ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ ΣΕ ΣΧΕΣΗ ΜΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ & ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΕΤΟΙΜΑΣΤΗΚΕ ΓΙΑ ΤΗΝ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΝΕΟΜΒΡΙΟΣ 2022

RAI Consultants Ltd

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

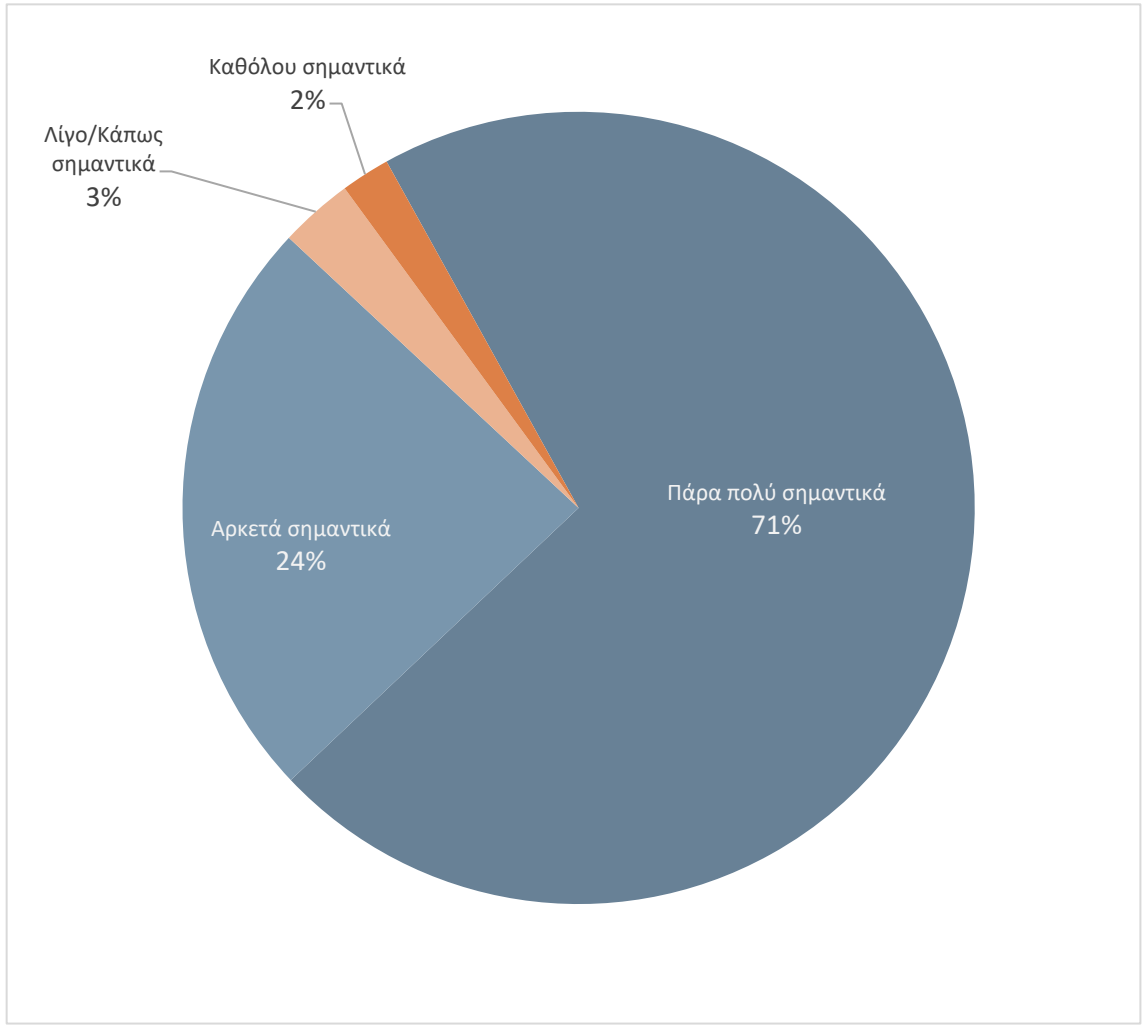
Εισαγωγή & Μεθοδολογία

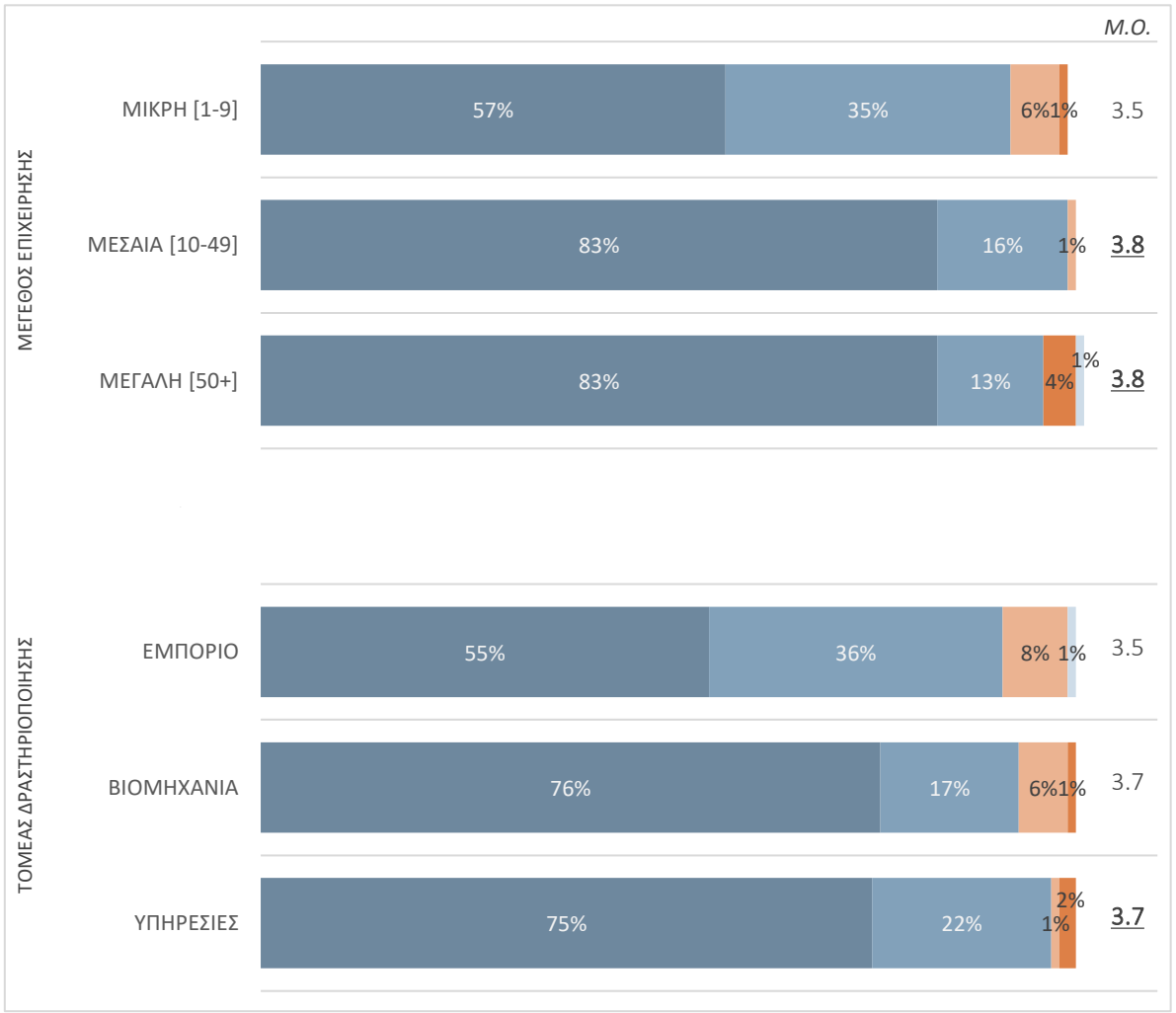
Αντικείμενο Μελέτης	Αντικείμενο της Σύμβασης αποτελεί η Παροχή Υπηρεσιών διεξαγωγής έρευνας σε επιχειρήσεις, σε σχέση με τον τρόπο χειρισμού θεμάτων κυβερνοασφάλειας, αποτίμησης της σημαντικότητας που αποδίδεται στα θέματα κυβερνοασφάλειας, τον τρόπο αντιμετώπισης περιστατικών κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας, στις συνέπειες από περιστατικά κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας κτλ.	
Κάλυψη	Η έρευνα ήταν Παγκύπρια και αφορούσε τους τομείς οικονομικής δραστηριότητα όπως αυτοί καθορίζονται από την Στατιστική Υπηρεσία:	Εμπορίου (NACE κατηγορία G) Βιομηχανίας | Μεταποίησης (NACE κατηγορίες B,C, D, E, F) Υπηρεσιών (NACE κατηγορίες H, I, J, K, L, M, N, P, Q, R)
Μέγεθος Δείγματος	Για τους σκοπούς της παρούσας μελέτης έγιναν συνολικά 450 επιτυχείς συνεντεύξεις εκ των οποίων:	207 επιχειρήσεις είχαν συνολικό αριθμό απασχολουμένων μέχρι 9 άτομα (Μικρή) 132 επιχειρήσεις είχαν συνολικό αριθμό απασχολουμένων 10-49 άτομα (Μεσαία) 111 επιχειρήσεις είχαν συνολικό αριθμό απασχολουμένων από 50 άτομα και άνω (Μεγάλη)
Μέθοδος δειγματοληψίας	Η επιλογή του δείγματος έγινε με τη μέθοδο της τυχαίας πολυσταδιακής στρωματοποιημένης δειγματοληψίας και αντικατοπτρίζει την αριθμητική και γεωγραφική διασπορά των υπό μελέτη επιχειρήσεων.	
Ερωτηματολόγιο & Συλλογή στοιχείων	Δομημένο ερωτηματολόγιο, το οποίο ετοίμασαν στη βασική του μορφή οι υπεύθυνοι της ΑΨΑ Τηλεφωνικές συνεντεύξεις από το τηλεφωνικό κέντρο της RAI Consultants Ηλεκτρονικά από τους ίδιους τους συμμετέχοντες, μέσω email, που περιλάμβανε τον σύνδεσμο (link) για την συμπλήρωση της έρευνας	
Ημερομηνίες διεξαγωγής	29 Σεπτεμβρίου – 3 Νοεμβρίου 2022	

ΑΝΑΛΥΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Πόσο σημαντικά είναι για την εταιρία/ επιχείρηση σας τα θέματα διαχείρισης ασφάλειας και κινδύνων στον κυβερνοχώρο;

Βάση: Όλοι οι ερωτώμενοι



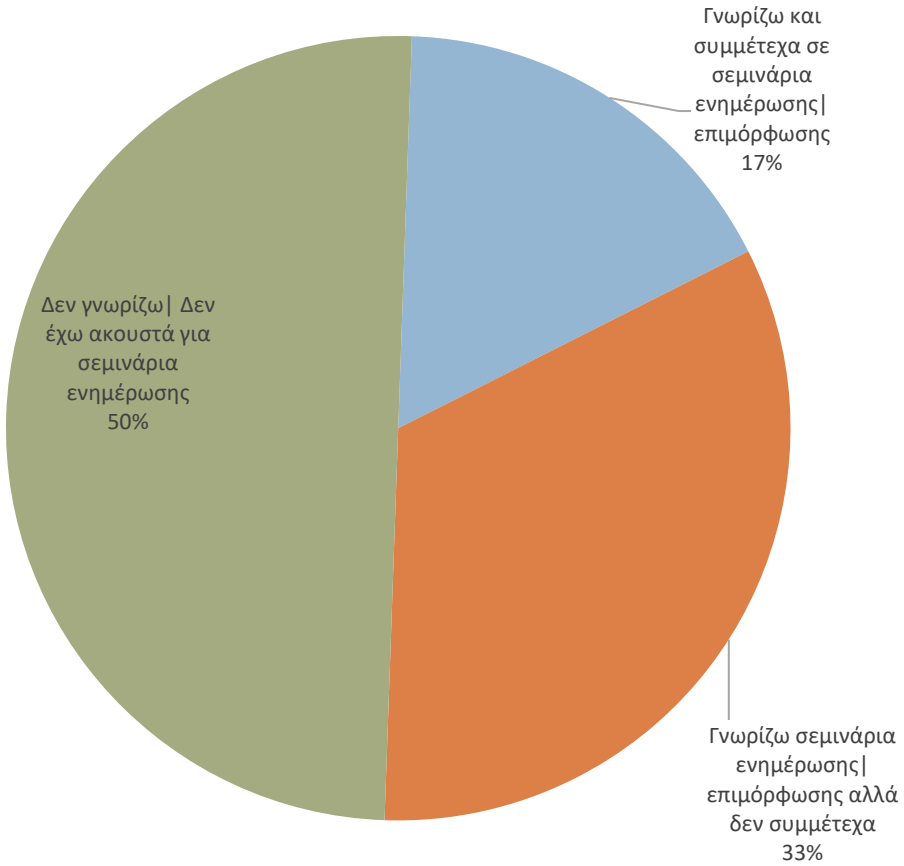


Πόσο συχνά προβαίνει η εταιρία σας σε εφαρμογή ή ενημέρωση ΤΕΧΝΙΚΩΝ | ΔΙΟΙΚΗΤΙΚΩΝ μέτρων κυβερνοασφάλειας;

Βάση: Όλοι οι ερωτώμενοι

Υπάρχουν διάφορα σεμινάρια ενημέρωσης και εκπαίδευσης/καθοδήγησης για την ασφάλεια στο διαδίκτυο. Ποια σεμινάρια γνωρίζετε ή έχετε ακουστά; | Σε ποια, αν κάποια, έχετε συμμετάσχει;

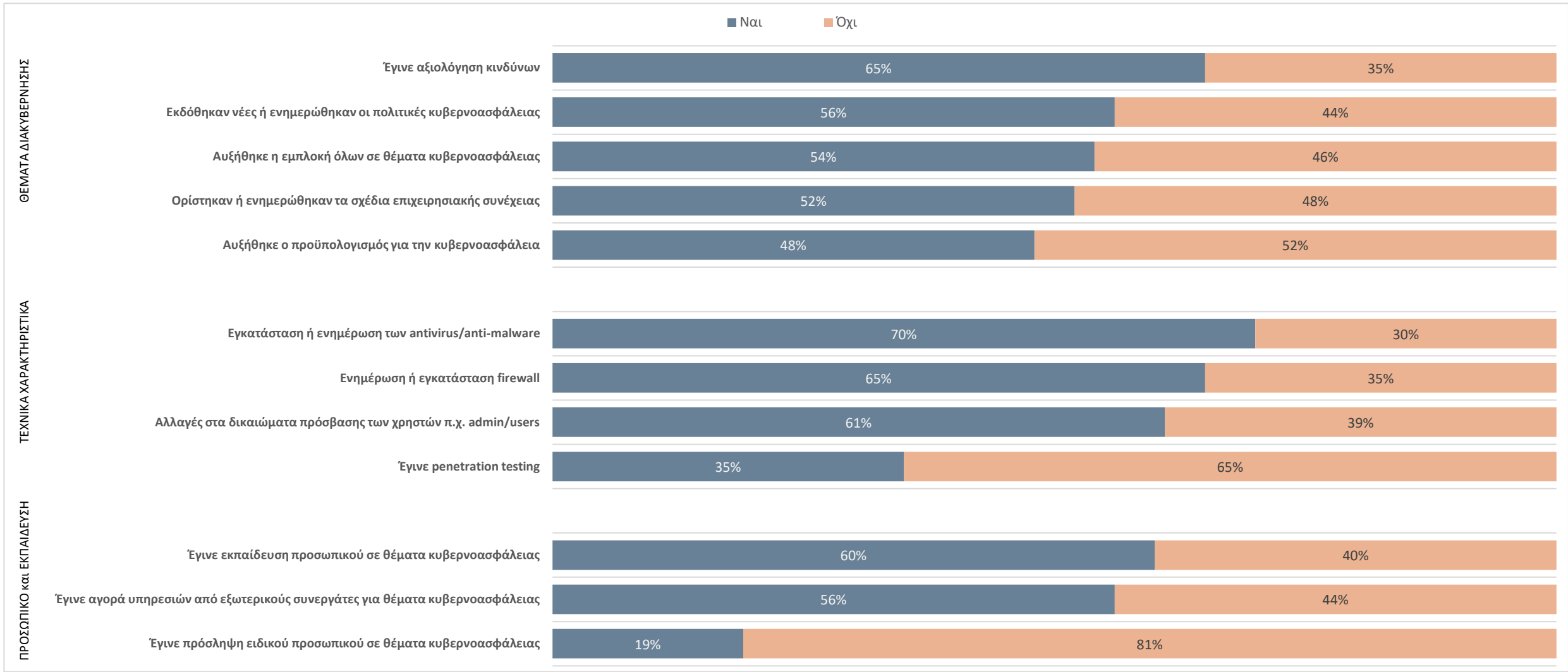
Βάση: Όλοι οι ερωτώμενοι



	Γνώση	Συμμετοχή
Σερφάρω στο Διαδίκτυο με Ασφάλεια (ΚΕΠΑ)	23%	3%
Ημερίδα για τη Διεθνή Ημέρα Ασφαλούς Διαδικτύου	17%	2%
Cyberbullying - Εκφοβισμός μέσω Διαδικτύου (CYTA)	16%	4%
CyberSafety: Ένα Καλύτερο Διαδίκτυο για τα Παιδιά στην Κύπρο (ΣΧΟΛΗ ΓΟΝΕΩΝ)	11%	2%
DIGITAL SECURITY STAKEHOLDERS CONFERENCE (ΑΨΑ| Εθνικό CSIRT-CY)	10%	3%
Course on Cybersecurity Organisational and Defensive Capabilities (ΑΨΑ|Εθνικό CSIRT-CY ESDC)	8%	3%
Μαθητική Ημερίδα "Ασφαλές διαδίκτυο για όλους" (ΥΠ.ΠΑΙΔΕΙΑΣ)	7%	1%
"Together for a better internet"	6%	1%
ITU Cyber Drill - ALERT (Applied Learning for Emergency Response Teams)	3%	1%
ISACA Conference	1%	1%
in house seminars (unsp)	3%	1%
ΔΕΝ συμμετείχα σε κάποιο		33%
Όχι, δεν γνωρίζω σεμινάρια ενημέρωσης και εκπαίδευσης	50%	50%

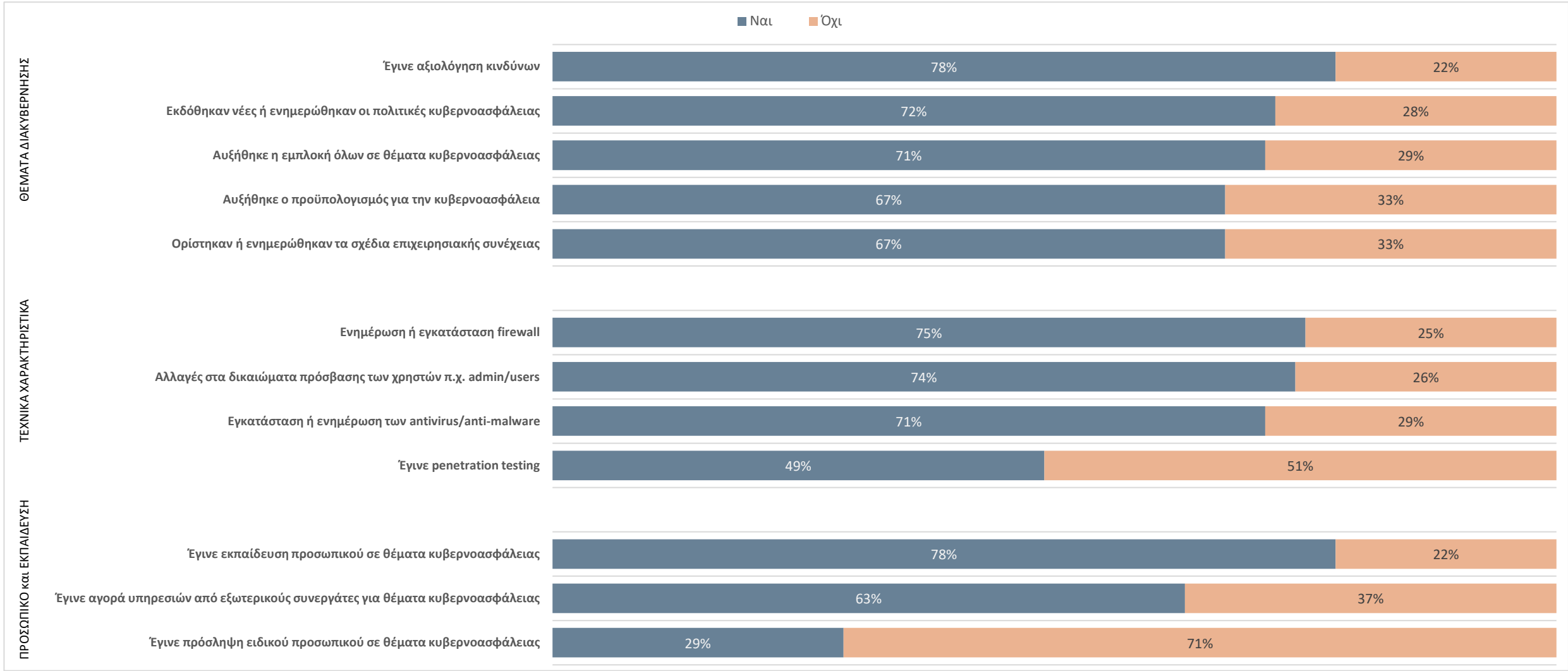
Τι από τα ακόλουθα έχετε αλλάξει σε θέματα κυβερνοασφάλειας, εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι γνωρίζουν σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια



Τι από τα ακόλουθα έχετε αλλάξει σε θέματα κυβερνοασφάλειας, εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι συμμετείχαν σε σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια

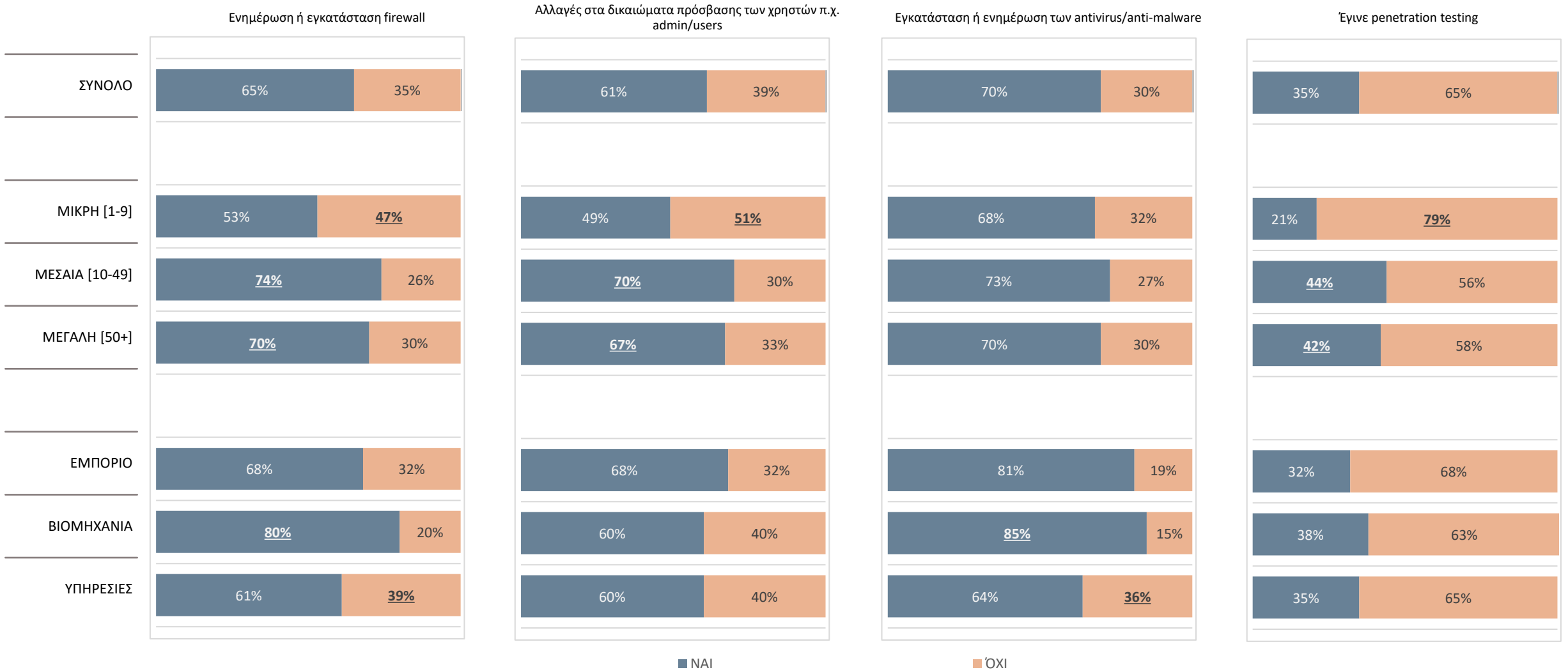


Τι από τα ακόλουθα έχετε αλλάξει σε σχέση με την ΔΙΑΚΥΒΕΡΝΗΣΗ στον οργανισμό, εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι γνωρίζουν σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια

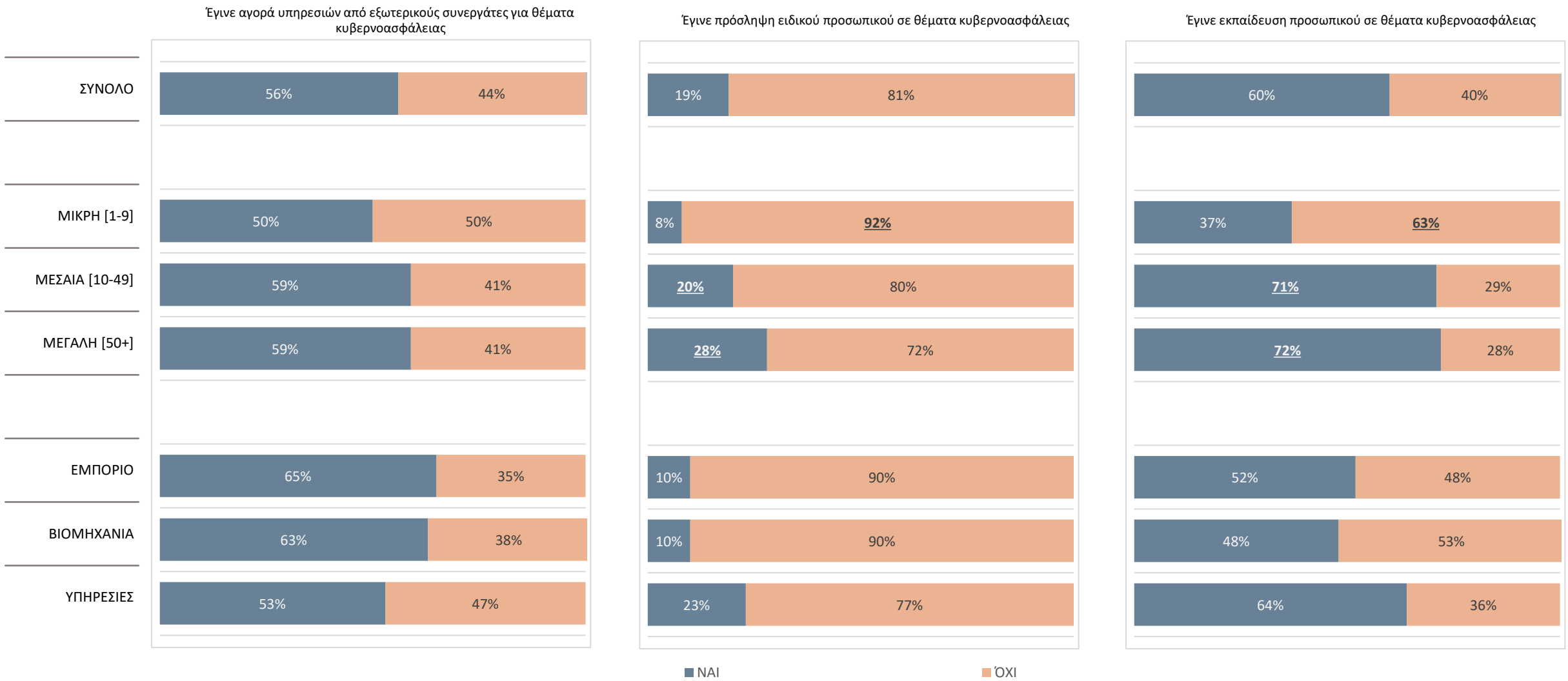
Τι από τα ακόλουθα ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ, έχετε αλλάξει εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι γνωρίζουν σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια



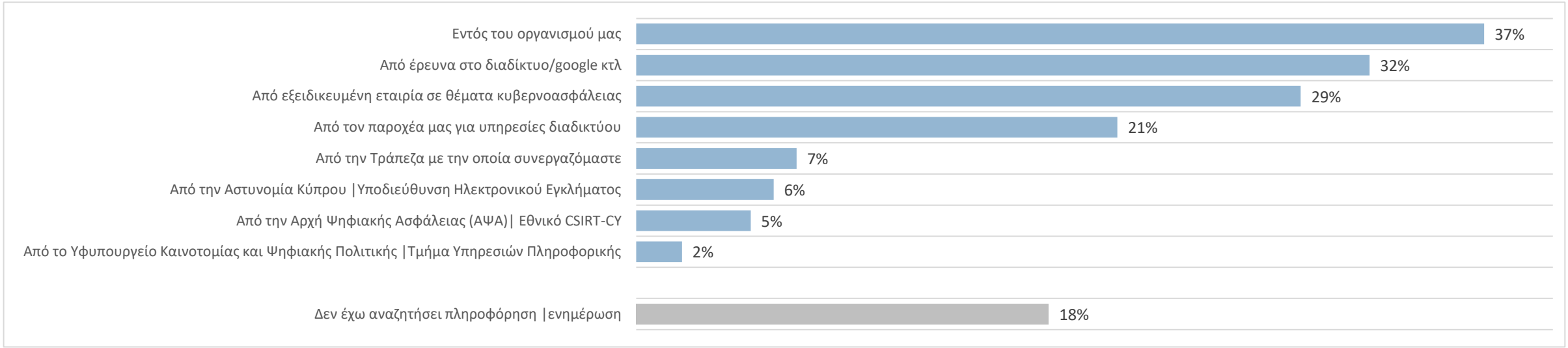
Και τι από τα ακόλουθα έχετε αλλάξει όσον αφορά στο ΠΡΟΣΩΠΙΚΟ και ΕΚΠΑΙΔΕΥΣΗ του προσωπικού;

Βάση: Όλοι όσοι γνωρίζουν σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια



Τον τελευταίο χρόνο, από που έχετε αναζητήσει πληροφόρηση, συμβουλή ή καθοδήγηση σε θέματα απειλών στον κυβερνοχώρο, για την εταιρία σας;

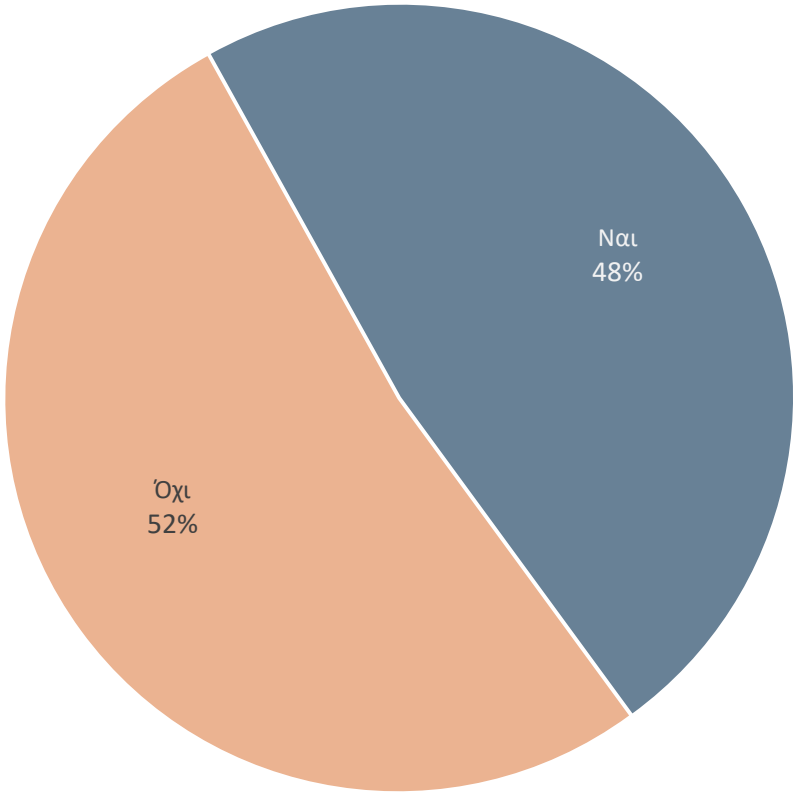
Βάση: Όλοι οι ερωτώμενοι

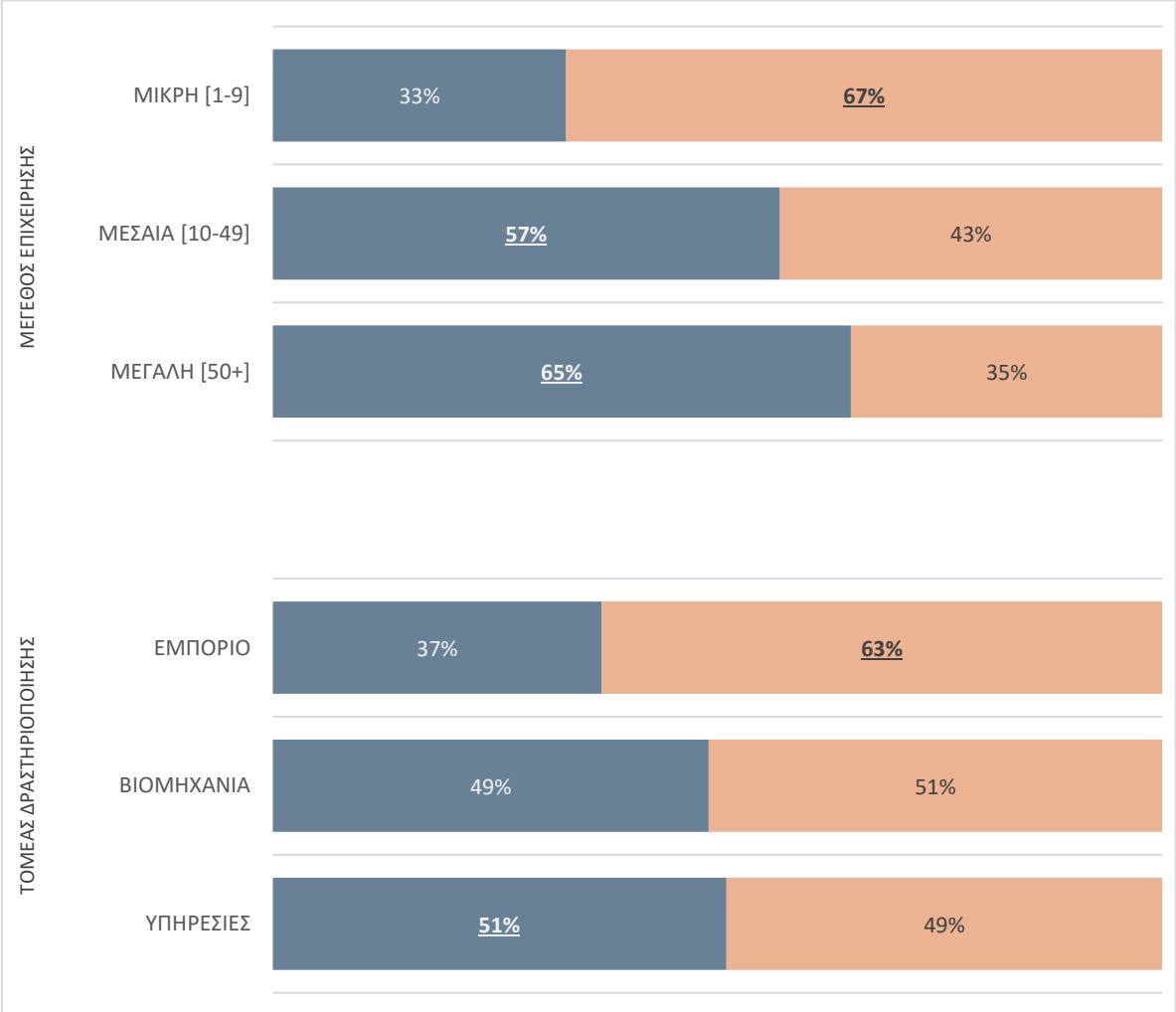


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Εντός του οργανισμού μας	18%	**45%**	**62%**	19%	35%	**43%**
Από έρευνα στο διαδίκτυο/google κτλ	28%	36%	38%	22%	28%	**37%**
Από εξειδικευμένη εταιρία σε θέματα κυβερνοασφάλειας	16%	**32%**	**50%**	27%	32%	28%
Από τον παροχέα μας για υπηρεσίες διαδικτύου	22%	23%	17%	**34%**	23%	17%
Από την Τράπεζα με την οποία συνεργαζόμαστε	9%	6%	6%	10%	7%	7%
Από την Αστυνομία Κύπρου |Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος	2%	**8%**	**9%**	4%	**11%**	5%
Από την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)| Εθνικό CSIRT-CY	1%	3%	**14%**	0%	**8%**	**6%**
Από το Υφυπουργείο Καινοτομίας και Ψηφιακής Πολιτικής |Τμήμα Υπηρεσιών Πληροφορικής	0%	**5%**	**5%**	0%	**4%**	3%
Δεν έχω αναζητήσει πληροφόρηση |ενημέρωση	**27%**	**14%**	5%	19%	18%	17%

Γνωρίζετε την Αρχή Ψηφιακής Ασφάλειας και το ρόλο που έχει;

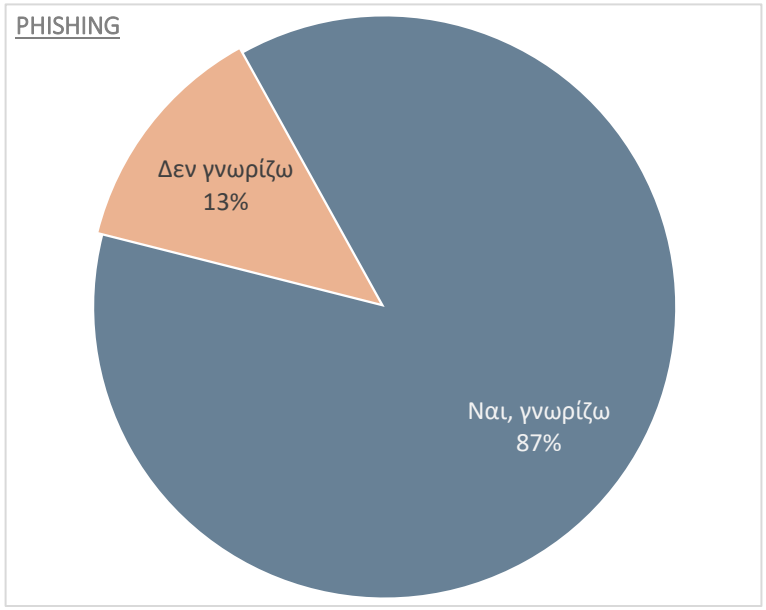
Βάση: Όλοι οι ερωτώμενοι

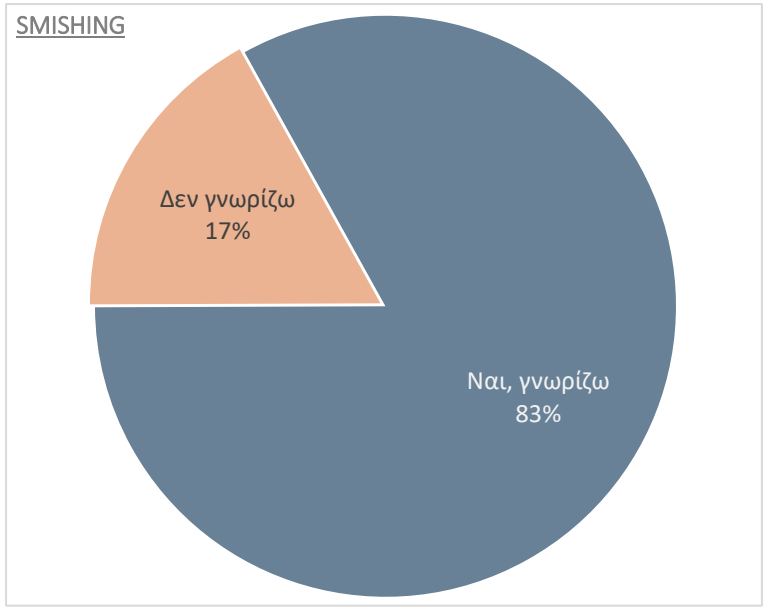


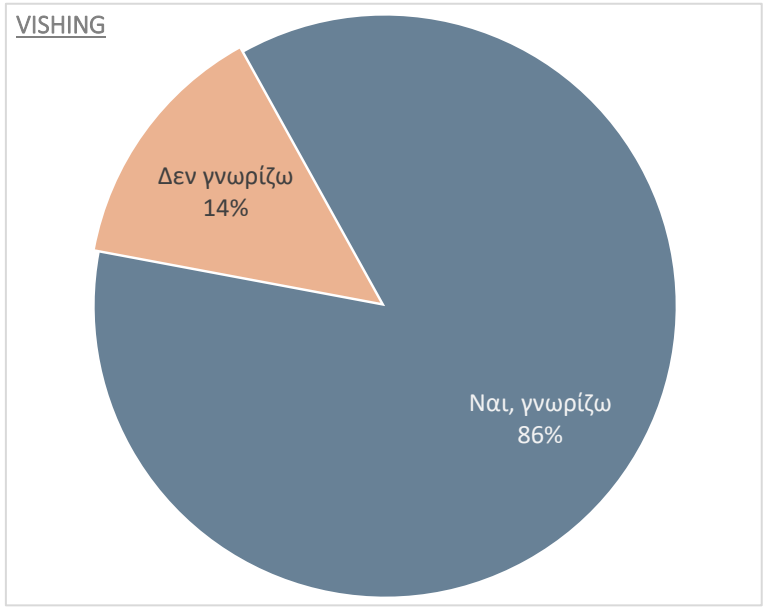


Γνώση μεθόδων που χρησιμοποιούνται για απάτες| επιθέσεις μέσω e-mail, sms ή μέσω τηλεφωνικής επικοινωνίας

Βάση: Όλοι οι ερωτώμενοι



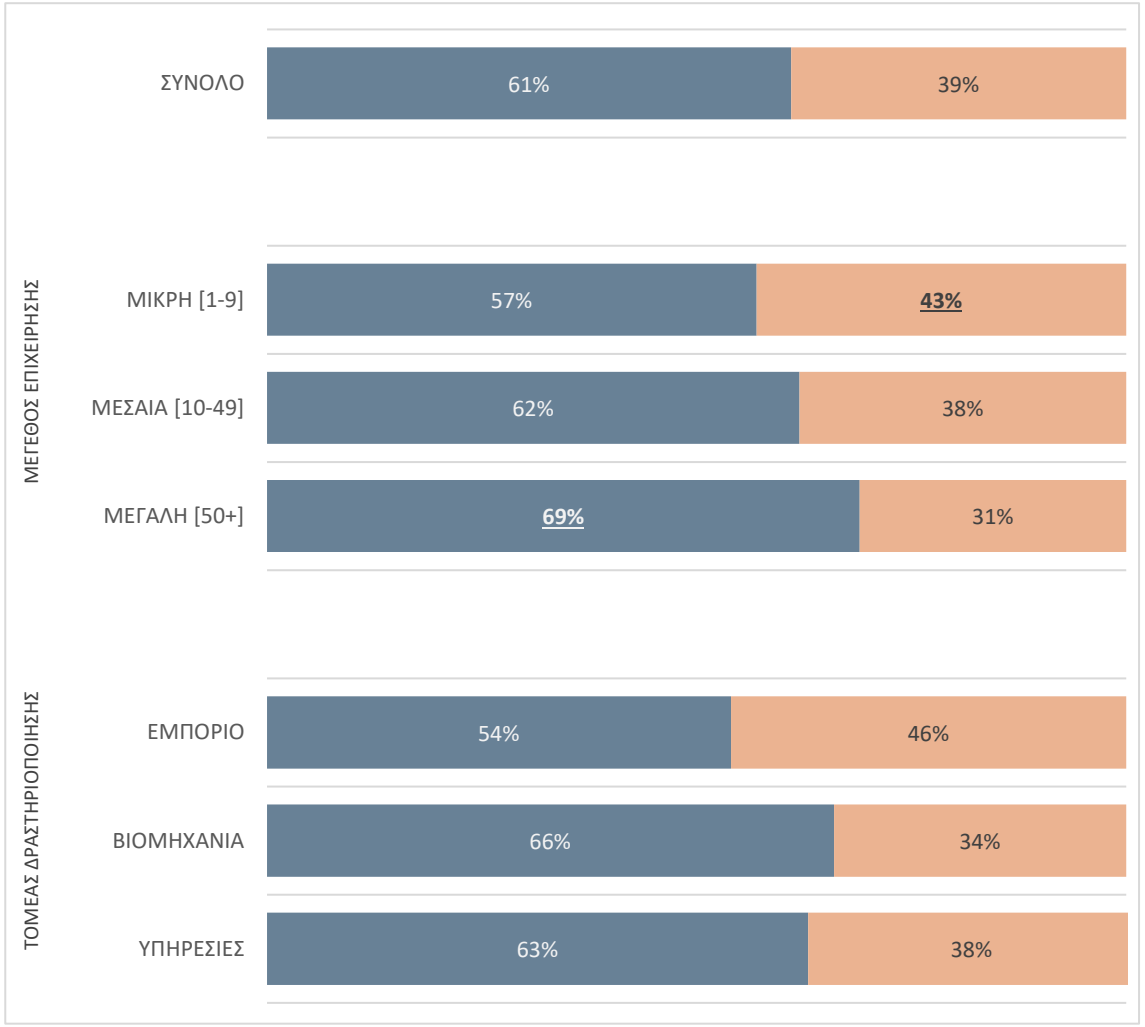


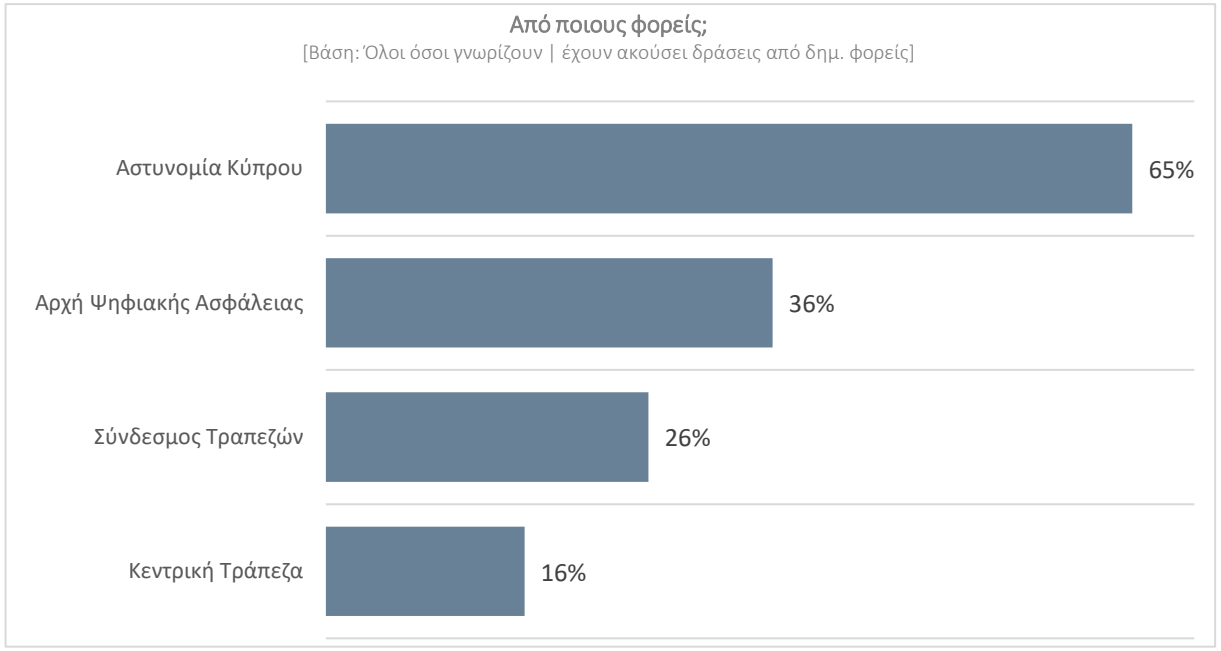


		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
PHISHING	Ναι, γνωρίζω	80%	**89%**	**98%**	86%	85%	89%
	Δεν γνωρίζω	**20%**	**11%**	2%	14%	15%	11%
SMISHING	Ναι, γνωρίζω	78%	84%	**91%**	82%	79%	84%
	Δεν γνωρίζω	**22%**	16%	9%	18%	21%	16%
VISHING	Ναι, γνωρίζω	83%	85%	**94%**	86%	86%	86%
	Δεν γνωρίζω	**17%**	**15%**	6%	14%	14%	14%

Γνωρίζετε ή έχετε ακούσει για κάποια δράση από δημόσιους φορείς σε σχέση με απάτες μέσω email, sms ή τηλεφωνικών κλήσεων; | Από ποιους φορείς;

Βάση: Όλοι οι ερωτώμενοι

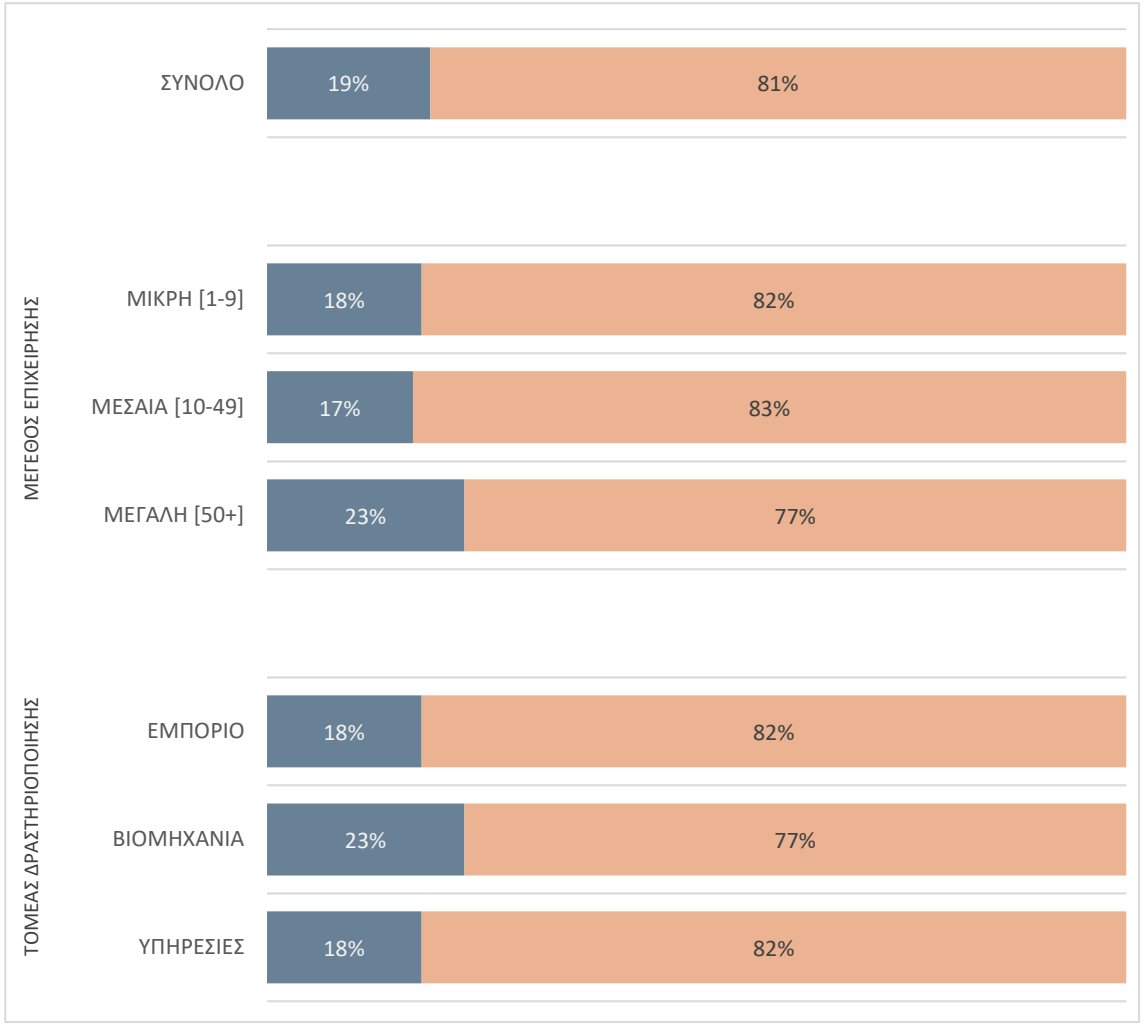


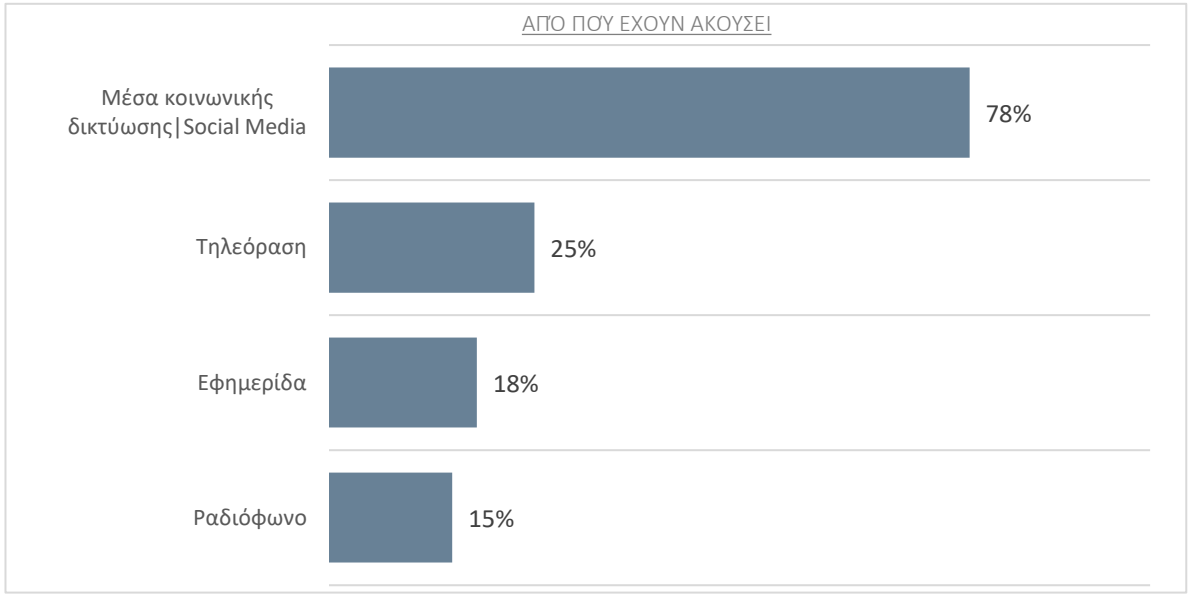


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Αστυνομία Κύπρου	68%	63%	64%	73%	66%	63%
Αρχή Ψηφιακής Ασφάλειας	23%	35%	**57%**	22%	28%	**42%**
Σύνδεσμος Τραπεζών	21%	28%	**34%**	22%	34%	26%
Κεντρική Τράπεζα	16%	15%	18%	10%	19%	17%

Γνωρίζετε ή έχετε ακούσει για την δράση ΑΣΠΙS; | Από πού έχετε ακούσει/μάθει για την δράση ΑΣΠΙΣ

Βάση: Όλοι οι ερωτώμενοι

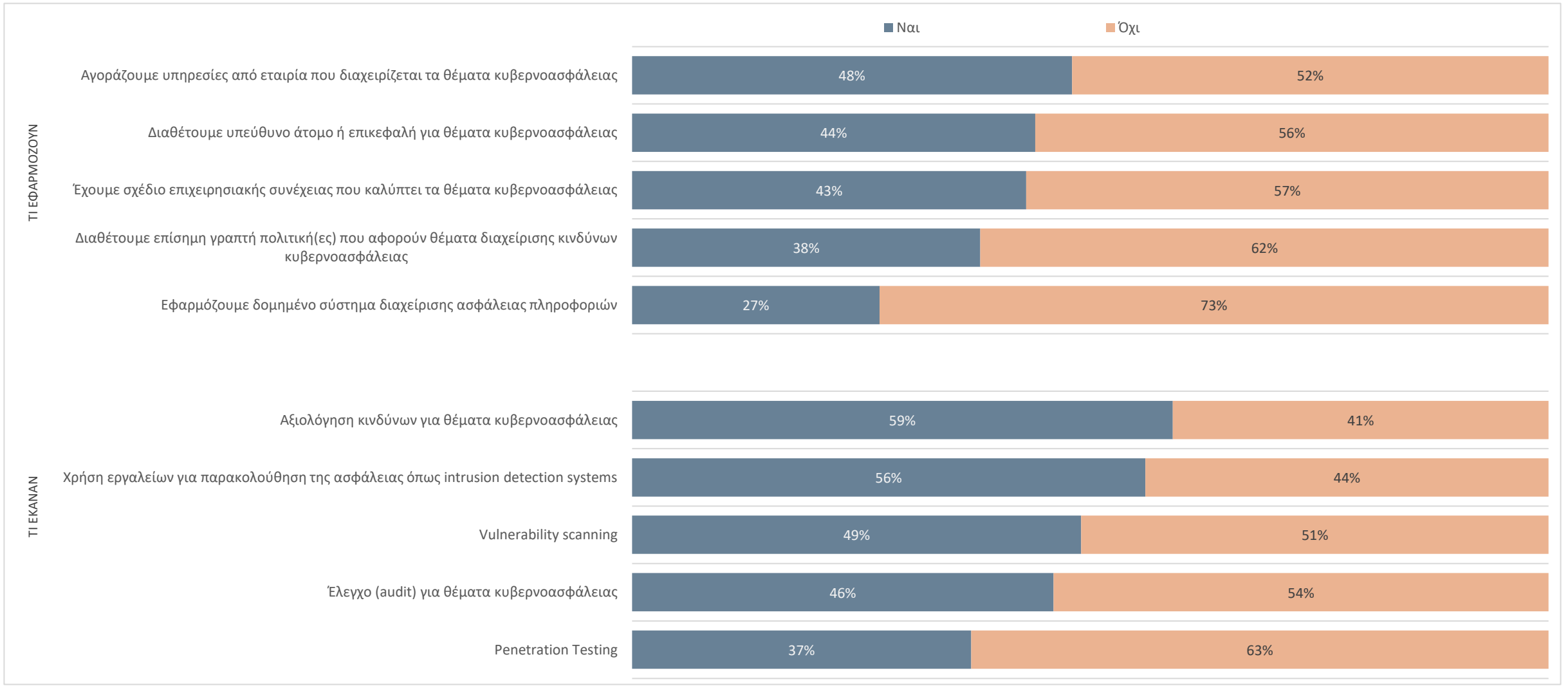




	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Μέσα κοινωνικής δικτύωσης | Social Media	68%	78%	92%	56%	88%	81%
Τηλεόραση	27%	22%	24%	38%	25%	21%
Εφημερίδα	19%	22%	12%	31%	31%	9%
Ραδιόφωνο	11%	17%	20%	31%	19%	9%

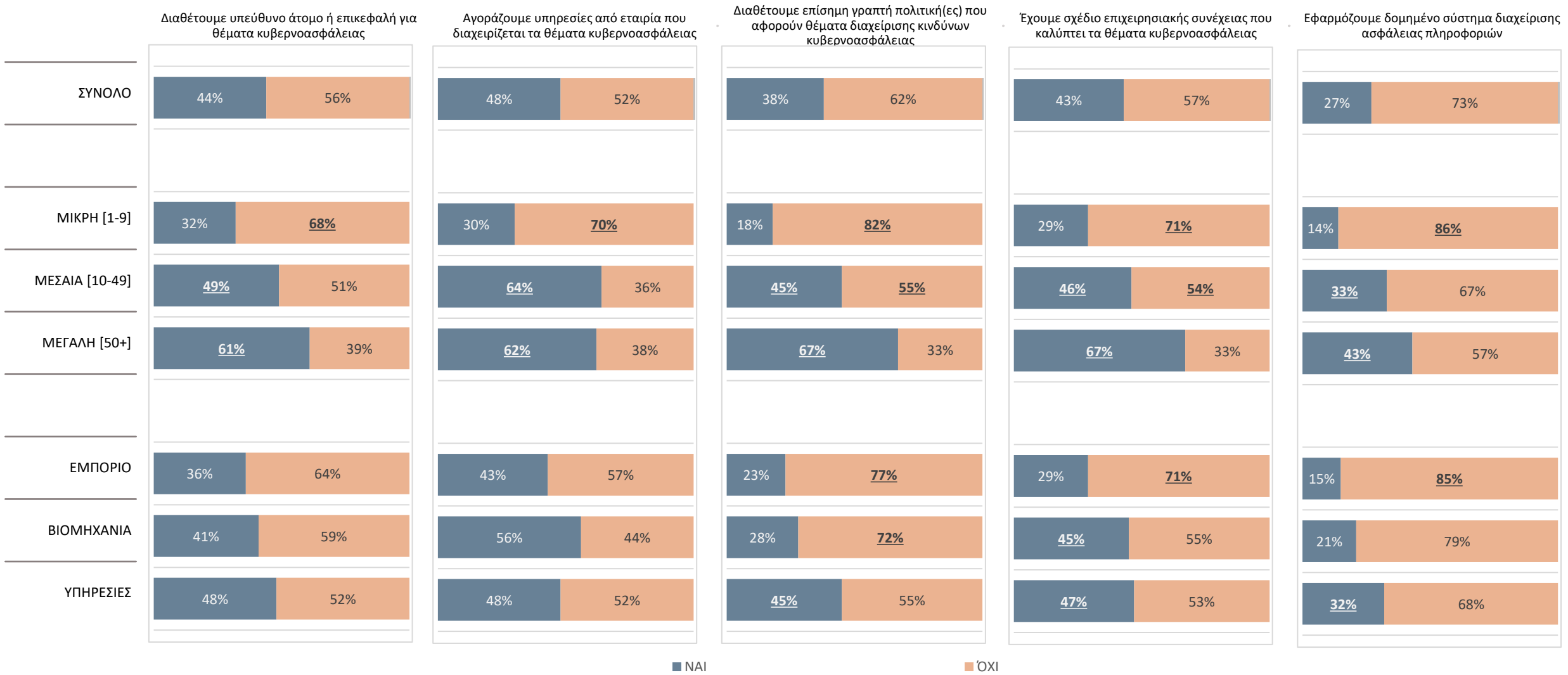
Ποιες από τις ακόλουθες αρχές διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας εφαρμόζετε στην εταιρεία; | Και ποια από τα ακόλουθα έχετε κάνει τους τελευταίους 12 μήνες για να εντοπίσετε κινδύνους;

Βάση: Όλοι οι ερωτώμενοι



Ποιες από τις ακόλουθες αρχές διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας εφαρμόζετε στην εταιρεία;

Βάση: Όλοι οι ερωτώμενοι

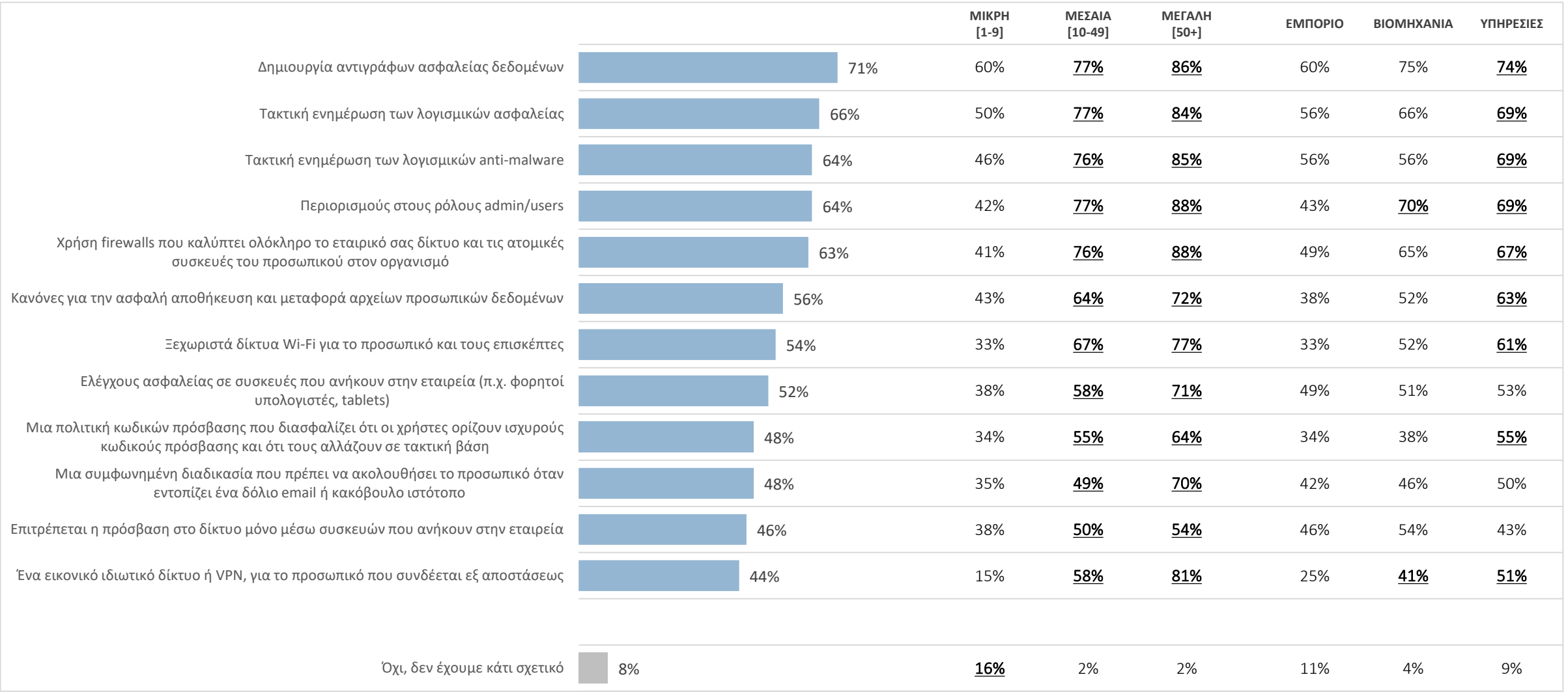


Και ποια από τα ακόλουθα έχετε κάνει τους τελευταίους 12 μήνες για να εντοπίσετε κινδύνους που αφορούν την κυβερνοασφάλεια της εταιρίας;

Βάση: Όλοι οι ερωτώμενοι

Ποιους από τους ακόλουθους κανόνες ή ελέγχους εφαρμόζετε στην επιχείρηση | εταιρεία σας;

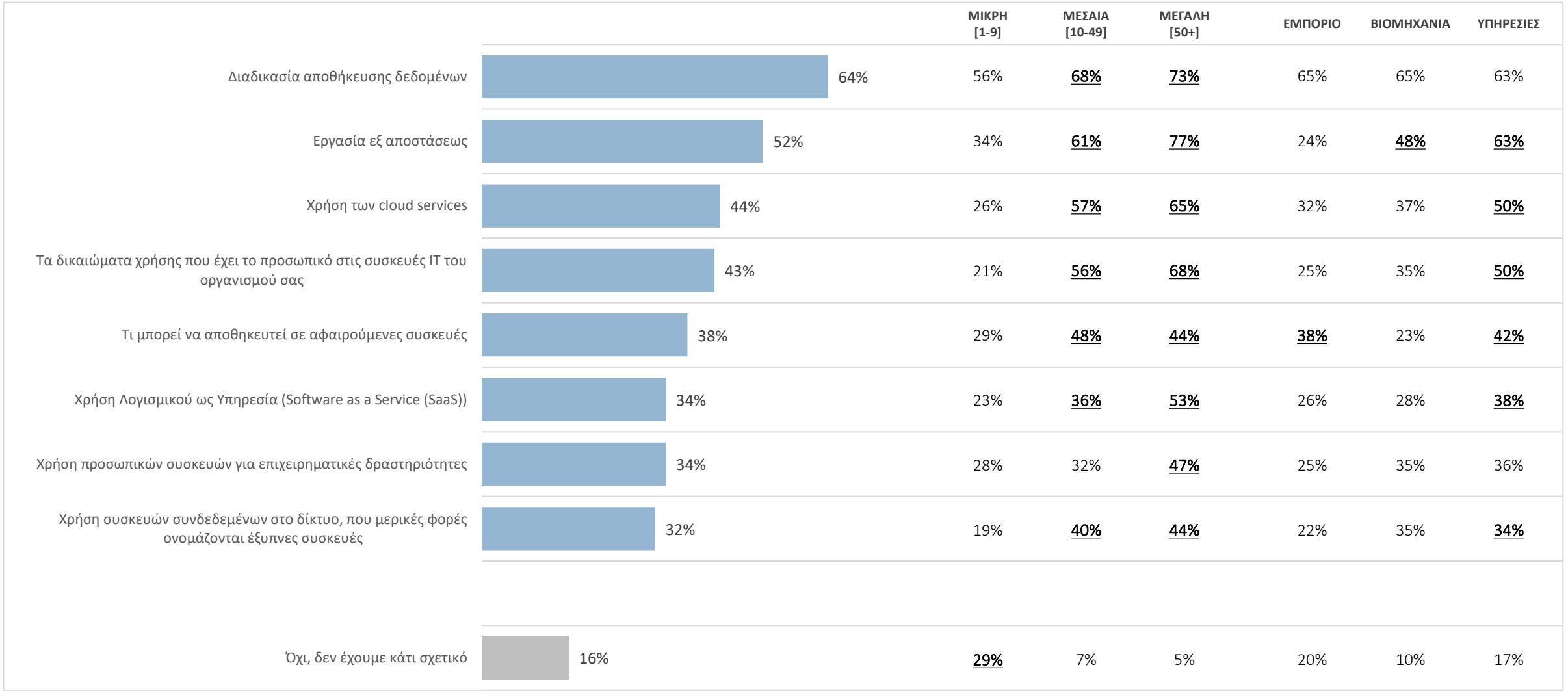
Βάση: Όλοι οι ερωτώμενοι



		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Δημιουργία αντιγράφων ασφαλείας δεδομένων	71%	60%	**77%**	**86%**	60%	75%	**74%**
Τακτική ενημέρωση των λογισμικών ασφαλείας	66%	50%	**77%**	**84%**	56%	66%	**69%**
Τακτική ενημέρωση των λογισμικών anti-malware	64%	46%	**76%**	**85%**	56%	56%	**69%**
Περιορισμούς στους ρόλους admin/users	64%	42%	**77%**	**88%**	43%	**70%**	**69%**
Χρήση firewalls που καλύπτει ολόκληρο το εταιρικό σας δίκτυο και τις ατομικές συσκευές του προσωπικού στον οργανισμό	63%	41%	**76%**	**88%**	49%	65%	**67%**
Κανόνες για την ασφαλή αποθήκευση και μεταφορά αρχείων προσωπικών δεδομένων	56%	43%	**64%**	**72%**	38%	52%	**63%**
Ξεχωριστά δίκτυα Wi-Fi για το προσωπικό και τους επισκέπτες	54%	33%	**67%**	**77%**	33%	52%	**61%**
Ελέγχους ασφαλείας σε συσκευές που ανήκουν στην εταιρεία (π.χ. φορητοί υπολογιστές, tablets)	52%	38%	**58%**	**71%**	49%	51%	53%
Μια πολιτική κωδικών πρόσβασης που διασφαλίζει ότι οι χρήστες ορίζουν ισχυρούς κωδικούς πρόσβασης και ότι τους αλλάζουν σε τακτική βάση	48%	34%	**55%**	**64%**	34%	38%	**55%**
Μια συμφωνημένη διαδικασία που πρέπει να ακολουθήσει το προσωπικό όταν εντοπίζει ένα δόλιο email ή κακόβουλο ιστότοπο	48%	35%	**49%**	**70%**	42%	46%	50%
Επιτρέπεται η πρόσβαση στο δίκτυο μόνο μέσω συσκευών που ανήκουν στην εταιρεία	46%	38%	**50%**	**54%**	46%	54%	43%
Ένα εικονικό ιδιωτικό δίκτυο ή VPN, για το προσωπικό που συνδέεται εξ αποστάσεως	44%	15%	**58%**	**81%**	25%	**41%**	**51%**
Όχι, δεν έχουμε κάτι σχετικό	8%	**16%**	2%	2%	11%	4%	9%

Ποιες από τις ακόλουθες πτυχές, εάν υπάρχουν, καλύπτονται από την πολιτική ή τις πολιτικές σας σχετικά με την κυβερνοασφάλεια;

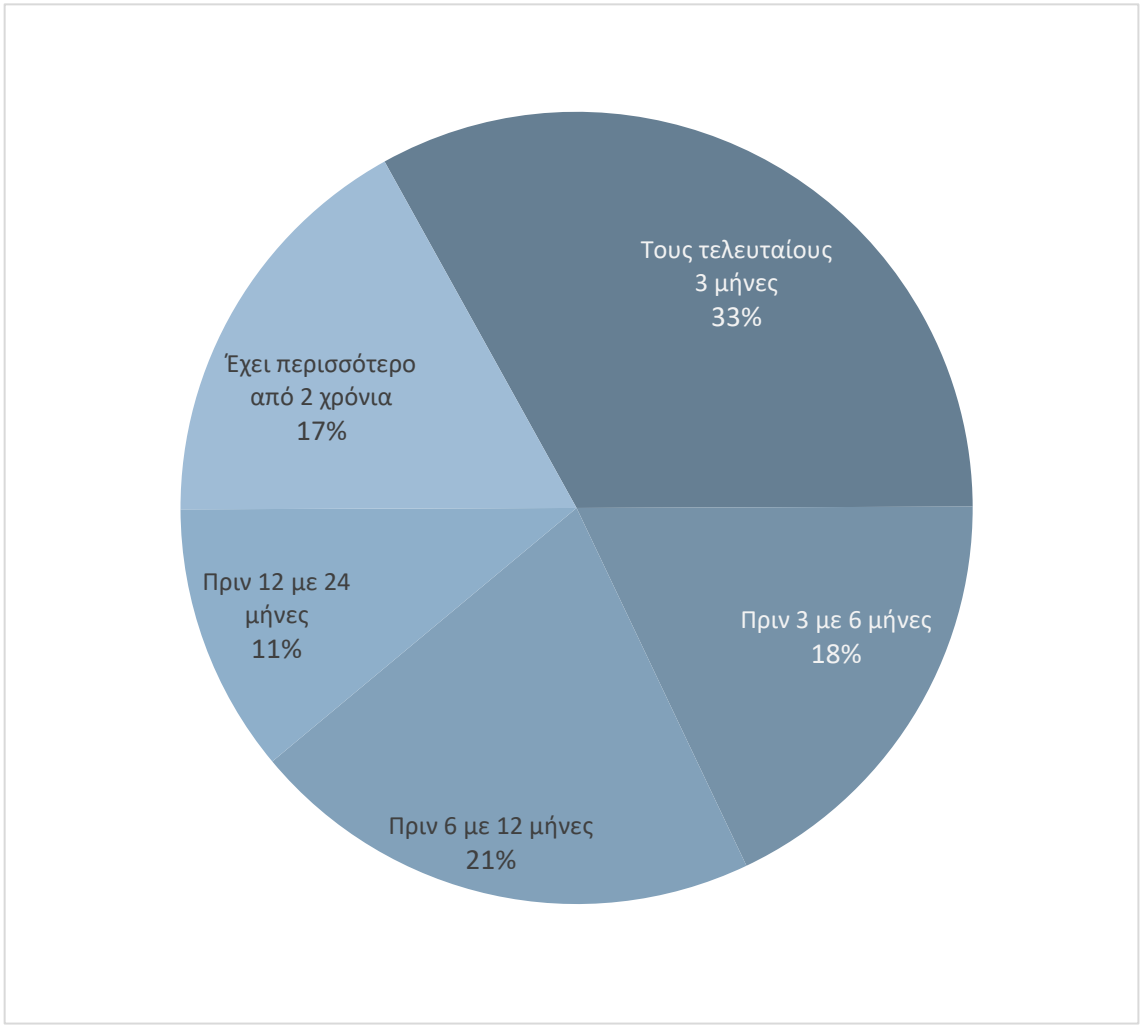
Βάση: Όλοι οι ερωτώμενοι

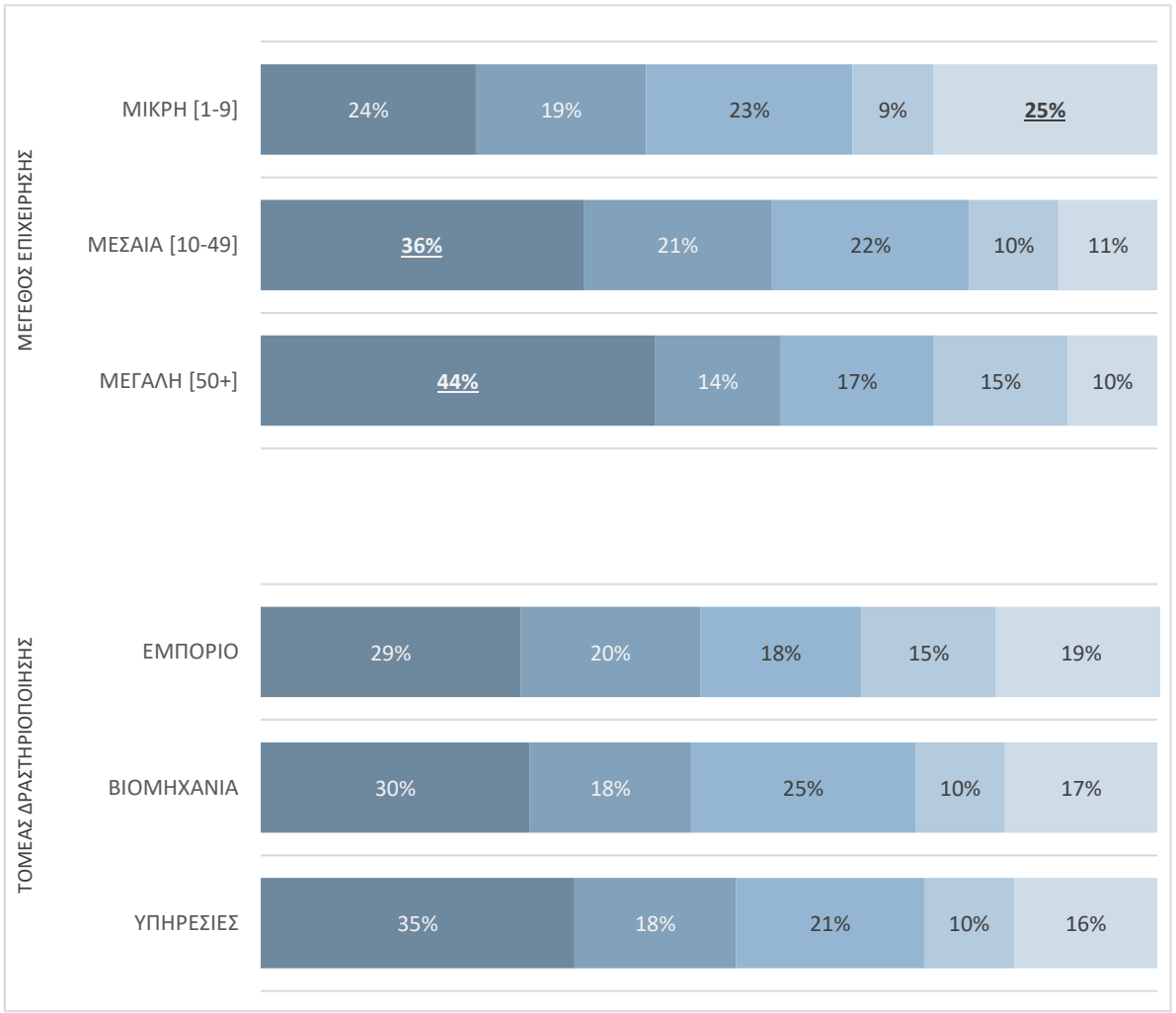


		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Διαδικασία αποθήκευσης δεδομένων	64%	56%	**68%**	**73%**	65%	65%	63%
Εργασία εξ αποστάσεως	52%	34%	**61%**	**77%**	24%	**48%**	**63%**
Χρήση των cloud services	44%	26%	**57%**	**65%**	32%	37%	**50%**
Τα δικαιώματα χρήσης που έχει το προσωπικό στις συσκευές IT του οργανισμού σας	43%	21%	**56%**	**68%**	25%	35%	**50%**
Τι μπορεί να αποθηκευτεί σε αφαιρούμενες συσκευές	38%	29%	**48%**	**44%**	**38%**	23%	**42%**
Χρήση Λογισμικού ως Υπηρεσία (Software as a Service (SaaS))	34%	23%	**36%**	**53%**	26%	28%	**38%**
Χρήση προσωπικών συσκευών για επιχειρηματικές δραστηριότητες	34%	28%	32%	**47%**	25%	35%	36%
Χρήση συσκευών συνδεδεμένων στο δίκτυο, που μερικές φορές ονομάζονται έξυπνες συσκευές	32%	19%	**40%**	**44%**	22%	35%	**34%**
Όχι, δεν έχουμε κάτι σχετικό	16%	**29%**	7%	5%	20%	10%	17%

Πότε δημιουργήθηκαν ή ενημερώθηκαν ή έτυχαν αναθεώρησης για τελευταία φορά κάποιες από τις πολιτικές σας για την κυβερνοασφάλεια για να βεβαιωθείτε ότι συμβαδίζουν με τις τεχνολογικές εξελίξεις;

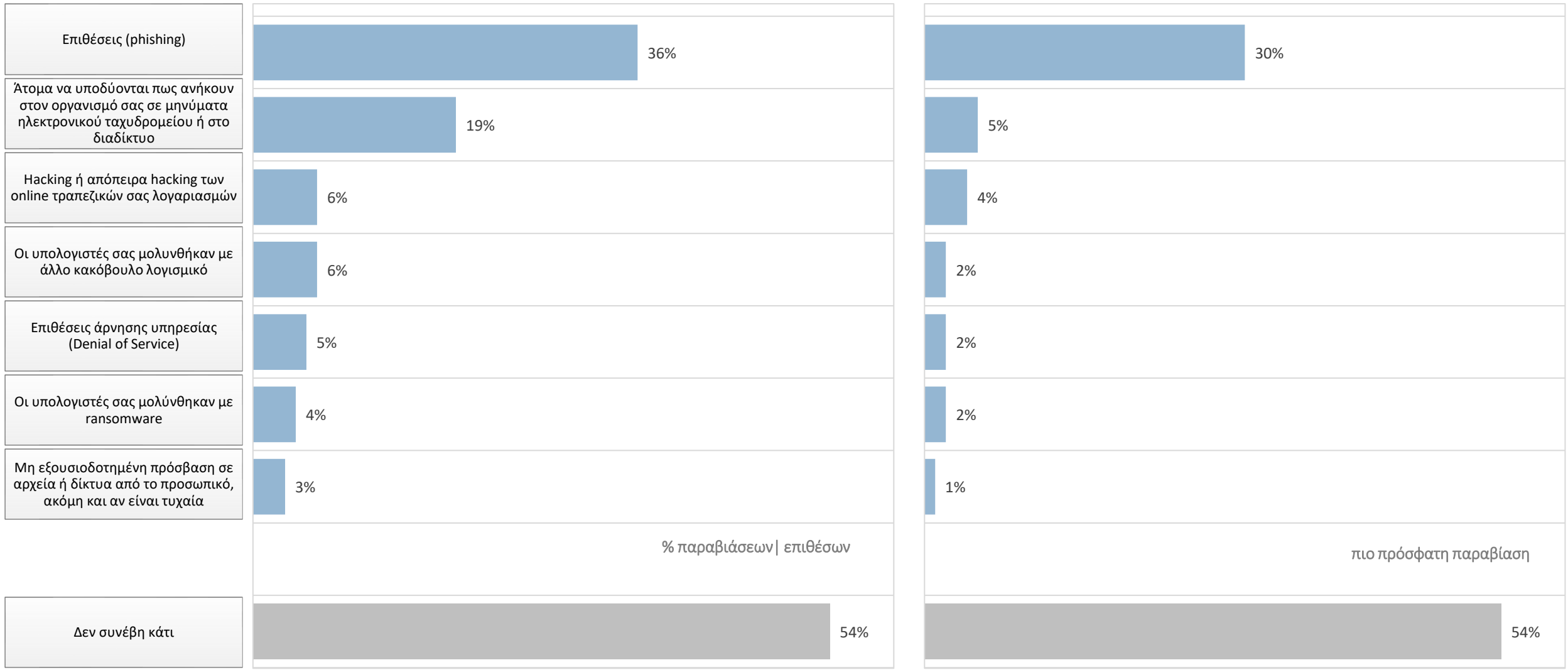
Βάση: Όλοι οι ερωτώμενοι





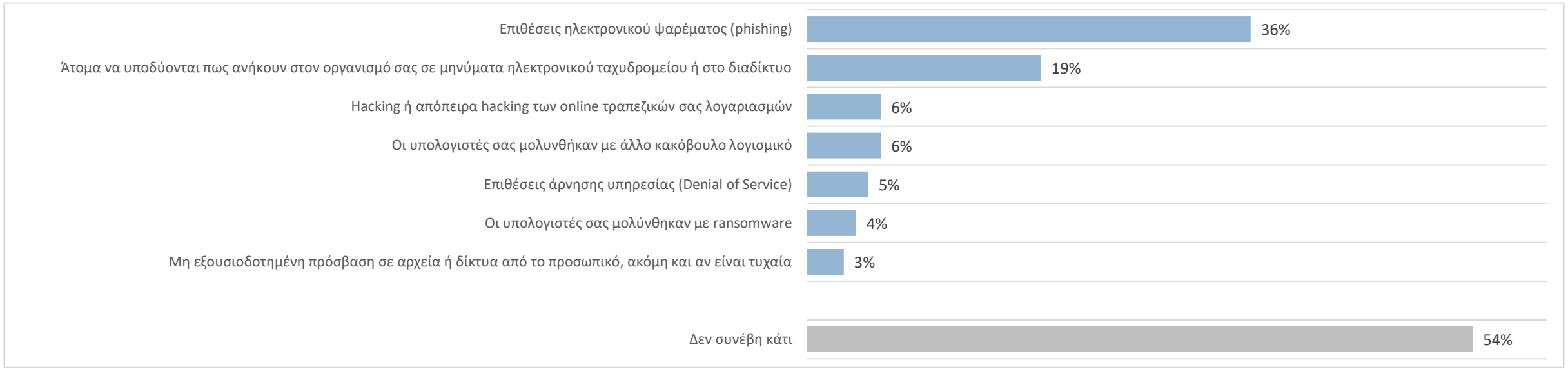
Τους τελευταίους 12 μήνες, τι από τα παρακάτω συνέβη στην εταιρεία |επιχείρηση |οργανισμό; Και ποια ήταν η πιο πρόσφατη παραβίαση κυβερνοασφάλειας |επίθεση, που δεχτήκατε;

Βάση: Όλοι οι ερωτώμενοι



Τους τελευταίους 12 μήνες, τι από τα παρακάτω συνέβη στην εταιρεία |επιχείρηση |οργανισμό;

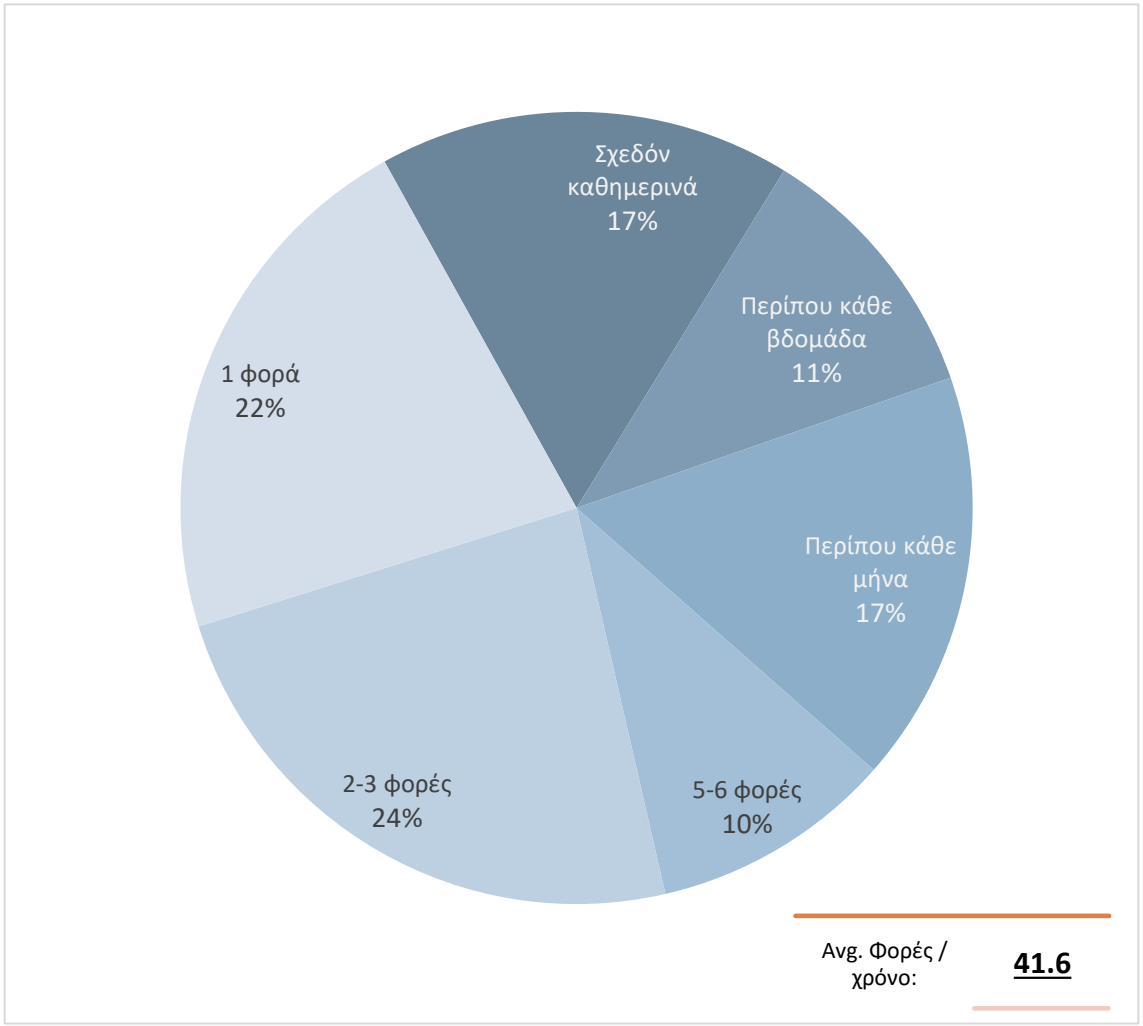
Βάση: Όλοι οι ερωτώμενοι

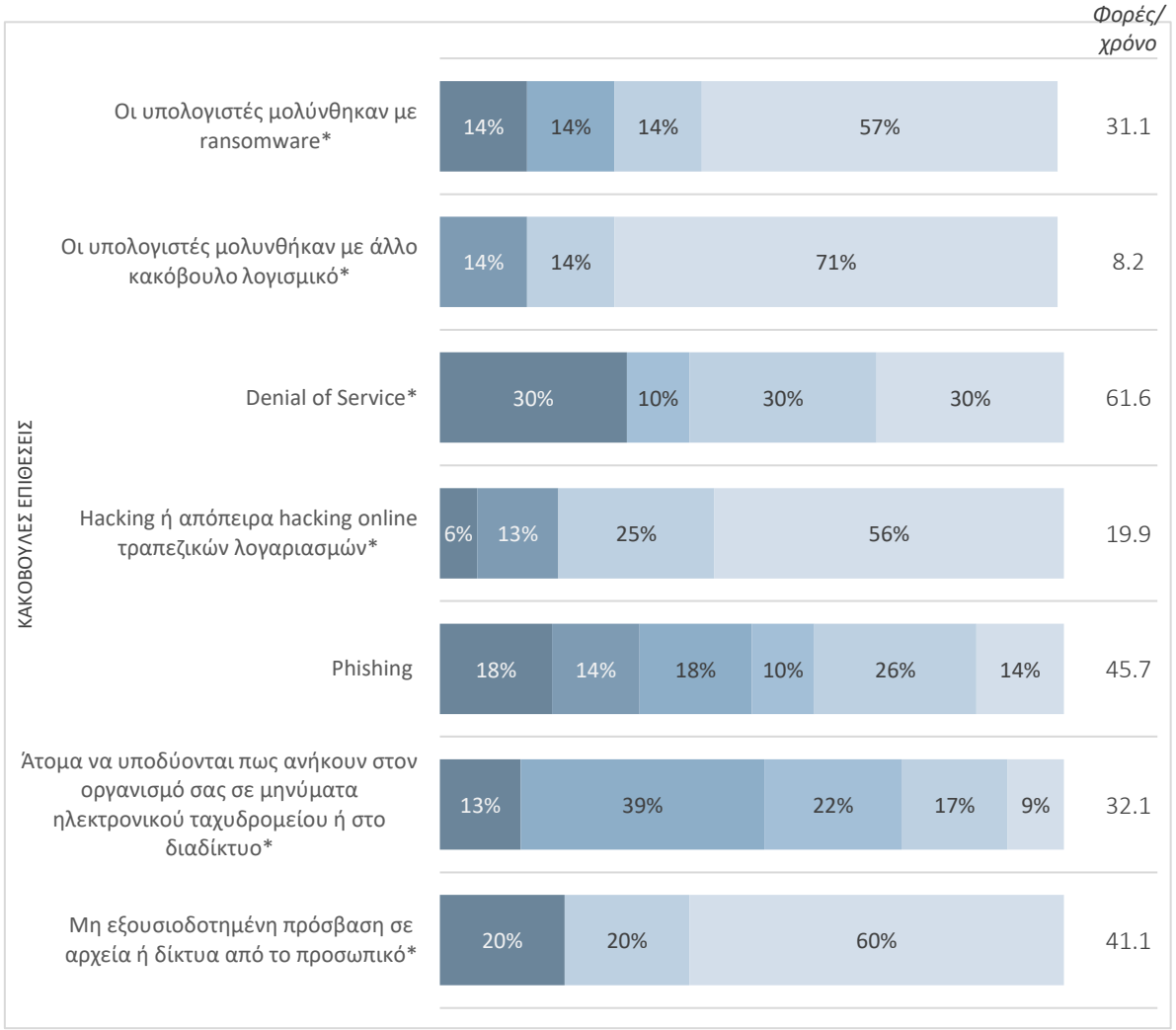


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Επιθέσεις ηλεκτρονικού ψαρέματος (phishing)	25%	34%	**58%**	26%	35%	**39%**
Άτομα να υποδύονται πως ανήκουν στον οργανισμό σας σε μηνύματα ηλεκτρονικού ταχυδρομείου ή στο διαδίκτυο	8%	**20%**	**37%**	15%	21%	19%
Hacking ή απόπειρα hacking των online τραπεζικών σας λογαριασμών	8%	4%	7%	8%	6%	6%
Οι υπολογιστές σας μολυνθήκαν με άλλο κακόβουλο λογισμικό	6%	3%	7%	9%	6%	5%
Επιθέσεις άρνησης υπηρεσίας (Denial of Service)	3%	2%	**13%**	4%	8%	5%
Οι υπολογιστές σας μολύνθηκαν με ransomware	2%	5%	5%		**7%**	4%
Μη εξουσιοδοτημένη πρόσβαση σε αρχεία ή δίκτυα από το προσωπικό, ακόμη και αν είναι τυχαία	1%	4%	**6%**	7%	1%	3%
Δεν συνέβη κάτι	**63%**	**59%**	32%	63%	52%	52%

Τους τελευταίους 12 μήνες, πόσο συχνά αντιμετωπίσατε κάποια από τις παραβιάσεις ή τις επιθέσεις αυτές;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση

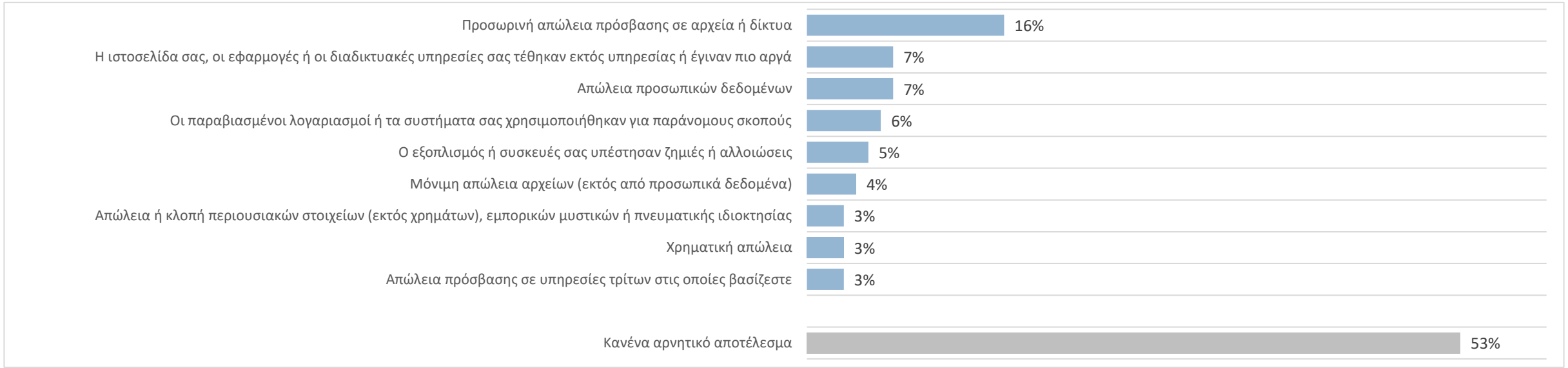




** Μικτή βάση | στατιστικά μη σημαντικό*

Λαμβάνοντας υπόψιν όλες τις παραβιάσεις ή κυβερνοεπιθέσεις που αντιμετωπίσατε τους τελευταίους 12 μήνες, ποια από τα ακόλουθα συνέβησαν ως αποτέλεσμα τους;

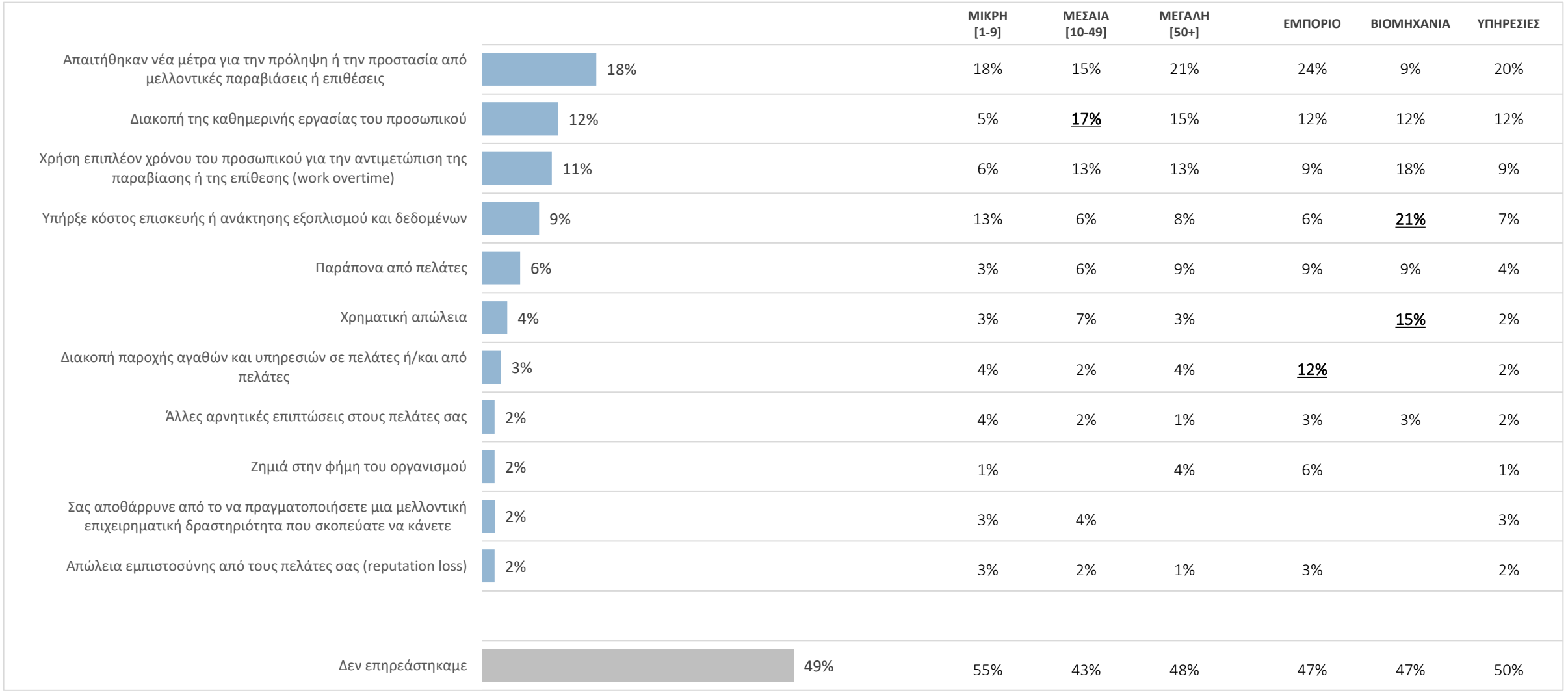
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Προσωρινή απώλεια πρόσβασης σε αρχεία ή δίκτυα	22%	13%	11%	15%	12%	17%
Η ιστοσελίδα σας, οι εφαρμογές ή οι διαδικτυακές υπηρεσίες σας τέθηκαν εκτός υπηρεσίας ή έγιναν πιο αργά	5%	6%	9%	9%	6%	7%
Απώλεια προσωπικών δεδομένων	6%	7%	7%	0%	3%	9%
Οι παραβιασμένοι λογαριασμοί ή τα συστήματα σας χρησιμοποιήθηκαν για παράνομους σκοπούς	5%	7%	7%	3%	**18%**	4%
Ο εξοπλισμός ή συσκευές σας υπέστησαν ζημιές ή αλλοιώσεις	4%	7%	5%	6%	6%	5%
Μόνιμη απώλεια αρχείων (εκτός από προσωπικά δεδομένα)	8%	4%	1%	6%	0%	5%
Απώλεια ή κλοπή περιουσιακών στοιχείων (εκτός χρημάτων), εμπορικών μυστικών ή πνευματικής ιδιοκτησίας	4%	4%	1%	6%	0%	3%
Χρηματική απώλεια	1%	4%	4%	**6%**	**12%**	0%
Απώλεια πρόσβασης σε υπηρεσίες τρίτων στις οποίες βασίζεστε	5%	4%	0%	3%	0%	4%
Κανένα αρνητικό αποτέλεσμα	53%	48%	57%	50%	56%	54%

Πως έχουν επηρεάσει την εταιρεία/ επιχείρηση /τον οργανισμό αυτές οι παραβιάσεις ή επιθέσεις;

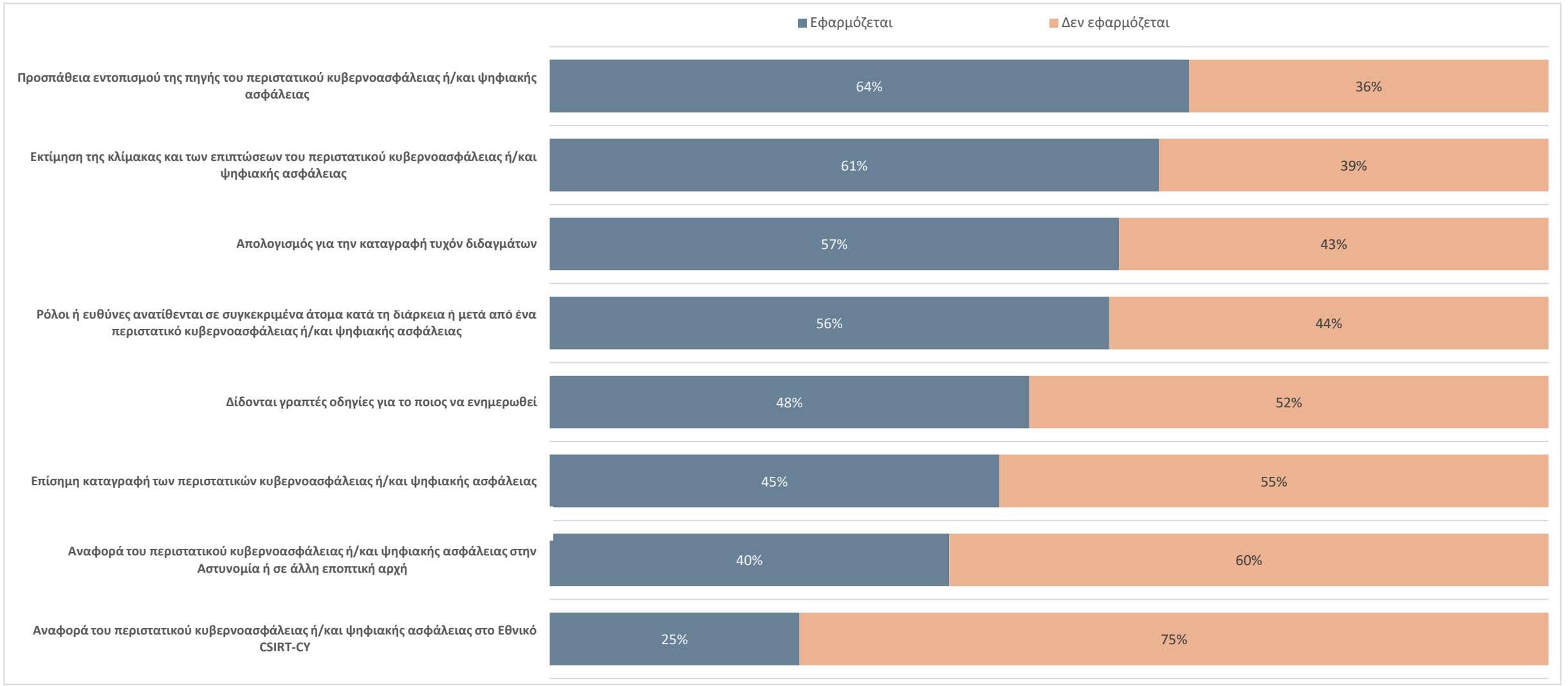
Βάση: Όλοι οι ερωτώμενοι



		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Απαιτήθηκαν νέα μέτρα για την πρόληψη ή την προστασία από μελλοντικές παραβιάσεις ή επιθέσεις	18%	18%	15%	21%	24%	9%	20%
Διακοπή της καθημερινής εργασίας του προσωπικού	12%	5%	**17%**	15%	12%	12%	12%
Χρήση επιπλέον χρόνου του προσωπικού για την αντιμετώπιση της παραβίασης ή της επίθεσης (work overtime)	11%	6%	13%	13%	9%	18%	9%
Υπήρξε κόστος επισκευής ή ανάκτησης εξοπλισμού και δεδομένων	9%	13%	6%	8%	6%	**21%**	7%
Παράπονα από πελάτες	6%	3%	6%	9%	9%	9%	4%
Χρηματική απώλεια	4%	3%	7%	3%		**15%**	2%
Διακοπή παροχής αγαθών και υπηρεσιών σε πελάτες ή/και από πελάτες	3%	4%	2%	4%	**12%**		2%
Άλλες αρνητικές επιπτώσεις στους πελάτες σας	2%	4%	2%	1%	3%	3%	2%
Ζημιά στην φήμη του οργανισμού	2%	1%		4%	6%		1%
Σας αποθάρρυνε από το να πραγματοποιήσετε μια μελλοντική επιχειρηματική δραστηριότητα που σκοπεύατε να κάνετε	2%	3%	4%				3%
Απώλεια εμπιστοσύνης από τους πελάτες σας (reputation loss)	2%	3%	2%	1%	3%		2%
Δεν επηρεάστηκαμε	49%	55%	43%	48%	47%	47%	50%

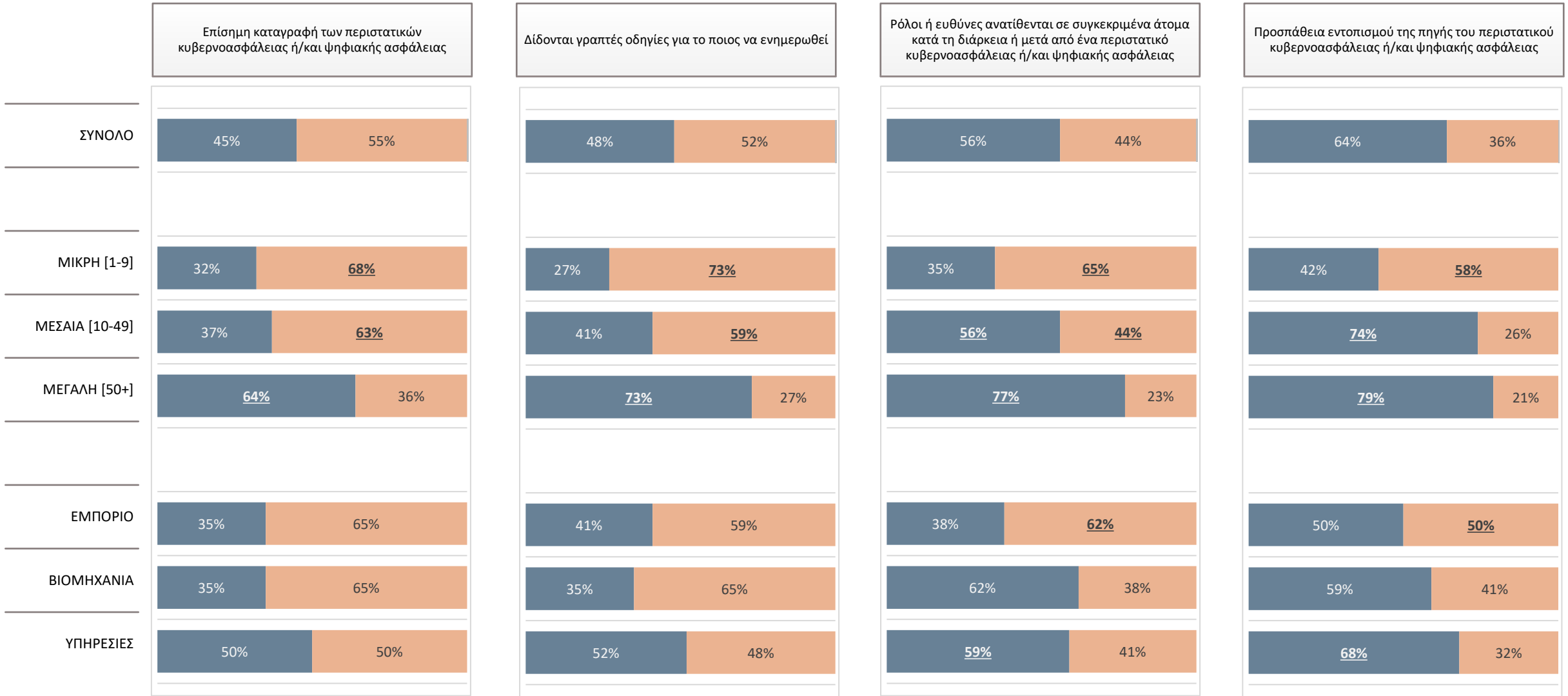
Ποια από τα παρακάτω κάνετε ή εφαρμόζετε, όταν αντιμετωπίζετε ένα περιστατικό κυβερνοασφάλειας;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



Ποια από τα παρακάτω κάνετε ή εφαρμόζετε, όταν αντιμετωπίζετε ένα περιστατικό κυβερνοασφάλειας;

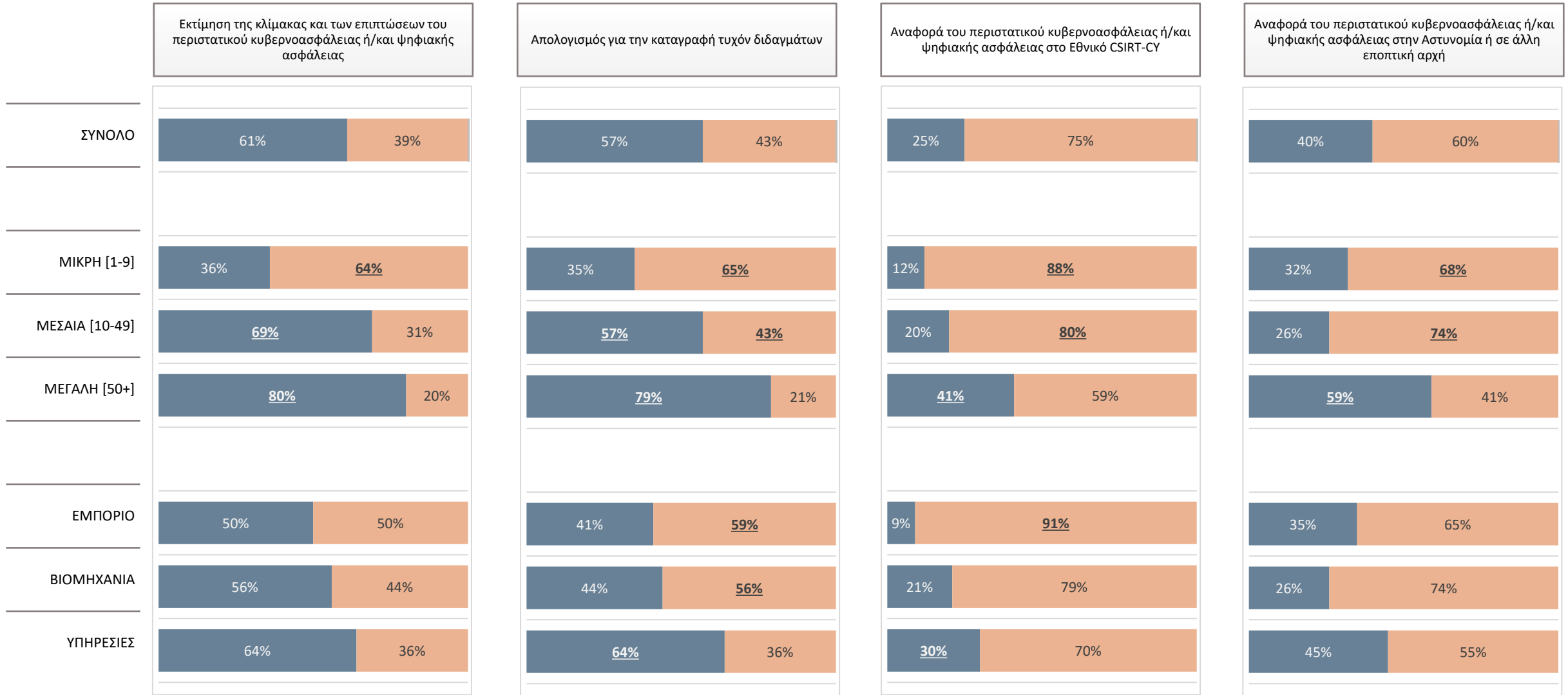
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



Ποια από τα παρακάτω κάνετε ή εφαρμόζετε, όταν αντιμετωπίζετε ένα περιστατικό κυβερνοασφάλειας;

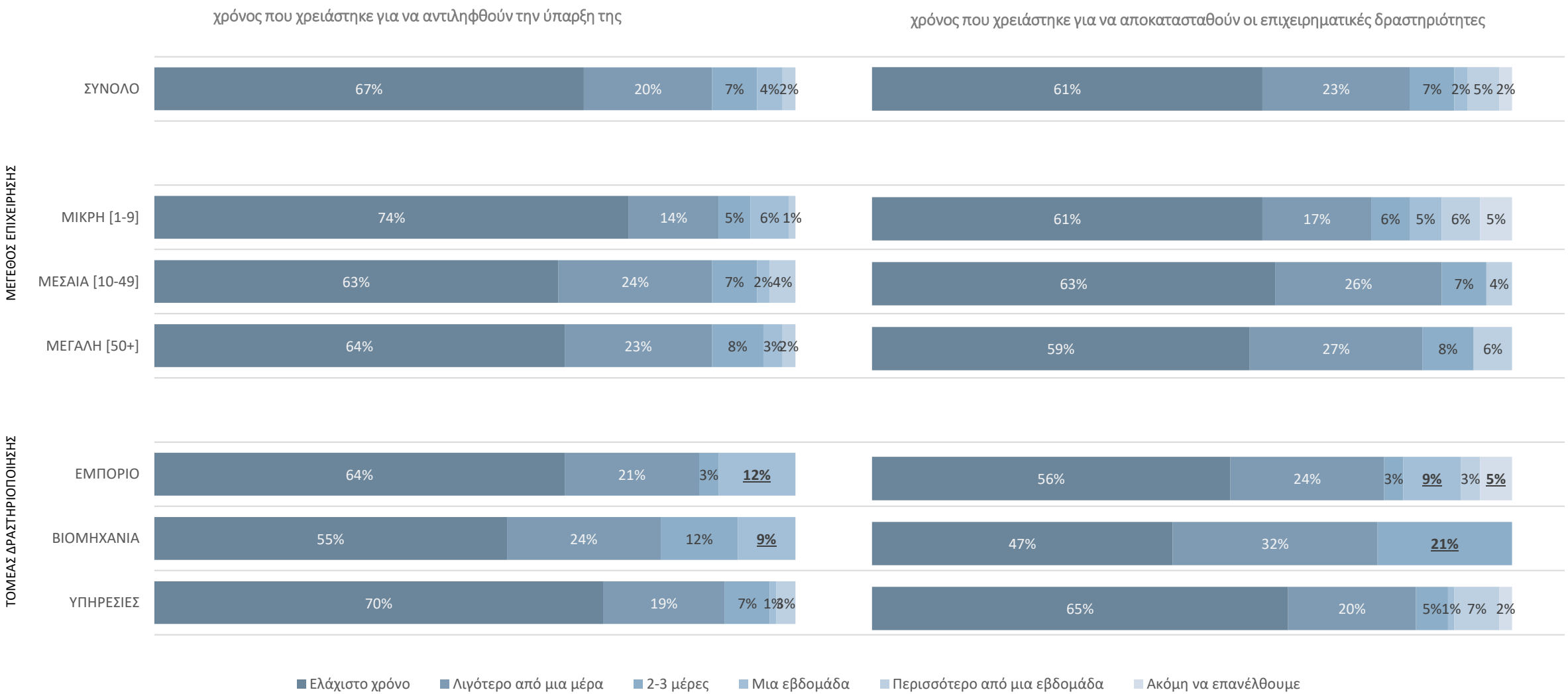
... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



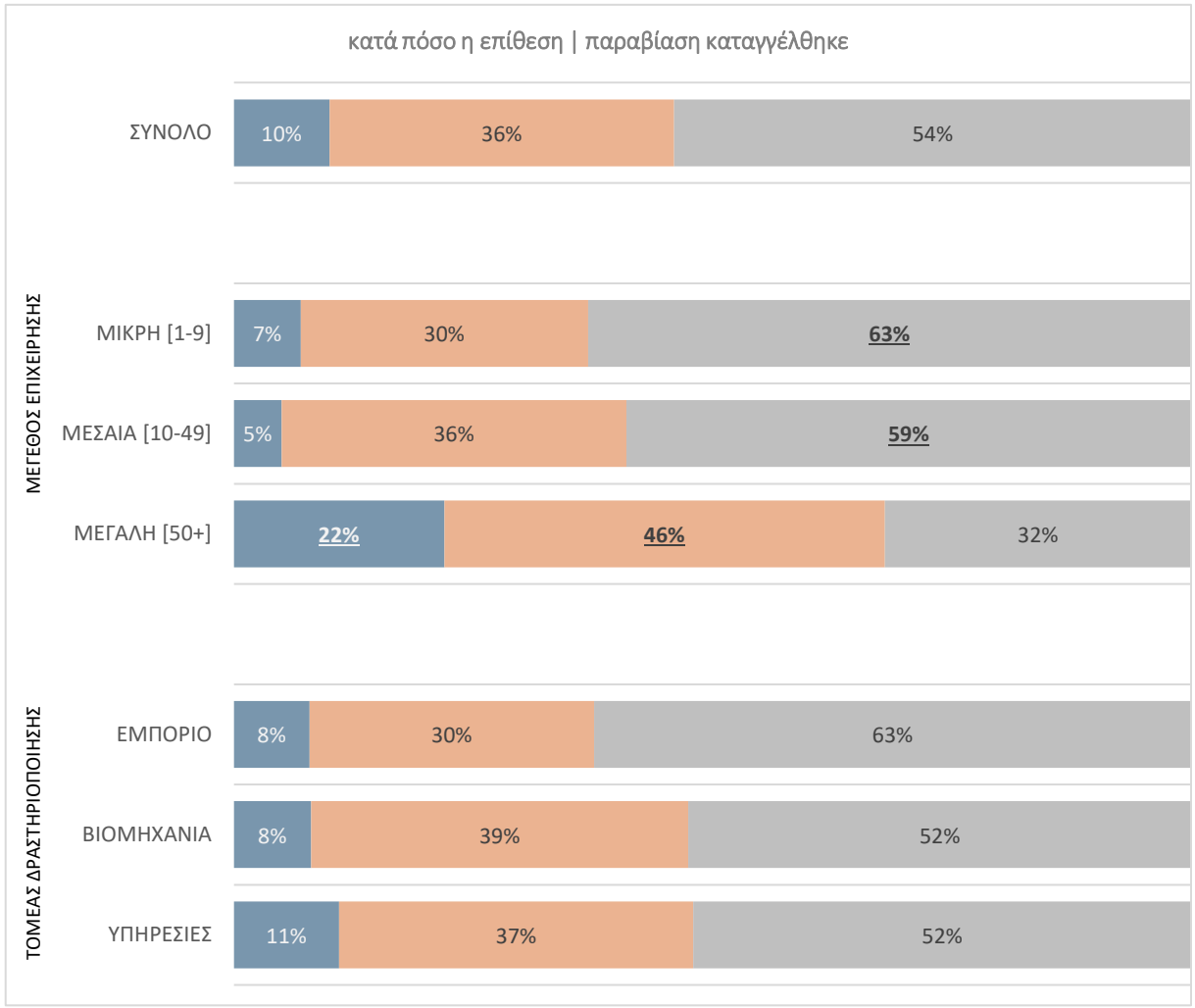
Σκεπτόμενοι την πιο πρόσφατη παραβίαση κυβερνοασφάλειας, που δεχτήκατε, πόσος χρόνος χρειάστηκε για να αντιληφθείτε την ύπαρξη της; | Και πόσος χρόνος χρειάστηκε για να αποκατασταθούν οι επιχειρηματικές σας δραστηριότητες;

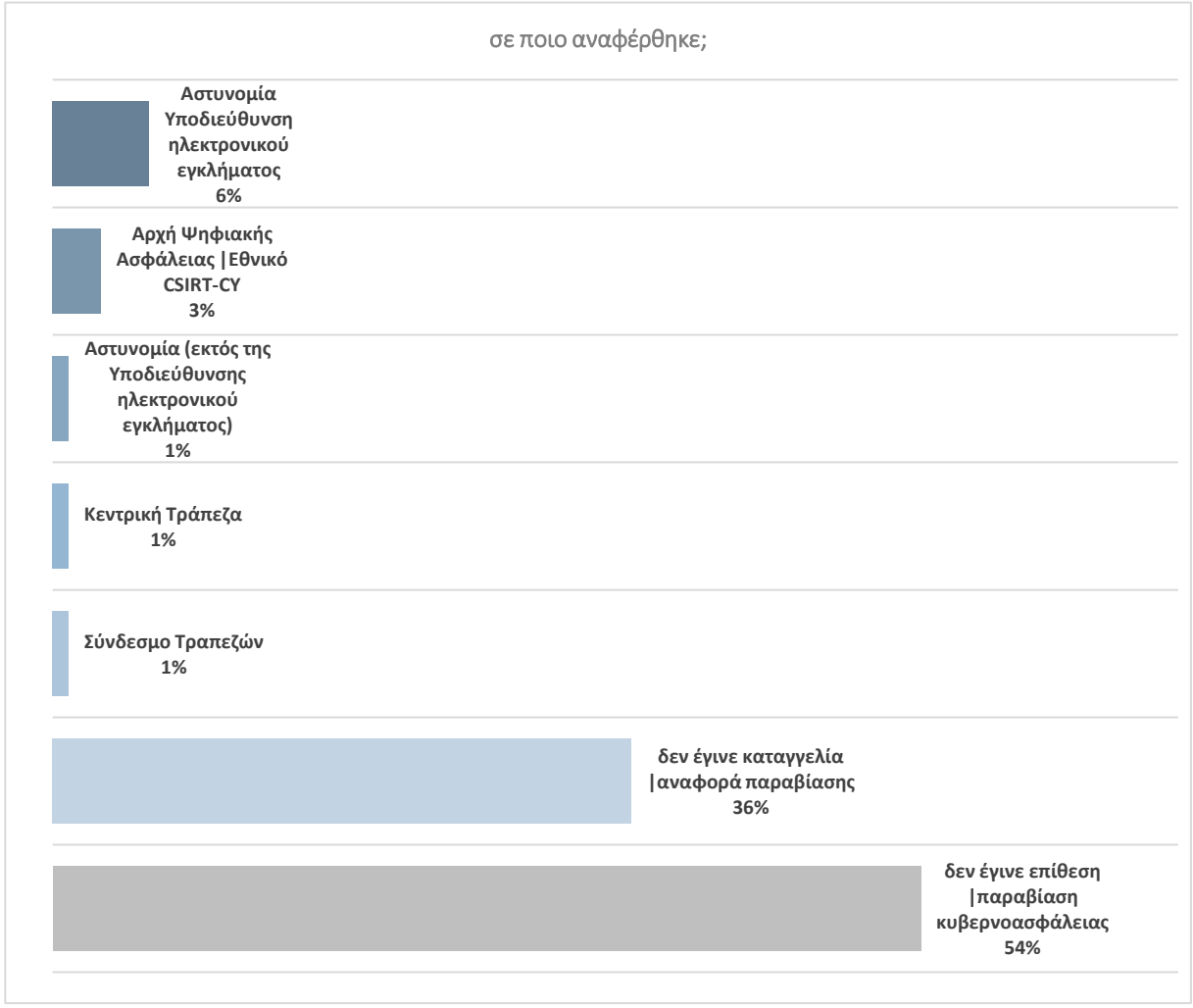
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



Αυτή η παραβίαση/επίθεση, καταγγέλθηκε ή αναφέρθηκε σε οποιονδήποτε ΕΚΤΟΣ του οργανισμού σας; | Σε ποιον/ποιους καταγγέλθηκε ή αναφέρθηκε;

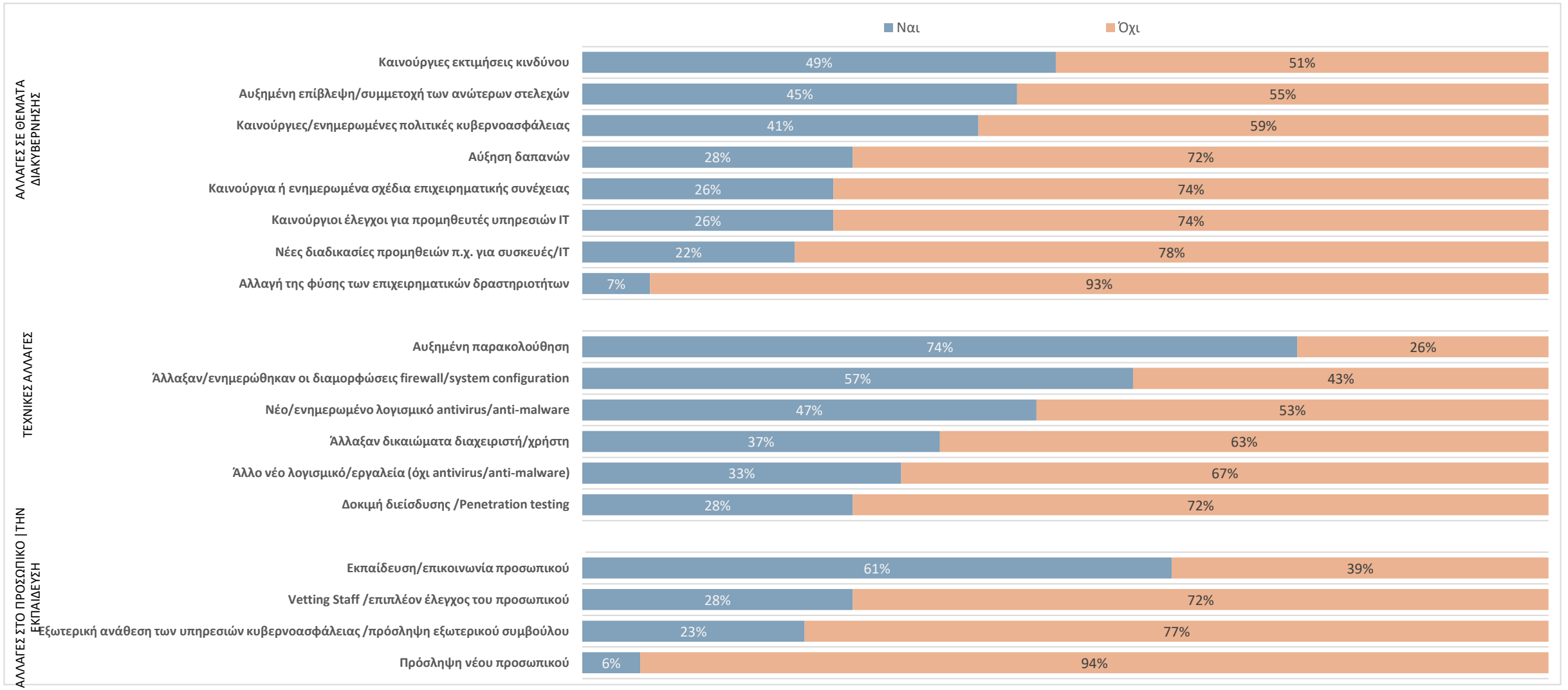
Βάση: Όλοι οι ερωτώμενοι





Μετά από αυτήν την παραβίαση| επίθεση, τι από τα ακόλουθα έχετε κάνει για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



Μετά από αυτήν την παραβίαση/επίθεση, τι *αλλαγές κάνατε σε σχέση με την διακυβέρνηση*, για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση

Μετά από αυτήν την παραβίαση/επίθεση, τι *αλλαγές κάνατε σε σχέση με την διακυβέρνηση*, για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

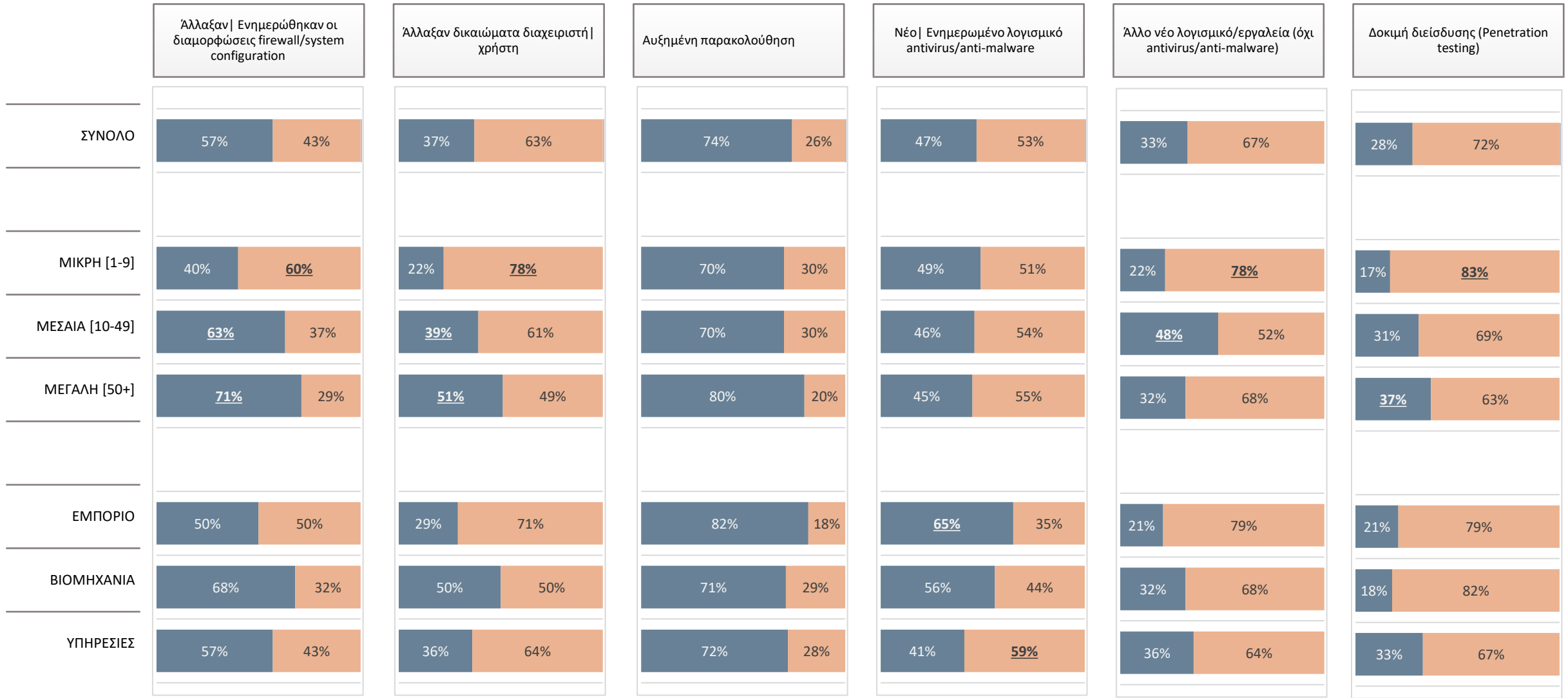
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση

... συνέχεια

Μετά από αυτήν την παραβίαση/επίθεση, τι *τεχνικές αλλαγές κάνατε*, για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

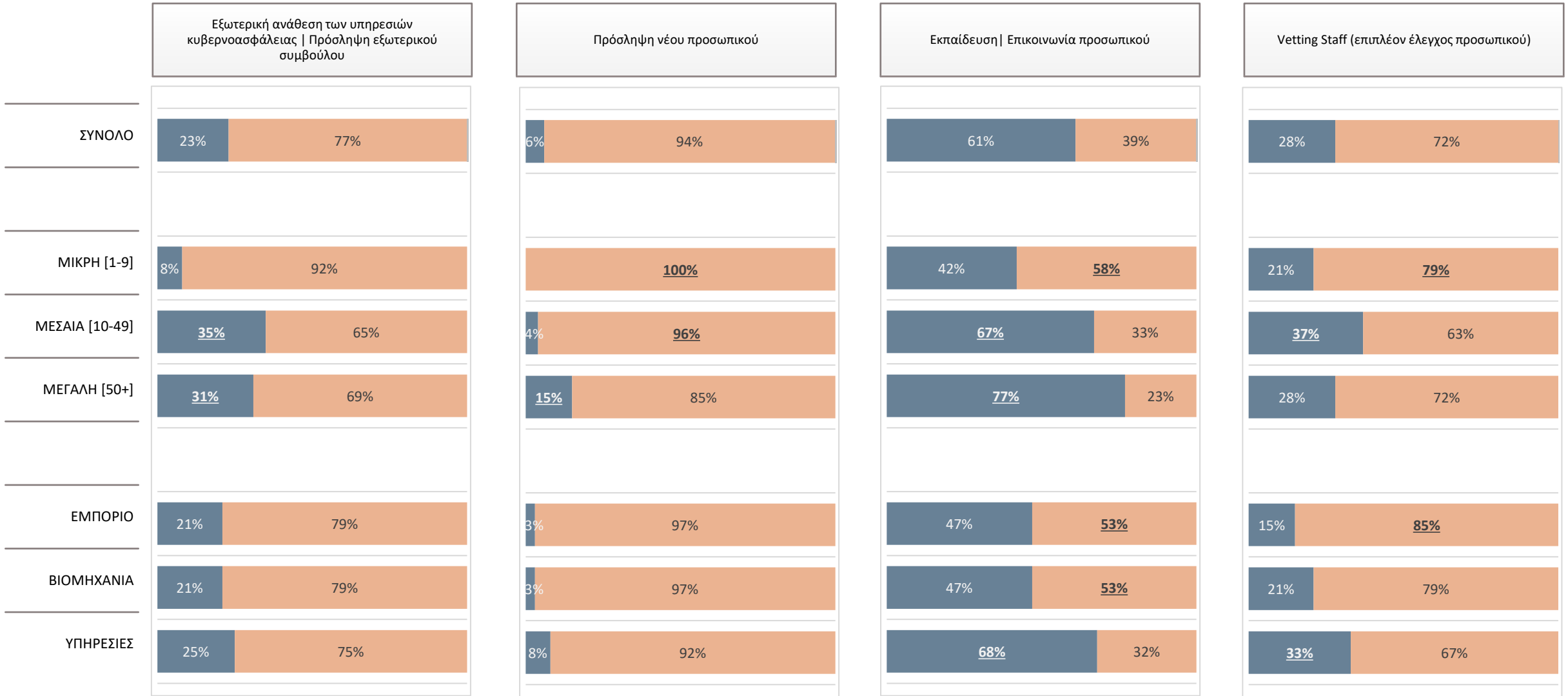
... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



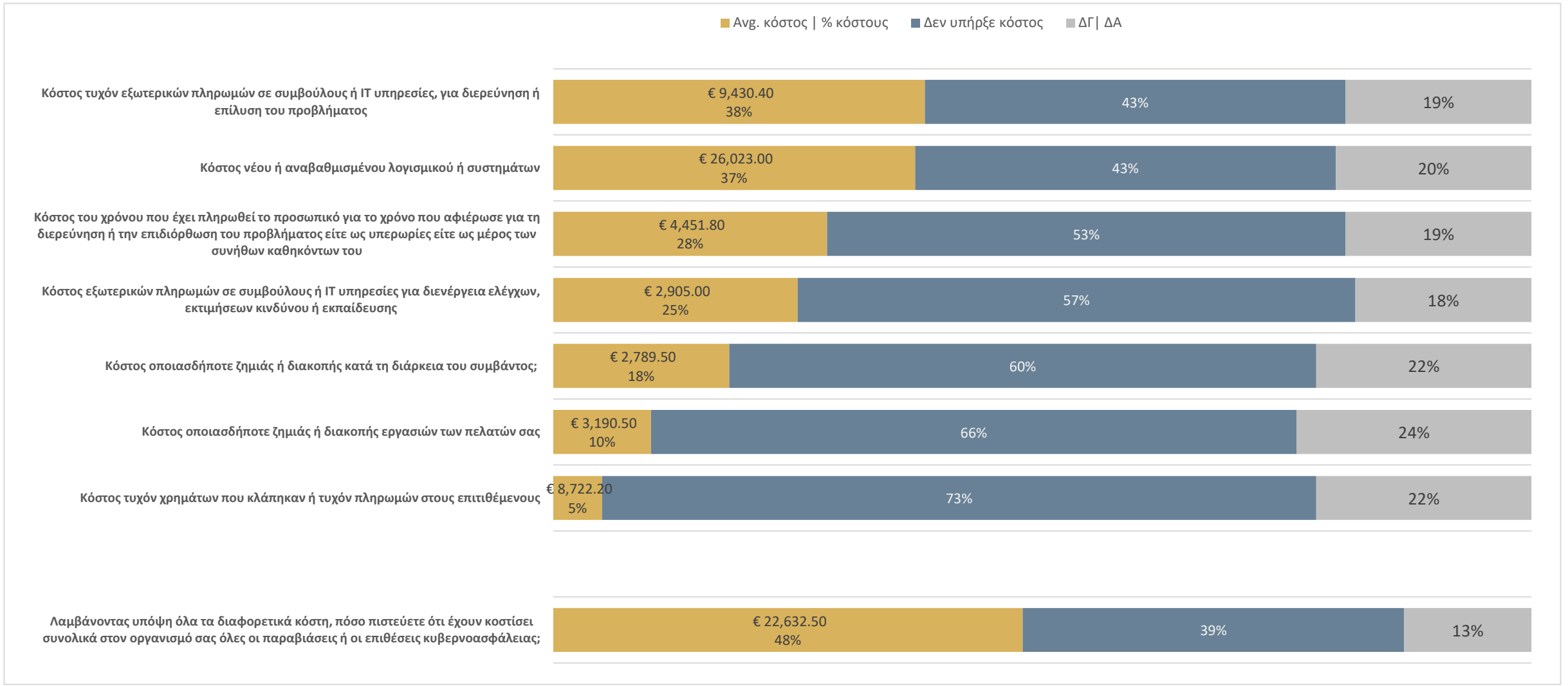
Μετά από αυτήν την παραβίαση/επίθεση, τι *αλλαγές κάνατε σε σχέση με την εκπαίδευση και το προσωπικό*, για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



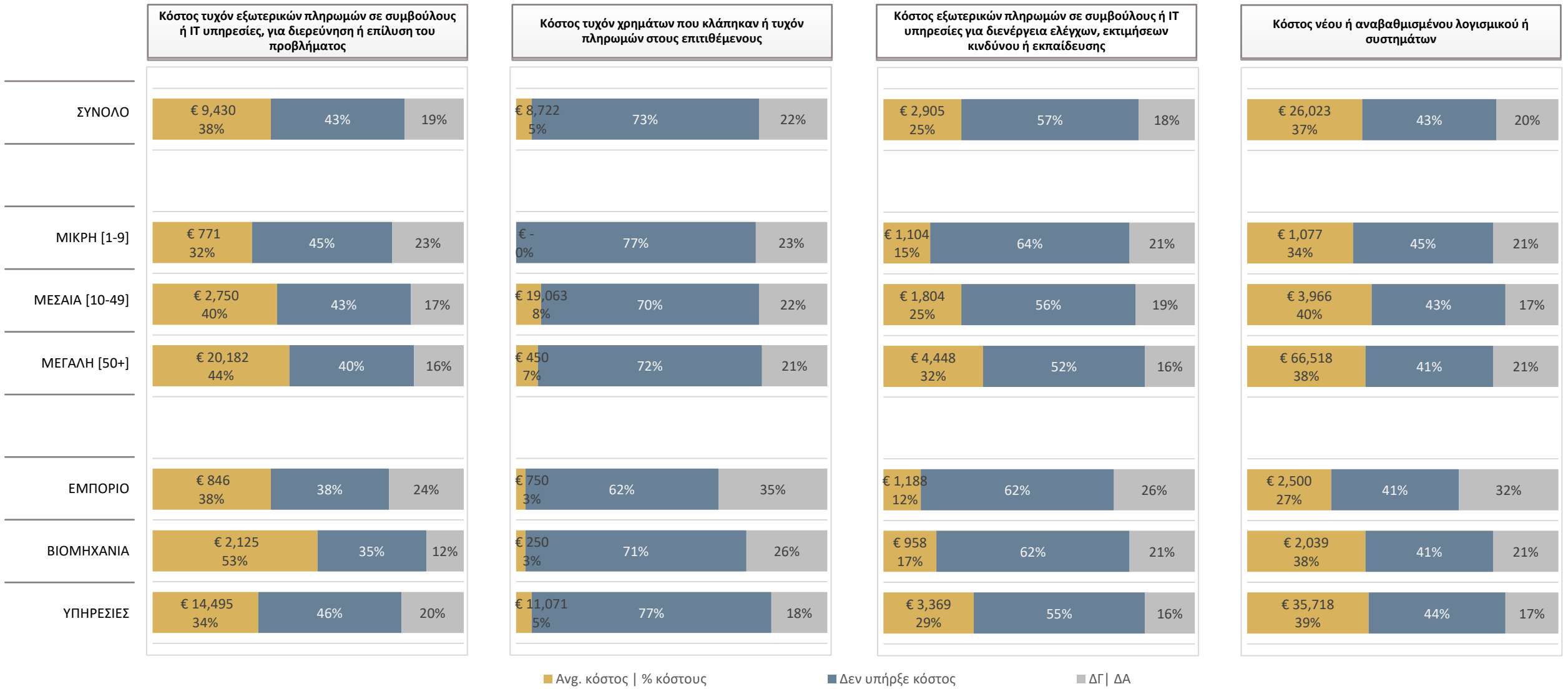
Ποια είναι, τα κατά προσέγγιση, κόστη, της πιο πρόσφατης παραβίασης| επίθεσης, που δεχτήκατε στην εταιρεία σας;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



Ποια είναι, τα κατά προσέγγιση, κόστη, της πιο πρόσφατης παραβίασης| επίθεσης, που δεχτήκατε στην εταιρεία σας;

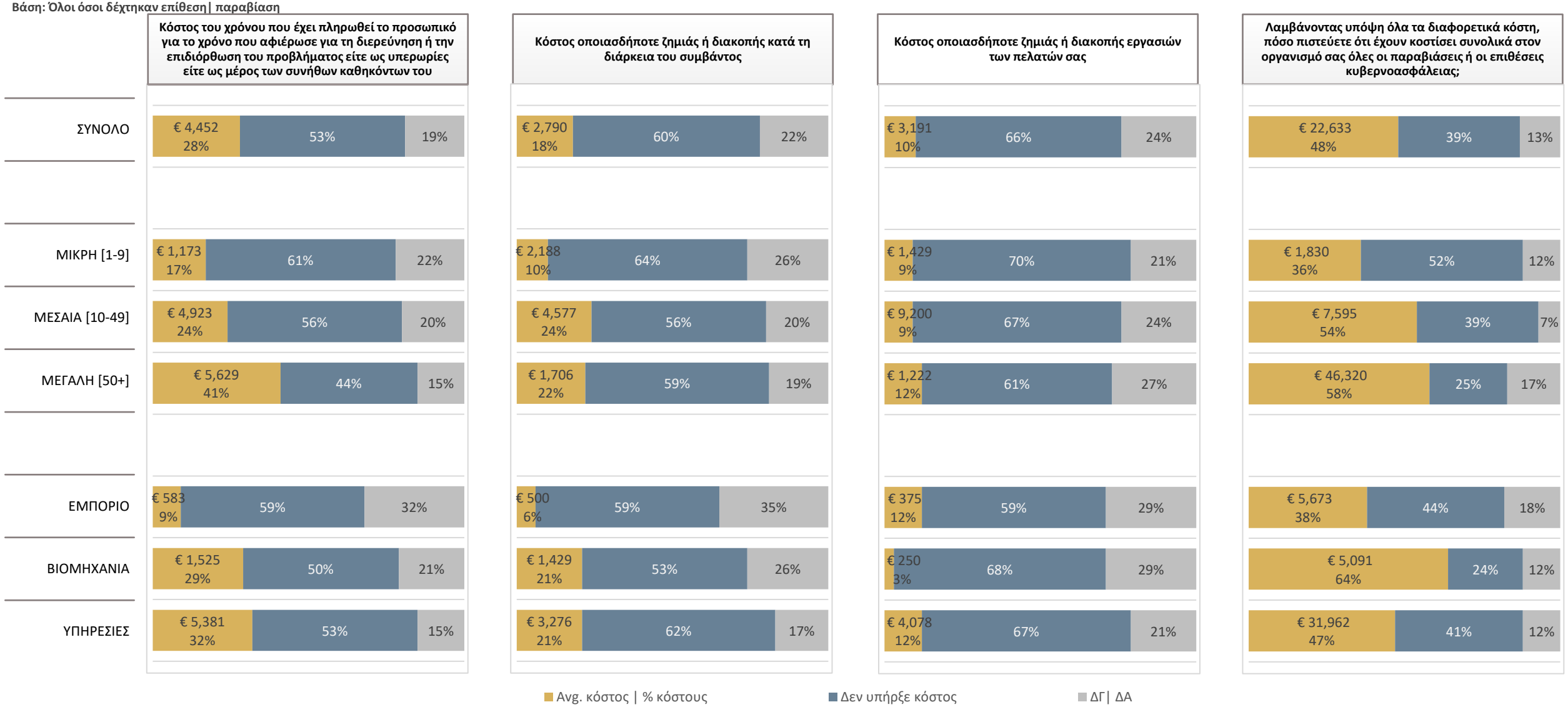
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



Ποια είναι, τα κατά προσέγγιση, κόστη, της πιο πρόσφατης παραβίασης| επίθεσης, που δεχτήκατε στην εταιρεία σας;

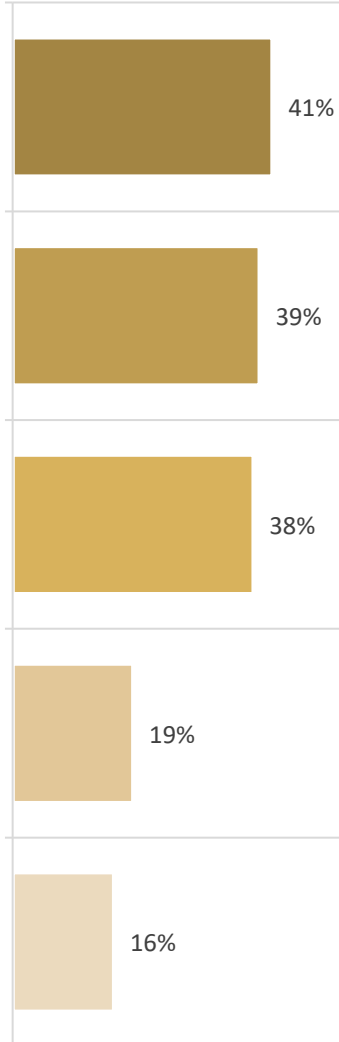
... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



Γιατί πιστεύετε ότι δεν είχατε κανένα περιστατικό παραβίασης ή επίθεσης κυβερνοασφάλειας;

Βάση: Όλοι όσοι δεν δέχτηκαν επίθεση| παραβίαση

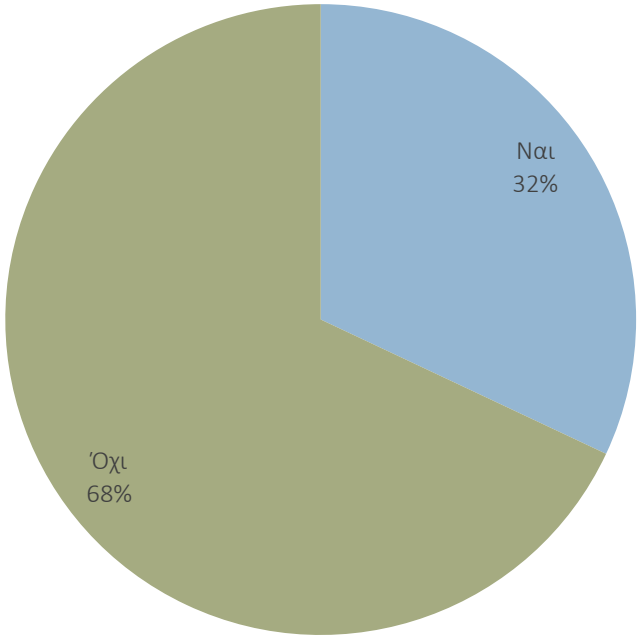


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Η εταιρία μας δεν αποτελεί 'στόχο'	**52%**	**36%**	14%	51%	43%	37%
Καλή προετοιμασία	25%	**51%**	**64%**	28%	**57%**	39%
Έγκαιρη λήψη μέτρων	19%	**56%**	**64%**	32%	43%	39%
Σωστή εκπαίδευση προσωπικού	6%	**31%**	**42%**	12%	22%	21%
Μπορεί να υπήρξαμε θύμα και δεν το αντιληφθήκαμε	16%	13%	25%	14%	8%	19%

Τους τελευταίους 12 μήνες, έχετε πραγματοποιήσει κάποια εκπαίδευση ή ενημέρωση για θέματα κυβερνοασφάλειας, για το προσωπικό, που ΔΕΝ εμπλέκεται άμεσα στα θέματα αυτά; | Σε ποια μέλη του προσωπικού;

Βάση: Όλοι οι ερωτώμενοι

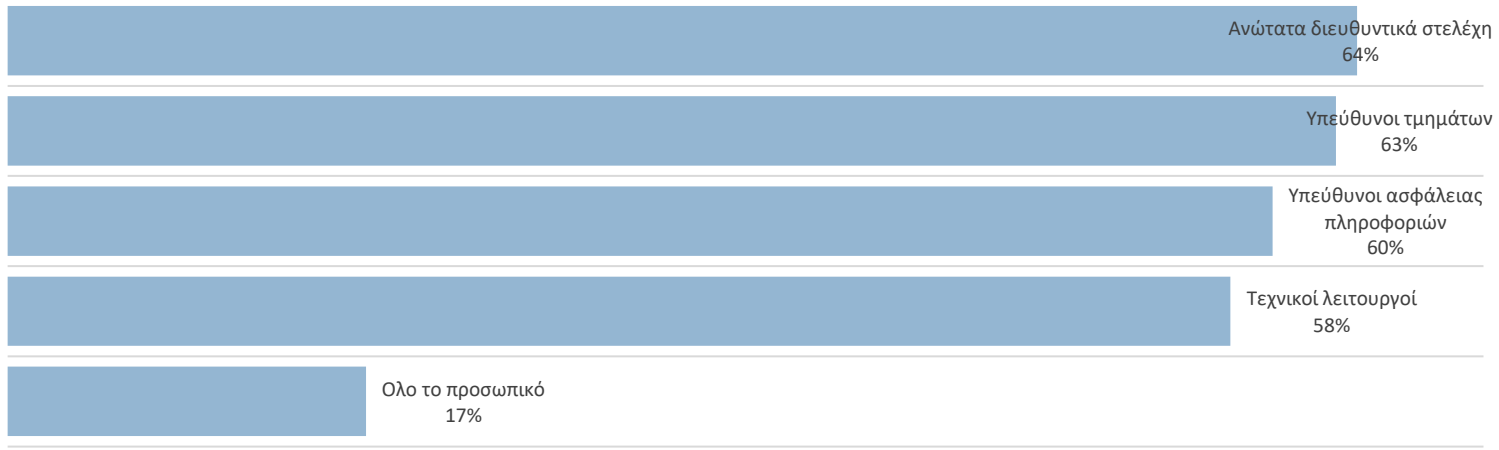
έχετε πραγματοποιήσει κάποια εκπαίδευση ή ενημέρωση για θέματα κυβερνοασφάλειας, για το προσωπικό;



	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Ναι	15%	**41%**	**54%**	12%	24%	**41%**
Όχι	**85%**	59%	46%	88%	76%	59%

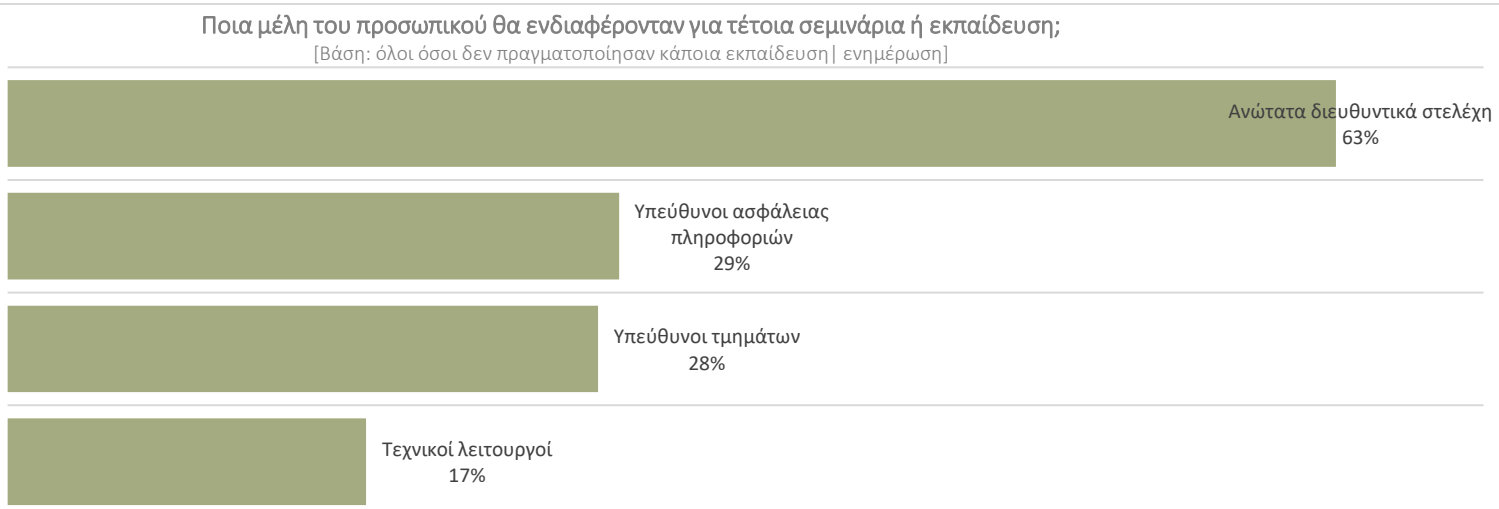
Ποια μέλη του προσωπικού έλαβαν μέρος στα σεμινάρια/εκπαίδευση;

[Βάση: όλοι όσοι πραγματοποίησαν κάποια εκπαίδευση| ενημέρωση]



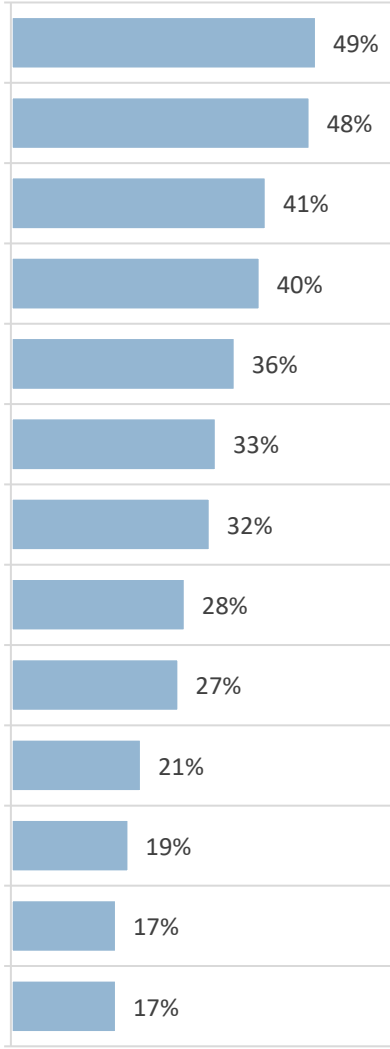
Ποια μέλη του προσωπικού θα ενδιαφέρονταν για τέτοια σεμινάρια ή εκπαίδευση;

[Βάση: όλοι όσοι δεν πραγματοποίησαν κάποια εκπαίδευση| ενημέρωση]



Σε ποια από τα παρακάτω θέματα θα προτιμούσατε να εστιάζουν τα σεμινάρια κατάρτισης;

Βάση: Όλοι οι ερωτώμενοι



		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Αξιολόγηση και διαχείριση κινδύνων κυβερνοασφάλειας	49%	40%	48%	**68%**	38%	52%	**52%**
Κατευθυντήριες γραμμές και μέτρα κυβερνοασφάλειας (για μικρομεσαίες επιχειρήσεις)	48%	42%	**56%**	48%	30%	**56%**	**51%**
Ανάπτυξη δυνατοτήτων κυβερνοασφάλειας και καλλιέργεια κουλτούρας ασφάλειας στις επιχειρήσεις	41%	31%	**43%**	**56%**	35%	46%	41%
Ευκαιρίες χρηματοδότησης και αξιοποίησης κονδυλίων για ανάπτυξη της κυβερνοασφάλειας στις επιχειρήσεις	40%	30%	**50%**	**46%**	35%	42%	41%
Αντιμετώπιση κυβερνοεπιθέσεων και αδικημάτων στον κυβερνοχώρο	36%	28%	**39%**	**47%**	32%	31%	38%
Θέματα κυβερνοασφάλειας τα οποία εστιάζουν στον τομέα δραστηριοποίησης της εταιρείας	33%	29%	36%	37%	20%	**35%**	**37%**
Έρευνα και καινοτομία για θέματα κυβερνοασφάλειας	32%	29%	33%	39%	27%	30%	34%
Ο ρόλος της Αρχής Ψηφιακής Ασφάλειας και του Εθνικού CSIRT-CY και οι υπηρεσίες που παρέχουν στον ιδιωτικό τομέα	28%	21%	**31%**	37%	21%	27%	30%
Κατευθυντήριες γραμμές και μέτρα κυβερνοασφάλειας (για μεγάλες επιχειρήσεις)	27%	16%	26%	**50%**	35%	23%	26%
Στρατηγική κυβερνοασφάλειας της Κυπριακής Δημοκρατίας	21%	15%	20%	**31%**	14%	**34%**	19%
Εθνικό πλαίσιο κυβερνοασφάλειας	19%	12%	**23%**	**26%**	15%	21%	19%
Δομές κυβερνοασφάλειας στην Κυπριακή Δημοκρατία	17%	11%	18%	**27%**	14%	14%	19%
Το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (NCCC-CY) και τα κίνητρα για τη συμμετοχή των επιχειρήσεων στην Κοινότητα...	17%	11%	**21%**	**24%**	13%	18%	18%

ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ ΣΕ ΣΧΕΣΗ ΜΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ & ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΕΤΟΙΜΑΣΤΗΚΕ ΓΙΑ ΤΗΝ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΝΕΟΜΒΡΙΟΣ 2022

RAI Consultants Ltd

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ