ISSUE

ΜΕ ΤΗ ΣΥΝΕΡΓΑΣΙΑ & ΤΗ ΧΟΡΗΓΙΑ ΤΗΣ

EMC²

Έρευνα για την Ασφάλεια Πληροφοριών 2013

Το IT Security Professional σε συνεργασία με την EMC Hellas πραγματοποίησαν έρευνα στις Ελληνικές επιχειρήσεις με βασικούς πυλώνες τις επενδύσεις για την ασφάλεια πληροφοριών, τις στρατηγικές που εφαρμόζονται για την προστασία των δεδομένων και τις πολιτικές που υιοθετούνται σχετικά με τις νέες τάσεις στο IT, υπό το πρίσμα των υπευθύνων των IT υποδομών.

Έχουν περάσει σχεδόν 2,5 χρόνια από τότε που πραγματοποιήσαμε την πρώτη μας έρευνα για την Ασφάλεια των Πληροφοριών στις Ελληνικές Επιχειρήσεις. Σε αυτά τα 2,5 χρόνια είναι αλήθεια ότι έχουν αλλάξει αρκετά πράγματα μέσα στο οικοσύστημα του IT των επιχειρήσεων. Η αποθήκευση και διαχείρι-

ση των πληροφοριών ηλεκτρονικά, εξελίσσεται και λαμβάνει διάφορες μορφές. Ο όγκος των δεδομένων αυξάνεται συνεχώς. Ταυτόχρονα αυξάνονται ποιοτικά και ποσοτικά οι κίνδυνοι και οι τρωτότητες, ενώ οι νέες τάσεις στο IT επιβάλλουν την επαναδιαμόρφωση των στρατηγικών και την υιοθέτηση νέων τεχνολογιών για την προστασία των πληροφοριών. Σε αυτό το περιβάλλον όμως, δεν πρέπει να παραβλέπουμε το γεγονός ότι οι οικονομικές συνθήκες έχουν δυσκολέψει αρκετά, με αποτέλεσμα να υπάρχει ένας γενικότερος περιορισμός στις επενδύσεις για οτιδήποτε αφορά στις υποδομές του IT.

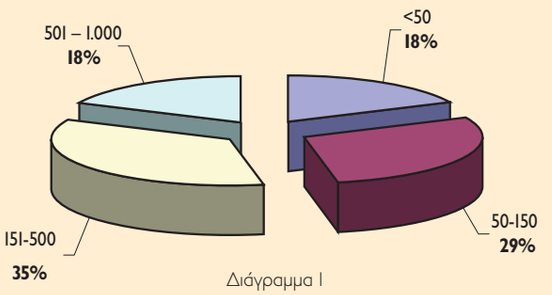
Σε αυτά τα πλαίσια πραγματοποιήσαμε με την πολύτιμη συνεργασία και χορηγία της **EMC Hellas** μια νέα έρευνα για την Ασφάλεια Πληροφοριών, από την οποία προέκυψαν ιδιαίτερα ενδιαφέροντα ευρήματα.

Ως μια πρώτη αποτίμηση και έχοντας γνώση έρευνες που έχουν πραγματοποιηθεί παγκοσμίως με παρόμοια ερωτήματα, είναι αξιοσημείωτο ότι τα αποτελέσματα της δικής μας έρευνας δεν απέχουν πολύ με αυτά των αντίστοιχων ερευνών που διενεργούνται εκτός Ελλάδας. Το στοιχείο αυτό δείχνει ότι παρόλο το γεγονός ότι η οικονομική κρίση έχει οδηγήσει στον περιορισμό των budget, τα ζητήματα που αφορούν στην ασφάλεια πληροφοριών γενικότερα, αντιμετωπίζονται πλέον στην Ελλάδα με μεγαλύτερη προσοχή και ωριμότητα. Αν θέλαμε να ξεχωρίσουμε κάποια από τα ευρήματα της έρευνας, θα μπορούσαμε να επισημάνουμε το γεγονός ότι έχει αυξηθεί η πίστη για την αποτελεσματικότητα των μέτρων που λαμβάνουν οι επιχειρήσεις για την ασφάλεια των πληροφοριών, μιας και η πλειοψηφία του δείγματος δήλωσαν αρκετά σίγουροι για αυτά. Επίσης οι εφαρμογές Backup/

Ταυτότητα της έρευνας

Η έρευνα πραγματοποιήθηκε κατά τους μήνες Απρίλιο - Μάιο και ως δείγμα επιλέχθηκαν **200 Ελληνικές επιχειρήσεις** από ένα μεγάλο φάσμα δραστηριοτήτων και κλίμακας. Συγκεκριμένα, όπως διακρίνουμε και από το **διάγραμμα 1**, το 18 % των επιχειρήσεων που έλαβαν μέρος στην έρευνα απασχολούν μεταξύ 501 και 1000 εργαζόμενους, ενώ υπάρχουν και πολλές εταιρείες (35%) με 151 έως 500 εργαζόμενους. Το υπόλοιπο 47 % του δείγματος περιλαμβάνει επιχειρήσεις με κάτω από 150 εργαζόμενους.

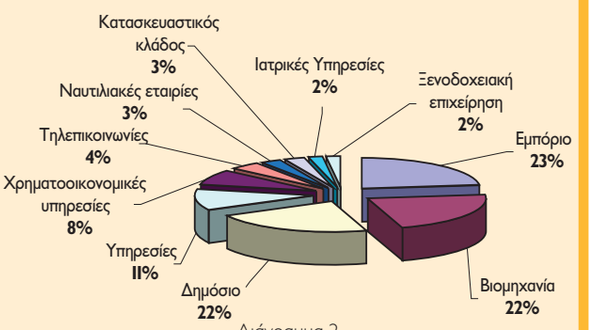
Αριθμός εργαζομένων



Διάγραμμα 1

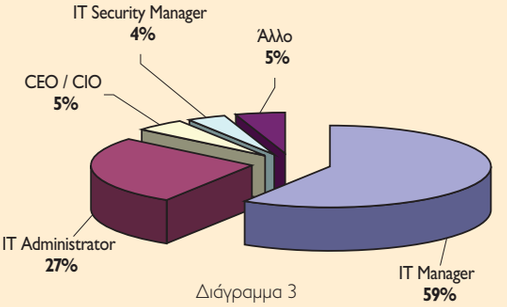
Αναφορικά με τη δραστηριότητα των επιχειρήσεων που έλαβαν μέρος - και όπως απεικονίζονται στο **διάγραμμα 2** - το 23 % θεωρούνται εμπορικές επιχειρήσεις, ενώ το 22 % ανήκουν στην ευρύτερη κατηγορία των βιομηχανιών παραγωγής προϊόντων. Επίσης επιλέχθηκε και απάντησε στην έρευνα ένα σημαντικό ποσοστό (22%) από Οργανισμούς και φορείς του δημοσίου και ένα 11 % που ανήκει γενικότερα στο κλάδο των επιχειρήσεων παροχής υπηρεσιών κάθε είδους. Όπως διακρίνουμε στο **διάγραμμα 3**, το 59 % των προσώπων που απάντησαν στο ερωτηματολόγιο της έρευνας κατέχει τον τίτλο του IT Manager και το 27 % τον τίτλο του IT Administrator.

Δραστηριότητα επιχείρησης



Διάγραμμα 2

Θέση υπευθύνου



Διάγραμμα 3

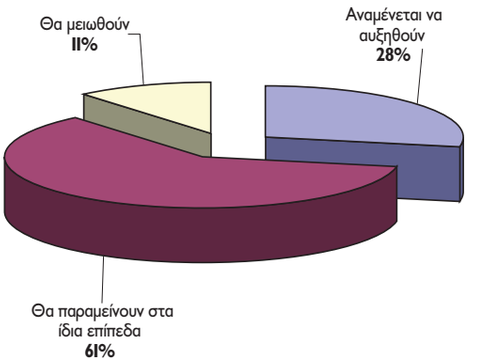
Διάγραμμα 1, 2, 3

Business Continuity αποτελούν προτεραιότητα για τις επιχειρήσεις, με την πολύ μεγάλη πλειοψηφία αυτών να δηλώνει ότι τις εντάσσει στη στρατηγική ασφάλειας. Επίσης, όπως προκύπτει από την έρευνα, η απροσεξία ή απειρία των εργαζομένων αύξησαν κατά κύριο λόγο την έκθεση σε κινδύνους για την ασφάλεια πληροφοριών τους τελευταίους 12 μήνες. Ακόμα ενδιαφέρον παρουσιάζει το γεγονός ότι σχεδόν τα 2/3 των ερωτηθέντων δήλωσαν ότι στις επιχειρήσεις τους εφαρμόζεται περιορισμένη ή καθόλου πρόσβαση σε ιστοσελίδες κοινωνικής δικτύωσης.

Επενδύσεις σχετικά με την Ασφάλεια Πληροφοριών

Στα ενδότερα της έρευνας και επιχειρώντας να αξιολογήσουμε το πώς οι Ελληνικές επιχειρήσεις λειτουργούν σε σχέση με τις επενδύσεις που σχετίζονται με την Ασφάλεια Πληροφοριών σήμερα, διαπιστώσαμε ότι σε σχετική ερώτηση το 61 % του συνόλου απάντησε ότι οι **επενδύσεις για την ασφάλεια πληροφοριών** θα παραμείνουν στα ίδια επίπεδα σε σχέση με τον προηγούμενο χρόνο, κάτι που ακούγεται φυσιολογικό, λαμβάνοντας υπόψη το ευρύτερο οικονομικό περιβάλλον. Επίσης, όπως διακρίνουμε και στο **διάγραμμα 4**, υπάρχει ένα 28 % των επιχειρήσεων που δηλώνουν ότι θα αυξήσουν τις επενδύσεις για το συγκεκριμένο τομέα, κάτι που κρίνεται αρκετά ενθαρρυντικό σε μια περίοδο όπως αυτή που διανύουμε.

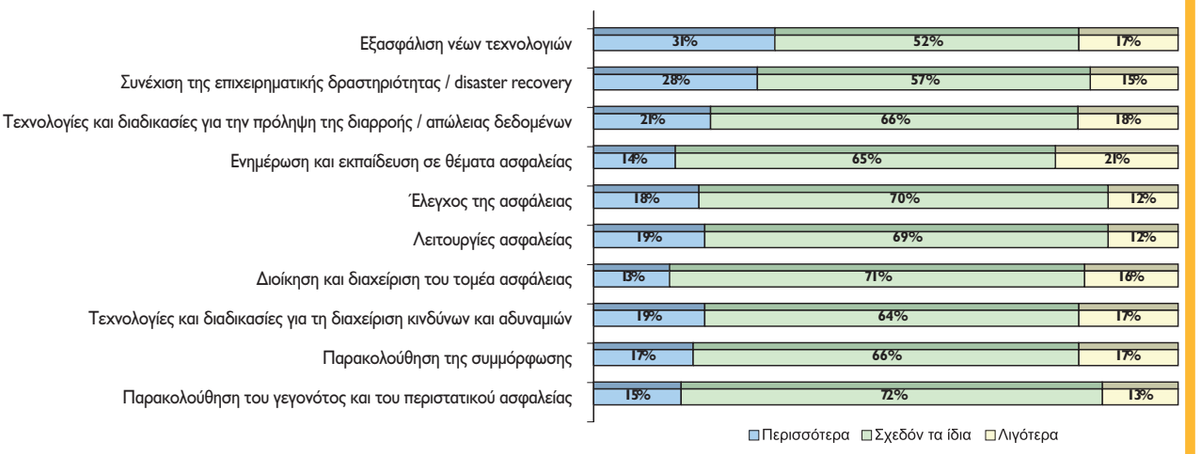
Πως αναμένετε να κυμανθούν τον επόμενο χρόνο οι επενδύσεις για την ασφάλεια πληροφοριών στην επιχείρησή σας σε σχέση με τον προηγούμενο χρόνο;



Διάγραμμα 4

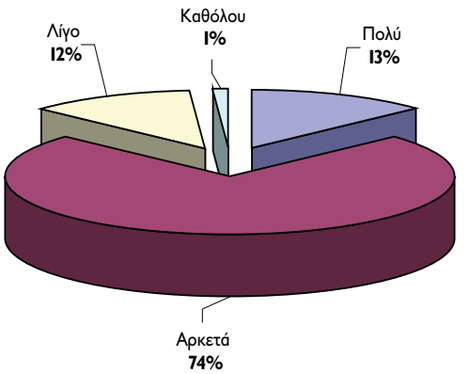
Στη συνέχεια επιχειρήσαμε να αναλύσουμε περισσότερο τον τρόπο της κατανομής των χρημάτων που σκοπεύουν να δαπανήσουν οι επιχειρήσεις τη χρονιά που διανύουμε, στους διάφορους τομείς που σχετίζονται με την ασφάλεια πληροφοριών - με την ευρύτερη έννοια. Από τα αποτελέσματα σχετικής ερώτησης, όπως αυτά απεικονίζονται στο **διάγραμμα 5**, συμπεραίνουμε ότι στους περισσότερους τομείς

Συγκριτικά με το προηγούμενο έτος, η εταιρία σας σκοπεύει να δαπανήσει περισσότερα χρήματα, σχεδόν τα ίδια η λιγότερα μέσα στο 2013 για τις ακόλουθες δραστηριότητες;



Διάγραμμα 5

Πόσο σίγουροι είστε οτι οι ενέργειες για την ασφάλεια των πληροφοριών είναι αποτελεσματικές;



Διάγραμμα 6

τα χρήματα που θα δαπανηθούν θα είναι σχεδόν τα ίδια, κάτι που είναι φυσιολογικό, λαμβάνοντας υπόψη και το αποτέλεσμα του προηγούμενου ερωτήματος. Παρόλα αυτά, υπάρχουν επιχειρήσεις σε ποσοστό 31% που δηλώνουν ότι **θα δαπανήσουν περισσότερα χρήματα** για την εξασφάλιση νέων τεχνολογιών και ακολουθεί με μικρή διαφορά η συνέχιση της επιχειρηματικής δραστηριότητας (28%), ενώ ένα 21 % του δείγματος δήλωσαν ότι θα αυξήσουν τις δαπάνες για τεχνολογίες σχετικά με το DLP.

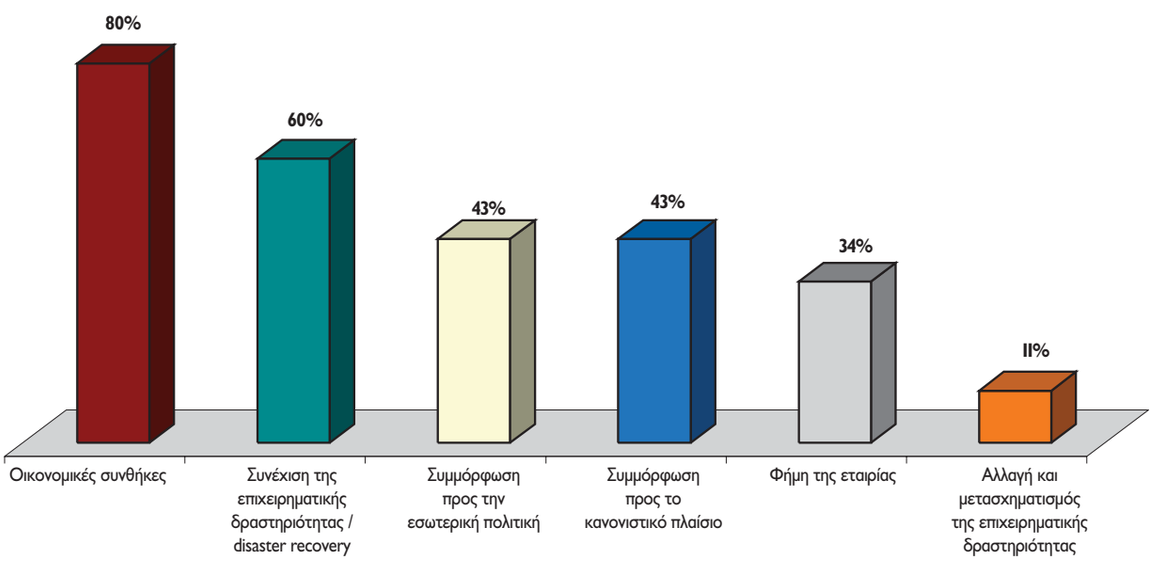
Αναζητώντας στη συνέχεια το βαθμό εμπιστοσύνης στην **αποτελεσματικότητα των ενεργειών που υιοθετούν οι επιχειρήσεις σε σχέση με την ασφάλεια των πληροφοριών** διαπιστώσαμε σύμφωνα και με τα όσα απεικονίζονται στο **διάγραμμα 6** ότι το 74% δηλώνουν αρκετά σίγουρες για την αποτελεσματικότητα αυτών των ενεργειών, ένα 13% δηλώνουν πολύ σίγουρες, ενώ συνολικά μόλις το 13% δηλώνουν λίγο ή καθόλου σίγουρες, κάτι που μπορεί να δείχνει αρκετά θετικό αν βασίζεται σε πραγματικά γεγονότα, αλλά παράλληλα ίσως εμπεριέχει και το στοιχείο ενός επικίνδυνου εφησυχασμού.

Αναφορικά με το ποιοι είναι οι **παράγοντες που επηρεάζουν τις δαπάνες** για την ασφάλεια πληροφοριών, κρίνεται φυσιολογικό ότι το 80% των επιχειρήσεων απάντησαν ότι είναι οι οικονομικές συνθήκες, ενώ καταγράφεται και ένα 60% να δηλώνουν ότι σε αυτούς τους παράγοντες είναι η διασφάλιση της συνέχισης της επιχειρηματικής δραστηριότητας και ένα 43% η συμμόρφωση προς την εσωτερική πολιτική και το κανονιστικό πλαίσιο (**διάγραμμα 7**).

Αξιολόγηση της Στρατηγικής Ασφάλειας και των Απειλών

Με στόχο να αξιολογήσουμε τις προτεραιότητες σε σχέση με τη στρατηγική ασφάλειας που υιοθετεί η κάθε επιχείρηση, θέσαμε στη διάθεση των ερωτηθέντων ορισμένες βασικές επιλογές λειτουργιών, που μπορούν να ενσωματωθούν στη

Ποιά είναι τα επιχειρηματικά ζητήματα ή οι παράγοντες που επηρεάζουν τις δαπάνες της εταιρίας σας για την ασφάλεια των πληροφοριών;

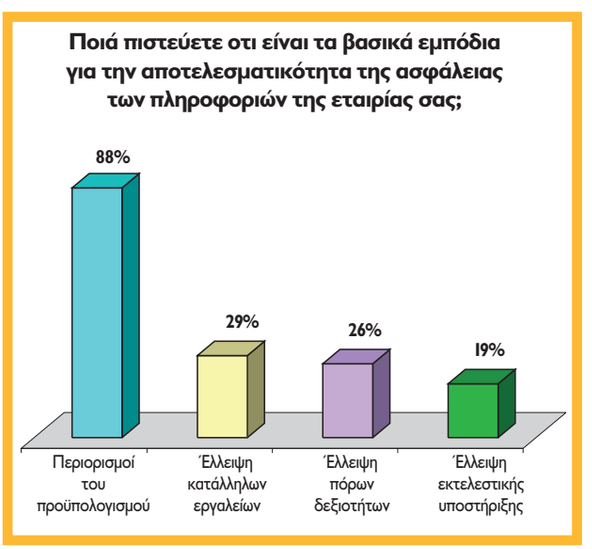


Διάγραμμα 7

Διάγραμμα 8

βασική αυτή στρατηγική. Όπως λοιπόν φαίνεται και από το **διάγραμμα 8**, στην κορυφή των **λειτουργιών που εντάσσονται στη στρατηγική ασφάλειας**, με ποσοστό 96% βρίσκεται το Backup & Business Continuity και ακολουθούν με ιδιαίτερα υψηλά ποσοστά ο έλεγχος χρηστών κατά την πρόσβαση (83%) και η ασφάλεια των εφαρμογών (82%).

Επιχειρώντας στη συνέχεια να αναδείξουμε τα **βασικά εμπόδια για την αποτελεσματικότητα της ασφάλειας των πληροφοριών** θέσαμε σχετική ερώτηση και τα αποτελέσματα που λάβαμε καταδεικνύουν σε ποσοστό 88% ότι οι περιορισμοί του προϋπολογισμού αποτελούν το μεγαλύτερο - με διαφορά - ανασταλτικό παράγοντα, όπως βλέπουμε και στο **διάγραμμα 9**.

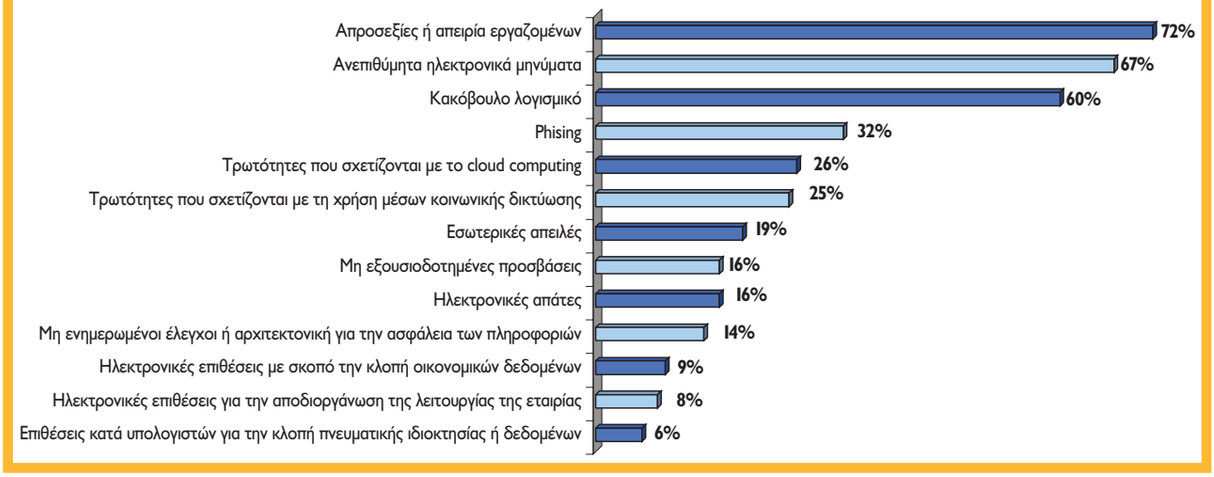


Διάγραμμα 9

Αναφορικά τώρα με τα ευρήματα της έκθεσης για τις **απειλές και τις τρωτότητες** που αντιμετώπισαν οι επιχειρήσεις τους τελευταίους 12 μήνες, διακρίνουμε στο **διάγραμμα 10** ότι το μεγαλύτερο ποσοστό του δείγματος (72%) απάντησαν ότι ήταν η απροσεξία και η απειρία των εργαζομένων. Μεγάλο ποσοστό (67%) στο ίδιο ερώτημα καταλαμβάνει και η απειλή των ανεπιθύμητων ηλεκτρονικών μηνυμάτων, ενώ ακολουθεί με 60% το κακόβουλο λογισμικό.

Με στόχο στη συνέχεια να διερευνήσουμε τους τρόπους που επιλέγουν οι εταιρίες να αξιολογήσουν την **αποτελεσματικότητα και την αποδοτικότητα της ασφάλειας πληροφοριών** απευθύναμε στους ερωτηθέντες σχετικό ερώτημα, από το οποίο προκύπτει ότι κάθε επιχείρηση επιλέγει αρκετούς τρόπους για να το πετύχει αυτό. Συγκεκριμένα, η πλειοψηφία αυτών (76%) μας απάντησαν ότι επιλέγουν διαδικασίες εσωτερικού ελέγχου, ενώ όπως διακρίνουμε και στο **διάγραμμα 11**, για το ίδιο ερώτημα, πάνω από τις μισές εταιρείες (56%) μας απάντησαν ότι εφαρμόζουν εσωτερικές αυτοαξιολογήσεις με διαδικασίες

Ποιές απειλές και τρωτότητες αύξησαν κατά κύριο λόγο την έκθεση σε κινδύνους για την ασφάλεια πληροφοριών κατά τους τελευταίους 12 μήνες;



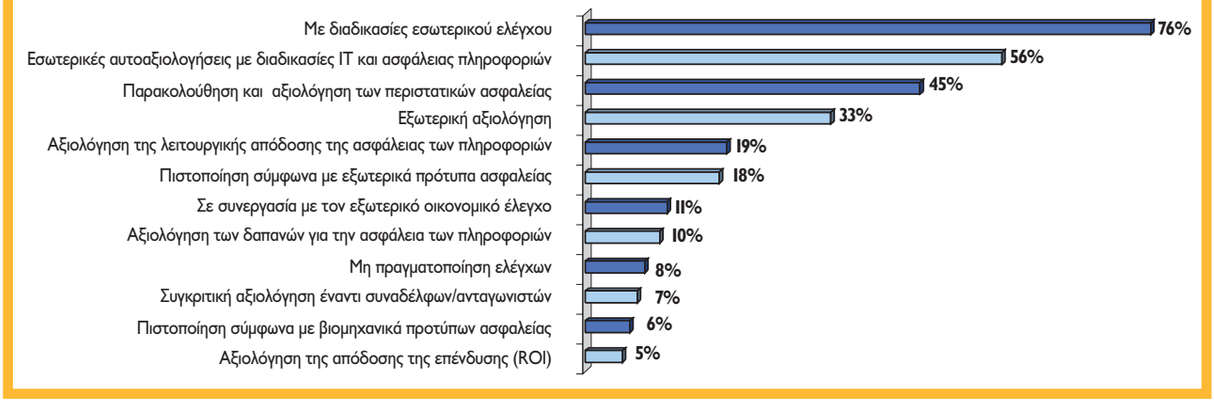
Διάγραμμα 10

IT και ασφάλειας πληροφοριών, ενώ ένα 45% υποστηρίζουν ότι η αξιολόγηση γίνεται μέσα από την παρακολούθηση των περιστατικών ασφαλείας και ένα 33% με εσωτερική αξιολόγηση.

Στη συνέχεια επιλέξαμε να διαγνώσουμε ποιους **παράγοντες αξιολογούν οι επιχειρήσεις ως οικονομικές απώλειες έπειτα από μια παραβίαση ασφάλειας**. Και εδώ, όπως βλέπουμε στο **διάγραμμα 12** οι απαντήσεις είναι παραπάνω από μία, με το 56% του δείγματος να θεωρεί τη ζημιά στην εμπορική επωνυμία και φήμη ως βασικό παράγοντα οικονομικών απωλειών και να ακολουθεί με ποσοστό 40% η απώλεια των πελατών.

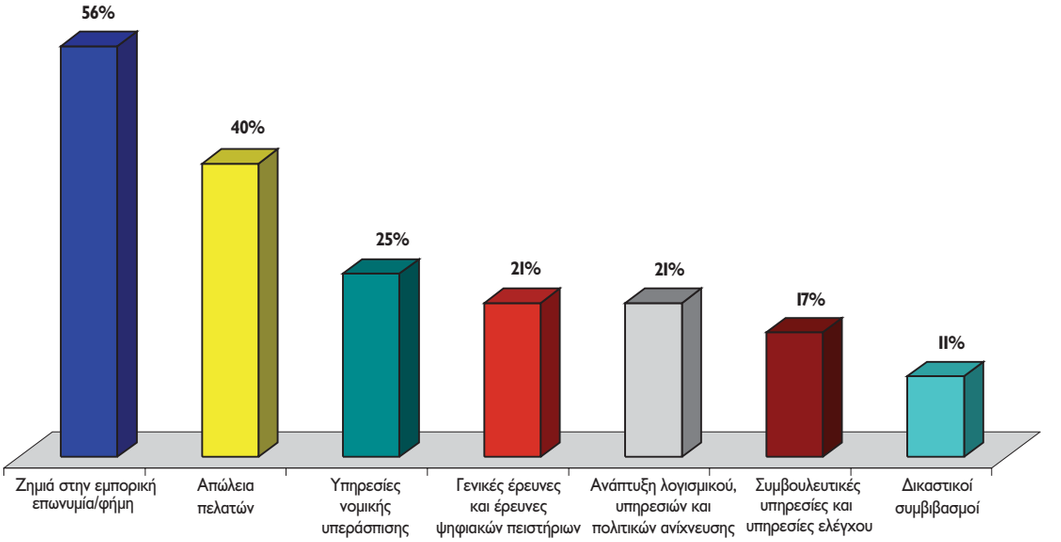
Η διαρροή των ευαίσθητων πληροφοριών αποτελεί θεμελιώδες ζήτημα στην αξιολόγηση μιας στρατηγικής ασφάλειας και για να επιτευχθεί απαιτούνται ορισμένες ενέργειες. Σε σχετική ερώτηση της έρευνας προκειμένου να αναδείξουμε **ποιες από αυτές τις ενέργειες λαμβάνουν οι ελληνικές επιχειρήσεις**, συμπεραίνουμε ότι με μικρές σχετικά διαφορές, οι περισσότερες από αυτές υιοθετούν κυρίως τέσσερις ενέργειες - και συγκεκριμένα, τους εσωτερικούς έλεγχους (61%), την κλειδωμένη/περιορισμένη χρήση hardware (59%), τη χρήση πρόσθετων μηχανισμών ασφαλείας για την προστασία των πληροφοριών (55%) και τον καθορισμό ειδικής πολιτικής αναφορικά με την αξιολόγηση και τη διαχείριση των ευαίσθητων πληροφοριών (55%). Σε αυτό το ερώτημα υπάρχουν και άλλες απαντήσεις που επέλεξαν αρ-

Με ποιό τρόπο η εταιρία σας αξιολογεί την αποτελεσματικότητα και την αποδοτικότητα της ασφάλειας των πληροφοριών;



Διάγραμμα 11

Ποιοί παράγοντες λαμβάνονται υπόψη ως οικονομικές απώλειες έπειτα από παραβιάσεις ασφάλειας;



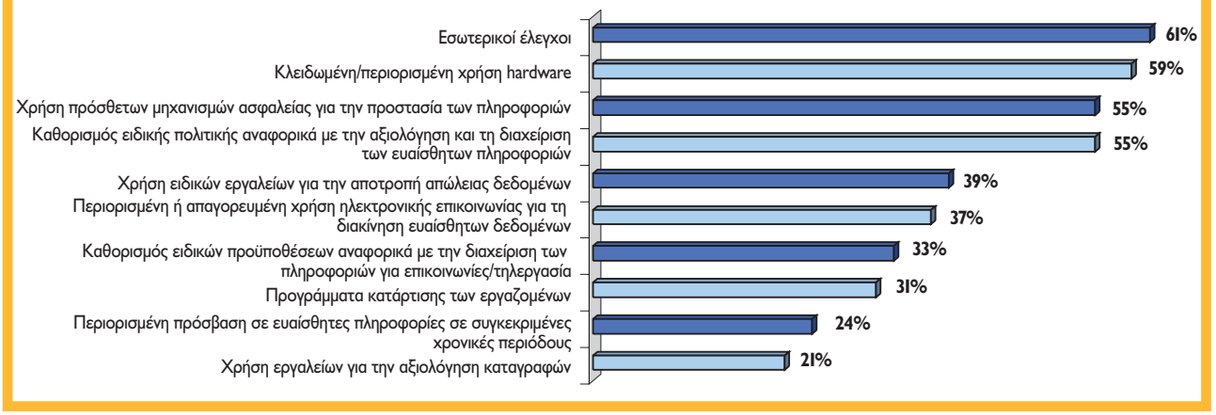
Διάγραμμα 12

κετές επιχειρήσεις, όπως βλέπουμε και στο σχετικό **διάγραμμα 13**.

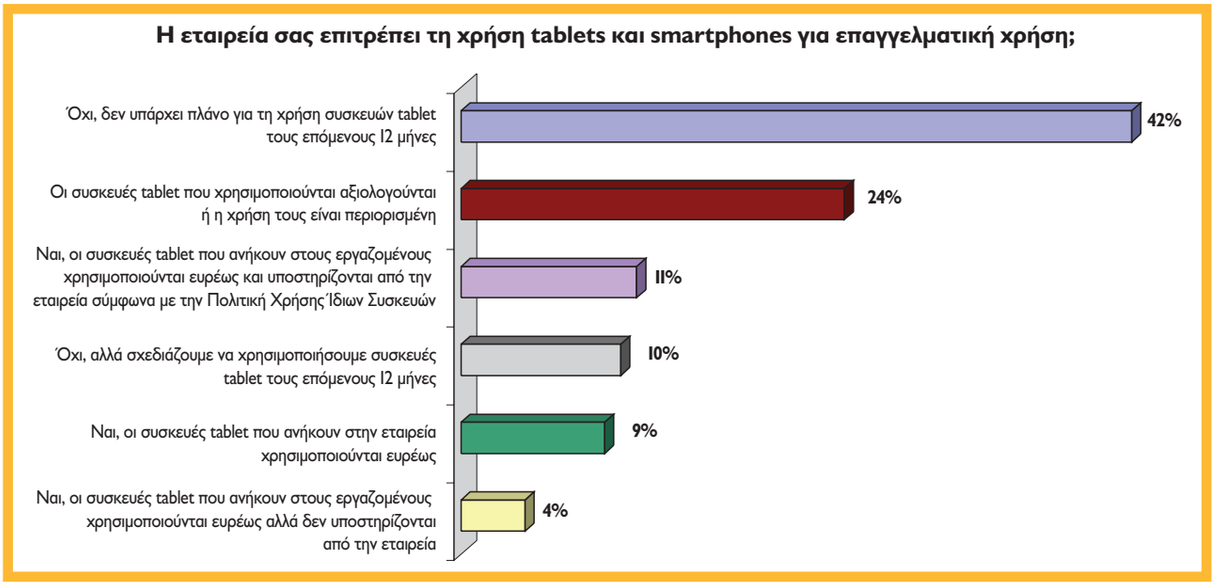
Διαχείριση Ρίσκων με βάση τις νέες τάσεις στο IT

Το mobility, το BYOD, το cloud και τα social media συνθέτουν ένα νέο τοπίο στο IT, που ουδείς μπορεί να αγνοήσει. Η μερική ή πλήρης υιοθέτηση των παραπάνω τάσεων έχει δημιουργήσει την ανάγκη για επανεξέταση ορισμένων πολιτικών που σχετίζονται με την προστασία των κρίσιμων επιχειρηματικών δεδομένων και για αυτό παρουσιάζουν ιδιαίτερο ενδιαφέρον τα σχετικά ευρήματα της έρευνας. Ξεκινώντας με ερώτημα που αφορά **στη χρήση των tablets και smartphones για επαγγελματική χρήση**, ένα σημαντικό μέρος του δείγματος, δηλαδή το 42%, μας δήλωσαν ότι δεν υπάρχει κανένα πλάνο για τη χρήση των συσκευών αυτών για τους επόμενους

Ποιές από τις παρακάτω ενέργειες έχει λάβει η εταιρία σας προκειμένου να ελέγξει τις διαρροές ευαίσθητων πληροφοριών;



Διάγραμμα 13

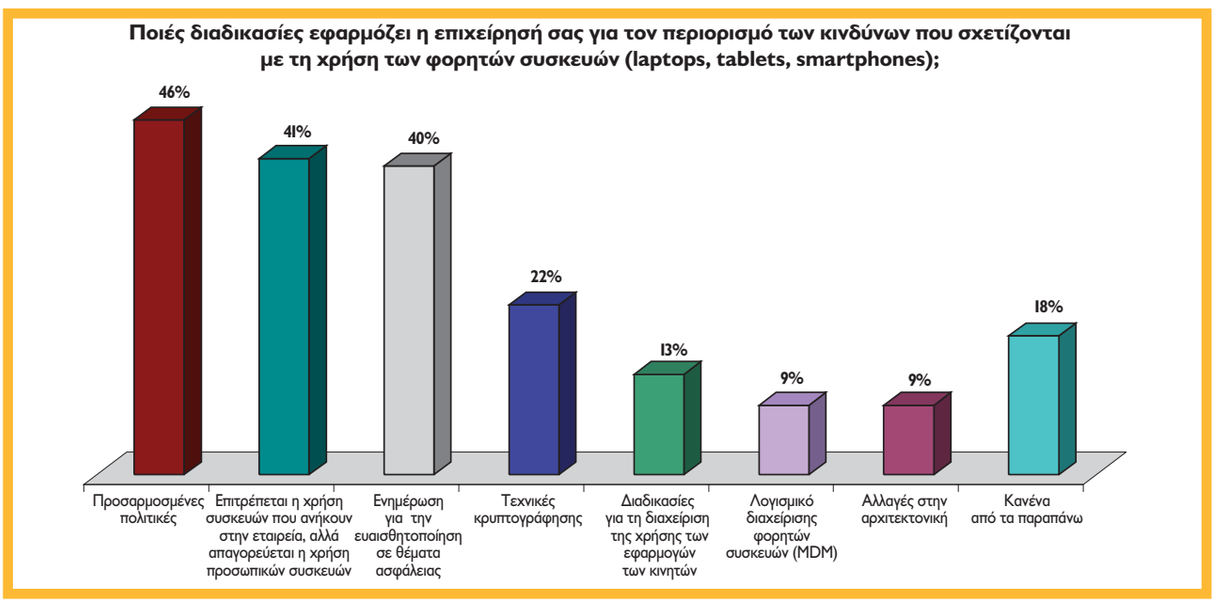


Διάγραμμα 14

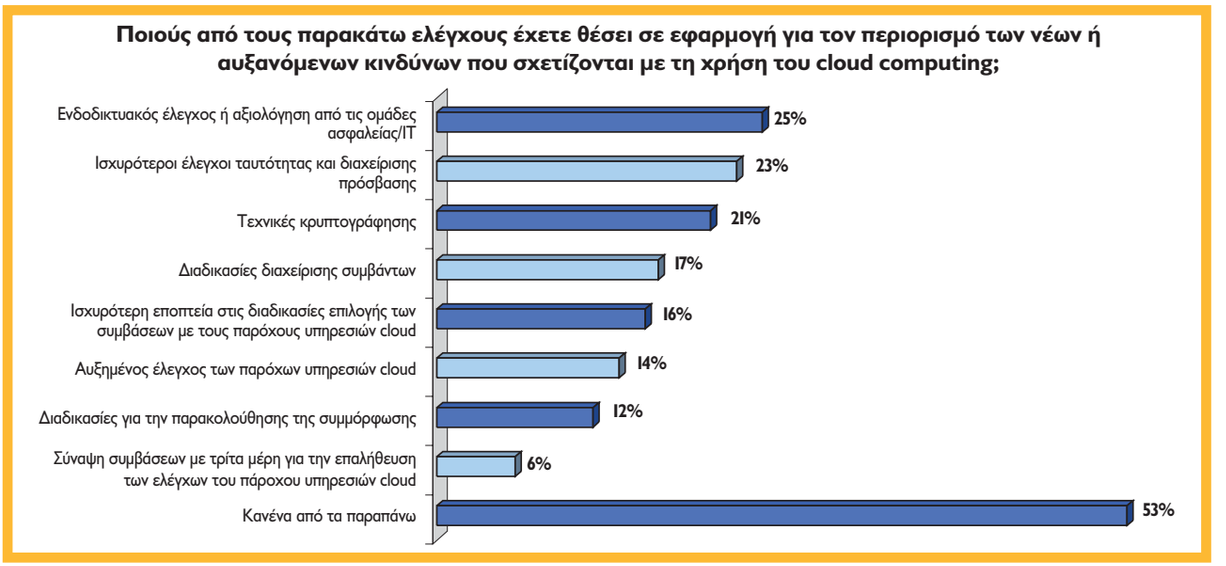
12 μήνες, ενώ το 24% δήλωσαν ότι οι συσκευές tablet που χρησιμοποιούνται, αξιολογούνται και η χρήση τους είναι περιορισμένη (**διάγραμμα 14)**.

Αναφορικά με τις διαδικασίες που εφαρμόζει η κάθε επιχείρηση για τον **περιορισμό των κινδύνων που σχετίζονται με τη χρήση φορητών συσκευών** συμπεραίνουμε ότι υπάρχει μια ποικιλία διαδικασιών που εφαρμόζονται, με τις πιο δημοφιλείς να είναι οι προσαρμοσμένες πολιτικές που επέλεξε το 46% του δείγματος, καθώς και η δυνατότητα χρήσης συσκευών που ανήκουν στην εταιρεία, αλλά όχι αυτών που είναι προσωπικές, όπως μας απάντησε το 41%. Επίσης, όπως βλέπουμε και στο **διάγραμμα 15** υπάρχει ένα 40% των ερωτηθέντων που δήλωσαν ότι στην επιχείρησή τους πραγματοποιείται ενημέρωση για την ευαισθητοποίηση σε σχετικά θέματα ασφάλειας που αφορούν στις φορητές συσκευές.

Μοιρασμένες ήταν οι απαντήσεις που λάβαμε σχετικά με τους ελέγχους που θέτουν σε εφαρμογή οι επιχειρήσεις για τον **περιορισμό νέων ή αυξανόμενων κινδύνων που σχετίζονται με τη χρήση του cloud**. Συγκεκριμένα, το 25% επιλέγουν τον ενδοδικτυακό έλεγχο ή την αξιολόγηση από ομάδες ασφαλείας/IT και το 23 % επιλέγουν ισχυρότερους ελέγχους ταυτότητας και διαχείρισης πρόσβασης, ενώ



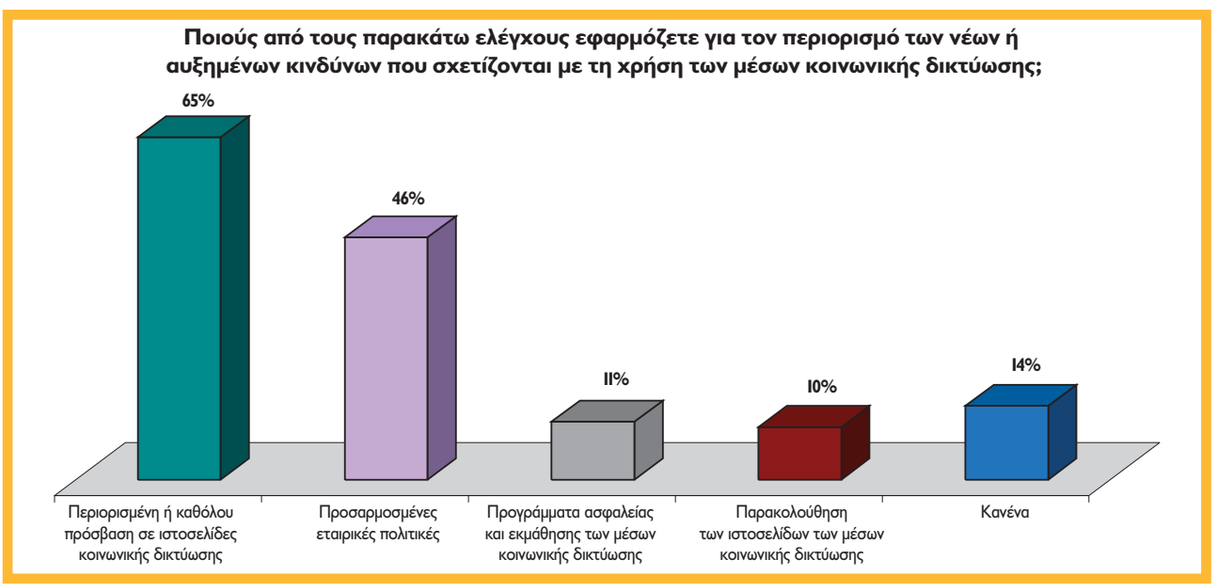
Διάγραμμα 15



Διάγραμμα 16

21% τεχνικές κρυπτογράφησης. Όπως διακρίνουμε και στο **διάγραμμα 16**, υπάρχει ένα μεγάλο ποσοστό (53 %) που δηλώνουν ότι στην επιχείρησή τους δεν εφαρμόζεται κανένας από τους διαθέσιμους ελέγχους και αυτό ίσως οφείλεται σε μεγάλο ποσοστό στο γεγονός ότι ίσως δεν έχουν ενσωματώσει στην επιχείρησή τους υποδομές cloud.

Κλείνοντας την έρευνά μας, επιλέξαμε να αξιολογήσουμε τις πολιτικές των επιχειρήσεων για την **αντιμετώπιση των κινδύνων που ίσως προκύπτουν από τη χρήση μέσων κοινωνικής δικτύωσης** μέσα στο χώρο εργασίας. Στη σχετική ερώτηση, ένα μεγάλο ποσοστό (65%) δήλωσαν ότι εφαρμόζεται περιορισμένη ή καθόλου πρόσβαση σε αντίστοιχες ιστοσελίδες από το χώρο εργασίας και ένα 46% δήλωσαν ότι εφαρμόζονται προσαρμοσμένες πολιτικές, όπως διακρίνουμε στο **διάγραμμα 17**. iTSecurity



Διάγραμμα 17