 2000).

Ο ρόλος του εσωτερικού ελέγχου έγκειται στο να λειτουργεί ανεξάρτητα, να ελέγχει την επίτευξη των στόχων της επιχείρησης και να συμβάλλει στην ορθή διεκπεραίωση των λειτουργιών της (Drogalas et al., 2015). Πιο συγκεκριμένα, ο εσωτερικός έλεγχος λαμβάνει υπόψη την εταιρική διακυβέρνηση και επικουρεί τη διαχείριση κινδύνων, στοχεύοντας στην επίτευξη της αποτελεσματικής λειτουργίας της επιχείρησης μέσω συμβουλών, προτάσεων και ελέγχων (Cohen & Sayag, 2010; Drogalas et al., 2015).

Κομμάτι του ρόλου του εσωτερικού ελέγχου αποτελεί επιπλέον και η διαφύλαξη της συμμόρφωσης της επιχείρησης με κανόνες και νόμους που πρέπει να διέπουν τη λειτουργία της, όπως επίσης και η εξασφάλιση ότι η επιχείρηση λειτουργεί με ακεραιότητα (Dittenhofer, 2001).

Ελέγχοντας την ορθή λειτουργία της επιχείρησης, ο εσωτερικός έλεγχος μπορεί να εντοπίσει διάφορες παραλείψεις και πιθανούς κινδύνους, με συνέπεια να λαμβάνονται τα απαραίτητα μέτρα για την αποφυγή αρνητικών συμβάντων. Ο εσωτερικός έλεγχος είναι αποτελεσματικός, όταν διασφαλίζει την ανεξαρτησία του από τη διοίκηση, όταν υπάρχει επαγγελματική κατάρτιση και εκπαίδευση των ατόμων που τον διενεργούν, αλλά και όταν επιτελεί τους σκοπούς των ενδιαφερόμενων μερών της επιχείρησης (Cohen & Sayag, 2010).

Η σωστή λειτουργία του εσωτερικού ελέγχου μπορεί να επιφέρει θετικές επιδράσεις στην επιχείρηση, μεταξύ άλλων τον περιορισμό των παραβιάσεων και των εξαπατήσεων, καθώς επίσης και την ακεραιότητα και ασφάλεια των πληροφοριών (Siouziou et al., 2017).

2.3 Εννοιολογικό πλαίσιο της ασφάλειας των ηλεκτρονικών υπηρεσιών

Η ραγδαία ανάπτυξη της τεχνολογίας και η χρήση των νέων τεχνολογιών από τις επιχειρήσεις δημιουργεί την ανάγκη για προστασία έναντι κακόβουλων ενεργειών που θα έχουν ως στόχο τα πληροφοριακά συστήματα (Gordon et al., 2003; Hannaford, 1995). Η ασφάλεια των ηλεκτρονικών υπηρεσιών αφορά την ασφάλεια στα πλαίσια του κυβερνοχώρου, δηλαδή μεταξύ δικτύων που επικοινωνούν μεταξύ τους μέσω υπολογιστών (Eling & Schnell, 2016).

Βασικό μέλημα των επιχειρήσεων είναι να έχουν πληροφοριακά συστήματα που δε θα επιτρέπουν την πρόσβαση σε μη εξουσιοδοτημένους χρήστες, ώστε να διασφαλίζεται ότι οι πληροφορίες τους δεν θα είναι ευάλωτες σε υποκλοπές ή σε άλλα περιστατικά παραβάσεων (Gordon et al., 2003). Οι Cebula and Young (2010) ορίζουν τους διαδικτυακούς κινδύνους ως «λειτουργικούς κινδύνους σε πληροφοριακά και τεχνολογικά στοιχεία, τα οποία έχουν συνέπειες που επηρεάζουν την εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των πληροφοριών ή των πληροφοριακών συστημάτων» (σελ.16).

Η ασφάλεια θα πρέπει να εντάσσεται στο λογισμικό, αλλά και στο λειτουργικό σύστημα των υπολογιστών, καθώς τα πληροφοριακά συστήματα θα πρέπει κι από μόνα τους να έχουν κάποιο επιθυμητό επίπεδο ασφάλειας. Επιπλέον, έμφαση πρέπει να δοθεί και στα δίκτυα μέσω των οποίων επικοινωνούν μεταξύ τους οι υπάλληλοι της επιχείρησης, αλλά και σε διοικητικό επίπεδο, αφού θα πρέπει να υπάρχει μια ενιαία πολιτική ασφαλείας που θα αποτρέπει και θα αντιμετωπίζει πιθανούς κινδύνους (Hannaford, 1995).

Οι επιχειρήσεις, πλέον, έρχονται αντιμέτωπες με νέους κινδύνους, όπως οι επιθέσεις που λαμβάνουν χώρα στον ψηφιακό κόσμο (Trim & Lee, 2010). Οι επιθέσεις αυτές μπορούν να έχουν κάποιες από τις εξής μορφές:

- Εξαπάτηση: οι εισβολείς στα πληροφοριακά συστήματα έχουν ως στόχο να παραποιήσουν τα δεδομένα, ώστε να εξασφαλίσουν το προσωπικό τους όφελος, ζημιώνοντας άλλα πρόσωπα.
- Δημιουργία προβλημάτων στα πληροφοριακά συστήματα μέσω κακόβουλων λογισμικών: οι εισβολείς στοχεύουν στο να παρέμβουν στην ορθή λειτουργία των συστημάτων και να περιορίσουν τη λειτουργικότητά τους. Χαρακτηριστικά παραδείγματα είναι οι ιοί και οι Δούρειοι Ίπποι (Hannaford, 1995; Souppaya & Scarfone, 2013).

- Κλοπή δεδομένων (Kahyaoglu & Caliyurt, 2018).

Όλα τα παραπάνω μπορούν να οδηγήσουν σε σοβαρές αρνητικές συνέπειες για την επιχείρηση, όπως έλλειψη εμπιστοσύνης και απώλεια πελατών που συντελούν σε απώλειες σε οικονομικό επίπεδο (Eling & Schnell, 2016).

Η αποτελεσματικότητα της ασφάλειας των ηλεκτρονικών διαδικασιών και συστημάτων, με βάση τους Steinbart et al. (2015) and Steinbart et al. (2018) μπορεί να μετρηθεί με τον αριθμό των περιστατικών παραβίασης του τελευταίου χρόνου, με την τάση αυτών των περιστατικών τα τελευταία 3 χρόνια και με τον αριθμό των περιστατικών που ανιχνεύθηκαν και αντιμετωπίστηκαν προτού προκαλέσουν αρνητικές συνέπειες στην επιχείρηση.

Σύμφωνα με τα προαναφερθέντα, γίνεται κατανοητό ότι η ύπαρξη πολιτικών ασφαλείας, αλλά και συστημάτων διαχείρισης κινδύνων είναι επιτακτική(Gordon et al., 2003). Η έμφαση στην ασφάλεια πρέπει να δοθεί στη φάση σχεδιασμού των συστημάτων, καθώς μετέπειτα δε θα λειτουργήσει ορθά (Bednar et al., 2013). Παρόλα αυτά, δεν έχει δημιουργηθεί κάποιο συγκεκριμένο μοντέλο για τη διαχείριση της ασφάλειας των ηλεκτρονικών υπηρεσιών που να χρησιμοποιείται ευρέως από τις επιχειρήσεις (Atoum et al., 2014; Eling & Schnell, 2016).

Κεφάλαιο 3: Επισκόπηση ερευνών

3.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο αναλύονται σημαντικές ερευνητικές προσεγγίσεις σχετικές με το θέμα της διπλωματικής εργασίας. Αρχικά, παρουσιάζονται έρευνες σχετικά με την αναγκαιότητα και συμβολή του εσωτερικού ελέγχου στην ασφάλεια των ηλεκτρονικών διαδικασιών. Στη συνέχεια του κεφαλαίου, αναλύονται έρευνες που αφορούν την αναγκαιότητα ύπαρξης εξειδικευμένων γνώσεων από την πλευρά των εσωτερικών ελεγκτών και έρευνες σχετικές με το ρόλο του ανθρώπινου παράγοντα στην ασφάλεια. Στο τέλος του κεφαλαίου, παρατίθενται έρευνες που αφορούν τα πλαίσια και τις πολιτικές ασφαλείας.

3.2 Ρόλος εσωτερικού ελέγχου στην ασφάλεια ηλεκτρονικών υπηρεσιών

Σε μια επιχείρηση πραγματοποιούνται και έλεγχοι IT, δηλαδή έλεγχοι που αφορούν την Τεχνολογία Πληροφοριών και διενεργούνται είτε από εξωτερικούς είτε από εσωτερικούς ελεγκτές, με στόχο την ομαλή λειτουργία των πληροφοριακών συστημάτων και την αποφυγή συμβάντων εξαπάτησης (Merhout & Havelka, 2008).

Σύμφωνα με τους Abdolmohammadi and Boss (2010), οι εσωτερικοί ελεγκτές θα πρέπει να διεξάγουν αυτούς τους ελέγχους, καθώς έχουν πιο στενή και άμεση σχέση με την επιχείρηση. Οι Coram et al. (2008), σε έρευνα που διεξήγαγαν σε 324 επιχειρήσεις στην Αυστραλία και τη Νέα Ζηλανδία, κατέληξαν ότι οι επιχειρήσεις που έχουν εσωτερικό έλεγχο εντοπίζουν πιο εύκολα τις απάτες που αφορούν υπεξαίρεση των περιουσιακών στοιχείων της επιχείρησης, σε σχέση με αυτές που έχουν εξωτερικούς ελεγκτές.

Οι Merhout and Havelka (2008), μέσω της τεχνικής της ονομαστικής ομάδας, εξέτασαν σε δύο στάδια την ποιότητα του ελέγχου IT έχοντας ως δείγμα οικονομικούς και IT ελεγκτές, καθώς και στελέχη ελέγχου IT. Η έρευνά τους οδήγησε στο συμπέρασμα ότι ένας από τους παράγοντες που επηρεάζουν την ποιότητα των ελέγχων είναι η συνεργασία μεταξύ των διαφόρων τμημάτων της επιχείρησης, του ελεγχόμενου τμήματος αλλά και της ανώτατης διοίκησης, καθώς έτσι υπάρχει καλύτερη ροή πληροφοριών.

Οι ίδιοι, λίγα χρόνια αργότερα, επεσήμαναν ότι αυτοί οι έλεγχοι είναι σημαντικοί, καθώς στοχεύουν στην ασφάλεια και την ακεραιότητα των πληροφοριών (Havelka & Merhout, 2013). Την ίδια άποψη υποστηρίζουν και οι Ransbotham and Mitra (2009) τονίζοντας ότι ο έλεγχος από την πλευρά των εσωτερικών ελεγκτών μπορεί να επιφέρει θετικά αποτελέσματα στις προσπάθειες της επιχείρησης για ασφάλεια.

Σύμφωνα με την έρευνα της Van Peursem (2004), η οποία αφορούσε τις απόψεις των εσωτερικών ελεγκτών για τα καθήκοντά τους σε δείγμα εσωτερικών ελεγκτών της Νέας Ζηλανδίας, μέλη του Ινστιτούτου των Εσωτερικών Ελεγκτών, ο ρόλος των εσωτερικών ελεγκτών είναι κυρίως συμβουλευτικός παρά επιβλητικός.

Εξειδικεύοντας το ρόλο τους αυτό, την επόμενη χρονιά, η Van Peursem (2005) διεξήγαγε συνεντεύξεις με ανάλογο δείγμα, από τις οποίες συνάγεται ότι οι εσωτερικοί ελεγκτές επικοινωνούν καθημερινά με υπαλλήλους της επιχείρησης και του τομέα IT, αλλά και με στελέχη μεσαίου επιπέδου σε ένα κλίμα συνεργασίας και ανταλλαγής απόψεων.

Η συνεργασία με τους υπαλλήλους του τομέα IT οδηγεί σε αύξηση των περιστατικών παραβίασης που ανιχνεύονται και εκμηδενίζονται προτού δημιουργήσουν ζημιογόνες επιπτώσεις στην επιχείρηση (Steinbart et al., 2018). Ο ρόλος τους είναι συμβουλευτικός και όχι παρεμβατικός στη διοίκηση, καθώς δεν λαμβάνουν οι ίδιοι αποφάσεις. Όπως επισημαίνει η Bou-Raad (2000), άπτεται της διοίκησης να αποφασίσει αν θα αποδεχτεί τις προτάσεις των εσωτερικών ελεγκτών ή όχι.

Επιπλέον, οι Stewart and Subramaniam (2010) τονίζουν ότι ο εσωτερικός έλεγχος έχει σε μεγάλο βαθμό συμβουλευτικό χαρακτήρα έχοντας ως απώτερο σκοπό την προσθήκη αξίας, το οποίο επαληθεύεται και από την έρευνα των Dittenhofer et al.(2011) σχετικά με τη συμπεριφορά και το ρόλο των εσωτερικών ελεγκτών.

Ο Bhattacharyya (2015) επισημαίνει ότι ο συμβουλευτικός χαρακτήρας τους προκύπτει από την ανεξαρτησία τους και συνεπώς την καλύτερη κατανόηση από μέρους τους των λειτουργιών των διαφόρων τμημάτων της επιχείρησης. Έχοντας επικοινωνία με στελέχη αλλά και υπαλλήλους, λειτουργεί ως «καθοδηγητής» και όχι ως «αστυνομικός».

Οι Steinbart et al. (2015) επισημαίνουν ότι η συμβολή του εσωτερικού ελέγχου στην ασφάλεια των πληροφοριακών συστημάτων έγκειται στο ότι απαιτείται ένας ανεξάρτητος από τη δημιουργία αυτών των συστημάτων παράγοντας, ο οποίος θα ελέγχει τη σωστή λειτουργία τους, άποψη που ασπάζονται και οι Islam et al. (2018).

Σύμφωνα με τους Maher and Akers (2003), η διεύρυνση του ρόλου των εσωτερικών ελεγκτών περιλαμβάνει και το να λειτουργούν ως σύμβουλοι στον τομέα της Τεχνολογίας Πληροφοριών (IT) και πιο συγκεκριμένα, στην ανάπτυξη των συστημάτων. Το ζήτημα που προκύπτει όμως, είναι αν οι εσωτερικοί ελεγκτές συνεχίζουν να δρουν ανεξάρτητα ή όχι. Διενεργώντας έρευνα σε 241 Διευθύνοντες Συμβούλους σχετικά με την άποψή τους επί αυτού του ζητήματος προέκυψε ότι θεωρούν πως το να παραμείνουν ανεξάρτητοι οι εσωτερικοί ελεγκτές είναι πιο σημαντικό από το να παρέχουν συμβουλές. Ο ρόλους τους, σύμφωνα με αυτούς, είναι ο έλεγχος της συνολικής ορθότητας των συστημάτων. Η ανεξαρτησία των εσωτερικών ελεγκτών έγκειται στο να επιτελούν το έργο τους χωρίς να επηρεάζονται

από την επιχείρηση ή από οποιοδήποτε ελεγχόμενο τμήμα και να παρέχουν αναφορές (Stoel et al., 2012).

Τα παραπάνω επιβεβαιώνονται και από τον ορισμό του εσωτερικού ελέγχου από το Institute of Internal Auditors (1999) που τονίζει την ανεξαρτησία του, την παροχή συμβουλών και τη συμβολή του στη διαχείριση κινδύνων.

Σύμφωνα με το The IIA Research Foundation (2015), η συμβολή του εσωτερικού ελέγχου κρίνεται επιτακτική στην ασφάλεια των ηλεκτρονικών διαδικασιών, καθώς σύμφωνα με την έρευνά τους αποτελεί το βασικότερο κίνδυνο για τις επιχειρήσεις. Ο εσωτερικός έλεγχος πρέπει ετησίως να ελέγχει πόσο ευάλωτη είναι η επιχείρηση σε κινδύνους, να διασφαλίζει ότι η επιχείρηση μπορεί να ανταπεξέλθει σε περίπτωση ατυχήματος και ότι υπάρχουν αντίγραφα ασφαλείας σημαντικών πληροφοριών. Το ίδιο επισημαίνουν και οι Brody and Kearns (2009), αφού τα αντίγραφα ασφαλείας και τα πλάνα ανάκαμψης είναι μείζονος σημασίας.

Οι Bauer and Estep (2018) τονίζουν ότι οι εσωτερικοί ελεγκτές πρέπει να συνεργάζονται με τους ειδικούς της τεχνολογίας πληροφοριών. Για να εξετάσουν τη σχέση μεταξύ των δύο μερών διεξήγαγαν ημι-δομημένες συνεντεύξεις με ειδικούς και από τις δύο κατηγορίες στις 4 μεγαλύτερες ελεγκτικές εταιρίες, προσπαθώντας να μάθουν τη γνώμη που έχουν τα δύο μέρη για τη μεταξύ τους σχέση. Όταν οι σχέσεις μεταξύ των δύο μερών είναι καλές, ο έλεγχος είναι αποτελεσματικός, καθώς υπάρχει ανταλλαγή γνώσεων και ο εντοπισμός σφαλμάτων είναι πιο έγκαιρος.

Από τα παραπάνω προκύπτει ότι η συνεργασία μεταξύ των εσωτερικών ελεγκτών και των ειδικών της τεχνολογίας πληροφοριών, καθώς και ο συμβουλευτικός ρόλος των εσωτερικών ελεγκτών λειτουργούν καταλυτικά στην ασφάλεια. Συνεπώς, αυτοί οι παράγοντες αναμένεται να οδηγούν σε μείωση της συχνότητας εμφάνισης των περιστατικών παραβίασης.

Έτσι, καταλήγουμε στην πρώτη ερευνητική υπόθεση, η οποία είναι:

Μηδενική υπόθεση H_0: *Η καλή σχέση μεταξύ του εσωτερικού ελέγχου και των ειδικών της τεχνολογίας πληροφοριών δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

Εναλλακτική υπόθεση H_1: *Η καλή σχέση μεταξύ του εσωτερικού ελέγχου και των ειδικών της τεχνολογίας πληροφοριών συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

Ενώ η δεύτερη ερευνητική υπόθεση είναι:

Μηδενική υπόθεση H_0: *Ο συμβουλευτικός ρόλος του εσωτερικού ελέγχου δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

Εναλλακτική υπόθεση H_1: *Ο συμβουλευτικός ρόλος του εσωτερικού ελέγχου συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

3.3 Εσωτερικός έλεγχος, ασφάλεια και εξειδίκευση γνώσεων

Ο ρόλος των εσωτερικών ελεγκτών έχει διευρυνθεί και πλέον θα πρέπει να έχουν και γνώσεις σχετικές με την Τεχνολογία Πληροφοριών (IT), δηλαδή γνώσεις IT (Stoel et al., 2012). Στην έρευνα που διεξήγαγε το The IIA Research Foundation (2015) σχετικά με τους 10 πιο σημαντικούς τεχνολογικούς κινδύνους που αντιμετωπίζουν οι επιχειρήσεις, όγδοος στη σειρά είναι οι τεχνολογικές γνώσεις των εσωτερικών ελεγκτών. Μόνο το 10% των ερωτηθέντων κατείχαν γνώσεις τεχνολογίας. Η λύση σε αυτό το πρόβλημα πρέπει να δοθεί αξιολογώντας, αρχικά, τα κενά που έχουν οι εσωτερικοί ελεγκτές σε επίπεδο τεχνολογικών γνώσεων και μετέπειτα παρέχοντάς τους την κατάλληλη εκπαίδευση, αλλά και τη δυνατότητα συνεργασίας με τους ειδικούς της πληροφορικής.

Οι Richards et al. (2005) υποστήριξαν ότι οι εσωτερικοί ελεγκτές θα πρέπει να έχουν:

- βασικές τεχνολογικές γνώσεις, δηλαδή γνώσεις λογισμικού, λειτουργικού συστήματος και δικτύων
- γνώσεις που αφορούν την ασφάλεια και προστασία από κινδύνους
- γνώσεις που αφορούν τη χρήση των πληροφοριακών συστημάτων που είναι απαραίτητα για τη διεκπεραίωση του ρόλου τους

Σε μια εποχή παγκοσμιοποίησης και συνεχούς ένταξης νέων τεχνολογιών στις διεργασίες των επιχειρήσεων, ο Abu-Musa (2008) τονίζει ότι οι εσωτερικοί ελεγκτές είναι απαραίτητο να επιβλέπουν και να επιτελούν το ρόλο τους έχοντας περαιτέρω γνώσεις σχετικές με τα πληροφοριακά συστήματα και τις τεχνολογίες που χρησιμοποιούν.

Οι Curtis et al.(2009) επισημαίνουν την αναγκαιότητα της ύπαρξης τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών στο συνεχές εξελισσόμενο τεχνολογικό περιβάλλον, ώστε να αξιολογούν πιο αποτελεσματικά τα πληροφοριακά συστήματα και να εντοπίζουν κινδύνους εξαπάτησης της επιχείρησης.

Ακόμη ένα συμπέρασμα που προκύπτει από την έρευνα των Wallace et al. (2011) σε 636 μέλη του Ινστιτούτου Εσωτερικών Ελεγκτών αναφορικά με τους ελέγχους IT είναι ότι, εκτός από τους ειδικούς της πληροφορικής, που συχνά επιτελούν τέτοιους ελέγχους, η προσθήκη των εσωτερικών ελεγκτών θα έχει επιπλέον οφέλη και για αυτό το λόγο είναι απαραίτητο να έχουν γνώσεις τεχνολογικές.

Οι Abdolmohammadi and Boss (2010) υποστηρίζουν ότι οι εσωτερικοί ελεγκτές πρέπει να έχουν εξειδικευμένες γνώσεις σχετικές με τα συστήματα, ώστε να επικουρούν τη διοίκηση στη λήψη αποφάσεων. Είναι επιθυμητό να έχουν κάποια επίσημη πιστοποίηση, όπως η CISA που συνδυάζει τεχνολογικές και οικονομικές γνώσεις και βάσει της έρευνάς τους επιδρά θετικά στους ελέγχους IT και είναι στατιστικά σημαντική. Αυτή η πιστοποίηση είναι διεθνώς αναγνωρισμένη για ελέγχους IT, καθώς διασφαλίζει ότι έχουν εξειδικευμένες γνώσεις (Petterson, 2005).

Άλλες πιστοποιήσεις όπως οι CIA, CMA, CPA δεν επιδρούν θετικά στους ελέγχους IT ή δεν είναι στατιστικά σημαντικές. Το συμπέρασμα που προκύπτει από την έρευνα είναι ότι πρέπει να υπάρξει περισσότερη εκπαίδευση των εσωτερικών ελεγκτών σε θέματα τεχνολογίας, ώστε να μειωθεί ο αριθμός των περιστατικών παραβιάσεων.

Από τα παραπάνω εξάγεται η εξής ερευνητική υπόθεση:

Μηδενική υπόθεση H_0: *Η ύπαρξη εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

Εναλλακτική υπόθεση H_1: *Η ύπαρξη εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

3.4 Εσωτερικός έλεγχος, ασφάλεια και πολιτικές-πλαίσια

Οι επιχειρήσεις θα πρέπει να υποστηρίζουν την ασφάλειά τους μέσω πλαισίων ασφάλειας πληροφοριών. Πολλά από αυτά τα πλαίσια μπορούν να διακριθούν σε πολιτικές, πρότυπα και πρακτικές-διαδικασίες-οδηγούς (Whitman & Mattord, 2003). Οι πολιτικές ασφαλείας αποτελούν εργαλείο της Ανώτατης Διοίκησης, συμβαδίζουν με τους στόχους και την αποστολή της επιχείρησης και περιλαμβάνουν τις υποχρεώσεις των εργαζομένων σχετικά με την ασφάλεια (Lee & Lee, 2002; Whitman & Mattord, 2003). Σύμφωνα με τους D' Arcy and Hovav (2007) and Whitman et al. (2001), οι πολιτικές ασφαλείας αφορούν ενδελεχείς οδηγίες σχετικά με τη διατήρηση της ασφάλειας.

Το ενδιάμεσο στάδιο αφορά τα πρότυπα, τα οποία επικουρούν την εφαρμογή των πολιτικών (D' Arcy & Hovav, 2007). Το επόμενο στάδιο αφορά πρακτικές-διαδικασίες-οδηγούς που περιλαμβάνουν πρακτικές οδηγίες και βήματα που πρέπει να ακολουθούνται, ώστε να εφαρμόζονται οι πολιτικές ασφαλείας και τα πρότυπα (Upfold & Sewry, 2005; Whitman & Mattord, 2003).

Μπορούν να χρησιμοποιηθούν διάφορα σχέδια ασφαλείας από μια επιχείρηση, όπως το NIST special publications, που ασχολείται με διάφορες εκφάνσεις της ασφάλειας ή το εγχειρίδιο RFC2196, το οποίο αποτελεί ένα πλαίσιο ασφαλείας και διαδικασιών που αφορά το Διαδίκτυο (Upfold & Sewry, 2005). Επιπλέον, το NIST SP 800-30 ασχολείται με τη διαχείριση κινδύνων που αφορούν την ασφάλεια (Fenz et al., 2014).

Το να ακολουθεί η επιχείρηση ένα διεθνές πρότυπο ή πλαίσιο, είναι καλύτερο από το να δημιουργεί από μόνη της κανόνες ασφαλείας, καθώς πρόκειται για διεθνώς αναγνωρισμένες πρακτικές (Upfold & Sewry, 2005). Για παράδειγμα, το πρότυπο

ISO 17799 αποτελεί ένα διεθνές πρότυπο και αποτελεί τη βάση για τη χάραξη πολιτικών ασφαλείας (D' Arcy & Hovav, 2007; Tabor, 2009).

Το πρότυπο ISO/IEC 27001 θεωρείται ένα από τα πιο γνωστά πρότυπα, καθώς παρέχει αρκετά στοιχεία που προωθούν την ασφάλεια, όπως την επιλογή ανάμεσα σε 114 ελέγχους, ώστε να κατανοήσει η επιχείρηση τι πρέπει να υλοποιήσει. Ο τρόπος με τον οποίο θα υλοποιηθεί ο στόχος δεν αναφέρεται, με αποτέλεσμα την εμφάνιση του ISO/IEC 27002 που στοχεύει περισσότερο στη φάση της υλοποίησης, παρόλο που λειτουργεί επικουρικά στο επίσημο ISO/IEC 27001 (Stewart & Jürjens, 2017).

Το ISO/IEC 27002 περιλαμβάνει το ISO 17799 με προσθήκες και παρέχει γενικές αρχές-οδηγίες σχετικά με την υλοποίηση και βελτίωση της ασφάλειας (ISO, 2005). Η αναθεωρημένη έκδοση του ISO/IEC 27001 είναι το ISO/IEC 27005:2018 που ασχολείται με τη διαχείριση κινδύνων που αφορούν την ασφάλεια (ISO, 2018).

Γενικότερα, τα πρότυπα ISO είναι τα πιο ευρέως διαδεδομένα πρότυπα ασφαλείας, όπως και το πλαίσιο COBIT, καθώς χρησιμοποιούνται συχνά από τις επιχειρήσεις για να διατηρήσουν την ασφάλεια των πληροφοριών τους (Sahibudin et al., 2008). Το κανονιστικό πλαίσιο COBIT (Control Objectives for Information and related Technology) αναπτύσσει και παρέχει αξιόπιστες οδηγίες και πρακτικές που χρησιμοποιούνται παγκοσμίως από ελεγκτές, στελέχη και υπαλλήλους, με σκοπό να κατανοήσουν τις διαδικασίες που πρέπει να ακολουθήσουν για να υποστηριχθεί η ασφάλεια (ITGI, 2007; Sahibudin et al., 2008). Η επιτυχία του επιβεβαιώνεται από πολλές επιχειρήσεις που το έχουν χρησιμοποιήσει παγκοσμίως (Damianides, 2004).

Οι Kayworth and Whitten (2010) διεξήγαγαν συνεντεύξεις με στελέχη που ασχολούνται με την ασφάλεια της επιχείρησης, ώστε να ερευνήσουν την προσέγγιση που θα πρέπει να έχουν απέναντι στη διατήρηση της ασφάλειας. Από την έρευνά τους προέκυψε ότι απαιτείται και η συμβολή του εσωτερικού ελέγχου στη διαφύλαξη της ασφάλειας, καθώς αξιολογεί ανεξάρτητα τις πολιτικές ασφαλείας και παραθέτει τα αποτελέσματα στην Ανώτατη Διοίκηση έχοντας ως αποτέλεσμα την αποτελεσματική στρατηγική ασφαλείας.

Οι Islam et al. (2018) επισημαίνουν ότι ο εσωτερικός έλεγχος θα πρέπει να εξετάζει αν υπάρχουν και αν εφαρμόζονται οι πολιτικές ασφαλείας. Πριν την εφαρμογή μιας στρατηγικής που θα έχει ως στόχο την ασφάλεια των ηλεκτρονικών διαδικασιών, ο εσωτερικός έλεγχος θα πρέπει ανεξάρτητα να ελέγχει αν έχουν ληφθεί υπόψη όλοι οι πιθανοί κίνδυνοι και αν η στρατηγική αυτή συμβαδίζει με τη στρατηγική της επιχείρησης (Kahyaoglu & Caliyurt, 2018).

Από τα παραπάνω προκύπτει ότι οι πολιτικές και τα πλαίσια ασφαλείας είναι ζωτικής σημασίας για την επιχείρηση, όσον αφορά τον τομέα της ασφάλειας. Η ύπαρξη και διασφάλιση αυτών από την πλευρά των εσωτερικών ελεγκτών κρίνεται επιτακτική, καθώς θα συμβάλλουν στη δημιουργία μιας στρατηγικής ασφαλείας που θα έχει ως στόχο τη μείωση της συχνότητας εμφάνισης των περιστατικών παραβίασης.

Συνεπώς, εξάγεται η κάτωθι ερευνητική υπόθεση:

Μηδενική υπόθεση H_0: *Οι πολιτικές-πρότυπα ασφαλείας που ελέγχονται από τον εσωτερικό έλεγχο δε συνδέονται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

Εναλλακτική υπόθεση H_1: *Οι πολιτικές-πρότυπα ασφαλείας που ελέγχονται από τον εσωτερικό έλεγχο συνδέονται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

3.5 Εσωτερικός έλεγχος, ασφάλεια και ανθρώπινος παράγοντας

Μια επιχείρηση μπορεί να δεχτεί επιθέσεις στα συστήματά της από εξωτερικούς ή εσωτερικούς παράγοντες. Οι εσωτερικοί παράγοντες αφορούν τους υπαλλήλους της, οι οποίοι εσκεμμένα ή μη, συμμετέχουν σε περιστατικά παραβιάσεων και βάσει ερευνών αποτελούν μεγάλο κομμάτι αυτών των περιστατικών(Abawajy, 2014; Guo et al., 2011; Stanton et al., 2005). Αυτή τους η συμπεριφορά μπορεί να προέρχεται από ελλιπή πληροφόρηση και εκπαίδευσή τους σχετικά με τους κανόνες ασφαλείας (Stewart & Jürjens, 2017).

Οι D' Arcy and Hovav (2007), με βάση την έρευνά τους σε εργαζομένους επιχειρήσεων στην Αμερική, τονίζουν ότι ο αριθμός των περιστατικών παραβίασης μπορούν να μειωθούν, αν οι εργαζόμενοι εκπαιδεύονται και ενημερώνονται τακτικά για την πολιτική και τους κανόνες ασφαλείας που πρέπει να τηρούν, καθώς η επίλυση του προβλήματος δεν μπορεί να προέλθει στηριζόμενοι μόνο στα τεχνικά θέματα (π.χ. τείχη προστασίας κ.ά.).

Οι Stanton et al.(2005) εξέτασαν τη συμπεριφορά εργαζομένων στην Αμερική σε θέματα ασφαλείας και κατέληξαν ότι οι χρήστες δεν τηρούν τους βασικούς κανόνες ασφαλείας και για αυτό το λόγο προτείνουν ότι πρέπει να υπάρξει περαιτέρω εκπαίδευση, αλλά και έλεγχός τους.

Ο Abawajy (2014) επισημαίνει την αναγκαιότητα ενός προγράμματος ενημέρωσης του προσωπικού σχετικά με τους κανόνες ασφαλείας, ώστε να κάνουν σωστή χρήση των συστημάτων και να διασφαλίζεται η μείωση των περιστατικών παραβίασης. Η ενημέρωση μπορεί να γίνει μέσω φυλλαδίων, σεμιναρίων, παρακολούθησης στοχευμένων βίντεο, συμμετοχής σε εκπαιδευτικά παιχνίδια ή μέσω προσομοίωσης ατυχημάτων, όπου στέλνονται κακόβουλα μηνύματα στους εργαζομένους για να διαπιστωθεί αν θα ανταποκριθούν σε αυτά και ύστερα ακολουθεί ενημέρωση και εκπαίδευσή τους.

Την ίδια άποψη ασπάζονται και οι Thomson and von Solms(1998), οι οποίοι τονίζουν ότι η ύπαρξη ενός προγράμματος ενημέρωσης και εκπαίδευσης των εργαζομένων κρίνεται επιτακτική, καθώς υπενθυμίζονται οι πολιτικές ασφαλείας και

η συμπεριφορά των εργαζομένων αλλάζει, ώστε να έχει ως κύριο στόχο την ασφάλεια.

Σύμφωνα με τους Ng et al. (2009), οι εργαζόμενοι λειτουργούν καταλυτικά στην ασφάλεια των ηλεκτρονικών υπηρεσιών, καθώς όντες χρήστες των πληροφοριακών συστημάτων, πρέπει να είναι προσεκτικοί και να τηρούν τους κανόνες ασφαλείας. Οι D'Arcy et al. (2009) τονίζουν ότι τα προγράμματα ενημέρωσης και εκπαίδευσης των εργαζομένων μπορούν να λειτουργήσουν αποτρεπτικά σε περιστατικά παραβίασης, καθώς ενημερώνουν τους εργαζομένους σχετικά με τις επιτρεπτές ενέργειες που μπορούν να εκτελέσουν, αλλά και τις συνέπειες που θα επιβληθούν σε περίπτωση παραβίασης.

Μέσω αυτών των προγραμμάτων, γίνεται κατανοητό ότι οι εργαζόμενοι αντιλαμβάνονται τις πολιτικές ασφαλείας (Whitman et al., 2001). Η επιτήρηση, από πλευράς της επιχείρησης, των ενεργειών των εργαζομένων θεωρείται επίσης ότι μπορεί να συμβάλλει θετικά στην ασφάλεια των ηλεκτρονικών υπηρεσιών (D'Arcy et al., 2009).

Οι Werlinger et al. (2009) εξέτασαν τις προκλήσεις που αντιμετωπίζουν οι εργαζόμενοι του τομέα της Τεχνολογίας Πληροφοριών στην προσπάθειά τους να παρέχουν όσο το δυνατόν περισσότερη ασφάλεια στην επιχείρηση. Η έρευνα είχε τη μορφή ημι-δομημένων συνεντεύξεων με 36 ειδικούς του τομέα της Τεχνολογίας Πληροφοριών που ασχολούνται με την ασφάλεια σε 17 οργανισμούς. Ένα από τα αποτελέσματα της έρευνας είναι ότι υπάρχει ελλιπής εκπαίδευση των εργαζομένων σε θέματα ασφαλείας, με συνέπεια να μην αντιλαμβάνονται σε μεγάλο βαθμό τους κινδύνους που ελλοχεύουν.

Σύμφωνα με τους Stafford et al. (2018), οι εσωτερικοί ελεγκτές πρέπει να ελέγχουν αν τηρούνται οι πολιτικές ασφαλείας από τους εργαζομένους και να διασφαλίζουν ότι οι εργαζόμενοι εκπαιδεύονται σε θέματα ασφάλειας. Ο ρόλος τους έγκειται, επίσης, στο να εντοπίσουν τους εργαζομένους που έχουν λιγότερη επίγνωση των πολιτικών ασφαλείας και γενικότερα στο να συμβαδίσουν τους στόχους της επιχείρησης που αφορούν την ασφάλεια με τις καθημερινές διεργασίες που λαμβάνουν χώρα. Μέσω συνεντεύξεων με επαγγελματίες ελεγκτές εντόπισαν ότι συνομιλώντας με τους εργαζομένους, οι εσωτερικοί ελεγκτές μπορούν να αντιληφθούν αν τηρούνται οι απαραίτητοι κανόνες ή ακόμα μπορούν να ελέγξουν το ιστορικό περιηγήσεώς τους.

Από τα παραπάνω εξάγεται η εξής ερευνητική υπόθεση:

Μηδενική υπόθεση H_0: *Η ενημέρωση-εκπαίδευση των εργαζομένων σε θέματα ασφαλείας δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

Εναλλακτική υπόθεση H_1: *Η ενημέρωση-εκπαίδευση των εργαζομένων σε θέματα ασφαλείας συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης*

Κεφάλαιο 4: Μεθοδολογία έρευνας

4.1 Εισαγωγή

Από το τέταρτο κεφάλαιο αρχίζει η ανάλυση του εμπειρικού μέρους της διπλωματικής εργασίας και πιο συγκεκριμένα, αναλύεται η έρευνα που διεξήχθη με σκοπό να εξεταστούν οι παράγοντες που επιδρούν στην ασφάλεια των ηλεκτρονικών διαδικασιών και ταυτόχρονα σχετίζονται με τον εσωτερικό έλεγχο. Στην αρχή του κεφαλαίου, παρουσιάζεται ο πληθυσμός και το δείγμα της εμπειρικής έρευνας. Στην πορεία, αναλύεται ενδελεχώς το περιεχόμενο του ερωτηματολογίου της εμπειρικής έρευνας, καθώς και η μεθοδολογία της στατιστικής ανάλυσης.

4.2 Πληθυσμός - Δείγμα

Ο εσωτερικός έλεγχος αποτελεί αναπόσπαστο και υποχρεωτικό κομμάτι όλων των επιχειρήσεων που είναι εισηγμένες στο Χρηματιστήριο Αθηνών. Έχοντας ως στόχο να εξεταστούν οι παράγοντες που σχετίζονται με τον εσωτερικό έλεγχο και επιδρούν στην ασφάλεια, ως δείγμα επιλέχθηκαν αποκλειστικά οι εσωτερικοί ελεγκτές που εργάζονται σε οντότητες εισηγμένες στο Χρηματιστήριο Αθηνών.

4.3 Ερωτηματολόγιο έρευνας

Το ερωτηματολόγιο αποτελεί τον καθοριστικό παράγοντα στη διεξαγωγή μιας έρευνας και γι’ αυτό το λόγο σχεδιάστηκε με πολλή προσοχή, ώστε να είναι σαφές και κατανοητό. Μετά από λεπτομερή έρευνα της διεθνούς βιβλιογραφίας, δημιουργήθηκε ηλεκτρονικό ερωτηματολόγιο μέσω των φορμών της Google, το οποίο στάλθηκε μέσω e-mail σε οντότητες εισηγμένες στο Χρηματιστήριο Αθηνών, ώστε να ερευνηθεί η σχέση μεταξύ των εσωτερικών ελεγκτών και των ειδικών της ασφάλειας πληροφοριών, το επίπεδο τεχνολογικών γνώσεων των εσωτερικών ελεγκτών, η ύπαρξη πολιτικών-πλαισίων ασφαλείας και η ενημέρωση και εκπαίδευση του προσωπικού σε θέματα ασφάλειας.

Οι ερωτήσεις του ερωτηματολογίου είναι 25, κλειστού τύπου και πολλαπλής επιλογής με βάση την κλίμακα τύπου Likert, όπου ο ερωτώμενος καλείται να δηλώσει το βαθμό στον οποίο ισχύουν οι εκάστοτε προτάσεις-ερωτήσεις σχετικά με το αντικείμενο της έρευνας. Στόχος ήταν η ταχεία συμπλήρωσή του και γι’ αυτό το λόγο διαχωρίστηκε σε πέντε (5) μέρη-θεματικές ενότητες, τα οποία αναλύονται στη συνέχεια.

Το μέρος Α του ερωτηματολογίου αποτελείται από 6 ερωτήσεις. Αρχικά, ο ερωτώμενος καλείται να απαντήσει σε τρεις (3) ερωτήσεις που αφορούν γενικά

χαρακτηριστικά της επιχείρησης και πιο συγκεκριμένα τον τομέα δραστηριότητας, τον αριθμό των εργαζομένων και τον ετήσιο κύκλο εργασιών (ερωτήσεις 1-3).

Στη συνέχεια, παρατίθενται τρεις (3) ερωτήσεις (ερωτήσεις 4-6) που αφορούν τα περιστατικά παραβιάσεων των πληροφοριακών συστημάτων της επιχείρησης. Ειδικότερα, οι ερωτήσεις 4 και 6 προήλθαν από την έρευνα των Steinbart et al. (2015), ενώ η ερώτηση 5 προήλθε από τους Steinbart et al. (2018). Οι ερωτήσεις αυτές στοχεύουν στην εξέταση της ασφάλειας μέσω των συμβάντων παραβιάσεων και επιθέσεων.

Το μέρος Β αποτελείται από έξι (6) ερωτήσεις (ερωτήσεις 7-12) και διερευνά το ρόλο του εσωτερικού ελέγχου στην ασφάλεια. Πιο συγκεκριμένα, στην αρχή παρατίθενται δύο (2) ερωτήσεις (ερωτήσεις 7-8) που προέρχονται από την έρευνα των Steinbart et al. (2015) και εξετάζουν το βαθμό του συμβουλευτικού ρόλου των εσωτερικών ελεγκτών έναντι του επιβλητικού ρόλου. Το δεύτερο μέρος ολοκληρώνεται με την παράθεση 4 ερωτήσεων (ερωτήσεις 9-12) που προήλθαν από τους Steinbart et al. (2018), μέσω των οποίων διερευνάται ο βαθμός συνεργασίας και καλής σχέσης των εσωτερικών ελεγκτών με τους ειδικούς της ασφάλειας πληροφοριών.

Το μέρος Γ του ερωτηματολογίου απαρτίζεται από τέσσερις (4) ερωτήσεις (ερωτήσεις 13-16) και ασχολείται με τις τεχνολογικές γνώσεις των εσωτερικών ελεγκτών. Ειδικότερα, δημιουργήθηκαν τέσσερις (4) ερωτήσεις με βάση την έρευνα των Stoel et al. (2012). Οι ερωτήσεις αυτές στοχεύουν στο να διερευνηθεί ο βαθμός ύπαρξης εξειδικευμένων γνώσεων τεχνολογίας και ασφάλειας από την πλευρά των εσωτερικών ελεγκτών, καθώς και ο βαθμός εκπαίδευσής τους σε περίπτωση μη ύπαρξης τεχνολογικών γνώσεων. Επιπλέον, διερευνάται η κατοχή ή μη από την πλευρά των εσωτερικών ελεγκτών της βασικής πιστοποίησης για ασφάλεια CISA.

Το μέρος Δ αποτελείται από πέντε (5) ερωτήσεις (ερωτήσεις 17-21) και ασχολείται με τις πολιτικές, τα πρότυπα και τα πλαίσια ασφαλείας που εφαρμόζονται στην κάθε οντότητα. Οι πρώτες 4 ερωτήσεις (ερωτήσεις 17-20) προήλθαν από την έρευνα των Upfold and Sewry (2005), ενώ η τελευταία ερώτηση (ερώτηση 21) προήλθε από τον Abu-Musa (2008). Αυτές οι ερωτήσεις διερευνούν το βαθμό κατά τον οποίο η κάθε οντότητα υιοθετεί και ακολουθεί συγκεκριμένα πρότυπα ή πλαίσια ασφαλείας, αλλά και την ύπαρξη μιας ενιαίας πολιτικής ασφαλείας πληροφοριών που να εφαρμόζεται στην επιχείρηση. Επιπρόσθετα, εξετάζουν και το βαθμό κατά τον οποίο ο εσωτερικός έλεγχος συμβάλλει στην εφαρμογή των παραπάνω.

Τέλος, το μέρος Ε αποτελείται από τέσσερις (4) ερωτήσεις (ερωτήσεις 22-25) και ασχολείται με την εκπαίδευση και τα προγράμματα ενημέρωσης του προσωπικού σε θέματα ασφάλειας ηλεκτρονικών διαδικασιών. Αρχικά, παρατίθενται 2 ερωτήσεις (ερωτήσεις 22-23) από τους D'Arcy et al. (2009), οι οποίες εξετάζουν το βαθμό κατά τον οποίο η επιχείρηση έχει συγκεκριμένες οδηγίες που καθορίζουν τη σωστή χρήση των πληροφοριακών συστημάτων από τους υπαλλήλους, αλλά και το βαθμό κατά τον

οποίο η επιχείρηση παρέχει εκπαίδευση στους εργαζομένους, ώστε να είναι ενημερωμένοι σε θέματα σωστής χρήσης και ασφάλειας πληροφοριών.

Στη συνέχεια, παρατίθεται μία (1) ερώτηση (ερώτηση 24) από τους Upfold and Sewry (2005), ώστε να εξεταστεί ο βαθμός κατά τον οποίο οι εργαζόμενοι είναι γνώστες της πολιτικής ασφάλειας πληροφοριών της επιχείρησης. Το μέρος Ε ολοκληρώνεται με την ερώτηση 25 από το The IIA Research Foundation (2015) σχετικά με το βαθμό διαφύλαξης, από την πλευρά των εσωτερικών ελεγκτών, της υποχρεωτικής ύπαρξης προγραμμάτων ενημέρωσης του προσωπικού για την ασφάλεια.

4.4 Μεθοδολογία Στατιστικής Ανάλυσης

Μετά τη συγκέντρωση των ερωτηματολογίων ακολουθεί η επεξεργασία τους. Ειδικότερα, για τη στατιστική επεξεργασία και ανάλυση των απαντήσεων του ερωτηματολογίου χρησιμοποιήθηκε το στατιστικό πακέτο λογισμικού SPSS 20 (Statistical Package for Social Sciences), το οποίο χρησιμοποιείται ευρέως στην πραγματοποίηση ποσοτικών ερευνών.

Οι απαντήσεις των ερωτηματολογίων καταγράφηκαν από τη φόρμα της Google σε ένα λογιστικό φύλλο excel και μετά, τα δεδομένα μεταφέρθηκαν και εισήχθησαν στο στατιστικό πακέτο λογισμικού SPSS. Τα δεδομένα επεξεργάστηκαν και προέκυψαν τα αποτελέσματα σε μορφή πινάκων και διαγραμμάτων.

Έχοντας ως στόχο την πληρέστερη ανάλυση των αποτελεσμάτων, διεξήχθη περιγραφική στατιστική, αλλά και ανάλυση παλινδρόμησης.

Κεφάλαιο 5: Αποτελέσματα Έρευνας

5.1 Εισαγωγή

Στο παρόν κεφάλαιο θα ακολουθήσει η ανάλυση και παρουσίαση των ευρημάτων που προέκυψαν από την έρευνα. Όπως, αναφέρθηκε και στο προηγούμενο κεφάλαιο, η επεξεργασία των στοιχείων που προέκυψαν από τα ερωτηματολόγια διεξήχθη μέσω του στατιστικού πακέτου SPPS. Από αυτό, προέκυψαν περιγραφικά στοιχεία, γραφήματα, πίνακες συσχετίσεων μεταξύ των μεταβλητών, καθώς και ανάλυση πολλαπλής παλινδρόμησης.

5.2 Παρουσίαση Αποτελεσμάτων Περιγραφικής Στατιστικής

Μέσω του στατιστικού πακέτου SPSS, δημιουργήθηκε για κάθε ερώτηση ένας πίνακας συχνότητας, ποσοστού, έγκυρου και αθροιστικού ποσοστού, ενώ ακολουθεί και σχηματική απεικόνιση των απαντήσεων με γράφημα (ραβδόγραμμα).

Τα ερωτηματολόγια απαντήθηκαν συνολικά από 72 επιχειρήσεις.

5.2.1 Δημογραφικά στοιχεία

Το πρώτο μέρος αφορά γενικές ερωτήσεις (ερωτήσεις 1-3) για τις επιχειρήσεις που έλαβαν μέρος στην έρευνα, καθώς και ερωτήσεις που αφορούν τα περιστατικά παραβίασης (ερωτήσεις 4-6). Η ερώτηση 1 εξετάζει τον τομέα δραστηριοποίησης των επιχειρήσεων. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

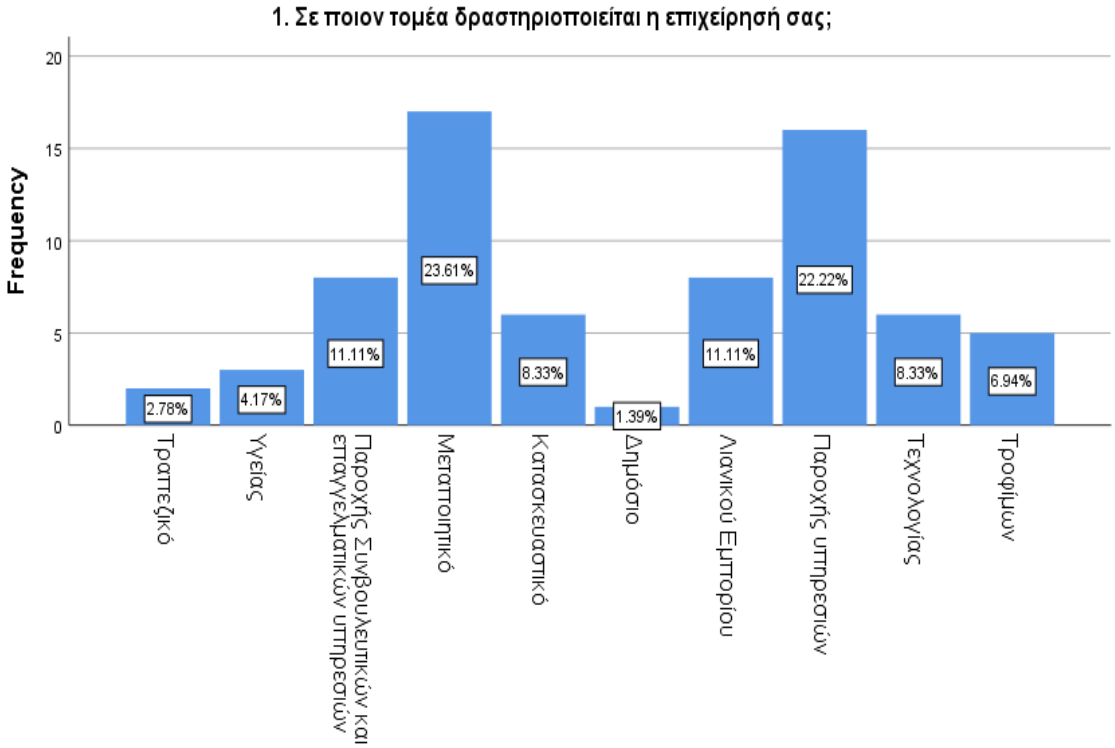
1. Σε ποιον τομέα δραστηριοποιείται η επιχείρησή σας;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Τραπεζικό	2	2.8	2.8	2.8
	Υγείας	3	4.2	4.2	6.9
	Παροχής Συμβουλευτικών και επαγγελματικών υπηρεσιών	8	11.1	11.1	18.1
	Μεταποιητικό	17	23.6	23.6	41.7
	Κατασκευαστικό	6	8.3	8.3	50.0
	Δημόσιο	1	1.4	1.4	51.4
	Λιανικού Εμπορίου	8	11.1	11.1	62.5
	Παροχής υπηρεσιών	16	22.2	22.2	84.7
	Τεχνολογίας	6	8.3	8.3	93.1
	Τροφίμων	5	6.9	6.9	100.0
	Total	72	100.0	100.0	

Πίνακας 1- Περιγραφικά στατιστικά ερώτησης 1

Από τις 72 επιχειρήσεις που έλαβαν μέρος στην έρευνα, οι 17 δραστηριοποιούνται στον μεταποιητικό (ποσοστό 23.6%), 16 στον τομέα παροχής υπηρεσιών (ποσοστό 22.2%), 8 στο λιανικό εμπόριο (ποσοστό 11.1%), 8 στον τομέα παροχής συμβουλευτικών και επαγγελματικών υπηρεσιών (ποσοστό 11.1%), 6 στον κατασκευαστικό (ποσοστό 8.3%), 6 στον τομέα τεχνολογίας (ποσοστό 8.3%), 5 στον τομέα τροφίμων (ποσοστό 6.9%), 3 στον τομέα υγείας (ποσοστό 4.2%), 2 στον τραπεζικό τομέα (ποσοστό 2.8%) και 1 στο δημόσιο (ποσοστό 1.4%).

Τα παραπάνω αποτελέσματα παρουσιάζονται και διαγραμματικά:



Εικόνα 1-Διάγραμμα ράβδων ερώτησης 1

Η ερώτηση 2 διερευνά τον αριθμό των υπαλλήλων της επιχείρησης. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

2. Ποιος είναι, προσεγγιστικά, ο αριθμός των υπαλλήλων της επιχείρησής σας;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	10-50	1	1.4	1.4	1.4
	50-250	4	5.6	5.6	6.9
	Πάνω από 250	67	93.1	93.1	100.0
	Total	72	100.0	100.0	

Πίνακας 2- Περιγραφικά στατιστικά ερώτησης 2

Όπως φαίνεται στον παραπάνω πίνακα, η πλειοψηφία των επιχειρήσεων έχει πάνω από 250 υπαλλήλους (ποσοστό 93.1%) και ακολουθούν 4 επιχειρήσεις (ποσοστό 5.6%) με 50-250 υπαλλήλους, ενώ μόνο 1 επιχείρηση έχει 10-50 υπαλλήλους (ποσοστό 1.4%).

Τα παραπάνω αποτελέσματα παρουσιάζονται και διαγραμματικά:

Εικόνα 2-Διάγραμμα ράβδων ερώτησης 2

Στην ερώτηση 3 εξετάζεται ο ετήσιος κύκλος εργασιών της επιχείρησης. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

3. Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών της επιχείρησής σας;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Κάτω από 2 εκατομμύρια	1	1.4	1.4	1.4
	10-50 εκατομμύρια	3	4.2	4.2	5.6
	Πάνω από 50 εκατομμύρια	68	94.4	94.4	100.0
	Total	72	100.0	100.0	

Πίνακας 3- Περιγραφικά στατιστικά ερώτησης 3

Όπως προκύπτει από τον πίνακα, παρατηρούμε ότι 68 από τις 72 επιχειρήσεις έχουν ετήσιο κύκλο εργασιών πάνω από 50 εκατομμύρια (ποσοστό 94.4%), 3 έχουν ετήσιο κύκλο εργασιών 10-50 εκατομμύρια (ποσοστό 4.2%) και 1 επιχείρηση έχει ετήσιο κύκλο εργασιών κάτω από 2 εκατομμύρια (ποσοστό 1.4%).

Τα αποτελέσματα εμφανίζονται και διαγραμματικά:

Εικόνα 3-Διάγραμμα ράβδων ερώτησης 3

Η ερώτηση 4 αφορά τον αριθμό των επιθέσεων ή διαρροών που δέχτηκαν οι επιχειρήσεις στα πληροφοριακά τους συστήματα τους τελευταίους 12 μήνες. Στη συνέχεια, παρατίθεται ο πίνακας των αποτελεσμάτων.

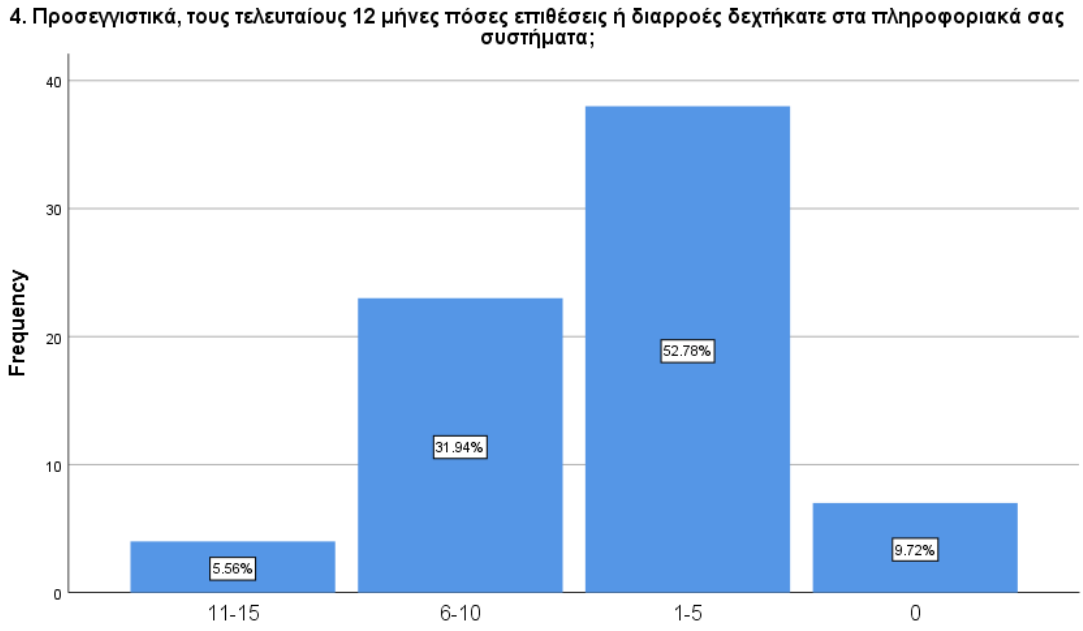
4. Προσεγγιστικά, τους τελευταίους 12 μήνες πόσες επιθέσεις ή διαρροές δεχτήκατε στα πληροφοριακά σας συστήματα;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	11-15	4	5.6	5.6	5.6
	6-10	23	31.9	31.9	37.5
	1-5	38	52.8	52.8	90.3
	0	7	9.7	9.7	100.0
	Total	72	100.0	100.0	

Πίνακας 4 -Περιγραφικά στατιστικά ερώτησης 4

Παρατηρούμε ότι το μεγαλύτερο ποσοστό των επιχειρήσεων, ήτοι το 52.8%, δέχτηκε 1-5 επιθέσεις τους τελευταίους 12 μήνες, το 31.9% δέχτηκε 6-10 επιθέσεις, το 9.7% δε δέχτηκε καμία επίθεση, ενώ το 5.6% δέχτηκε 11-15 επιθέσεις.

Τα αποτελέσματα απεικονίζονται και διαγραμματικά:



Εικόνα 4-Διάγραμμα ράβδων ερώτησης 4

Η ερώτηση 5 διερευνά πόσα από τα περιστατικά της ερώτησης 4 ανιχνεύτηκαν και αντιμετωπίστηκαν πριν δημιουργήσουν λειτουργικά προβλήματα, οικονομική ζημία ή απώλεια φήμης. Στη συνέχεια, παρατίθεται ο πίνακας των αποτελεσμάτων.

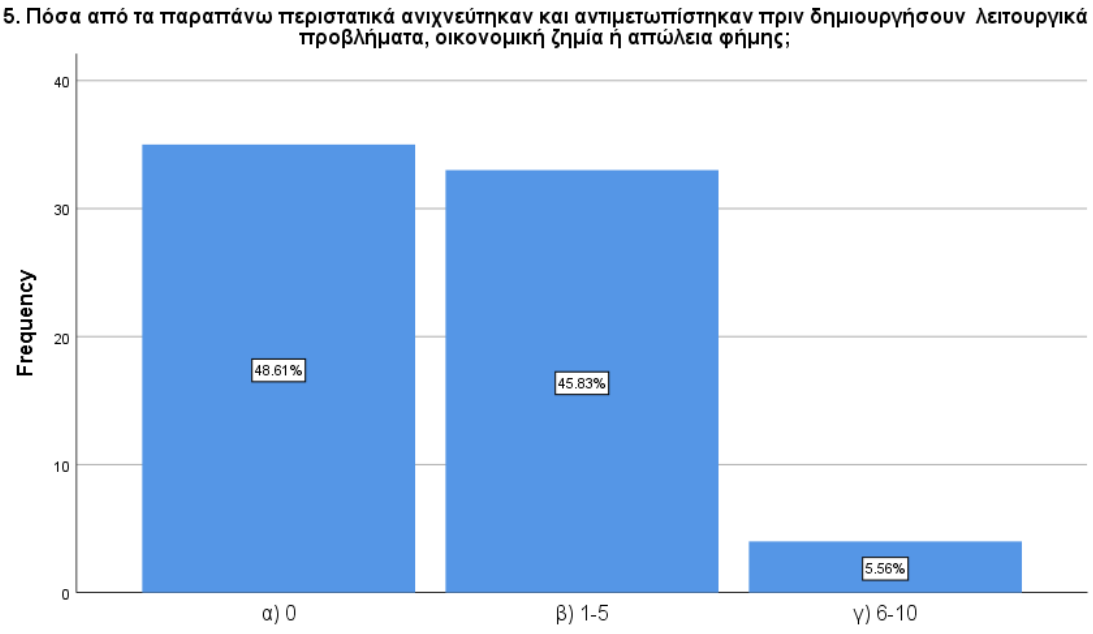
5. Πόσα από τα παραπάνω περιστατικά ανιχνεύτηκαν και αντιμετωπίστηκαν πριν δημιουργήσουν λειτουργικά προβλήματα, οικονομική ζημία ή απώλεια φήμης;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	35	48.6	48.6	48.6
	1-5	33	45.8	45.8	94.4
	6-10	4	5.6	5.6	100.0
	Total	72	100.0	100.0	

Πίνακας 5 -Περιγραφικά στατιστικά ερώτησης 5

Σύμφωνα με τον ανωτέρω πίνακα, το μεγαλύτερο ποσοστό των επιχειρήσεων, ήτοι το 48.6%, απάντησε ότι κανένα από τα περιστατικά της ερώτησης 4 δεν ανιχνεύτηκε προτού δημιουργήσει λειτουργικά προβλήματα, οικονομική ζημία ή απώλεια φήμης, το 45.8% απάντησε ότι 1-5 από τα παραπάνω περιστατικά ανιχνεύτηκαν προτού δημιουργήσουν λειτουργικά προβλήματα, οικονομική ζημία ή απώλεια φήμης, ενώ το 5.6% απάντησε ότι 6-10 περιστατικά ανιχνεύτηκαν προτού δημιουργήσουν λειτουργικά προβλήματα, οικονομική ζημία ή απώλεια φήμης.

Τα αποτελέσματα απεικονίζονται και διαγραμματικά:



Εικόνα 5-Διάγραμμα ράβδων ερώτησης 5

Η ερώτηση 6 διερευνά την τάση των περιστατικών παραβιάσεων τα τελευταία τρία χρόνια. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

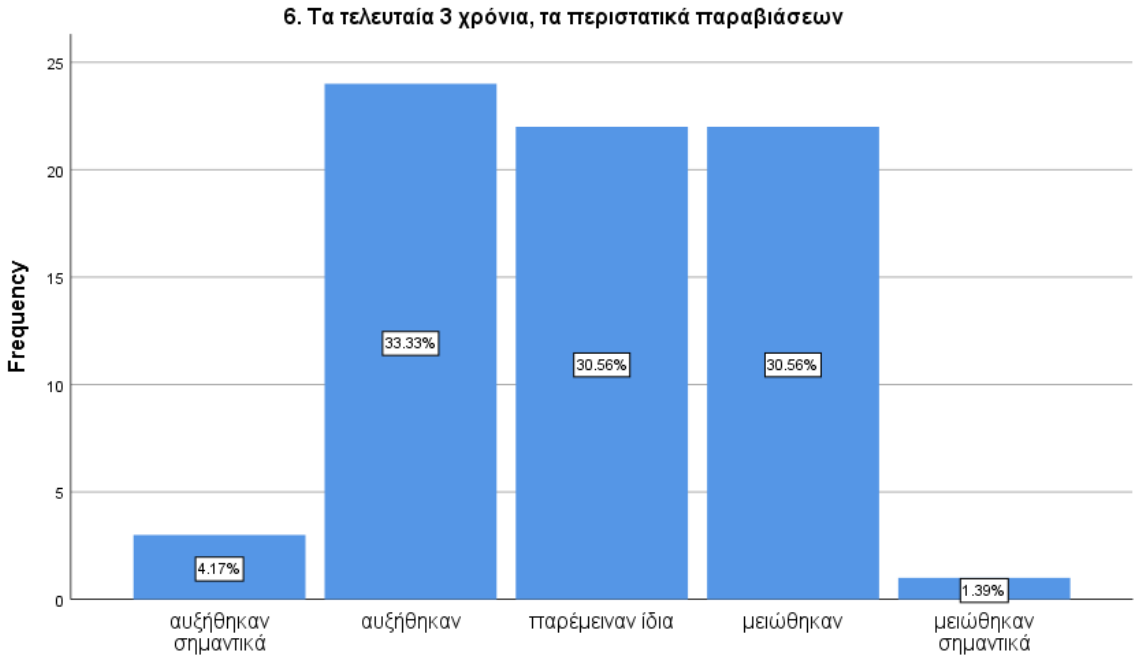
6. Τα τελευταία 3 χρόνια, τα περιστατικά παραβιάσεων

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	αυξήθηκαν σημαντικά	3	4.2	4.2	4.2
	αυξήθηκαν	24	33.3	33.3	37.5
	παρέμειναν ίδια	22	30.6	30.6	68.1
	μειώθηκαν	22	30.6	30.6	98.6
	μειώθηκαν σημαντικά	1	1.4	1.4	100.0
	Total	72	100.0	100.0	

Πίνακας 6 -Περιγραφικά στατιστικά ερώτησης 6

Όπως προκύπτει από τον Πίνακα 6, το μεγαλύτερο ποσοστό των ερωτηθέντων, ήτοι το 33.3%, υποστηρίζει ότι τα περιστατικά παραβίασης αυξήθηκαν τα τελευταία τρία χρόνια, ενώ προκύπτει ότι υπάρχει ισοβαθμία στις απαντήσεις των ερωτηθέντων με 30.6%, οι οποίοι υποστηρίζουν ότι παρέμειναν ίδια και με 30.6% υποστηρίζουν ότι μειώθηκαν. Από την άλλη, το 4.2% υποστηρίζει ότι αυξήθηκαν σημαντικά, ενώ το 1.4% ότι μειώθηκαν σημαντικά. Επομένως, ένα μεγάλο ποσοστό (68.1%) υποστηρίζει ότι τα περιστατικά αυξήθηκαν ή παρέμειναν τα ίδια.

Τα αποτελέσματα παρουσιάζονται και διαγραμματικά:



Εικόνα 6-Διάγραμμα ράβδων ερώτησης 6

5.2.2 Συμβουλευτικός ρόλος των εσωτερικών ελεγκτών

Οι ερωτήσεις 7-9 αφορούν το βαθμό στον οποίο οι εσωτερικοί ελεγκτές λειτουργούν συμβουλευτικά. Πιο συγκεκριμένα, η ερώτηση 7 εξετάζει το βαθμό στον οποίο οι εσωτερικοί ελεγκτές συμβουλεύουν τα διάφορα τμήματα σχετικά με την αποτελεσματικότητα και αποδοτικότητά τους. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

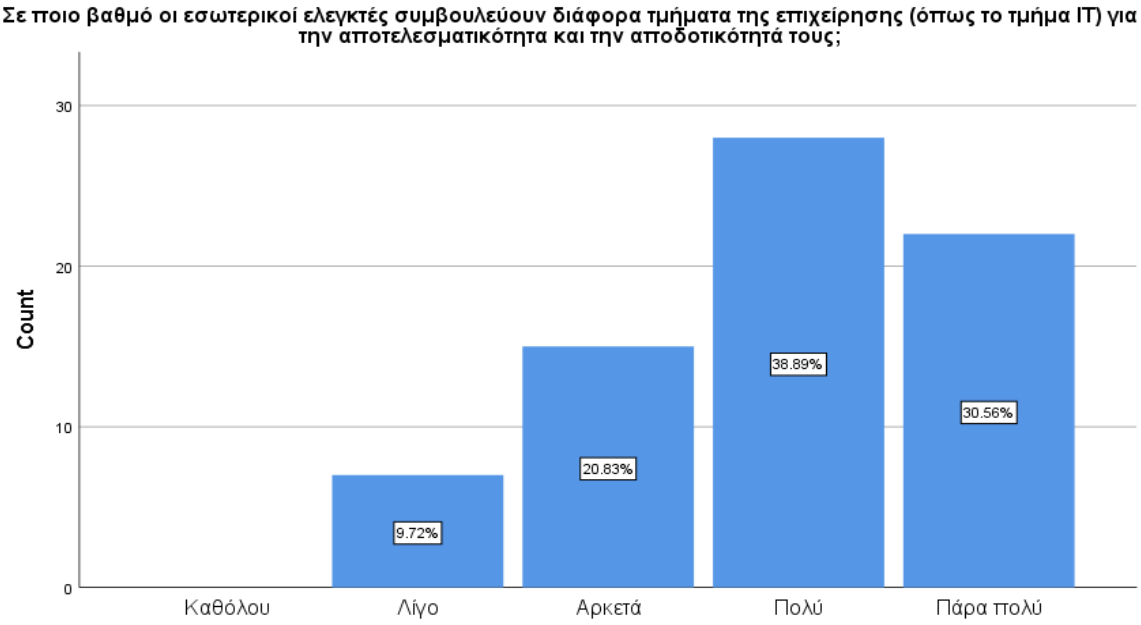
7. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές συμβουλεύουν διάφορα τμήματα της επιχείρησης (όπως το τμήμα IT) για την αποτελεσματικότητα και την αποδοτικότητά τους;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Λίγο	7	9.7	9.7	9.7
	Αρκετά	15	20.8	20.8	30.6
	Πολύ	28	38.9	38.9	69.4
	Πάρα πολύ	22	30.6	30.6	100.0
	Total	72	100.0	100.0	

Πίνακας 7 -Περιγραφικά στατιστικά ερώτησης 7

Όπως διαφαίνεται από τον παραπάνω πίνακα, το 38.9% των ερωτηθέντων απάντησε ότι οι εσωτερικοί ελεγκτές συμβουλεύον πολύ τα διάφορα τμήματα της επιχείρησης, το 30.6% απάντησε ότι οι εσωτερικοί ελεγκτές συμβουλεύον πάρα πολύ τα διάφορα τμήματα, το 20.8% απάντησε ότι οι εσωτερικοί ελεγκτές συμβουλεύουν αρκετά, ενώ στον αντίποδα το 9.7% θεωρεί ότι οι εσωτερικοί ελεγκτές συμβουλεύον λίγο τα διάφορα τμήματα. Συνεπώς, προκύπτει ότι το 90.3% των ερωτηθέντων θεωρεί ότι οι εσωτερικοί ελεγκτές λειτουργούν σε μεγάλο βαθμό συμβουλευτικά στα διάφορα τμήματα της επιχείρησης.

Τα αποτελέσματα παρουσιάζονται και διαγραμματικά:



Εικόνα 7-Διάγραμμα ράβδων ερώτησης 7

Στην ερώτηση 8 ερευνάται ο βαθμός στον οποίο οι εσωτερικοί ελεγκτές λειτουργούν σαν «παίκτες» μιας ομάδας και όχι σαν όργανα επιβολής κανόνων. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

8. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές λειτουργούν σαν «παίκτες» μιας ομάδας και όχι σαν όργανα επιβολής κανόνων;

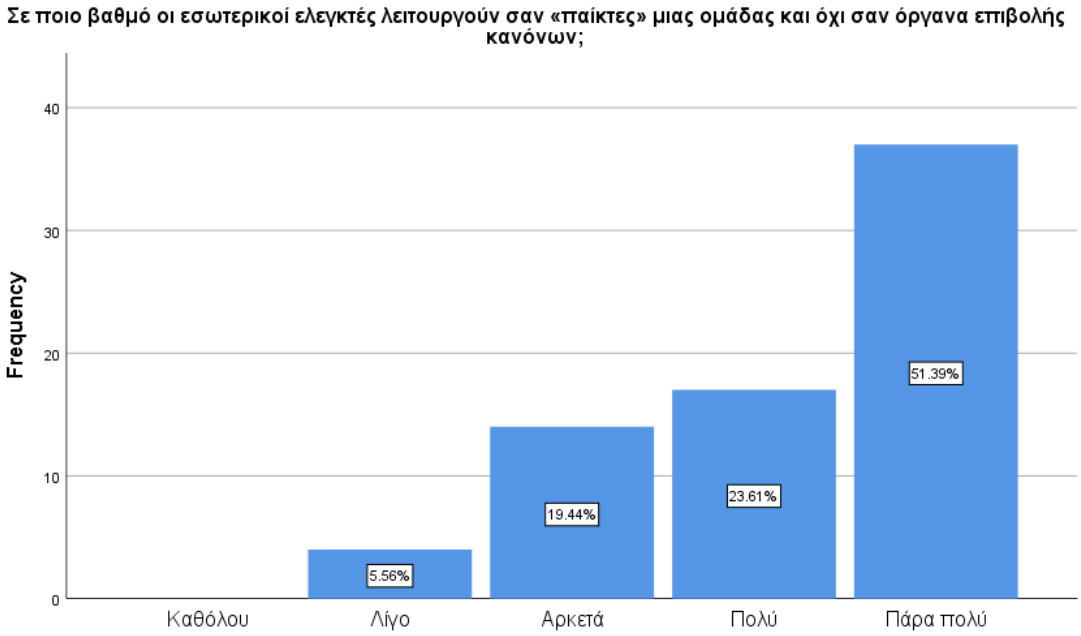
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Λίγο	4	5.6	5.6	5.6
	Αρκετά	14	19.4	19.4	25.0
	Πολύ	17	23.6	23.6	48.6
	Πάρα πολύ	37	51.4	51.4	100.0
	Total	72	100.0	100.0	

Πίνακας 8 -Περιγραφικά στατιστικά ερώτησης 8

Από τον παραπάνω πίνακα προκύπτει ότι το μεγαλύτερο ποσοστό των επιχειρήσεων, ήτοι το 51.4%, θεωρεί ότι οι εσωτερικοί ελεγκτές λειτουργούν πάρα πολύ σαν «παίκτες» μιας ομάδας και όχι σαν όργανα επιβολής κανόνων, το 23.6% υποστηρίζει ότι οι εσωτερικοί ελεγκτές λειτουργούν πολύ σαν «παίκτες» μιας ομάδας και όχι σαν όργανα επιβολής κανόνων, ενώ το 19.4% θεωρεί ότι λειτουργούν αρκετά σαν «παίκτες» μιας ομάδας και όχι σαν όργανα επιβολής κανόνων. Στον αντίποδα, το 5.6% υποστηρίζει ότι οι εσωτερικοί ελεγκτές λειτουργούν λίγο σαν «παίκτες» μιας

ομάδας. Συνεπώς, η πλειοψηφία των ερωτηθέντων -το 94.4%- θεωρεί ότι οι εσωτερικοί ελεγκτές λειτουργούν συμβουλευτικά.

Τα αποτελέσματα παρουσιάζονται και διαγραμματικά:



Εικόνα 8-Διάγραμμα ράβδων ερώτησης 8

Η ερώτηση 9 εξετάζει το βαθμό στον οποίο οι εσωτερικοί ελεγκτές ασχολούνται με την ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

9. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές ασχολούνται με την ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών;

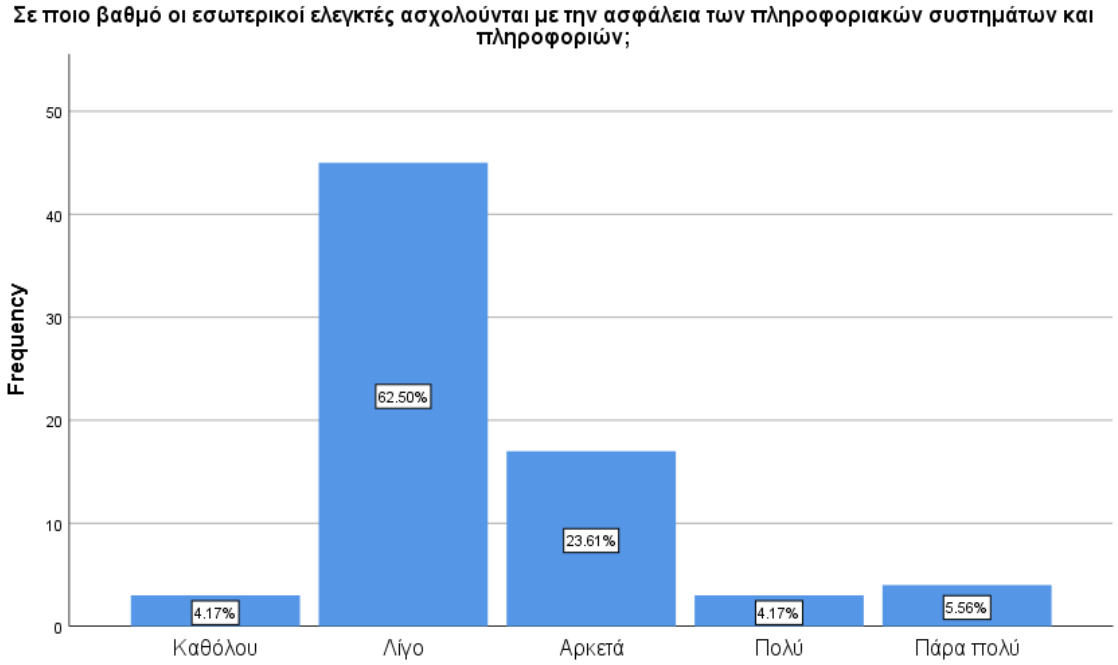
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	3	4.2	4.2	4.2
	Λίγο	45	62.5	62.5	66.7
	Αρκετά	17	23.6	23.6	90.3
	Πολύ	3	4.2	4.2	94.4
	Πάρα πολύ	4	5.6	5.6	100.0
	Total	72	100.0	100.0	

Πίνακας 9 -Περιγραφικά στατιστικά ερώτησης 9

Από τον παραπάνω πίνακα αποδεικνύεται ότι το 62.5% των ερωτηθέντων επιχειρήσεων υποστηρίζει ότι οι εσωτερικοί ελεγκτές ασχολούνται λίγο με την

ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών, το 23.6% υποστηρίζει ότι ασχολούνται αρκετά, ενώ το 5.6% υποστηρίζει ότι ασχολούνται πάρα πολύ με την ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών. Με ποσοστό 4.2% προκύπτει ισοβαθμία ότι οι εσωτερικοί ελεγκτές ασχολούνται πολύ, αλλά και καθόλου με την ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών. Συνεπώς, το 66.7% των επιχειρήσεων υποστηρίζει ότι οι εσωτερικοί ελεγκτές ασχολούνται σε πολύ μικρό βαθμό με την ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 9-Διάγραμμα ράβδων ερώτησης 9

5.2.3 Σχέση μεταξύ εσωτερικών ελεγκτών και ειδικών της τεχνολογίας πληροφοριών

Στη συνέχεια, οι ερωτήσεις 10-12 αφορούν τη σχέση μεταξύ των εσωτερικών ελεγκτών και των ειδικών της τεχνολογίας πληροφοριών. Όσον αφορά την ερώτηση 10, πραγματεύεται το βαθμό στον οποίο οι ειδικοί για την ασφάλεια πληροφοριών συνεργάζονται με τους εσωτερικούς ελεγκτές, ώστε να διασφαλίζουν ότι τα πληροφοριακά συστήματα είναι ασφαλή και αξιόπιστα. Τα αποτελέσματα δίδονται στον παρακάτω πίνακα.

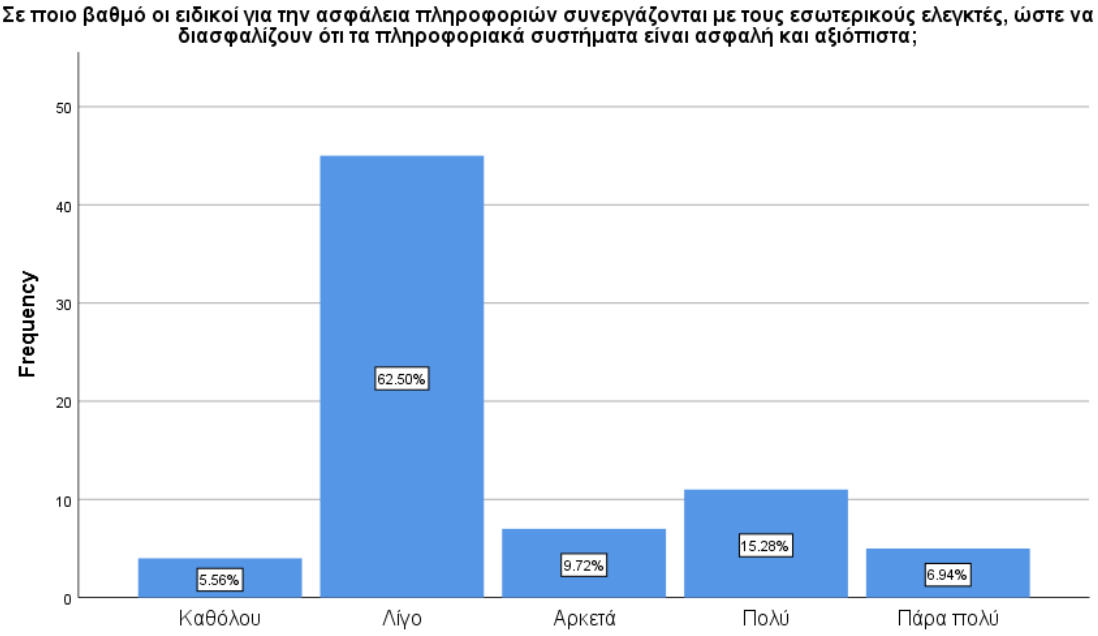
10. Σε ποιο βαθμό οι ειδικοί για την ασφάλεια πληροφοριών συνεργάζονται με τους εσωτερικούς ελεγκτές, ώστε να διασφαλίζουν ότι τα πληροφοριακά συστήματα είναι ασφαλή και αξιόπιστα;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	4	5.6	5.6	5.6
	Λίγο	45	62.5	62.5	68.1
	Αρκετά	7	9.7	9.7	77.8
	Πολύ	11	15.3	15.3	93.1
	Πάρα πολύ	5	6.9	6.9	100.0
	Total	72	100.0	100.0	

Πίνακας 10 -Περιγραφικά στατιστικά ερώτησης 10

Από τον πίνακα φαίνεται ότι η πλειοψηφία των επιχειρήσεων, ήτοι το 62.5%, θεωρεί ότι οι ειδικοί για την ασφάλεια πληροφοριών συνεργάζονται λίγο με τους εσωτερικούς ελεγκτές, ώστε να διασφαλίζουν ότι τα πληροφοριακά συστήματα είναι ασφαλή και αξιόπιστα, το 15.3% θεωρεί ότι συνεργάζονται πολύ, το 9.7% θεωρεί ότι συνεργάζονται αρκετά, ενώ το 6.9% θεωρεί ότι συνεργάζονται πάρα πολύ. Στον αντίποδα, μόλις το 5.6% θεωρεί ότι δε συνεργάζονται καθόλου. Συνεπώς, η συντριπτική πλειοψηφία, με ποσοστό 68.1%, θεωρεί ότι ειδικοί για την ασφάλεια πληροφοριών συνεργάζονται σε πολύ μικρό βαθμό με τους εσωτερικούς ελεγκτές, ώστε να διασφαλίζουν ότι τα πληροφοριακά συστήματα είναι ασφαλή και αξιόπιστα.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 10-Διάγραμμα ράβδων ερώτησης 10

Η ερώτηση 11 πραγματεύεται κατά πόσο η τριβή μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών είναι περιορισμένη. Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

11. Σε ποιο βαθμό η τριβή μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών είναι περιορισμένη;

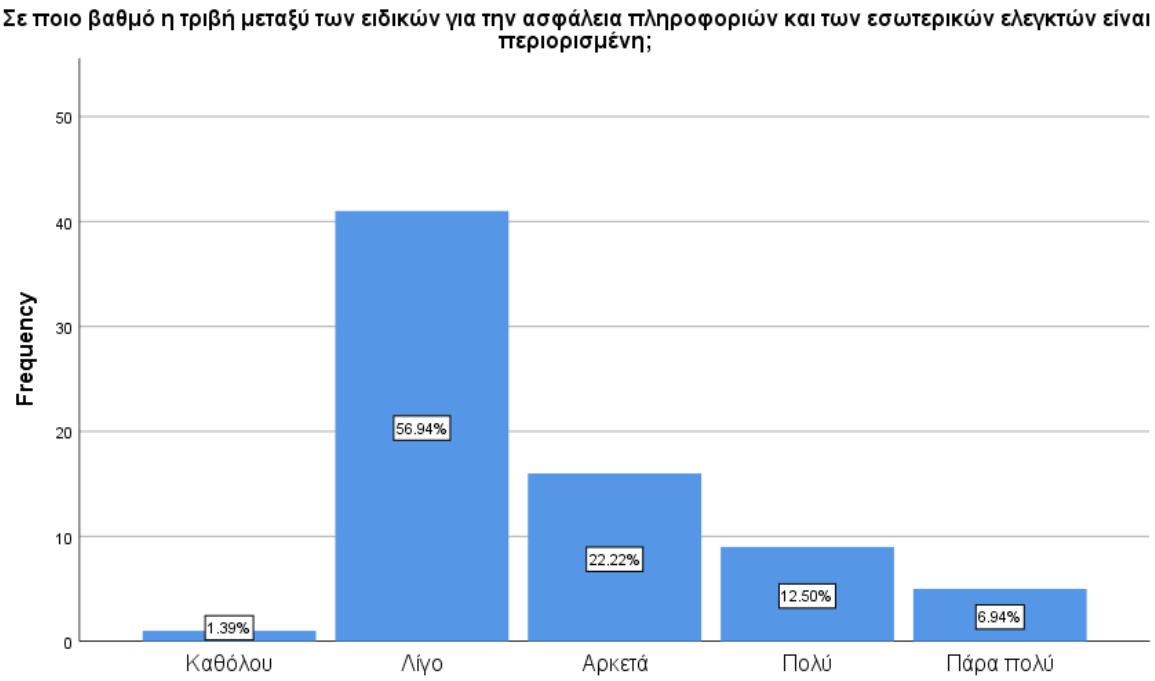
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	1	1.4	1.4	1.4
	Λίγο	41	56.9	56.9	58.3
	Αρκετά	16	22.2	22.2	80.6
	Πολύ	9	12.5	12.5	93.1
	Πάρα πολύ	5	6.9	6.9	100.0
	Total	72	100.0	100.0	

Πίνακας 11 -Περιγραφικά στατιστικά ερώτησης 11

Όπως προκύπτει από τον Πίνακα 11, το μεγαλύτερο ποσοστό των ερωτηθέντων, ήτοι το 56.9%, υποστηρίζει ότι η τριβή μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών είναι περιορισμένη σε μικρό βαθμό (λίγο), το 22.2% υποστηρίζει ότι είναι αρκετά περιορισμένη η τριβή, το 12.5% ότι είναι πολύ περιορισμένη, ενώ το 6.9% ότι είναι πάρα πολύ περιορισμένη. Αντίθετα, πολύ μικρό είναι το ποσοστό (1.4%) όσων υποστηρίζουν ότι η τριβή δεν είναι καθόλου περιορισμένη. Συνεπώς, το 58.3% θεωρεί ότι η τριβή μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών δεν είναι περιορισμένη.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:

:



Εικόνα 11-Διάγραμμα ράβδων ερώτησης 11

Όσον αφορά την ερώτηση 12, εξετάζει το βαθμό κατά τον οποίο η σχέση μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών χαρακτηρίζεται ως προσωπική και στενή. Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

12. Σε ποιο βαθμό η σχέση μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών χαρακτηρίζεται ως προσωπική και στενή;

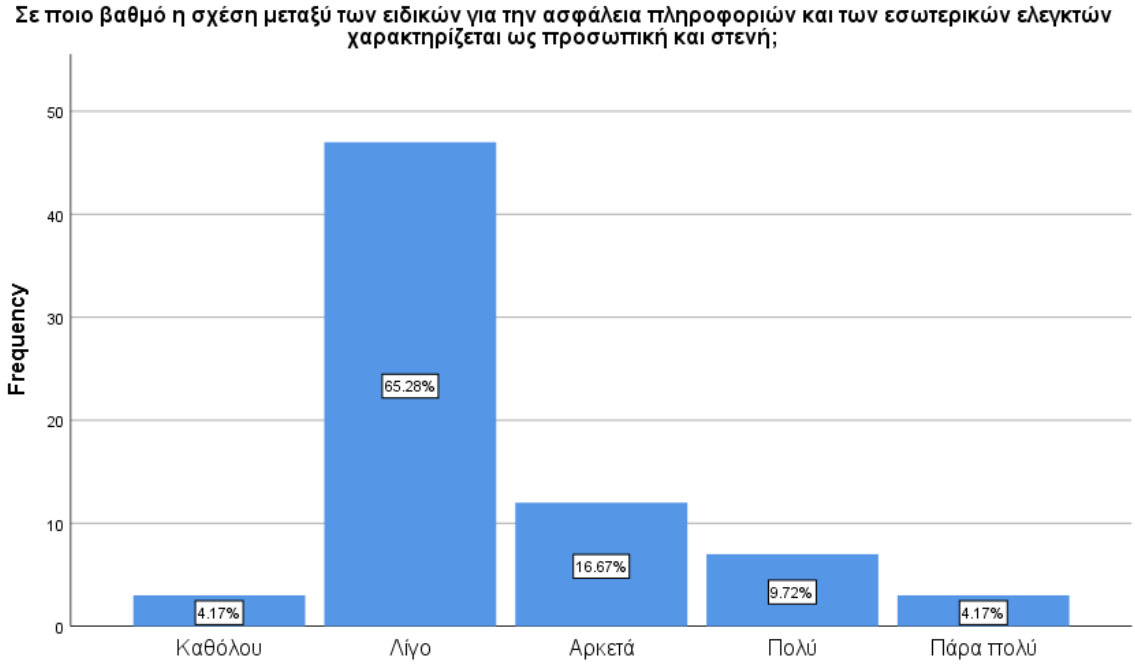
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	3	4.2	4.2	4.2
	Λίγο	47	65.3	65.3	69.4
	Αρκετά	12	16.7	16.7	86.1
	Πολύ	7	9.7	9.7	95.8
	Πάρα πολύ	3	4.2	4.2	100.0
	Total	72	100.0	100.0	

Πίνακας 12 -Περιγραφικά στατιστικά ερώτησης 12

Από τον παραπάνω πίνακα προκύπτει ότι η πλειοψηφία των ερωτηθέντων, ήτοι το 65.3%, θεωρεί ότι η σχέση μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών χαρακτηρίζεται λίγο, δηλαδή σε μικρό

βαθμό, ως προσωπική και στενή, το 16.7% θεωρεί ότι η σχέση είναι αρκετά προσωπική και στενή, ενώ το 9.7% θεωρεί ότι η σχέση είναι πολύ προσωπική και στενή. Στον αντίποδα, προκύπτει ότι υπάρχει ισοβαθμία στις απαντήσεις των ερωτηθέντων με 4.2%, οι οποίοι υποστηρίζουν ότι η σχέση δεν είναι καθόλου προσωπική και στενή και με 4.2% υποστηρίζουν ότι η σχέση είναι πάρα πολύ προσωπική και στενή. Συνεπώς, το 69.4% των ερωτηθέντων θεωρεί ότι η σχέση μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών δεν είναι πολύ προσωπική και στενή.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 12-Διάγραμμα ράβδων ερώτησης 12

5.2.4 Εξειδικευμένες τεχνολογικές γνώσεις

Οι ερωτήσεις 13-16 σχετίζονται με το βαθμό ύπαρξης εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών. Η ερώτηση 13 διερευνά το βαθμό στον οποίο οι εσωτερικοί ελεγκτές έχουν γνώσεις για την ασφάλεια των πληροφοριακών συστημάτων. Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

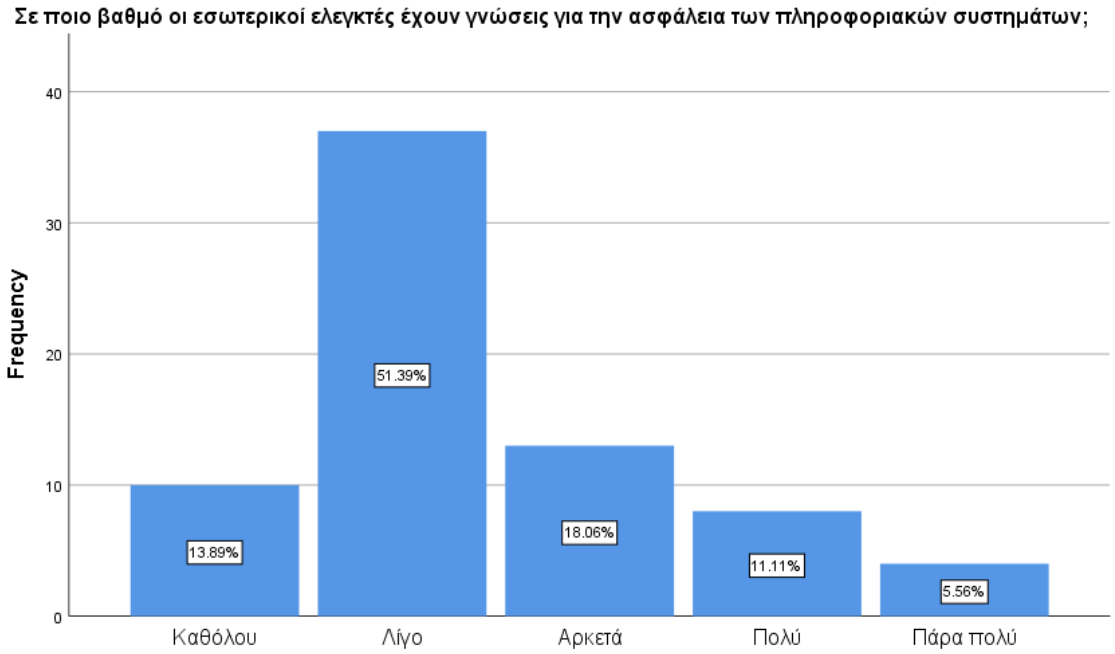
13. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές έχουν γνώσεις για την ασφάλεια των πληροφοριακών συστημάτων;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	10	13.9	13.9	13.9
	Λίγο	37	51.4	51.4	65.3
	Αρκετά	13	18.1	18.1	83.3
	Πολύ	8	11.1	11.1	94.4
	Πάρα πολύ	4	5.6	5.6	100.0
	Total	72	100.0	100.0	

Πίνακας 13 -Περιγραφικά στατιστικά ερώτησης 13

Όπως προκύπτει από τον Πίνακα 13, το 51.4% των ερωτηθέντων υποστηρίζει ότι οι εσωτερικοί ελεγκτές έχουν λίγες γνώσεις για την ασφάλεια των πληροφοριακών συστημάτων, το 18.1% υποστηρίζει ότι έχουν αρκετές γνώσεις, ενώ το 13.9% υποστηρίζει ότι δεν έχουν καθόλου γνώσεις για την ασφάλεια των πληροφοριακών συστημάτων. Στον αντίποδα, το 11.1% υποστηρίζει ότι οι εσωτερικοί ελεγκτές έχουν πολλές γνώσεις για την ασφάλεια των πληροφοριακών συστημάτων και το 5.6% υποστηρίζει ότι έχουν πάρα πολλές. Συνεπώς, το 65.3% των ερωτηθέντων αποκρίθηκε ότι οι γνώσεις για την ασφάλεια των πληροφοριακών συστημάτων από την πλευρά των εσωτερικών ελεγκτών είναι περιορισμένες έως ανύπαρκτες.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 13-Διάγραμμα ράβδων ερώτησης 13

Η ερώτηση 14 διερευνά το βαθμό στον οποίο οι εσωτερικοί ελεγκτές έχουν εξειδικευμένες τεχνολογικές γνώσεις για τα συστήματα που χρησιμοποιούν. Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

14. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές έχουν εξειδικευμένες τεχνολογικές γνώσεις για τα συστήματα που χρησιμοποιούν;

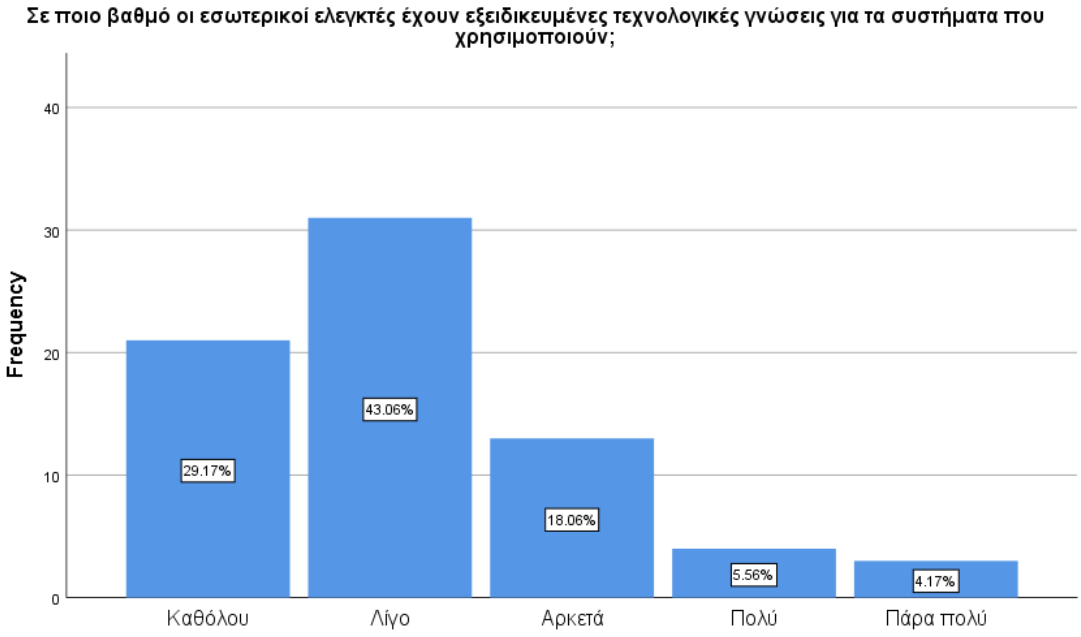
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	21	29.2	29.2	29.2
	Λίγο	31	43.1	43.1	72.2
	Αρκετά	13	18.1	18.1	90.3
	Πολύ	4	5.6	5.6	95.8
	Πάρα πολύ	3	4.2	4.2	100.0
	Total	72	100.0	100.0	

Πίνακας 14 -Περιγραφικά στατιστικά ερώτησης 14

Σύμφωνα με τον παραπάνω πίνακα, το 43.1% των επιχειρήσεων θεωρεί ότι οι εσωτερικοί ελεγκτές έχουν λίγες εξειδικευμένες τεχνολογικές γνώσεις για τα συστήματα που χρησιμοποιούν, το 29.2% θεωρεί ότι δεν έχουν καθόλου εξειδικευμένες τεχνολογικές γνώσεις, ενώ το 18.1% θεωρεί ότι έχουν αρκετές εξειδικευμένες τεχνολογικές γνώσεις. Αντίθετα, μικρό είναι το ποσοστό (5.6%) αυτών που θεωρούν ότι οι εσωτερικοί ελεγκτές έχουν πολλές εξειδικευμένες

τεχνολογικές γνώσεις, ενώ το 4.2% θεωρεί ότι έχουν πάρα πολλές. Συνεπώς, η συντριπτική πλειοψηφία, με ποσοστό 72.2%, υποστηρίζει ότι οι εσωτερικοί ελεγκτές έχουν ελάχιστες έως ανύπαρκτες εξειδικευμένες τεχνολογικές γνώσεις για τα συστήματα που χρησιμοποιούν.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 14-Διάγραμμα ράβδων ερώτησης 14

Στην ερώτηση 15 διερευνάται ο βαθμός στον οποίο υπάρχει εκπαίδευση των εσωτερικών ελεγκτών σχετικά με την ασφάλεια των πληροφοριακών συστημάτων. Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

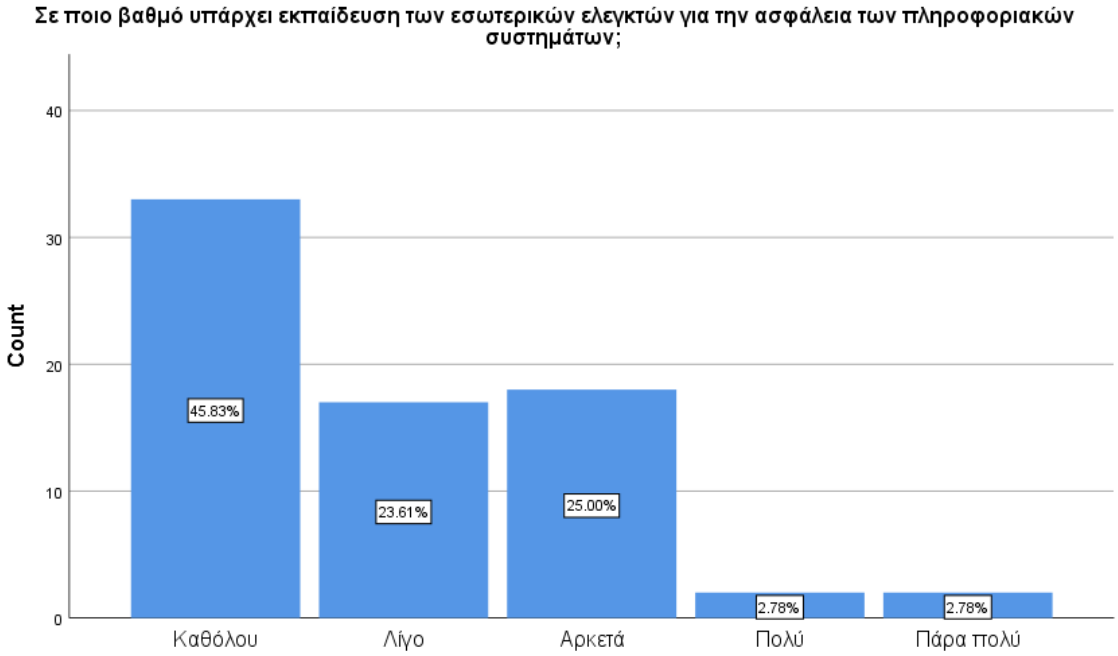
15. Σε ποιο βαθμό υπάρχει εκπαίδευση των εσωτερικών ελεγκτών για την ασφάλεια των πληροφοριακών συστημάτων;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	33	45.8	45.8	45.8
	Λίγο	17	23.6	23.6	69.4
	Αρκετά	18	25.0	25.0	94.4
	Πολύ	2	2.8	2.8	97.2
	Πάρα πολύ	2	2.8	2.8	100.0
	Total	72	100.0	100.0	

Πίνακας 15 -Περιγραφικά στατιστικά ερώτησης 15

Από τον ανωτέρω πίνακα, προκύπτει ότι το 45.8% των ερωτηθέντων θεωρεί ότι δεν υπάρχει καθόλου εκπαίδευση των εσωτερικών ελεγκτών σχετικά με την ασφάλεια των πληροφοριακών συστημάτων, το 25% θεωρεί ότι υπάρχει αρκετή εκπαίδευση, ενώ το 23.6% θεωρεί ότι υπάρχει λίγη εκπαίδευση των εσωτερικών ελεγκτών σχετικά με την ασφάλεια των πληροφοριακών συστημάτων. Σε ισοβαθμία, με μικρό ποσοστό 2.8%, οι ερωτηθέντες θεωρούν ότι υπάρχει πολλή και πάρα πολλή εκπαίδευση. Συνεπώς, το 69.4% υποστηρίζει ότι η εκπαίδευση των εσωτερικών ελεγκτών σχετικά με την ασφάλεια των πληροφοριακών συστημάτων σχεδόν απουσιάζει.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 15-Διάγραμμα ράβδων ερώτησης 15

Η ερώτηση 16 εξετάζει το βαθμό κατά τον οποίο οι εσωτερικοί ελεγκτές κατέχουν την πιστοποίηση CISA (Certified Information Systems Auditor). Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

16. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές κατέχουν την πιστοποίηση CISA (Certified Information Systems Auditor);

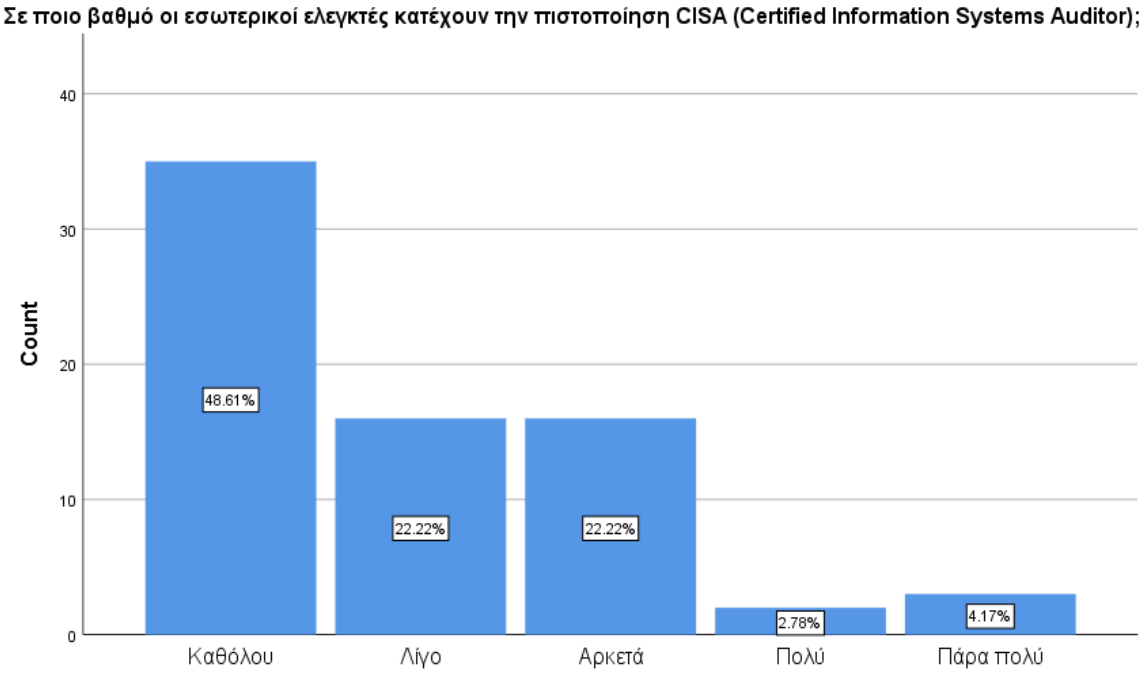
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	35	48.6	48.6	48.6
	Λίγο	16	22.2	22.2	70.8
	Αρκετά	16	22.2	22.2	93.1
	Πολύ	2	2.8	2.8	95.8
	Πάρα πολύ	3	4.2	4.2	100.0

Total	72	100.0	100.0	

Πίνακας 16 -Περιγραφικά στατιστικά ερώτησης 16

Σύμφωνα με τον Πίνακα 16, το 48.6% των ερωτηθέντων υποστηρίζει ότι οι εσωτερικοί ελεγκτές δεν κατέχουν την πιστοποίηση CISA (Certified Information Systems Auditor), ενώ με ισοβαθμία, το 22.2%, υποστηρίζει ότι την κατέχουν λίγο ή σε αρκετά ικανοποιητικό βαθμό. Μικρό είναι το ποσοστό, ήτοι 4.2%, το οποίο υποστηρίζει ότι οι εσωτερικοί ελεγκτές κατέχουν την πιστοποίηση CISA (Certified Information Systems Auditor) σε πάρα πολύ μεγάλο βαθμό, ενώ μόνο το 2.8% υποστηρίζει ότι την κατέχει σε πολύ μεγάλο βαθμό. Συνεπώς, το 70.8% των ερωτηθέντων υποστηρίζει ότι η πιστοποίηση CISA κατέχεται από ελάχιστους εσωτερικούς ελεγκτές.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 16-Διάγραμμα ράβδων ερώτησης 16

5.2.5 Πολιτικές- πρότυπα ασφαλείας

Οι ερωτήσεις 17-21 σχετίζονται με την ύπαρξη πολιτικών και προτύπων ασφαλείας που ελέγχονται από τους εσωτερικούς ελεγκτές. Η ερώτηση 17 διερευνά το βαθμό κατά τον οποίο οι ερωτηθέντες συμφωνούν ότι υπάρχει καταγεγραμμένη

Πολιτική Ασφαλείας Πληροφοριών. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

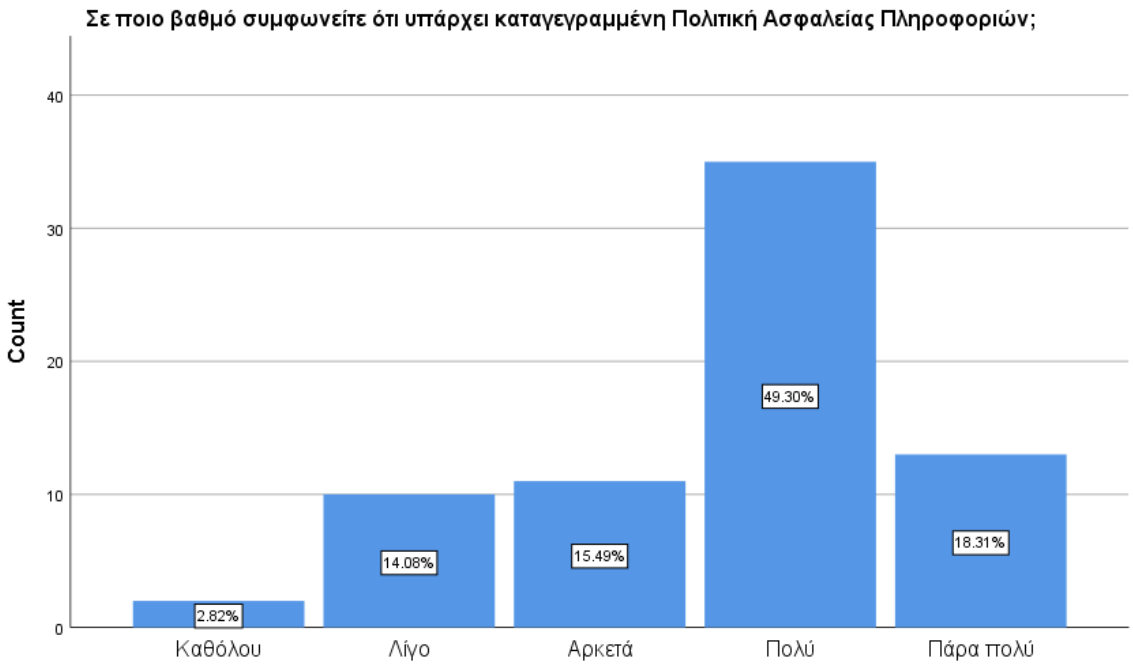
17. Σε ποιο βαθμό συμφωνείτε ότι υπάρχει καταγεγραμμένη Πολιτική Ασφαλείας Πληροφοριών;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	2	2.8	2.8	2.8
	Λίγο	10	13.9	14.1	16.9
	Αρκετά	11	15.3	15.5	32.4
	Πολύ	35	48.6	49.3	81.7
	Πάρα πολύ	13	18.1	18.3	100.0
	Total	71	98.6	100.0	
Missing	System	1	1.4		
Total		72	100.0		

Πίνακας 17 -Περιγραφικά στατιστικά ερώτησης 17

Από τον παραπάνω πίνακα προκύπτει ότι το 49.3% των ερωτηθέντων συμφωνεί πολύ ότι υπάρχει καταγεγραμμένη Πολιτική Ασφαλείας Πληροφοριών, το 18.3% συμφωνεί πάρα πολύ, ενώ το 15.5% συμφωνεί αρκετά. Ένα μικρότερο ποσοστό, ήτοι το 14.1%, συμφωνεί λίγο ότι υπάρχει καταγεγραμμένη Πολιτική Ασφαλείας Πληροφοριών, ενώ μόλις το 2.8% δε συμφωνεί καθόλου. Συνεπώς, το 67.6% των ερωτηθέντων ισχυρίζεται ότι υπάρχει καταγεγραμμένη Πολιτική Ασφαλείας Πληροφοριών σε μεγάλο βαθμό.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 17-Διάγραμμα ράβδων ερώτησης 17

Η ερώτηση 18 εξετάζει το βαθμό στον οποίο η εκάστοτε επιχείρηση χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005 κ.ά.). Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

18. Σε ποιο βαθμό η επιχείρησή σας χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005 κ.ά.);

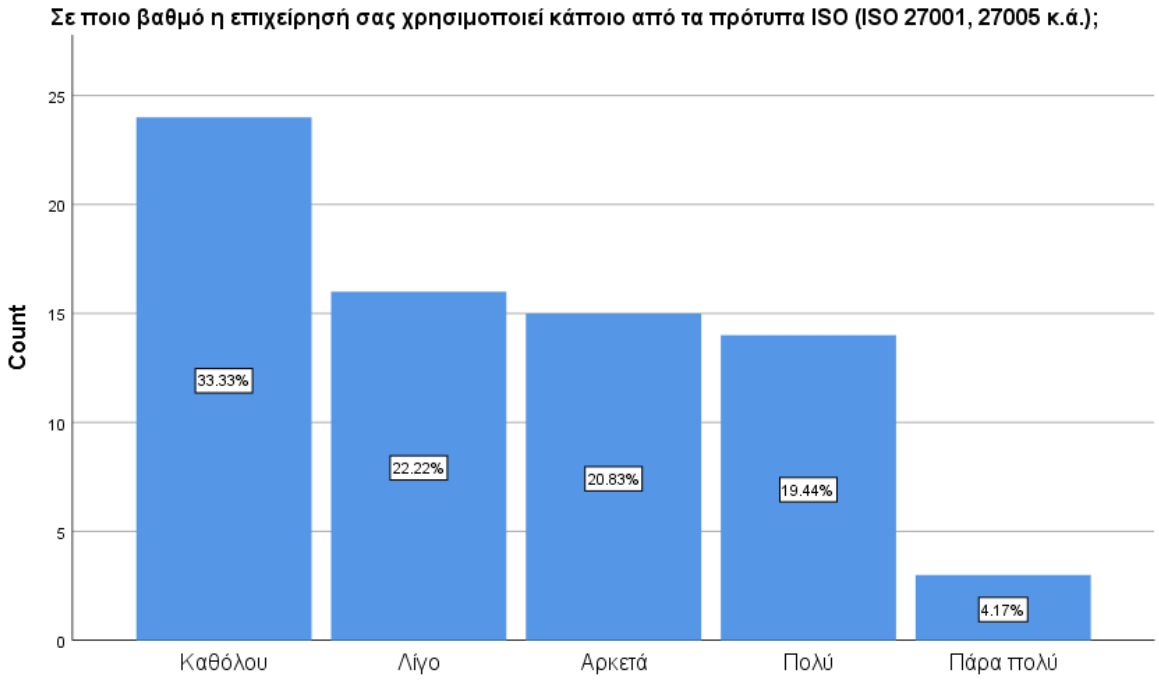
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	24	33.3	33.3	33.3
	Λίγο	16	22.2	22.2	55.6
	Αρκετά	15	20.8	20.8	76.4
	Πολύ	14	19.4	19.4	95.8
	Πάρα πολύ	3	4.2	4.2	100.0
	Total	72	100.0	100.0	

Πίνακας 18 -Περιγραφικά στατιστικά ερώτησης 18

Από τον Πίνακα 18 προκύπτει ότι το 33.3% των ερωτηθέντων ισχυρίζεται ότι δε χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005 κ.ά.), το 22.2% ισχυρίζεται ότι χρησιμοποιεί, σε μικρό βαθμό, λίγο, κάποιο από αυτά, ενώ το 20.8% ισχυρίζεται ότι χρησιμοποιεί αρκετά κάποιο από αυτά. Αντίθετα, το 19.4% υποστηρίζει ότι χρησιμοποιεί σε μεγάλο βαθμό, πολύ, κάποιο από τα πρότυπα ISO και το 4.2% υποστηρίζει ότι χρησιμοποιεί σε πάρα πολύ μεγάλο βαθμό κάποιο από

αυτά. Συνεπώς, το 55.6% των ερωτηθέντων ισχυρίζεται ότι δεν χρησιμοποιεί σε ικανοποιητικό βαθμό κάποιο από τα πρότυπα ISO (ISO 27001, 27005 κ.ά.).

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 18-Διάγραμμα ράβδων ερώτησης 18

Η ερώτηση 19 διερευνά το βαθμό κατά τον οποίο η εκάστοτε επιχείρηση χρησιμοποιεί το πλαίσιο COBIT. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

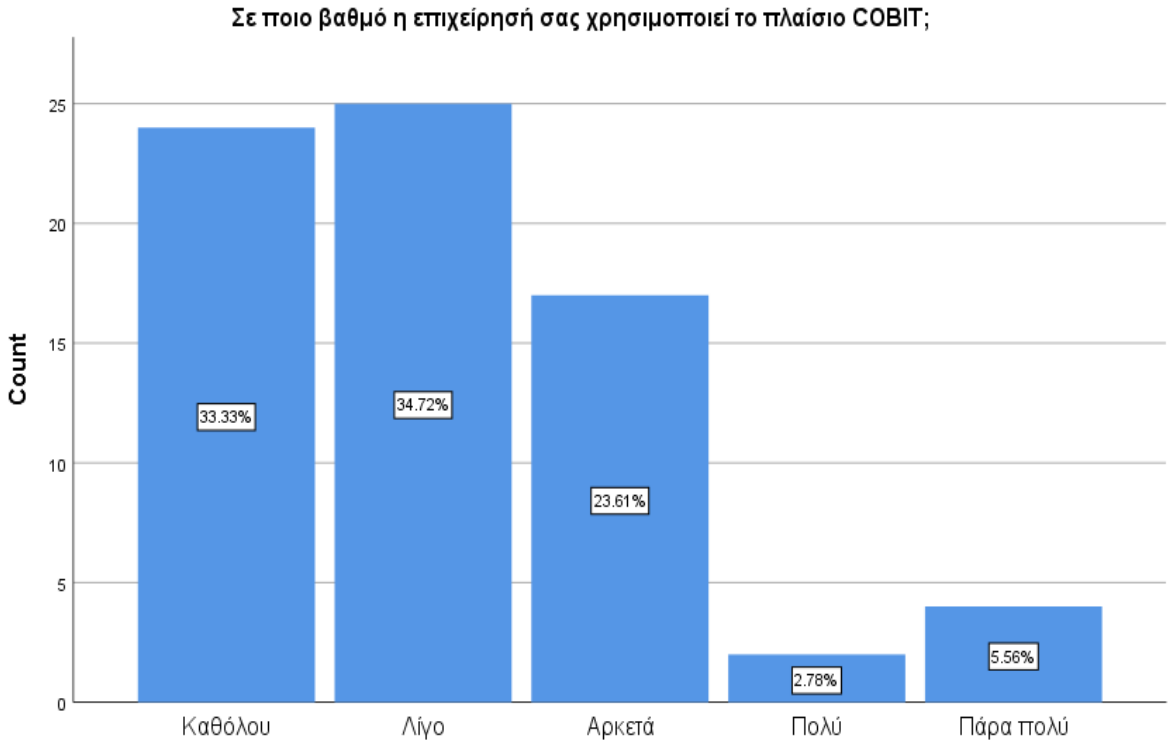
19. Σε ποιο βαθμό η επιχείρησή σας χρησιμοποιεί το πλαίσιο COBIT;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	24	33.3	33.3	33.3
	Λίγο	25	34.7	34.7	68.1
	Αρκετά	17	23.6	23.6	91.7
	Πολύ	2	2.8	2.8	94.4
	Πάρα πολύ	4	5.6	5.6	100.0
	Total	72	100.0	100.0	

Πίνακας 19 -Περιγραφικά στατιστικά ερώτησης 19

Ο ανωτέρω πίνακας αποδεικνύει ότι το 34.7% των επιχειρήσεων χρησιμοποιεί το πλαίσιο COBIT λίγο, το 33.3% δε χρησιμοποιεί το πλαίσιο COBIT, ενώ το 23.6% το χρησιμοποιεί αρκετά. Μόλις το 5.6% των επιχειρήσεων χρησιμοποιεί πολύ το πλαίσιο COBIT, ενώ πάρα πολύ το χρησιμοποιεί μόνο το 2.8%. Συνεπώς, το 68.1% δε χρησιμοποιεί το πλαίσιο COBIT σε ικανοποιητικό βαθμό.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 19-Διάγραμμα ράβδων ερώτησης 19

Η ερώτηση 20 εξετάζει το βαθμό κατά τον οποίο η εκάστοτε επιχείρηση χρησιμοποιεί τα πλαίσια NIST SP ή RFC2196:Site Security Handbook. Τα αποτελέσματα παρατίθενται στον παρακάτω πίνακα.

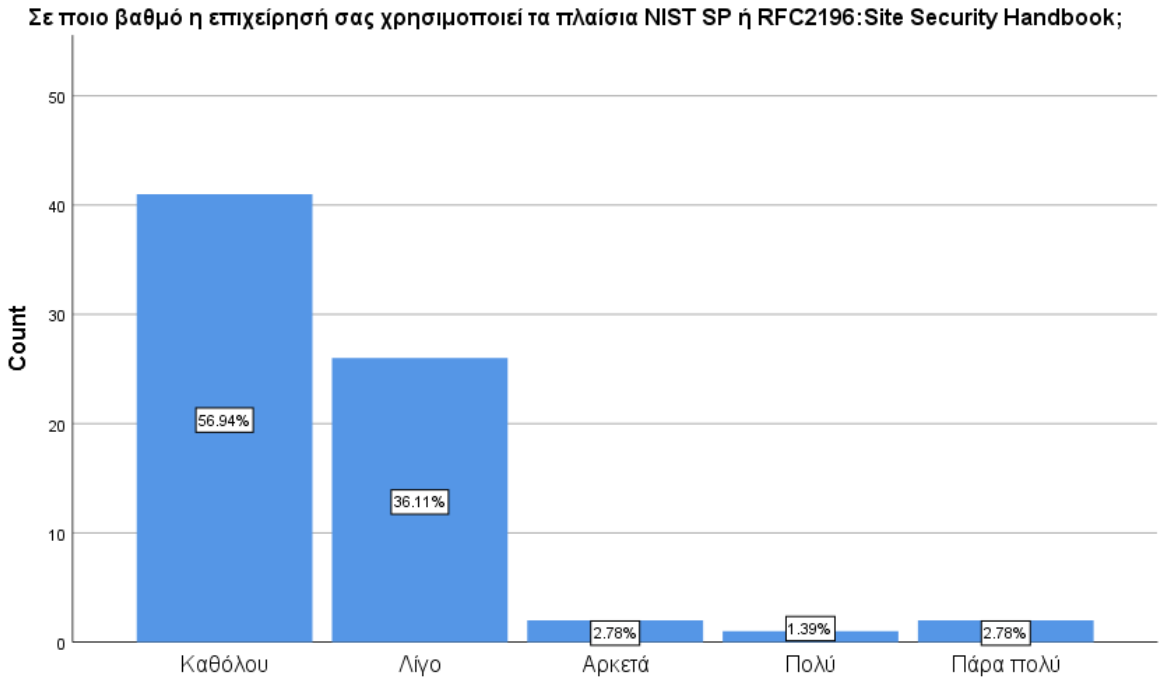
20. Σε ποιο βαθμό η επιχείρησή σας χρησιμοποιεί τα πλαίσια NIST SP ή RFC2196:Site Security Handbook;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	41	56.9	56.9	56.9
	Λίγο	26	36.1	36.1	93.1
	Αρκετά	2	2.8	2.8	95.8
	Πολύ	1	1.4	1.4	97.2
	Πάρα πολύ	2	2.8	2.8	100.0
	Total	72	100.0	100.0	

Πίνακας 20 -Περιγραφικά στατιστικά ερώτησης 20

Ο Πίνακας 20 καταδεικνύει ότι το 56.9% δε χρησιμοποιεί καθόλου τα πλαίσια NIST SP ή RFC2196:Site Security Handbook, ενώ το 36.1% χρησιμοποιεί λίγο κάποιο από τα δύο πλαίσια. Με ισοβαθμία, 2.8%, προκύπτει ότι τα πλαίσια NIST SP ή RFC2196:Site Security Handbook χρησιμοποιούνται αρκετά, αλλά και πάρα πολύ. Σε πάρα πολύ μικρό ποσοστό, ήτοι 1.4%, τα πλαίσια NIST SP ή RFC2196:Site Security Handbook χρησιμοποιούνται πολύ. Συνεπώς, το 93.1% των επιχειρήσεων δε χρησιμοποιούν αρκετά τα πλαίσια NIST SP ή RFC2196:Site Security Handbook.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 20-Διάγραμμα ράβδων ερώτησης 20

Η ερώτηση 21 πραγματεύεται το βαθμό κατά τον οποίο οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας. Τα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα.

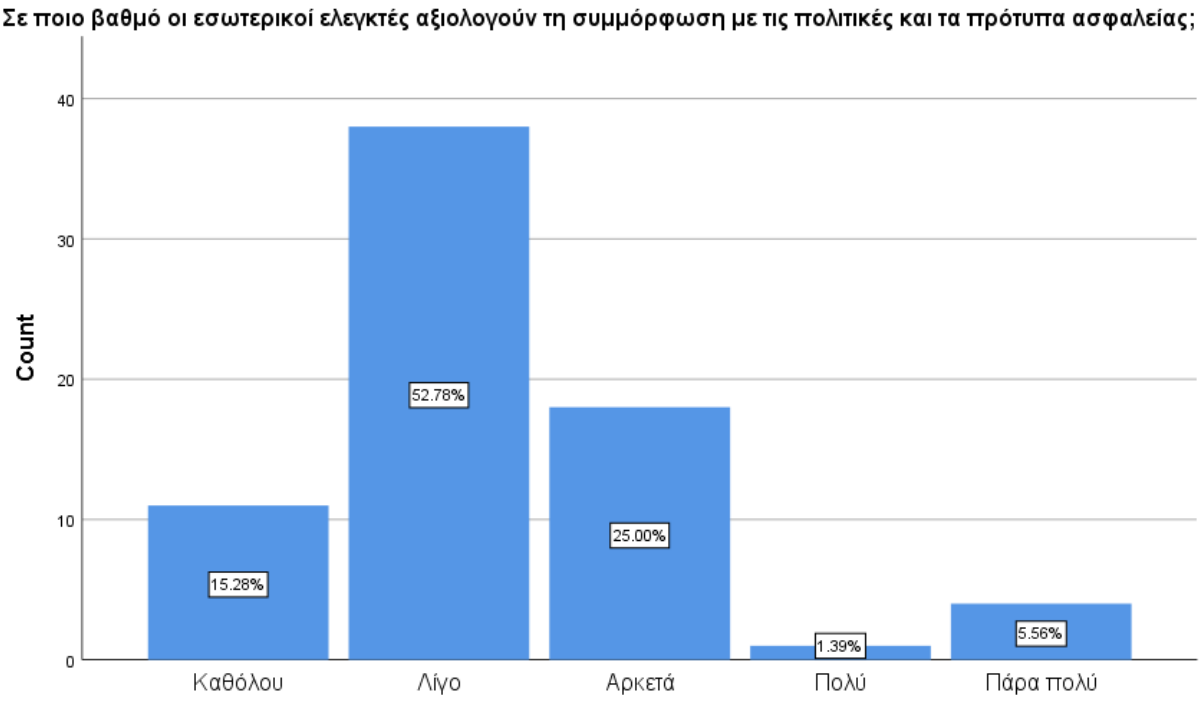
21. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	11	15.3	15.3	15.3
	Λίγο	38	52.8	52.8	68.1
	Αρκετά	18	25.0	25.0	93.1
	Πολύ	1	1.4	1.4	94.4
	Πάρα πολύ	4	5.6	5.6	100.0
	Total	72	100.0	100.0	

Πίνακας 21 -Περιγραφικά στατιστικά ερώτησης 21

Από τον παραπάνω πίνακα προκύπτει ότι το 52.8% των ερωτηθέντων ισχυρίζεται ότι οι εσωτερικοί ελεγκτές αξιολογούν λίγο τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας, το 25% ισχυρίζεται ότι αξιολογούν αρκετά τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας, ενώ το 15.3% ισχυρίζεται ότι οι εσωτερικοί ελεγκτές δεν αξιολογούν καθόλου τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας. Στον αντίποδα, το 5.6% υποστηρίζει ότι οι εσωτερικοί ελεγκτές αξιολογούν πάρα πολύ τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας, ενώ το 1.4% υποστηρίζει ότι αξιολογούν πολύ τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας. Συνεπώς, το 68.1% των ερωτηθέντων ισχυρίζεται ότι οι εσωτερικοί ελεγκτές αξιολογούν ελάχιστα τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 21-Διάγραμμα ράβδων ερώτησης 21

5.2.6 Ενημέρωση-εκπαίδευση των εργαζομένων σε θέματα ασφαλείας

Οι ερωτήσεις 22-25 αφορούν την ενημέρωση-εκπαίδευση των εργαζομένων σε θέματα ασφαλείας. Η ερώτηση 22 πραγματεύεται το βαθμό κατά τον οποίο η εκάστοτε επιχείρηση έχει συγκεκριμένους οδηγούς-οδηγίες που τονίζουν τι επιτρέπεται να κάνουν οι υπάλληλοι χρησιμοποιώντας τους υπολογιστές τους. Τα αποτελέσματα απεικονίζονται στον παρακάτω πίνακα.

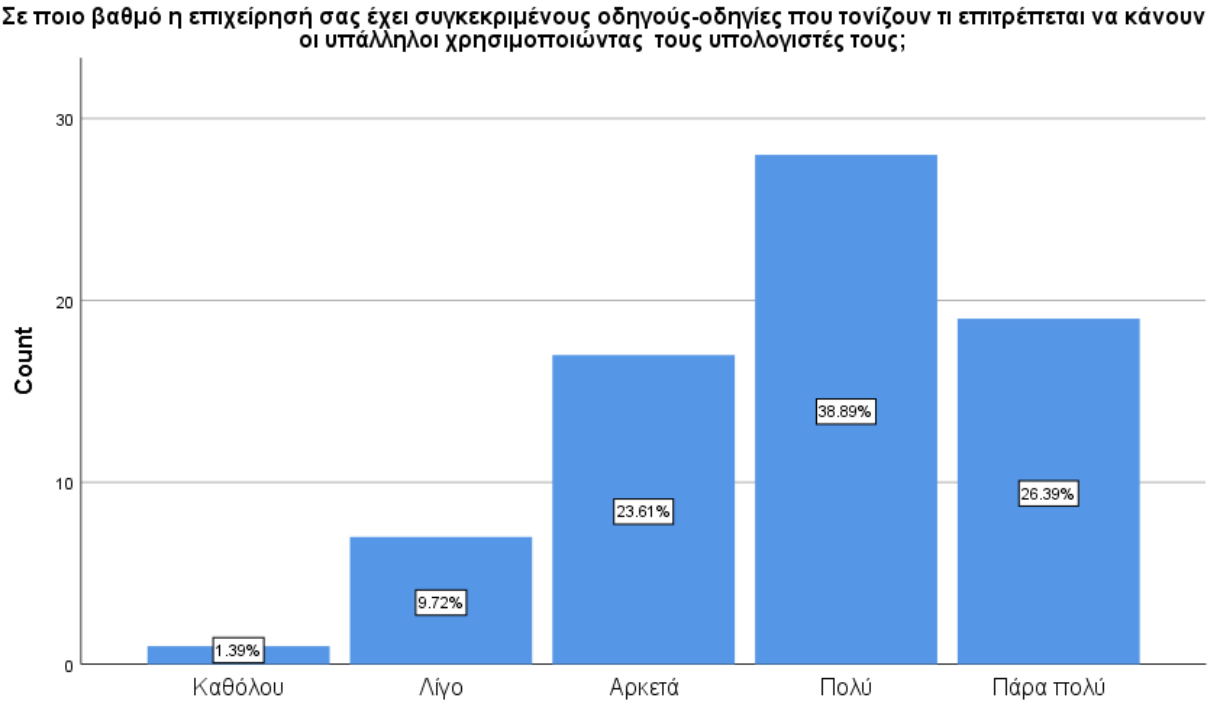
22. Σε ποιο βαθμό η επιχείρησή σας έχει συγκεκριμένους οδηγούς-οδηγίες που τονίζουν τι επιτρέπεται να κάνουν οι υπάλληλοι χρησιμοποιώντας τους υπολογιστές τους;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	1	1.4	1.4	1.4
	Λίγο	7	9.7	9.7	11.1
	Αρκετά	17	23.6	23.6	34.7
	Πολύ	28	38.9	38.9	73.6
	Πάρα πολύ	19	26.4	26.4	100.0
	Total	72	100.0	100.0	

Πίνακας 22 -Περιγραφικά στατιστικά ερώτησης 22

Ο παραπάνω πίνακας καταδεικνύει ότι το 38.9% των επιχειρήσεων έχει σε μεγάλο βαθμό, πολύ, συγκεκριμένους οδηγούς-οδηγίες που τονίζουν τι επιτρέπεται να κάνουν οι υπάλληλοι χρησιμοποιώντας τους υπολογιστές τους, το 26.4% έχει σε πολύ μεγάλο βαθμό, πάρα πολύ, ενώ το 23.6% έχει σε μέτριο βαθμό, αρκετά, συγκεκριμένους οδηγούς-οδηγίες που τονίζουν τι επιτρέπεται να κάνουν οι υπάλληλοι χρησιμοποιώντας τους υπολογιστές τους. Στον αντίποδα, το 9.7% έχει σε μικρό βαθμό, λίγο, συγκεκριμένους οδηγούς-οδηγίες, ενώ μόλις το 1.4% δεν έχει καθόλου συγκεκριμένους οδηγούς-οδηγίες. Συνεπώς, το 65.3% των επιχειρήσεων έχει σε αρκετά μεγάλο βαθμό συγκεκριμένους οδηγούς-οδηγίες που τονίζουν τι επιτρέπεται να κάνουν οι υπάλληλοι χρησιμοποιώντας τους υπολογιστές τους.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 22-Διάγραμμα ράβδων ερώτησης 22

Η ερώτηση 23 διερευνά το βαθμό στον οποίο η επιχείρηση παρέχει εκπαίδευση, ώστε να βοηθήσει τους υπαλλήλους της να βελτιώσουν την ενημέρωσή τους για τους υπολογιστές και τα ζητήματα ασφάλειας πληροφοριών. Τα αποτελέσματα απεικονίζονται στον παρακάτω πίνακα.

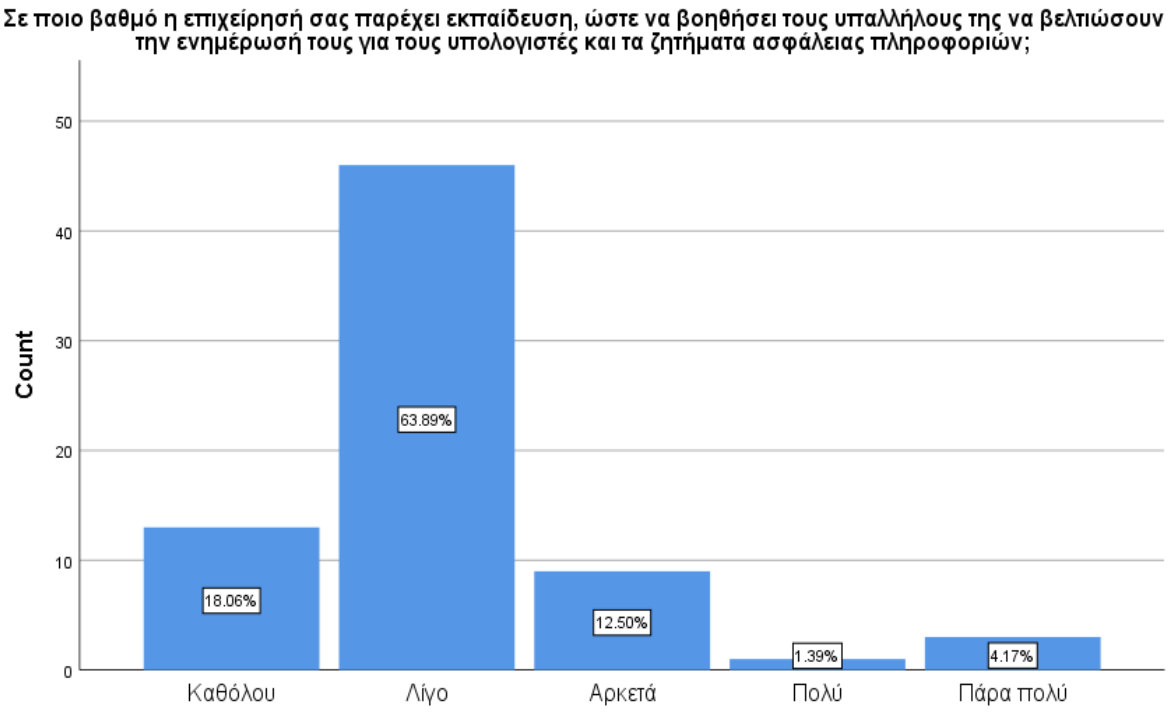
23. Σε ποιο βαθμό η επιχείρησή σας παρέχει εκπαίδευση, ώστε να βοηθήσει τους υπαλλήλους της να βελτιώσουν την ενημέρωσή τους για τους υπολογιστές και τα ζητήματα ασφάλειας πληροφοριών;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	13	18.1	18.1	18.1
	Λίγο	46	63.9	63.9	81.9
	Αρκετά	9	12.5	12.5	94.4
	Πολύ	1	1.4	1.4	95.8
	Πάρα πολύ	3	4.2	4.2	100.0
	Total	72	100.0	100.0	

Πίνακας 23 -Περιγραφικά στατιστικά ερώτησης 23

Σύμφωνα με τον Πίνακα 23, η πλειοψηφία των επιχειρήσεων, ήτοι το 63.9%, παρέχει σε μικρή κλίμακα, λίγο, εκπαίδευση, ώστε να βοηθήσει τους υπαλλήλους της να βελτιώσουν την ενημέρωσή τους για τους υπολογιστές και τα ζητήματα ασφάλειας πληροφοριών, το 18.1% δεν παρέχει καθόλου εκπαίδευση, ενώ το 12.5% παρέχει σε μέτρια κλίμακα, αρκετά, εκπαίδευση. Στον αντίποδα και με πολύ χαμηλά ποσοστά, το 4.2% παρέχει πάρα πολλή εκπαίδευση, ενώ το 1.4% παρέχει πολλή εκπαίδευση, ώστε να βοηθήσει τους υπαλλήλους της να βελτιώσουν την ενημέρωσή τους για τους υπολογιστές και τα ζητήματα ασφάλειας πληροφοριών. Συνεπώς, το 81.9% των επιχειρήσεων δεν παρέχει ικανοποιητικό επίπεδο εκπαίδευσης, ώστε να βοηθήσει τους υπαλλήλους της να βελτιώσουν την ενημέρωσή τους για τους υπολογιστές και τα ζητήματα ασφάλειας πληροφοριών.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 23-Διάγραμμα ράβδων ερώτησης 23

Στην ερώτηση 24 εξετάζεται ο βαθμός στον οποίο το προσωπικό γνωρίζει την Πολιτική Ασφάλειας Πληροφοριών. Τα αποτελέσματα απεικονίζονται στον παρακάτω πίνακα.

24. Σε ποιο βαθμό το προσωπικό γνωρίζει την Πολιτική Ασφάλειας Πληροφοριών;

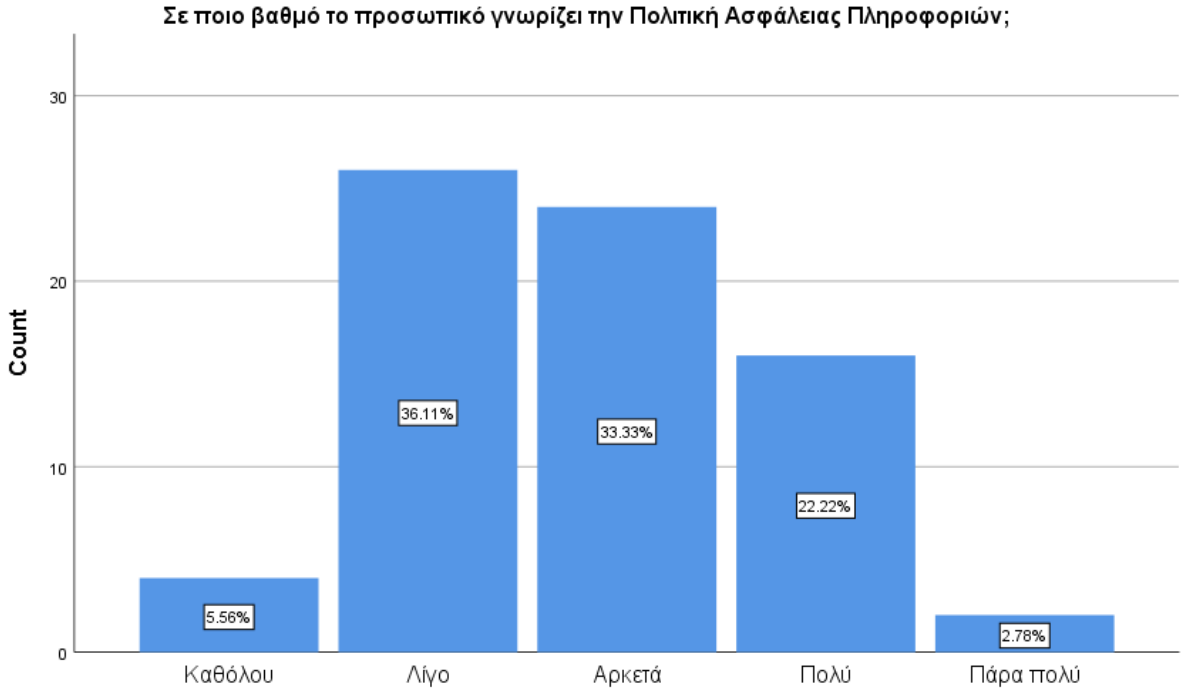
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	4	5.6	5.6	5.6
	Λίγο	26	36.1	36.1	41.7
	Αρκετά	24	33.3	33.3	75.0
	Πολύ	16	22.2	22.2	97.2
	Πάρα πολύ	2	2.8	2.8	100.0
	Total	72	100.0	100.0	

Πίνακας 24 -Περιγραφικά στατιστικά ερώτησης 24

Από τα παραπάνω αποτελέσματα προκύπτει ότι το 36.1% των ερωτηθέντων υποστηρίζει ότι το προσωπικό γνωρίζει σε μικρό βαθμό, λίγο, την Πολιτική Ασφάλειας Πληροφοριών, το 33.3% γνωρίζει αρκετά την Πολιτική Ασφάλειας Πληροφοριών, ενώ το 22.2% γνωρίζει σε μεγάλο βαθμό, πολύ, την Πολιτική

Ασφάλειας Πληροφοριών. Στον αντίποδα, το 5.6% υποστηρίζει ότι το προσωπικό δε γνωρίζει καθόλου την Πολιτική Ασφάλειας Πληροφοριών, ενώ το χαμηλό ποσοστό 2.8% υποστηρίζει ότι το προσωπικό γνωρίζει σε πολύ μεγάλο βαθμό, πάρα πολύ, την Πολιτική Ασφάλειας Πληροφοριών. Συνεπώς, το 41.7% των ερωτηθέντων ισχυρίζεται ότι το προσωπικό δε γνωρίζει σε μεγάλο βαθμό την Πολιτική Ασφάλειας Πληροφοριών.

Τα αποτελέσματα παρατίθενται και διαγραμματικά:



Εικόνα 24-Διάγραμμα ράβδων ερώτησης 24

Τέλος, η ερώτηση 25 ερευνά το βαθμό κατά τον οποίο οι εσωτερικοί ελεγκτές διασφαλίζουν ότι τα προγράμματα ενημέρωσης του προσωπικού για την ασφάλεια είναι υποχρεωτικά και ωφέλιμα. Τα αποτελέσματα απεικονίζονται στον παρακάτω πίνακα.

25. Σε ποιο βαθμό οι εσωτερικοί ελεγκτές διασφαλίζουν ότι τα προγράμματα ενημέρωσης του προσωπικού για την ασφάλεια είναι υποχρεωτικά και ωφέλιμα;

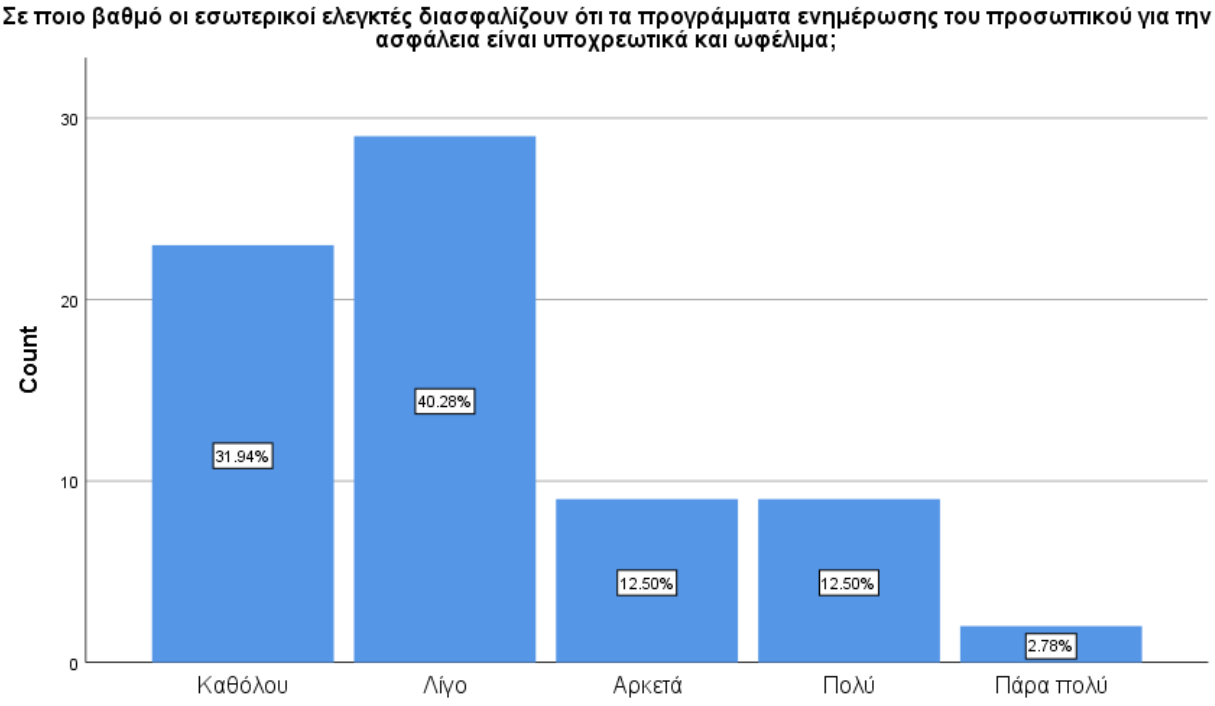
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Καθόλου	23	31.9	31.9	31.9
	Λίγο	29	40.3	40.3	72.2
	Αρκετά	9	12.5	12.5	84.7
	Πολύ	9	12.5	12.5	97.2
	Πάρα πολύ	2	2.8	2.8	100.0

Total	72	100.0	100.0	

Πίνακας 25 -Περιγραφικά στατιστικά ερώτησης 25

Ο Πίνακας 25 καταδεικνύει ότι το 40.3% των ερωτηθέντων ισχυρίζεται ότι οι εσωτερικοί ελεγκτές διασφαλίζουν σε μικρό βαθμό, λίγο, ότι τα προγράμματα ενημέρωσης του προσωπικού για την ασφάλεια είναι υποχρεωτικά και ωφέλιμα, ενώ το 31.9% ισχυρίζεται ότι οι εσωτερικοί ελεγκτές δε διασφαλίζουν καθόλου ότι τα προγράμματα ενημέρωσης του προσωπικού για την ασφάλεια είναι υποχρεωτικά και ωφέλιμα. Με ισοβαθμία 12.5%, υποστηρίζεται ότι οι εσωτερικοί ελεγκτές διασφαλίζουν αρκετά και πολύ ότι τα προγράμματα ενημέρωσης του προσωπικού για την ασφάλεια είναι υποχρεωτικά και ωφέλιμα, ενώ το μικρό ποσοστό 2.8% υποστηρίζει την παραπάνω άποψη πάρα πολύ. Συνεπώς, το 72.2% των ερωτηθέντων ισχυρίζεται ότι οι εσωτερικοί ελεγκτές διασφαλίζουν σε πολύ μικρό βαθμό ότι τα προγράμματα ενημέρωσης του προσωπικού για την ασφάλεια είναι υποχρεωτικά και ωφέλιμα.

Τα αποτελέσματα παρουσιάζονται και διαγραμματικά:



Εικόνα 25-Διάγραμμα ράβδων ερώτησης 25

5.3 Παρουσίαση Αποτελεσμάτων Ανάλυσης Παλινδρόμησης

5.3.1 Εισαγωγικά- Ανάλυση Αξιοπιστίας

Στην προηγούμενη ενότητα παρουσιάστηκαν τα αποτελέσματα, με τη μορφή πινάκων και διαγραμμάτων, που προέκυψαν από την περιγραφική στατιστική. Η έρευνα ολοκληρώνεται με την ανάλυση του οικονομετρικού μοντέλου της γραμμικής πολλαπλής παλινδρόμησης, ώστε να προσδιοριστούν οι παράγοντες που σχετίζονται με τον εσωτερικό έλεγχο και επιδρούν στην ασφάλεια των ηλεκτρονικών υπηρεσιών.

Η ομαδοποίηση των ερωτήσεων του ερωτηματολογίου σε παράγοντες έγινε εννοιολογικά και εξετάστηκε η αξιοπιστία της κάθε κλίμακας χρησιμοποιώντας το δείκτη Cronbach's Alpha. Συγκεκριμένα, δημιουργήθηκαν οι εξής κλίμακες:

- Ως εξαρτημένη μεταβλητή Υ θεωρείται η ασφάλεια των ηλεκτρονικών υπηρεσιών, η οποία ορίζεται ως το μέσο σκορ που προκύπτει από τις ερωτήσεις 4 και 6, στις οποίες έγινε αντίστροφη κωδικοποίηση. Η ερώτηση 5, που αρχικά είχε αποφασιστεί να χρησιμοποιηθεί και αυτή στη μέτρηση της εξαρτημένης μεταβλητής, δε χρησιμοποιήθηκε, καθώς διαπιστώθηκε ότι χρησιμοποιώντας δύο ερωτήσεις με κλίμακα διαστημάτων (ερωτήσεις 4 και 5), δε θα μπορούσε να εξαχθεί ορθά το μέσο σκορ των απαντήσεων.

Οι ανεξάρτητες μεταβλητές που προέκυψαν με βάση τη θεωρία είναι πέντε και είναι οι εξής:

- Συμβουλευτικός ρόλος των εσωτερικών ελεγκτών, που ορίζεται ως το μέσο σκορ των ερωτήσεων 7- 9
- Συνεργασία (καλή σχέση) μεταξύ των εσωτερικών ελεγκτών και των ειδικών της τεχνολογίας πληροφοριών, που ορίζεται ως το μέσο σκορ των ερωτήσεων 10-12
- Εξειδικευμένες τεχνολογικές γνώσεις των εσωτερικών ελεγκτών, που ορίζονται ως το μέσο σκορ των ερωτήσεων 13-16
- Πολιτικές –Πρότυπα ασφαλείας που ορίζονται ως το μέσο σκορ των ερωτήσεων 17-21
- Ενημέρωση- Εκπαίδευση, που ορίζεται ως το μέσο σκορ των ερωτήσεων 22-25

Ο παρακάτω πίνακας παρουσιάζει κάποια περιγραφικά στοιχεία των μεταβλητών, καθώς και το δείκτη αξιοπιστίας τους. Σύμφωνα με τον Kline (1999), καλή αξιοπιστία υποδηλώνεται, όταν η τιμή του συντελεστή άλφα κυμαίνεται πάνω από το 0.7. Όπως προκύπτει από τον Πίνακα 26, όλες οι τιμές του Cronbach's Alpha είναι πάνω από 0.7, οπότε όλες οι κλίμακες των ερωτήσεων είναι αξιόπιστες.

	Μέση τιμή	Τυπική Απόκλιση	Cronbach's Alpha
Ενημέρωση-Εκπαίδευση	2.7083	0.73278	0.743
Πολιτικές-Πρότυπα	2.0938	0.77985	0.736
Εξειδικευμένες Γνώσεις	2.1007	0.97654	0.945
Συνεργασία	2.5556	0.90036	0.922
Συμβουλευτικός ρόλος	4.0556	0.89031	0.861

Πίνακας 26- Πίνακας αξιοπιστίας

5.3.2 Πίνακας Συσχετίσεων

Στόχος της παλινδρόμησης είναι να διερευνηθεί αν οι μεταβλητές Ενημέρωση-Εκπαίδευση, Πολιτικές-Πρότυπα, Εξειδικευμένες Γνώσεις, Συνεργασία και Συμβουλευτικός ρόλος μπορούν να χρησιμοποιηθούν για την πρόβλεψη των τιμών της εξαρτημένης μεταβλητής. Αρχικά, έγινε έλεγχος συσχέτισής τους με την εξαρτημένη μεταβλητή, αλλά και μεταξύ τους. Τα αποτελέσματα των συσχετίσεων παρουσιάζονται στους παρακάτω 2 πίνακες.

Συσχετίσεις						
		Ενημέρωση-Εκπαίδευση	Πολιτικές-Πρότυπα	Εξειδικευμένες Γνώσεις	Συνεργασία	Συμβουλευτικός ρόλος
Y	r	-0.002	0.477	-0.157	-0.033	0.674
	p (2-tailed)	0.984	<0.01*	0.188	0.785	<0.01*
	N	72	72	72	72	72

Πίνακας 27- Συσχετίσεις εξαρτημένης μεταβλητής με τις ανεξάρτητες

Συσχετίσεις					
	Ενημέρωση-Εκπαίδευση	Πολιτικές-Πρότυπα	Εξειδικευμένες Γνώσεις	Συνεργασία	Συμβουλευτικός ρόλος
Ενημέρωση-Εκπαίδευση	1				
Πολιτικές-Πρότυπα	0.572	1			
Εξειδικευμένες	0.676	0.584	1		

Γνώσεις					
Συνεργασία	0.700	0.572	0.782	1	
Συμβουλευτικός ρόλος	-0.266	0.122	-0.478	-0.329	1

Πίνακας 28- Συσχετίσεις μεταξύ των ανεξάρτητων μεταβλητών

Λόγω του μεγάλου αριθμού του δείγματος (N=72 παρατηρήσεις) και της συνέχειας των μεταβλητών, ο έλεγχος συσχέτισης έγινε με το δείκτη του Pearson. Αυτός ο δείκτης εκφράζει τη συσχέτιση ως μια γραμμική σχέση (Creswell, 2016). Προκύπτει ότι υπάρχει στατιστικά σημαντική γραμμική συσχέτιση μεταξύ της εξαρτημένης μεταβλητής και της μεταβλητής «Πολιτικές- Πρότυπα», η οποία χαρακτηρίζεται μέτρια και θετική (r=0.477, p-τιμή<0.05). Αυτό σημαίνει ότι αύξηση στην τιμή της μεταβλητής «Πολιτικές- Πρότυπα» συνεπάγεται αύξηση της εξαρτημένης μεταβλητής. Επιπλέον, υπάρχει στατιστικά σημαντική γραμμική συσχέτιση μεταξύ της εξαρτημένης μεταβλητής και της μεταβλητής «Συμβουλευτικός ρόλος», η οποία χαρακτηρίζεται δυνατή και θετική (r=0.674. p-τιμή<0.05). Αυτό σημαίνει ότι αύξηση στην τιμή της μεταβλητή «Συμβουλευτικός ρόλος» συνεπάγεται αύξηση της εξαρτημένης μεταβλητής. Τέλος, δεν προκύπτει στατιστικά σημαντική συσχέτιση της εξαρτημένης μεταβλητής με τις άλλες ανεξάρτητες μεταβλητές.

Όσον αφορά τον Πίνακα 28, προκύπτει ότι οι μεταβλητές που συσχετίζονται με την εξαρτημένη μεταβλητή, δηλαδή, η μεταβλητή «Πολιτικές-Πρότυπα» και η μεταβλητή «Συμβουλευτικός ρόλος», έχουν μηδενική σχέση μεταξύ τους. Η μεταβλητή «Ενημέρωση- Εκπαίδευση» δε συσχετίζεται με καμία μεταβλητή, ενώ η μεταβλητή «Εξειδικευμένες Γνώσεις» συσχετίζεται σε μέτριο βαθμό με δύο άλλες μεταβλητές. Τέλος, η μεταβλητή «Συνεργασία» συσχετίζεται σημαντικά με άλλες τρεις μεταβλητές.

5.3.3 Ανάλυση πολλαπλής γραμμικής παλινδρόμησης

Δεδομένου ότι η σχέση μεταξύ των μεταβλητών Χ και Υ είναι γραμμική, θα χρησιμοποιήσουμε το παρακάτω θεωρητικό μοντέλο πολλαπλής γραμμικής παλινδρόμησης που εξετάζει την επίδραση πολλών ανεξάρτητων μεταβλητών σε μια εξαρτημένη (Creswell, 2016):

$$Y= b_o+ b_1X_1 + b_2X_2 + b_3X_3 + b_4X_4 + b_5X_5 + e_i \quad (1)$$

Όπου Υ είναι η εξαρτημένη μεταβλητή, X_1, X_2, X_3 , X_4 ,X_5 είναι οι ανεξάρτητες μεταβλητές, ενώ οι παράμετροι b_1, b_2, b_3, b_4, b_5 σχετίζονται με τις ανεξάρτητες μεταβλητές και εκφράζουν ποσοτικά τη σχέση που υπάρχει με την εξαρτημένη μεταβλητή, δηλαδή δείχνει πόσο αναμένεται να μεταβληθεί η εξαρτημένη μεταβλητή, αν η ανεξάρτητη μεταβλητή μεταβληθεί κατά μία μονάδα, δεδομένου ότι οι άλλες παράμετροι παραμένουν σταθερές. Η παράμετρος b_o δείχνει την τιμή της εξαρτημένης

μεταβλητής, όταν οι μεταβλητές πρόβλεψης είναι ίσες με το μηδέν. Τέλος, η παράμετρος e_i παρουσιάζει το σφάλμα πρόβλεψης (Creswell, 2016; Κατσής et al., 2010).

Σύμφωνα με τα παραπάνω, μπορούμε να ορίσουμε το συγκεκριμένο μοντέλο παλινδρόμησης που θέλουμε να εκτιμήσουμε:

$$\textit{Ασφάλεια ηλεκτρονικών υπηρεσιών} = b_o + b_1 * \textit{Πολιτικές-Πρότυπα} + b_2 * \textit{Τεχνολογικές Γνώσεις} + b_3 * \textit{Συνεργασία} + b_4 * \textit{Συμβουλευτικός ρόλος} + b_5 * \textit{Ενημέρωση-Εκπαίδευση} \quad (2)$$

Όπου οι τιμές b (συντελεστές παλινδρόμησης) μας πληροφορούν για τη σχέση της *Ασφάλειας ηλεκτρονικών υπηρεσιών* με την κάθε μεταβλητή πρόβλεψης, εφόσον η επίδραση όλων των άλλων μεταβλητών πρόβλεψης διατηρείται σταθερή. Αν ο συντελεστής παλινδρόμησης b έχει θετική τιμή, τότε συμπεραίνουμε ότι, όταν αυξάνεται κατά μία μονάδα καθεμία από τις ανεξάρτητες μεταβλητές, μεταβάλλεται θετικά η μέση τιμή της εξαρτημένης μεταβλητής. Αντιθέτως, όταν ο συντελεστής παλινδρόμησης b έχει αρνητική τιμή, τότε συμπεραίνουμε ότι, όταν αυξάνεται κατά μία μονάδα καθεμία από τις ανεξάρτητες μεταβλητές, μεταβάλλεται αρνητικά η μέση τιμή της εξαρτημένης μεταβλητής.

Ο Πίνακας 29 παρουσιάζει τη σύνοψη του μοντέλου με R^2=0.650 και προσαρμοσμένο R^2=0.623. Ως R^2 ορίζεται ο συντελεστής προσδιορισμού, ο οποίος δείχνει το ποσοστό της μεταβλητότητας που εξηγείται στην εξαρτημένη μεταβλητή από τις ανεξάρτητες μεταβλητές. Στο μοντέλο μας, προκύπτει ότι το 65% της διακύμανσης της ασφάλειας των ηλεκτρονικών υπηρεσιών ερμηνεύεται από τις ανεξάρτητες μεταβλητές, ενώ το υπόλοιπο 35% ερμηνεύεται από άλλους παράγοντες (Creswell, 2016; Κατσής et al., 2010).

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.806[a]	.650	.623	.47238

Predictors: (Constant), Ενημέρωση-Εκπαίδευση, Συμβουλευτικός ρόλος, Πολιτικές-Πρότυπα, Συνεργασία, Τεχνολογικές Γνώσεις

Πίνακας 29- Σύνοψη μοντέλου

Στη συνέχεια, ακολουθεί ο πίνακας ANOVA, ο οποίος ελέγχει αν το μοντέλο πολλαπλής παλινδρόμησης είναι στατιστικά σημαντικό. Αυτό σημαίνει ότι πρέπει

τουλάχιστον ένα από τα b_1, b_2,..,b_5 να είναι στατιστικά σημαντικά διάφορο του μηδενός. Ο έλεγχος υποθέσεων που θα λάβει χώρα είναι ο εξής:

H_o: $b_1 = b_2 = b_3 = b_4 = b_5 = 0$

H_1: *τουλάχιστον* ένα από τα b_1, b_2, b_3, b_4, b_5 είναι στατιστικά σημαντικά διαφορετικό του μηδενός

Η τιμή p του παραπάνω ελέγχου υποθέσεων δίνεται από τη στήλη Sig του Πίνακα 30 (Κατσής et al., 2010).

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	27.347	5	5.469	**24.510**	**.000[b]**
	Residual	14.728	66	.223		
	Total	42.075	71			

a. Dependent Variable: Y

b. Predictors: (Constant), Ενημέρωση-Εκπαίδευση, Συμβουλευτικός ρόλος, Πολιτικές-Πρότυπα, Συνεργασία, Τεχνολογικές Γνώσεις

Πίνακας 30- Πίνακας ANOVA

Αν η τιμή Sig < 0.05, απορρίπτεται η H_o και αποδεχόμαστε την H_1

Αν η τιμή Sig > 0.05, αποδεχόμαστε την H_o

Από τον Πίνακα 30, παρατηρείται ότι το F-τεστ έδειξε ότι το μοντέλο είναι στατιστικά σημαντικό σε επίπεδο σημαντικότητας 5%. (Απορρίφθηκε η μηδενική υπόθεση ότι όλοι οι συντελεστές είναι 0, αφού Sig =0.000 < 0.05). Αυτό σημαίνει ότι η εξαρτημένη μεταβλητή παρουσιάζει γραμμική σχέση με τουλάχιστον μία από τις ανεξάρτητες μεταβλητές.

Ύστερα, παρατίθεται ο πίνακας Coefficients. Από αυτόν τον πίνακα, μας ενδιαφέρει, αρχικά, η στήλη Β. Όπως επισημάνθηκε και παραπάνω, το Β απεικονίζει το συντελεστή παλινδρόμησης και δείχνει πόσο αναμένεται να μεταβληθεί η εξαρτημένη μεταβλητή, αν η ανεξάρτητη μεταβλητή μεταβληθεί κατά μία μονάδα, δεδομένου ότι όλες οι άλλες παράμετροι παραμένουν σταθερές. Για παράδειγμα, μια μονάδα αύξησης στη μεταβλητή «Συνεργασία», αυξάνει την ασφάλεια των ηλεκτρονικών υπηρεσιών κατά 0.044 μονάδες, διατηρώντας τους υπόλοιπους παράγοντες σταθερούς.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.438	.433		3.324	.001
	Πολιτικές-Πρότυπα	.605	.113	.613	5.348	.000
	Τεχνολογικές Γνώσεις	-.175	.116	-.222	-1.508	.136
	Συνεργασία	.044	.105	.051	.413	.681
	Συμβουλευτικός ρόλος	.416	.087	.481	4.787	.000
	Ενημέρωση-Εκπαίδευση	-.170	.107	-.162	-1.584	.118

Πίνακας 31- Πίνακας Coefficients

Με βάση τις τιμές της στήλης B, η εξίσωση παλινδρόμησης του μοντέλου μας διαμορφώνεται ως εξής:

Ασφάλεια ηλεκτρονικών υπηρεσιών = 1.438 + 0.605 * *Πολιτικές-Πρότυπα* – 0.175 * *Τεχνολογικές Γνώσεις* + 0.044 * *Συνεργασία* + 0.416 * *Συμβουλευτικός ρόλος* – 0.170 * *Ενημέρωση-Εκπαίδευση* (3)

Για να χρησιμοποιηθεί η παραπάνω εξίσωση, θα πρέπει να εξεταστεί αν ο κάθε συντελεστής b_1, b_2, b_3, b_4, b_5 ,ξεχωριστά, είναι στατιστικά σημαντικά διάφορος του μηδενός, δηλαδή να ελεγχθούν οι παρακάτω υποθέσεις:

1. H_o: $b_1 = 0$

   H_1: ο συντελεστής b_1 είναι στατιστικά σημαντικά διαφορετικός του μηδενός

2. H_o: $b_2 = 0$
   H_1: ο συντελεστής b_2 είναι στατιστικά σημαντικά διαφορετικός του μηδενός

3. H_o: $b_3 = 0$
   H_1: ο συντελεστής b_3 είναι στατιστικά σημαντικά διαφορετικός του μηδενός

4. H_o: $b_4 = 0$
   H_1: ο συντελεστής b_4 είναι στατιστικά σημαντικά διαφορετικός του μηδενός

5. H_o: $b_5 = 0$

   H_1: ο συντελεστής b_5 είναι στατιστικά σημαντικά διαφορετικός του μηδενός

Οι παραπάνω έλεγχοι υποθέσεων θα εξεταστούν από τις τιμές p, που δίνονται από τη στήλη sig του Πίνακα 31 (Κατσής et al., 2010). Με βάση τις τιμές των πινάκων t και sig θα γίνει και η αποδοχή ή απόρριψη των ερευνητικών μας υποθέσεων. Από τον Πίνακα 31 προκύπτει ότι:

- Για την πρώτη ανεξάρτητη μεταβλητή «Πολιτικές- Πρότυπα» προκύπτει t_1= 5.348 και sig =p-τιμή = 0.000 < 0.05, άρα απορρίπτεται η μηδενική υπόθεση και συνεπώς, ο συντελεστής b_1 είναι στατιστικά σημαντικός. Άρα, η μεταβλητή «Πολιτικές-Πρότυπα» επηρεάζει την ασφάλεια των ηλεκτρονικών υπηρεσιών και η ***Μηδενική υπόθεση H_0:*** *Οι πολιτικές-πρότυπα ασφαλείας που ελέγχονται από τον εσωτερικό έλεγχο δε συνδέονται αντίστροφα με τον αριθμό των περιστατικών παραβίασης* απορρίπτεται.

- Για τη δεύτερη ανεξάρτητη μεταβλητή «Τεχνολογικές Γνώσεις» προκύπτει ότι t_2= -1.508 και sig =p-τιμή = 0.136 > 0.05, άρα αποδεχόμαστε τη μηδενική υπόθεση και συνεπώς, ο συντελεστής b_2 είναι μη στατιστικά σημαντικός. Άρα, η μεταβλητή «Τεχνολογικές Γνώσεις» δεν επηρεάζει την ασφάλεια των ηλεκτρονικών υπηρεσιών και ***Μηδενική υπόθεση H_0:*** *Η ύπαρξη εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης* δεν απορρίπτεται.

- Για την τρίτη ανεξάρτητη μεταβλητή «Συνεργασία» προκύπτει ότι t_3= 0.413 και sig =p-τιμή = 0.681 > 0.05, άρα αποδεχόμαστε τη μηδενική υπόθεση και συνεπώς, ο συντελεστής b_3 είναι μη στατιστικά σημαντικός. Άρα, η μεταβλητή «Συνεργασία» δεν επηρεάζει την ασφάλεια των ηλεκτρονικών υπηρεσιών και η ***Μηδενική υπόθεση H_0:*** *Η καλή σχέση μεταξύ του εσωτερικού ελέγχου και των ειδικών της τεχνολογίας πληροφοριών δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης* δεν απορρίπτεται.

- Για την τέταρτη ανεξάρτητη μεταβλητή «Συμβουλευτικός Ρόλος» προκύπτει ότι t_4= 4.787 και sig =p-τιμή = 0.000 < 0.05, άρα απορρίπτεται η μηδενική υπόθεση και συνεπώς, ο συντελεστής b_4 είναι στατιστικά σημαντικός. Άρα, η μεταβλητή «Συμβουλευτικός Ρόλος» επηρεάζει την ασφάλεια των ηλεκτρονικών υπηρεσιών και η ***Μηδενική υπόθεση H_0***: *Ο συμβουλευτικός ρόλος του εσωτερικού ελέγχου δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης* απορρίπτεται.

- Για την πέμπτη ανεξάρτητη μεταβλητή «Ενημέρωση- Εκπαίδευση» προκύπτει ότι t_5= -1.584 και sig =p-τιμή = 0.118 > 0.05, άρα αποδεχόμαστε τη μηδενική υπόθεση και συνεπώς, ο συντελεστής b_5 είναι μη στατιστικά σημαντικός. Άρα, η μεταβλητή «Ενημέρωση- Εκπαίδευση» δεν επηρεάζει την ασφάλεια των ηλεκτρονικών υπηρεσιών και η ***Μηδενική υπόθεση H_0:*** *Η ενημέρωση-*

εκπαίδευση των εργαζομένων σε θέματα ασφαλείας δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης δεν απορρίπτεται.

Τα αποτελέσματα για όλες τις ερευνητικές μας υποθέσεις παρουσιάζονται στον παρακάτω πίνακα:

Μηδενική υπόθεση H_0	**Συμπέρασμα**
Η καλή σχέση μεταξύ του εσωτερικού ελέγχου και των ειδικών της τεχνολογίας πληροφοριών δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης	Δεν απορρίπτεται
Ο συμβουλευτικός ρόλος του εσωτερικού ελέγχου δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης	Απορρίπτεται
Η ύπαρξη εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης	Δεν απορρίπτεται
Οι πολιτικές-πρότυπα ασφαλείας που ελέγχονται από τον εσωτερικό έλεγχο δε συνδέονται αντίστροφα με τον αριθμό των περιστατικών παραβίασης	Απορρίπτεται
Η ενημέρωση-εκπαίδευση των εργαζομένων σε θέματα ασφαλείας δε συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης	Δεν απορρίπτεται

Πίνακας 32 – Ερευνητικές υποθέσεις

Όσον αφορά την πολυσυγγραμικότητα, δηλαδή την περίπτωση στην οποία κάποιες από τις ανεξάρτητες μεταβλητές έχουν υψηλή γραμμική συσχέτιση μεταξύ τους, τα αποτελέσματα για το συγκεκριμένο μοντέλο παρουσιάζονται στους Πίνακες 33 και 34. Όπως λέχθηκε και παραπάνω, για να ερμηνευτεί κάθε συντελεστής παλινδρόμησης, πρέπει όλες οι υπόλοιπες μεταβλητές να παραμένουν σταθερές. Σε περίπτωση που υπάρχει θέμα πολυσυγγραμικότητας, δεν ικανοποιείται αυτή η απαίτηση και συνεπώς το μοντέλο δεν μπορεί να χρησιμοποιηθεί, αφού οι συντελεστές δεν θα είναι εφαρμόσιμοι (Κατσής et al., 2010).

Οι Πίνακες 33 και 34 αφορούν τους διαγνωστικούς ελέγχους που έλαβαν χώρα για τη μέτρηση της πολυσυγγραμικότητας. Αρχικά, με βάση τον Πίνακα 33 προκύπτει ότι δεν υπάρχει θέμα πολυσυγγραμικότητας, αφού ο δείκτης VIF <10 για όλες τις ανεξάρτητες μεταβλητές. Επιπλέον, ο Πίνακας 34 επιβεβαιώνει τη μη ύπαρξη πολυσυγγραμικότητας, εφόσον οι τιμές του δείκτη Eigenvalue είναι μικρότερες του

10 και του Condition Index είναι μικρότερες του 30 για όλες τις ανεξάρτητες μεταβλητές (Κατσής et al., 2010). Συνεπώς, το μοντέλο μας δεν πάσχει από το πρόβλημα της πολυσυγγραμικότητας.

Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	Πολιτικές-Πρότυπα	**.404**	**2.475**
	Τεχνολογικές Γνώσεις	**.244**	**4.091**
	Συνεργασία	**.349**	**2.864**
	Συμβουλευτικός ρόλος	**.525**	**1.903**
	Ενημέρωση- Εκπαίδευση	**.507**	**1.971**

Πίνακας 33- Έλεγχος πολυσυγγραμικότητας

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions					
				(Constant)	Πολιτικές Πρότυπα	Τεχνολ. Γνώσεις	Συνεργασία	Συμβουλ. ρόλος	Ενημέρωση- Εκπαίδευση
1	1	5.686	**1.000**	.00	.00	.00	.00	.00	.00
	2	.191	**5.456**	.01	.00	.08	.02	.05	.00
	3	.057	**9.997**	.04	.65	.02	.04	.00	.01
	4	.029	**14.023**	.01	.00	.03	.20	.04	.90
	5	.028	**14.377**	.03	.00	.59	.74	.01	.03
	6	.009	**24.759**	.91	.35	.28	.01	.90	.05

a. Dependent Variable: Y

Πίνακας 34- Διαγνωστικός έλεγχος πολυσυγγραμικότητας

Κεφάλαιο 6: Συμπεράσματα, Περιορισμοί και Προτάσεις για Μελλοντική Έρευνα

6.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο της διπλωματικής εργασίας παρατίθενται τα ουσιαστικά συμπεράσματα της έρευνας, αλλά και της εργασίας γενικότερα. Το κεφάλαιο ολοκληρώνεται με την παράθεση των περιορισμών που προέκυψαν κατά την εκπόνηση της εργασίας, αλλά και των προτάσεων για μελλοντική έρευνα.

6.2 Συμπεράσματα

Η ασφάλεια των ηλεκτρονικών υπηρεσιών και των πληροφοριακών συστημάτων κρίνεται επιτακτική για όλες τις επιχειρήσεις σε μια εποχή που όλα είναι ψηφιοποιημένα. Ο εσωτερικός έλεγχος έχει αλλάξει και έχει εμπλουτίσει τις αρμοδιότητές του και πλέον θα πρέπει να συντελεί και αυτός στην ασφάλεια των ηλεκτρονικών υπηρεσιών με ποικίλους τρόπους. Τα αποτελέσματα της εκτενούς επισκόπησης ερευνών σκιαγραφούν τον καθοριστικό ρόλο του εσωτερικού ελέγχου στην ασφάλεια των πληροφοριακών συστημάτων.

Η παρούσα διπλωματική εργασία εκπονήθηκε, ώστε να διερευνήσει τους παράγοντες που σχετίζονται με τον εσωτερικό έλεγχο και επιδρούν στην ασφάλεια των πληροφοριακών συστημάτων στην Ελλάδα. Πιο συγκεκριμένα, διερευνήθηκε αν:

- η καλή σχέση μεταξύ του εσωτερικού ελέγχου και των ειδικών της τεχνολογίας πληροφοριών συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης,
- ο συμβουλευτικός ρόλος του εσωτερικού ελέγχου συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης,
- η ύπαρξη εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης,
- οι πολιτικές-πρότυπα ασφαλείας που ελέγχονται από τον εσωτερικό έλεγχο συνδέονται αντίστροφα με τον αριθμό των περιστατικών παραβίασης
- η ενημέρωση-εκπαίδευση των εργαζομένων σε θέματα ασφαλείας συνδέεται αντίστροφα με τον αριθμό των περιστατικών παραβίασης.

Η στατιστική ανάλυση πραγματοποιήθηκε μέσω του στατιστικού λογισμικού πακέτου SPSS, ώστε να διερευνηθούν οι σχέσεις και οι συσχετίσεις μεταξύ της εξαρτημένης μεταβλητής και των ανεξάρτητων μεταβλητών που αναφέρθηκαν στην προηγούμενη παράγραφο. Τα συμπεράσματα που εξήχθησαν από την εμπειρική έρευνα είναι αρκετά σημαντικά. Αρχικά, η πλειοψηφία των επιχειρήσεων κατατάσσεται στις μεγάλες επιχειρήσεις και τα περιστατικά παραβίασης σε αυτές τις επιχειρήσεις είναι υπαρκτά και τείνουν να αυξάνονται με την πάροδο του χρόνου.

Όσον αφορά το συμβουλευτικό ρόλο των εσωτερικών ελεγκτών, η πλειοψηφία των ερωτηθέντων υποστήριξε ότι οι εσωτερικοί ελεγκτές λειτουργούν σε πολύ μεγάλο βαθμό επικουρικά σε άλλα τμήματα, όπως το τμήμα IT. Όμως, η καλή σχέση μεταξύ των ειδικών της τεχνολογίας πληροφοριών και των εσωτερικών ελεγκτών υποστηρίζεται ότι είναι αρκετά περιορισμένη, με συνέπεια να υπάρχει τριβή μεταξύ των δύο μερών. Επιπλέον, η πλειοψηφία των ερωτηθέντων αποκρίθηκε ότι το επίπεδο των εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών είναι πολύ χαμηλό.

Όσον αφορά τις πολιτικές- πρότυπα ασφαλείας που ελέγχονται από τον εσωτερικό έλεγχο, προέκυψε ότι το μεγαλύτερο ποσοστό των επιχειρήσεων έχει κάποια καταγεγραμμένη Πολιτική Ασφαλείας Πληροφοριών, όμως δεν εφαρμόζει σε ικανοποιητικό βαθμό κάποια από τα βασικά πρότυπα και πλαίσια ασφαλείας (όπως ISO, COBIT κ.ά.). Τέλος, αναφορικά με την ενημέρωση και εκπαίδευση του προσωπικού σε θέματα ασφαλείας, η πλειοψηφία των ερωτηθέντων αποφάνθηκε ότι, παρόλο που οι επιχειρήσεις έχουν σε ικανοποιητικό βαθμό συγκεκριμένες οδηγίες που ορίζουν πώς πρέπει να γίνεται η ορθή χρήση των ηλεκτρονικών υπηρεσιών, δεν παρέχεται εκπαίδευση στο προσωπικό και οι εσωτερικοί ελεγκτές δε διασφαλίζουν ότι τα προγράμματα ενημέρωσης και εκπαίδευσης είναι υποχρεωτικά.

Με γνώμονα την εξαγωγή περισσότερο εξειδικευμένων αποτελεσμάτων, διεξήχθησαν οι συσχετίσεις μεταξύ των μεταβλητών και η ανάλυση παλινδρόμησης. Από τα αποτελέσματα προέκυψε ότι μόνο δύο από τις πέντε ανεξάρτητες μεταβλητές του μοντέλου είναι στατιστικά σημαντικές.

Πιο συγκεκριμένα, προέκυψε ότι υπάρχει στατιστικά σημαντική γραμμική θετική συσχέτιση μεταξύ της εξαρτημένης μεταβλητής (ασφάλεια των ηλεκτρονικών υπηρεσιών) και της ανεξάρτητης μεταβλητής «Συμβουλευτικός ρόλος», όπως και μεταξύ της εξαρτημένης μεταβλητής και της ανεξάρτητης μεταβλητής «Πολιτικές – Πρότυπα». Αυτό σημαίνει ότι μια αύξηση των ανεξάρτητων μεταβλητών συνεπάγεται και αύξηση στην ασφάλεια των ηλεκτρονικών υπηρεσιών. Από την παλινδρόμηση, επίσης, προέκυψε ότι αυτές οι δύο ανεξάρτητες μεταβλητές είναι στατιστικά σημαντικές και επιδρούν στην ασφάλεια των ηλεκτρονικών υπηρεσιών. Τα παραπάνω ευρήματα ταυτίζονται με τους Bhattacharyya (2015) and Van Peursem (2004), οι οποίοι επισημαίνουν τα οφέλη του καθοδηγητικού-συμβουλευτικού ρόλου του εσωτερικού ελέγχου, αλλά και με τους Islam et al. (2018), οι οποίοι τονίζουν ότι ο εσωτερικός έλεγχος πρέπει να εξετάζει τις πολιτικές ασφαλείας για την επίτευξη της μέγιστης δυνατής ασφάλειας.

Αναφορικά με τη μεταβλητή « Τεχνολογικές Γνώσεις», που σχετίζεται με τις εξειδικευμένες τεχνολογικές γνώσεις που πρέπει να έχουν οι εσωτερικοί ελεγκτές, αποδείχτηκε ότι δεν προκύπτει στατιστικά σημαντική γραμμική συσχέτιση της ασφάλειας των ηλεκτρονικών υπηρεσιών με αυτή. Από την παλινδρόμηση, επίσης, προέκυψε ότι αυτή η μεταβλητή δεν είναι στατιστικά σημαντική και συνεπώς δεν επιδρά στην ασφάλεια των ηλεκτρονικών υπηρεσιών. Τα ευρήματα αυτά αντιτίθενται

με την προϋπάρχουσα βιβλιογραφία, καθώς οι Abu-Musa (2008) και Curtis et al.(2009) υποστηρίζουν ότι η ύπαρξη εξειδικευμένων τεχνολογικών γνώσεων από την πλευρά των εσωτερικών ελεγκτών θα ενισχύσει το ρόλο τους στην ανίχνευση πιθανών παραβιάσεων στα πληροφοριακά συστήματα

Η ανεξάρτητη μεταβλητή «Συνεργασία» έχει να κάνει με την καλή σχέση μεταξύ των ειδικών της ασφάλειας των ηλεκτρονικών υπηρεσιών και των εσωτερικών ελεγκτών. Από την έρευνα προέκυψε ότι δεν υπάρχει στατιστικά σημαντική γραμμική συσχέτιση της ασφάλειας των ηλεκτρονικών υπηρεσιών με αυτή τη μεταβλητή. Από την παλινδρόμηση, επίσης, προέκυψε ότι η μεταβλητή «Συνεργασία» δεν είναι στατιστικά σημαντική και συνεπώς δεν επιδρά στην ασφάλεια των ηλεκτρονικών υπηρεσιών. Το αποτέλεσμα αυτό δε συνάδει με τις έρευνες των Bauer and Estep (2018) και Steinbart et al. (2018), οι οποίοι υποστηρίζουν ότι η συνεργασία επιφέρει ανταλλαγή γνώσεων και μέσω αυτής ανιχνεύονται περισσότερα περιστατικά παραβίασης προτού δημιουργήσουν οικονομική ή οποιαδήποτε άλλη απώλεια στην επιχείρηση.

Η πέμπτη και τελευταία ανεξάρτητη μεταβλητή του μοντέλου αφορά την ενημέρωση – εκπαίδευση του προσωπικού σε θέματα ασφαλείας και σύμφωνα με τα αποτελέσματα της έρευνας, δεν προέκυψε στατιστικά σημαντική γραμμική συσχέτιση της ασφάλειας των ηλεκτρονικών υπηρεσιών με αυτή τη μεταβλητή. Από την παλινδρόμηση, επίσης, προέκυψε ότι η μεταβλητή «Εκπαίδευση» δεν είναι στατιστικά σημαντική και συνεπώς δεν επιδρά στην ασφάλεια των ηλεκτρονικών υπηρεσιών. Το αποτέλεσμα αυτό δε συνάδει με τις έρευνες των Abawajy (2014) και D’ Arcy and Hovav (2007), οι οποίοι υποστηρίζουν ότι η εκπαίδευση και η ενημέρωση των εργαζομένων σε θέματα ασφαλείας είναι καταλυτική, καθώς οδηγεί σε μείωση των περιστατικών παραβίασης.

Συνοψίζοντας όλα τα παραπάνω ευρήματα από την εμπειρική έρευνα, αποδείχτηκε ότι μόνο δύο μεταβλητές, οι μεταβλητές «Συμβουλευτικός ρόλος» και «Πολιτικές – Πρότυπα», συσχετίζονται σε στατιστικά σημαντικό βαθμό με την ασφάλεια των ηλεκτρονικών υπηρεσιών και επιδρούν σε αυτή. Οι υπόλοιποι τρεις παράγοντες δε φαίνεται να συσχετίζονται γραμμικά με την ασφάλεια των ηλεκτρονικών υπηρεσιών, όμως μπορεί να έχουν κάποιας άλλης μορφής σχέση. Με άλλα λόγια, η σχέση τους με την εξαρτημένη μεταβλητή δεν είναι στατιστικά σημαντική και συνεπώς δεν αποδεικνύεται ότι επιδρούν στην ασφάλεια των ηλεκτρονικών υπηρεσιών.

6.3 Περιορισμοί

Όπως συμβαίνει με όλες τις έρευνες, τα ευρήματα της παρούσας έρευνας υπόκεινται σε κάποιους περιορισμούς. Αρχικά, ένας βασικός περιορισμός είναι το μικρό χρονικό διάστημα διεξαγωγής της εμπειρικής έρευνας, αλλά και το σχετικά μικρό μέγεθος του δείγματος (N=72), παρόλο που τα ερωτηματολόγια που

στάλθηκαν ήταν περισσότερα, δεν υπήρξε, όμως, μεγάλη ανταπόκριση από τις επιχειρήσεις.

Ο επόμενος βασικός περιορισμός αφορά τη μη ύπαρξη άλλων αντίστοιχων ερευνών που σχετίζονται με την ασφάλεια των ηλεκτρονικών υπηρεσιών και έχουν διεξαχθεί στην Ελλάδα, με συνέπεια να μην είναι η δυνατή η σύγκριση. Επιπλέον, προκύπτουν και κάποιοι περιορισμοί λόγω της χρήσης της κλίμακας Likert, όπως ότι σε αρκετές ερωτήσεις οι ερωτηθέντες έδωσαν ως απάντηση τη μεσαία απάντηση, πράγμα που αποδεικνύει ουδετερότητα και ενδεχόμενη αποφυγή μιας ειλικρινούς απάντησης που θα μπορούσε να επηρεάσει διαφορετικά τα αποτελέσματα της έρευνας.

Τέλος, ένας άλλος περιορισμός προκύπτει από το γεγονός ότι δεν μπορούμε να γνωρίζουμε το βαθμό αντικειμενικότητας και αμεροληψίας των απαντήσεων που έδωσαν οι ερωτηθέντες, καθώς οι απαντήσεις είναι προσωπικές και σε μεγάλο βαθμό υποκειμενικές.

6.4 Προτάσεις για Μελλοντική Έρευνα

Υπό το πρίσμα των περιορισμών που παρατέθηκαν παραπάνω, θα ήταν ωφέλιμο να διεξαχθεί μια μελλοντική έρευνα, η οποία θα διαρκέσει μεγαλύτερο χρονικό διάστημα και το δείγμα της θα είναι περισσότερο αντιπροσωπευτικό. Η έρευνα αυτή θα μπορούσε να χρησιμοποιήσει τις ίδιες μεταβλητές με την παρούσα ερευνητική μελέτη ή ακόμη να εμπλουτιστεί με περισσότερους παράγοντες. Τέλος, θα ήταν καλό να γίνει χρήση κάποιου άλλου στατιστικού πακέτου, με το οποίο θα εξακριβωθούν οι λόγοι για τους οποίους τρείς από τις πέντε ανεξάρτητες μεταβλητές δε βρέθηκαν ως στατιστικά σημαντικές, ενώ η επισκόπηση ερευνών τις καθιστούσε θεμελιώδεις για την ασφάλεια των ηλεκτρονικών υπηρεσιών.

Βιβλιογραφία

Ξενόγλωσση Βιβλιογραφία

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Abdolmohammadi, M. J., & Boss, S. R. (2010). Factors associated with IT audits by the internal audit function. *International Journal of Accounting Information Systems*, *11*(3), 140-151.

Abu-Musa, A.A. (2008). Information technology and its implications for internal auditing. *Managerial Auditing Journal*, *23*(5), 436-466.

Atoum, I., Otoom, A., & Ali, A.A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, *22*(3), 251-264.

Bauer, T., & Estep, C. (2018). *One Team or Two? Investigating Relationship Quality between Auditors and IT Specialists: Implications for Audit Team Identity and the Audit Process*. Available at : https://ssrn.com/abstract=2579198 [Accessed 5 February 2019].

Bednar, P., Sadok, M., & Katos, V. (2013). Contextual dependencies in information systems security. AIS SIGSEC and IFIP TC 11.1 *Workshop on Information Security & Privacy*, WISP 2013, Milan, Italy, 2013.

Bhattacharyya, A. K. (2015). Internal Audit - Its Role in Corporate Governance. Available at: https://ssrn.com/abstract=2621149 [Accessed 5 February 2019].

Bou-Raad, G. (2000). Internal auditors and a value-added approach: the new business regime", *Managerial Auditing Journal*, *15*(4), 182-187.

Brody, R. G., & Kearns, G. (2009). IT audit approaches for enterprise resource planning systems. *ICFAI Journal of Audit Practice*, *6*(2), 7-26.

Broom, A. (2009). Security consolidation and optimisation: Gaining the most from your IT assets. *Computer Fraud & Security*, *2009*(5), 15-17.

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks*. Carnegie Mellon University: Software Engineering Institute.

Cohen, A., & Sayag, G. (2010). The Effectiveness of Internal Auditing: An Empirical Examination of its Determinants in Israeli Organisations. *Australian Accounting Review*, *20*(3), 296-307.

Coram, P., Ferguson, C., & Moroney, R. (2008). Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud, *Accounting and Finance*, *48*(4), 543–559.

Creswell, J. (2016). *Η έρευνα στην εκπαίδευση- Σχεδιασμός, διεξαγωγή και αξιολόγηση ποσοτικής και ποιοτικής έρευνας* (μτφ. Ν. Κουβαράκου). Αθήνα: Εκδοτικός Όμιλος Ίων (έτος έκδοσης πρωτοτύπου 2015).

Curtis, M. B., Jenkins, J. G., Bedard, J. C., & Deis D. R. (2009). Auditors' training and proficiency in information systems: a research synthesis. *Journal of Information Systems, 23*(1), 79-96.

Damianides, M. (2004). How does SOX change IT? *Journal of Corporate Accounting & Finance, 15*(6), 35–41.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361–372.

Dittenhofer, M. (2001). Internal auditing effectiveness: an expansion of present methods. *Managerial Auditing Journal*, *16*(8), 443-450.

Drogalas, G., Karagiorgos, T., & Arampatzis, K. (2015). Factors associated with Internal Audit Effectiveness: Evidence from Greece. *Journal of Accounting and Taxation, 7*(7), 113-122.

Drogalas, G., Arampatzis, K., & Anagnostopoulou, E. (2016). The relationship between corporate governance, internal audit and audit committee: empirical evidence from Greece. *Corporate Ownership & Control*, *14*(1-4), 569-577.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance, 17*(5), 474-491.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*(5), 410-430.

Fielden, K. (2011). An holistic view of information security: A proposed framework. *International Journal of Infonomics, 4*(1/2), 427-434.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of ACM, 46*(3), 81-85.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236.

Hannaford, C. S. (1995). Can computer security really make a difference?. *Managerial Auditing Journal*, *10*(5), 10-15.

Havelka, D., & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems, 14*(3), 165-192.

Institute of Internal Auditors (1999). *Definition of Internal Auditing.* Altamonte Springs: The Institute of Internal Auditors.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/ cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, *33*(4), 377-409.

ISO (2005). ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security controls*. Available at: https://www.iso.org/standard/50297.html [Accessed 5 February 2019].

ISO (2018). ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management.* Available at: *https://www.iso.org/standard/75281.html* [Accessed 5 February 2019].

ITGI (2007). *COBIT 4.1*: control objectives for information and related technology. Rolling Meadows: IT Governance Institute.

Kahyaoglu, S. B., Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal, 33*(4), 360-376.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, *9*(3), 163-175.

Kline, P. (1999). *The Handbook of Psychological Testing* (2nd ed.). London: Routledge.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, *10*(2), 57–63.

Maher, M., & Akers, M. D. (2003). Internal audit's role in systems development: the CEO's perspective. *Internal Auditing*, *18*(1), 35-39.

Merhout, J. W., & Havelka, D. (2008). Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit. *Communications of the Association for Information Systems, 23*(26), 463-482.

Michael, C., & Charles, E. H. (2013). Unlike chess, everyone must continue playing after a cyber-attack. *Journal of Investment Compliance*, *14*(4), 5-12.

Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Petterson, M. (2005). The keys to effective IT auditing. *The Journal of Corporate Accounting & Finance*, *16*(5), 41-46.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: a conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.

Richards, D. A., Oliphant, A. S., & Le Grand, C. H. (2005). *Global Technology Audit Guide: Information Technology Controls.* Altamonte Springs: Institute of Internal Auditors. oook

Sahibudin, S., Sharifi, M., & Ayat, M. (2008, May). *Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations*, paper presented at the Second Asia International Conference on Modelling & Simulation, Malaysia. Retrieved from https://ieeexplore.ieee.org/document/4530569 [Accessed 5 February 2019].

Sarens, G., & De Beelde, I. (2006). Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies. *Managerial Auditing Journal, 21*(1), 63-80.

Siouziou, I., Toudas, K., & Menexiadis, M. (2017). Internal audit and systems of internal audit in Greek Banks. *China-USA Business Review, 16*(12), 576-587.

Souppaya, M., & Scarfone, K. (2013). "*Guide to Malware incident prevention and handling for desktops and laptops*", NIST Special Publication 800-83, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf [Accessed 5 February 2019].

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal, 33*(4), 410-424.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). An analysis of end-user security behaviors. *Computers & Security, 24*(2), 124–133.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems, 13*(3), 228-243.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2015). *The Influence of Internal Audit on Information Security Effectiveness: Perceptions of Internal Auditors*. Available at: https://dx.doi.org/10.2139/ssrn.2685943 [Accessed 5 February 2019].

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, In press.

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security, 25*(5), 494-534.

Stewart, J., & Subramaniam, N. (2010). Internal audit independence and objectivity: emerging research opportunities. *Managerial Auditing Journal, 25*(4), 328-360.

Stoel, D., Havelka, D., & Merhout. J.W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems, 13*(1), 60-79.

Tabor, S.W. (2009, August). *Exploring the Role of Frameworks & Methodologies in Information Security Management & Governance - Research in Progress*. Proceedings of the 15th Americas Conference on Information Systems, San

Francisco, California, USA. Retrieved from: https://www.researchgate.net/publication/220894066_Exploring_the_Role_of_Frameworks_Methodologies_in_Information_Security_Management_Governance_-_Research_in_Progress [Accessed 5 February 2019].

The IIA Research Foundation. (2015). *Navigating Technology's Top 10 Risks-Internal Audit's Role*. Available at: https://www.iia.nl/SiteFiles/Publicaties/Navigating%20Technology's%20Top%2010%20Risks%20_Small.pdf [Accessed 5 February 2019].

Thompson, D. (1998). 1997 computer crime and security survey. *Information Management & Computer Security, 6*(2), 78 – 101.

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: educating your users effectively, *Information Management & Computer Security*, *6*(4), 167-173.

Trim, P. R. J., & Lee, Y. I. (2010, June). *A security framework for protecting business, government and society from cyber attacks* in: IEEE 5th International Conference on System of Systems Engineering (SoSE), UK. Retrieved from https://ieeexplore.ieee.org/document/5544085 [Accessed 5 February 2019].

Upfold, C. T., & Sewry, D. A. (2005). *An investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape*, In: H. S. Venter, J. H. P. Eloff, L. Labuschagne, & M. M. Eloff (Eds.), *Proceedings of the ISSA 2005 new knowledge today conference*, 29 June–1 July 2005, South Africa, Article 082, 1–17. Retrieved from: https://www.researchgate.net/publication/33996619_An_investigation_of_information_security_in_small_and_medium_enterprises_SME's_in_the_Eastern_Cape [Accessed 5 February 2019].

Van Peursem, K. (2004). Internal auditors' role and authority: New Zealand evidence. *Managerial Auditing Journal*, *19*(3), 378-393.

Van Peursem, K. (2005). Conversations with internal auditors: The power of ambiguity. *Managerial Auditing Journal*, *20*(5), 489-512.

Wallace, L., Lin, H., & Cefaratti, M.A. (2011). Information security and Sarbanes-Oxley compliance: an exploratory study. *Journal of Information Systems, 25*(1), 185-211.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4-19.

Whitman, M. & Mattord, H. (2003). *Principles of Information Security* (1st ed.). Boston: Thomson Course Technology.

Whitman, M. E., Townsend, A. M., & Alberts, R. J. (2001). Information systems security and the need for policy. In M. Khosrowpour (Ed.), *Information Security Management: Global Challenges in the New Millennium* (pp. 9-18). Hershey: Idea Group Publishing.

Ελληνική Βιβλιογραφία

Κατσής, Α., Σιδερίδης, Γ., & Εμβαλωτής, Α. (2010). *Στατιστικές μέθοδοι στις κοινωνικές επιστήμες*. Αθήνα: Εκδόσεις Τόπος.

ΠΑΡΑΡΤΗΜΑ: ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΡΕΥΝΑΣ

Το παρόν ερωτηματολόγιο δημιουργήθηκε στα πλαίσια της εκπόνησης της διπλωματικής μου εργασίας που αφορά τη συνεισφορά του εσωτερικού ελέγχου στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων. Γι' αυτό το σκοπό, το δείγμα μου αφορά αποκλειστικά εσωτερικούς ελεγκτές.

Οι απαντήσεις είναι εμπιστευτικές και θα διασφαλιστεί η ανωνυμία των ερωτηματολογίων. Τα αποτελέσματα της έρευνας θα χρησιμοποιηθούν αποκλειστικά για το συγκεκριμένο σκοπό της έρευνας.

Για οποιαδήποτε διευκρίνηση, επικοινωνήστε μαζί μου στο e-mail: mtf18023@uom.edu.gr

Σας ευχαριστώ εκ των προτέρων για το χρόνο σας.

Η μεταπτυχιακή φοιτήτρια του Πανεπιστημίου Μακεδονίας,

Αναστασία Γώγου

ΜΕΡΟΣ Α: Πληροφορίες σχετικά με την επιχείρηση και Άλλες πληροφορίες

1. Σε ποιον τομέα δραστηριοποιείται η επιχείρησή σας;
   - Τραπεζικό
   - Παροχής συμβουλευτικών και επαγγελματικών υπηρεσιών
   - Μεταποιητικό
   - Κατασκευαστικό
   - Δημόσιο
   - Λιανικού εμπορίου
   - Παροχής υπηρεσιών
   - Τεχνολογίας

2. Ποιος είναι, προσεγγιστικά, ο αριθμός των υπαλλήλων της επιχείρησής σας;
   - Κάτω από 10
   - 10-50
   - 50-250
   - Πάνω από 250

3. Ποιος είναι, προσεγγιστικά, ο ετήσιος κύκλος εργασιών της επιχείρησής σας;
   - κάτω από 2 εκατομμύρια
   - 2-10 εκατομμύρια
   - 10-50 εκατομμύρια
   - Πάνω από 50 εκατομμύρια

4. Προσεγγιστικά, τους τελευταίους 12 μήνες πόσες επιθέσεις ή διαρροές δεχτήκατε στα πληροφοριακά σας συστήματα;
   - 0
   - 1-5
   - 6-10
   - 11-15
   - 16-20
   - 21-25
   - πάνω από 25

5. Πόσα από τα παραπάνω περιστατικά ανιχνεύτηκαν και αντιμετωπίστηκαν πριν δημιουργήσουν λειτουργικά προβλήματα, οικονομική ζημία ή απώλεια φήμης;
   - 0
   - 1-5
   - 6-10

- 11-15
- 16-20
- 21-25
- πάνω από 25

6. Τα τελευταία 3 χρόνια, τα περιστατικά παραβιάσεων
   - μειώθηκαν σημαντικά
   - μειώθηκαν
   - παρέμειναν ίδια
   - αυξήθηκαν
   - αυξήθηκαν σημαντικά

ΜΕΡΟΣ Β: Εσωτερικός έλεγχος και ασφάλεια πληροφοριών

Σε ποιο βαθμό οι εσωτερικοί ελεγκτές:	Καθόλου	Λίγο	Αρκετά	Πολύ	Πάρα πολύ
7. συμβουλεύουν διάφορα τμήματα της επιχείρησης (όπως το τμήμα ΙΤ) για την αποτελεσματικότητα και την αποδοτικότητά τους;					
8. λειτουργούν σαν «παίκτες» μιας ομάδας και όχι σαν όργανα επιβολής κανόνων;					
9. ασχολούνται με την ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών;					
Σε ποιο βαθμό					
10. οι ειδικοί για την ασφάλεια πληροφοριών συνεργάζονται με τους εσωτερικούς ελεγκτές, ώστε να διασφαλίζουν ότι τα πληροφοριακά συστήματα είναι ασφαλή και αξιόπιστα;					
11. η τριβή μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών είναι περιορισμένη;					

12. η σχέση μεταξύ των ειδικών για την ασφάλεια πληροφοριών και των εσωτερικών ελεγκτών χαρακτηρίζεται ως προσωπική και στενή;					

ΜΕΡΟΣ Γ: Εσωτερικοί ελεγκτές και τεχνολογικές γνώσεις

Σε ποιο βαθμό:	Καθόλου	Λίγο	Αρκετά	Πολύ	Πάρα πολύ
13. οι εσωτερικοί ελεγκτές έχουν γνώσεις για την ασφάλεια των πληροφοριακών συστημάτων;					
14. οι εσωτερικοί ελεγκτές έχουν εξειδικευμένες τεχνολογικές γνώσεις για τα συστήματα που χρησιμοποιούν;					
15. υπάρχει εκπαίδευση των εσωτερικών ελεγκτών για την ασφάλεια των πληροφοριακών συστημάτων;					
16. οι εσωτερικοί ελεγκτές κατέχουν την πιστοποίηση CISA (Certified Information Systems Auditor);					

ΜΕΡΟΣ Δ: Πολιτικές- Πρότυπα

Σε ποιο βαθμό:	Καθόλου	Λίγο	Αρκετά	Πολύ	Πάρα πολύ

17. συμφωνείτε ότι υπάρχει καταγεγραμμένη Πολιτική Ασφαλείας Πληροφοριών;					
18. η επιχείρησή σας χρησιμοποιεί κάποιο από τα πρότυπα ISO (ISO 27001, 27005 κ.ά.);					
19. η επιχείρησή σας χρησιμοποιεί το πλαίσιο COBIT;					
20. η επιχείρησή σας χρησιμοποιεί τα πλαίσια NIST SP ή RFC2196:Site Security Handbook;					
21. οι εσωτερικοί ελεγκτές αξιολογούν τη συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας;					

ΜΕΡΟΣ Ε: Εκπαίδευση προσωπικού και προγράμματα ενημέρωσης για την ασφάλεια

Σε ποιο βαθμό:	Καθόλου	Λίγο	Αρκετά	Πολύ	Πάρα πολύ
22. η επιχείρησή σας έχει συγκεκριμένους οδηγούς-οδηγίες που τονίζουν τι επιτρέπεται να κάνουν οι υπάλληλοι χρησιμοποιώντας τους υπολογιστές τους;					
23. η επιχείρησή σας παρέχει εκπαίδευση, ώστε να βοηθήσει τους υπαλλήλους της να βελτιώσουν την ενημέρωσή τους για τους υπολογιστές και τα ζητήματα ασφάλειας πληροφοριών;					
24. το προσωπικό γνωρίζει την Πολιτική Ασφάλειας					

Πληροφοριών;					
25. οι εσωτερικοί ελεγκτές διασφαλίζουν ότι τα προγράμματα ενημέρωσης του προσωπικού για την ασφάλεια είναι υποχρεωτικά και ωφέλιμα;					