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

ΕΤΟΙΜΑΣΤΗΚΕ ΓΙΑ ΤΗΝ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΝΟΕΜΒΡΙΟΣ 2025

RAI Consultants Ltd

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

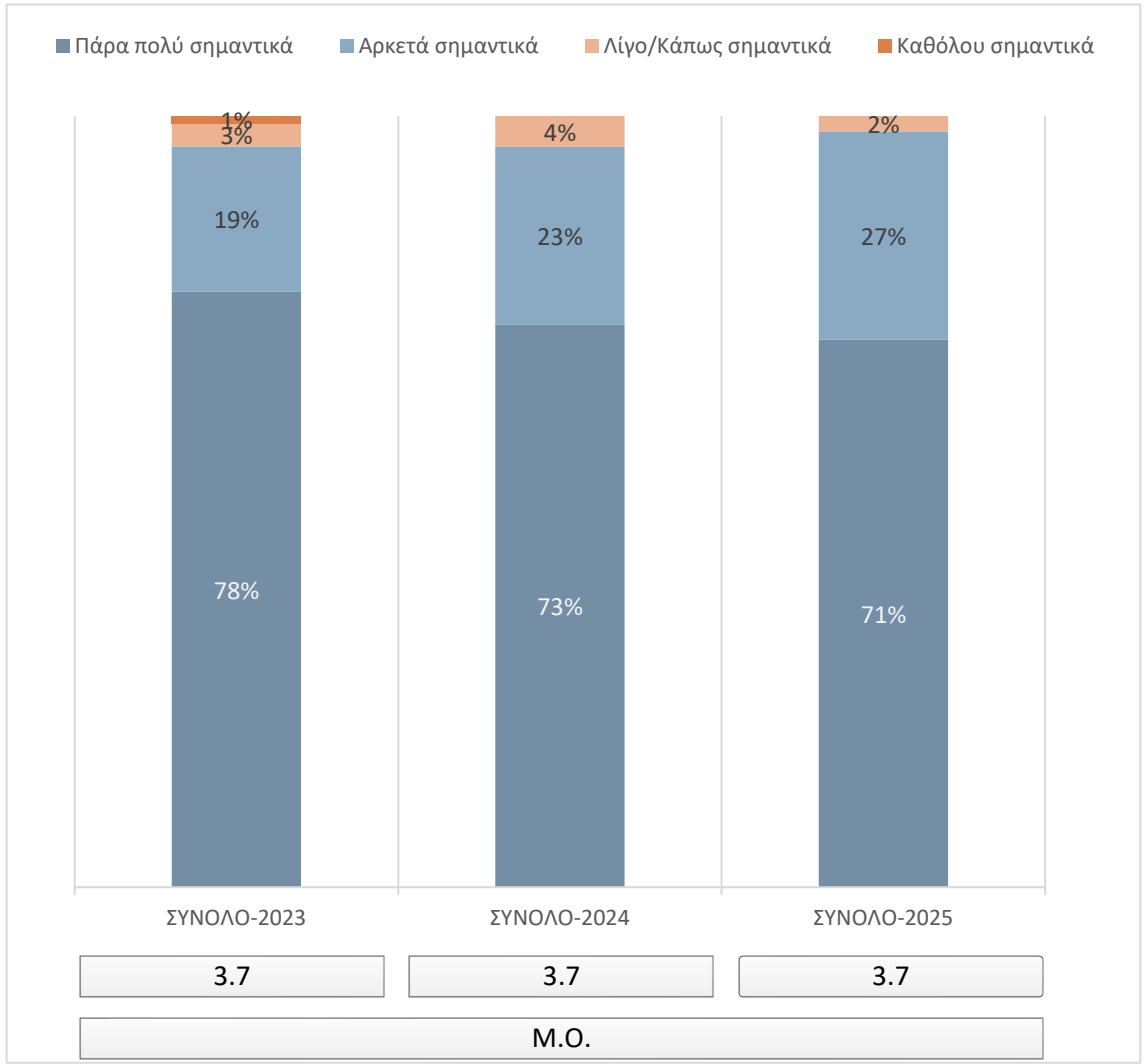
Εισαγωγή & Μεθοδολογία

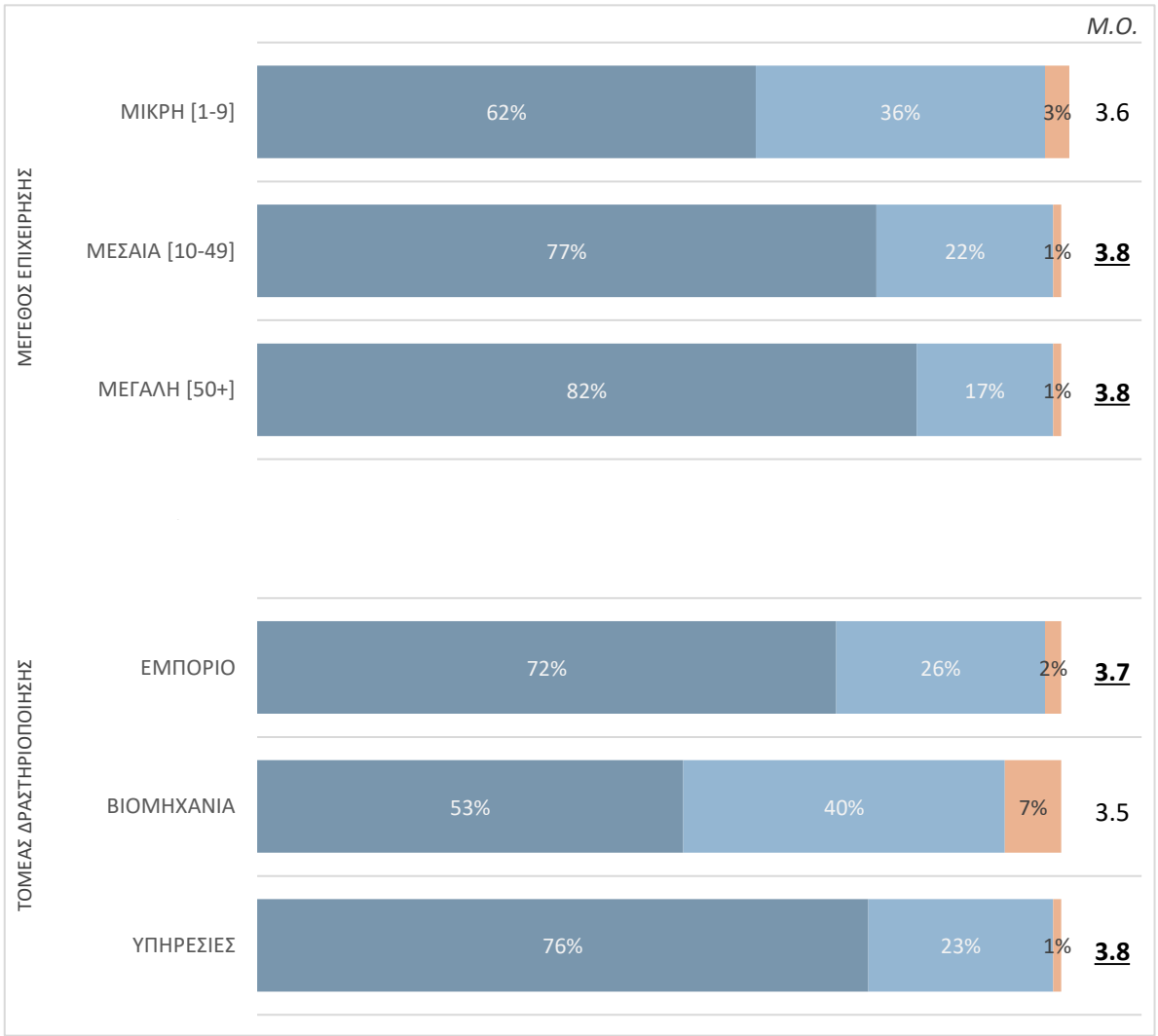
Αντικείμενο Μελέτης	Αντικείμενο της Σύμβασης αποτελεί η Παροχή Υπηρεσιών διεξαγωγής έρευνας σε επιχειρήσεις, σε σχέση με τον τρόπο χειρισμού θεμάτων κυβερνοασφάλειας, αποτίμησης της σημαντικότητας που αποδίδεται στα θέματα κυβερνοασφάλειας, τον τρόπο αντιμετώπισης περιστατικών κυβερνοασφάλειας ή/και 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 **459** επιτυχείς συνεντεύξεις εκ των οποίων:	198 επιχειρήσεις είχαν συνολικό αριθμό απασχολουμένων μέχρι 9 άτομα (Μικρή) 162 επιχειρήσεις είχαν συνολικό αριθμό απασχολουμένων 10-49 άτομα (Μεσαία) 99 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	Σεπτέμβριος - Νοέμβριος 2025	
Σύγκριση αποτελεσμάτων	Τα αποτελέσματα του έργου συγκρίνονται με τα αποτελέσματα της ίδιας έρευνας που διεξάχθηκαν τον Νοέμβριο 2023 &τον Οκτώβριο 2024	

ΑΝΑΛΥΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

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

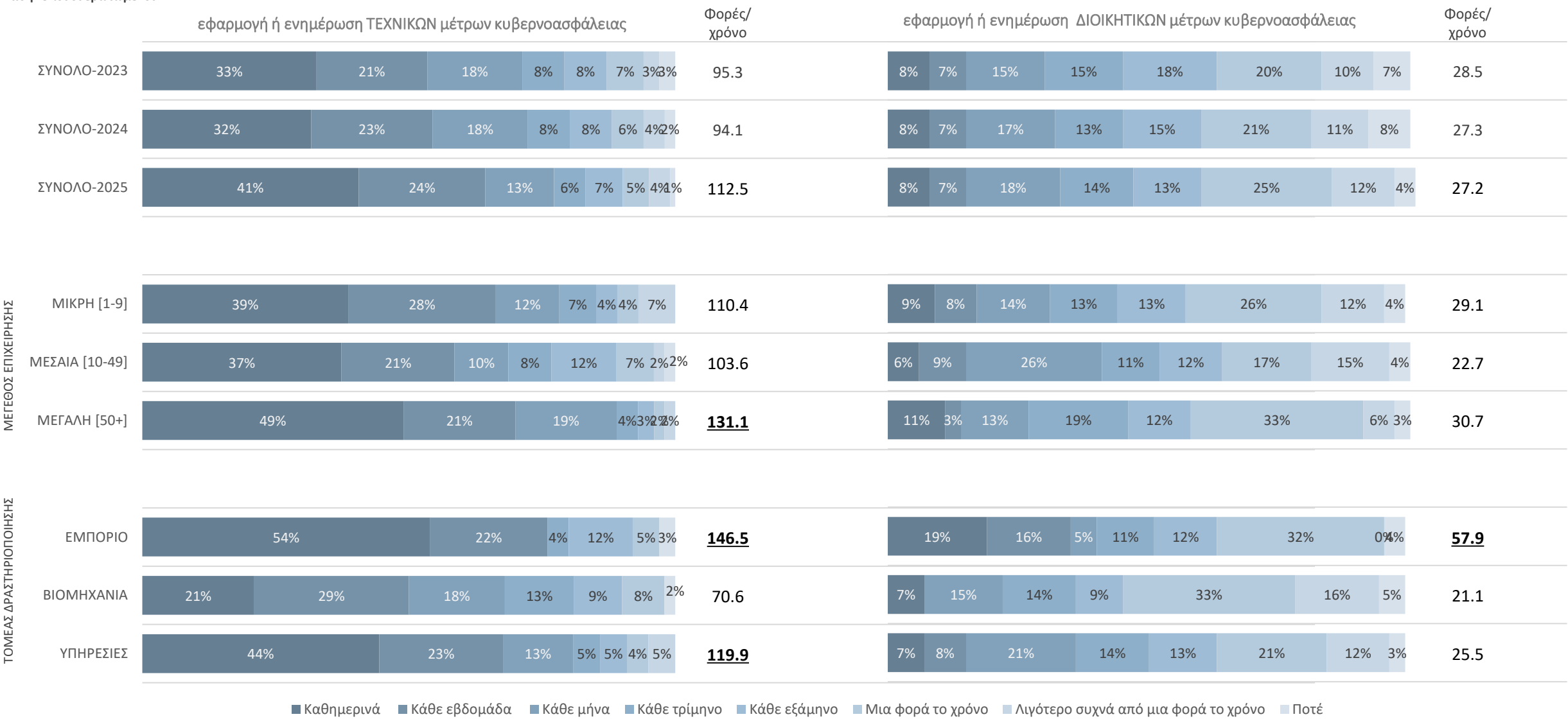
Βάση: Όλοι οι ερωτώμενοι





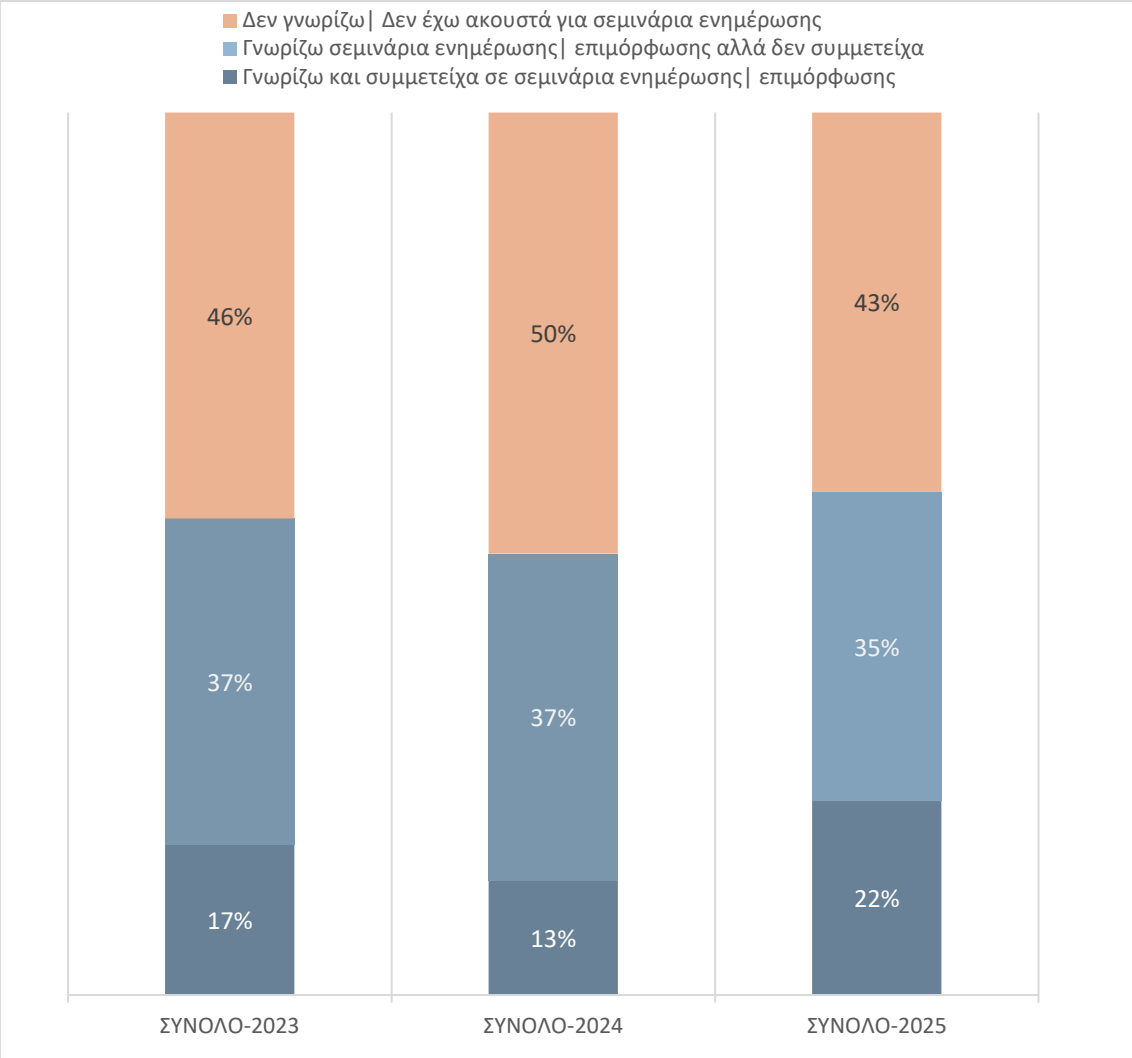
Πόσο συχνά προβαίνει η εταιρία σας σε εφαρμογή ή ενημέρωση ΤΕΧΝΙΚΩΝ | ΔΙΟΙΚΗΤΙΚΩΝ μέτρων κυβερνοασφάλειας;

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;

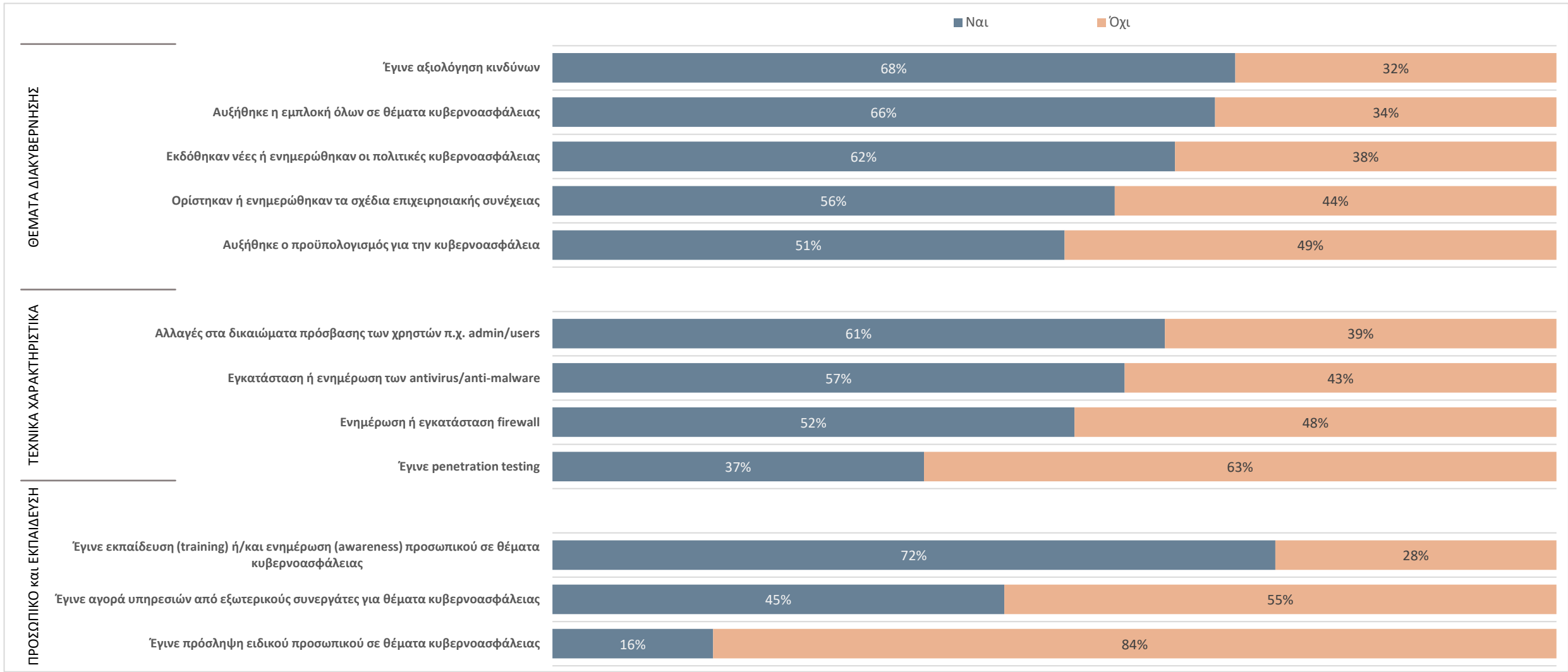
Βάση: Όλοι οι ερωτώμενοι



	Γνώση	Συμμετοχή
Σερφάρω στο Διαδίκτυο με Ασφάλεια (ΚΕΠΑ)	24%	6%
DIGITAL SECURITY STAKEHOLDERS CONFERENCE (ΑΨΑ| Εθνικό CSIRT-CY)	23%	11%
Cyberbullying - Εκφοβισμός μέσω Διαδικτύου (CYTA)	21%	4%
Ημερίδα για τη Διεθνή Ημέρα Ασφαλούς Διαδικτύου	17%	5%
Course on Cybersecurity Organisational and Defensive Capabilities (ΑΨΑ|Εθνικό CSIRT-CY ESDC)	16%	5%
CyberSafety: Ένα Καλύτερο Διαδίκτυο για τα Παιδιά στην Κύπρο (ΣΧΟΛΗ ΓΟΝΕΩΝ)	13%	3%
Μαθητική Ημερίδα "Ασφαλές διαδίκτυο για όλους" (ΥΠ.ΠΑΙΔΕΙΑΣ)	9%	0%
ITU Cyber Drill - ALERT (Applied Learning for Emergency Response Teams)	4%	2%
"Together for a better internet"	3%	2%
Seminars by ICTAcademy/NIS2res	2%	2%

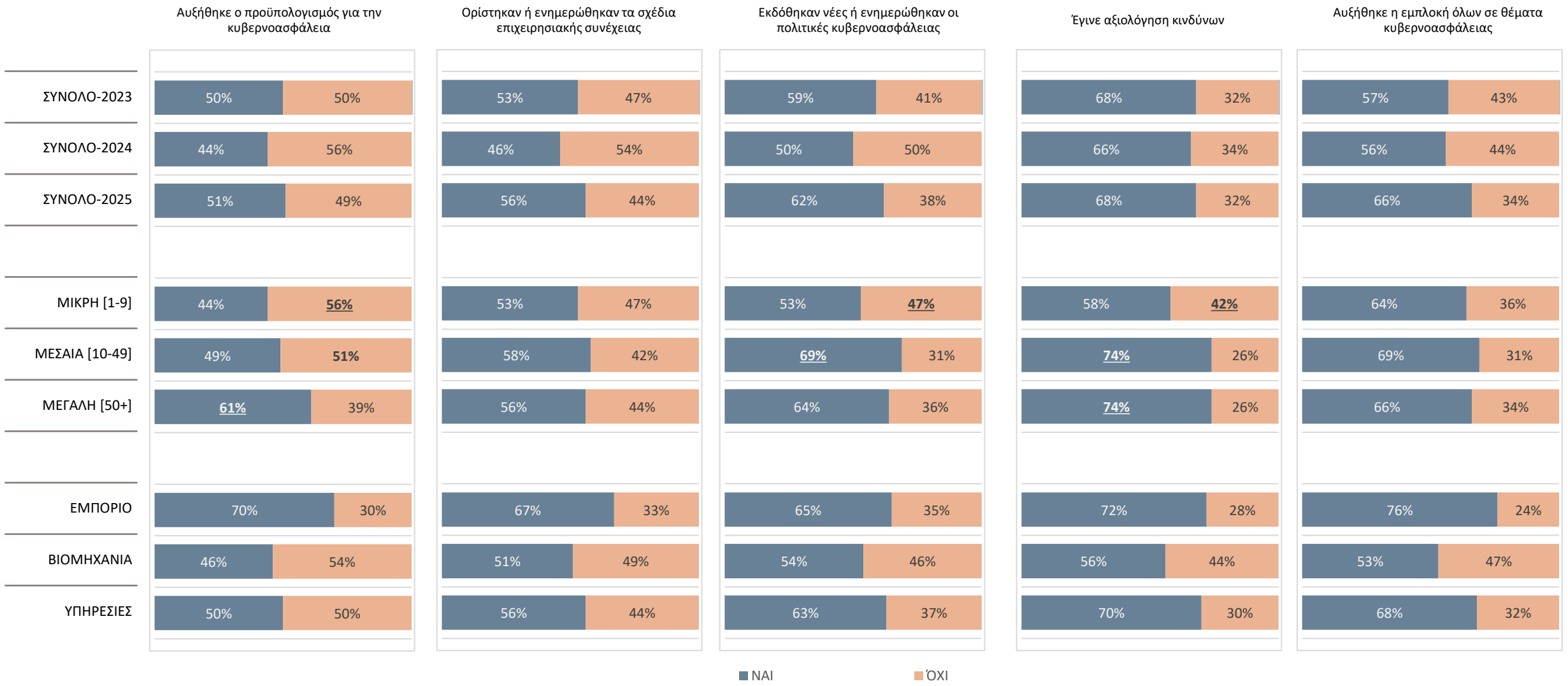
Τι από τα ακόλουθα έχετε αλλάξει σε θέματα κυβερνοασφάλειας, εξαιτίας αυτών των σεμιναρίων;

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

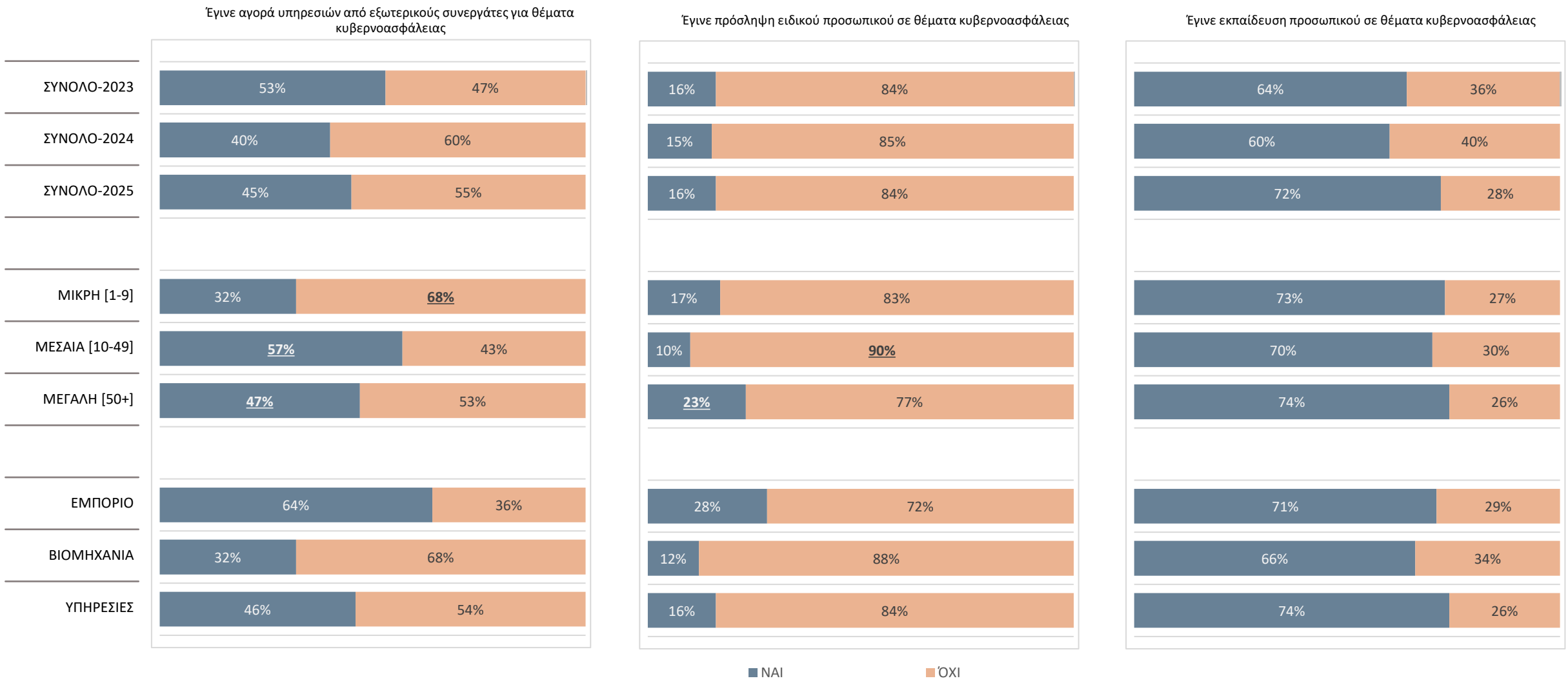


Τι από τα ακόλουθα ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ, έχετε αλλάξει εξαιτίας αυτών των σεμιναρίων;

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

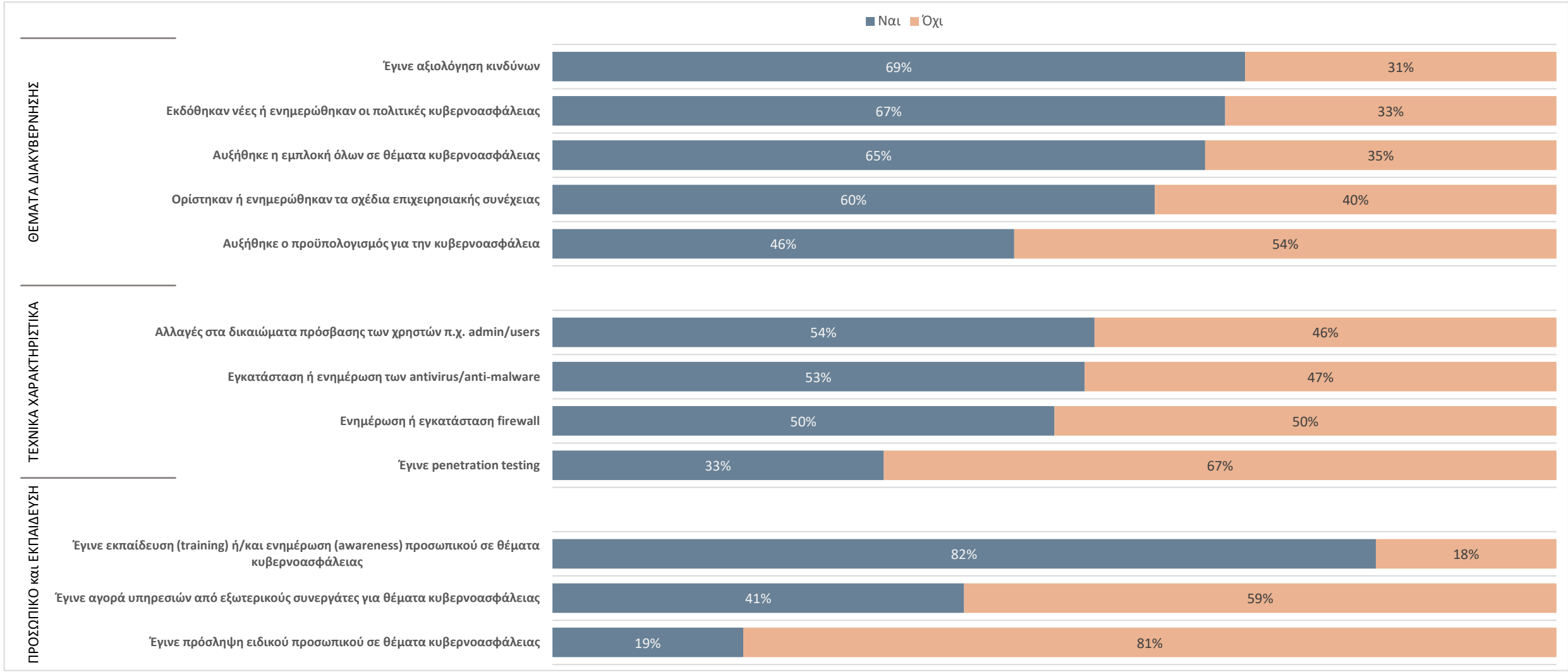
Και τι από τα ακόλουθα έχετε αλλάξει όσον αφορά στο ΠΡΟΣΩΠΙΚΟ και ΕΚΠΑΙΔΕΥΣΗ του προσωπικού;

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



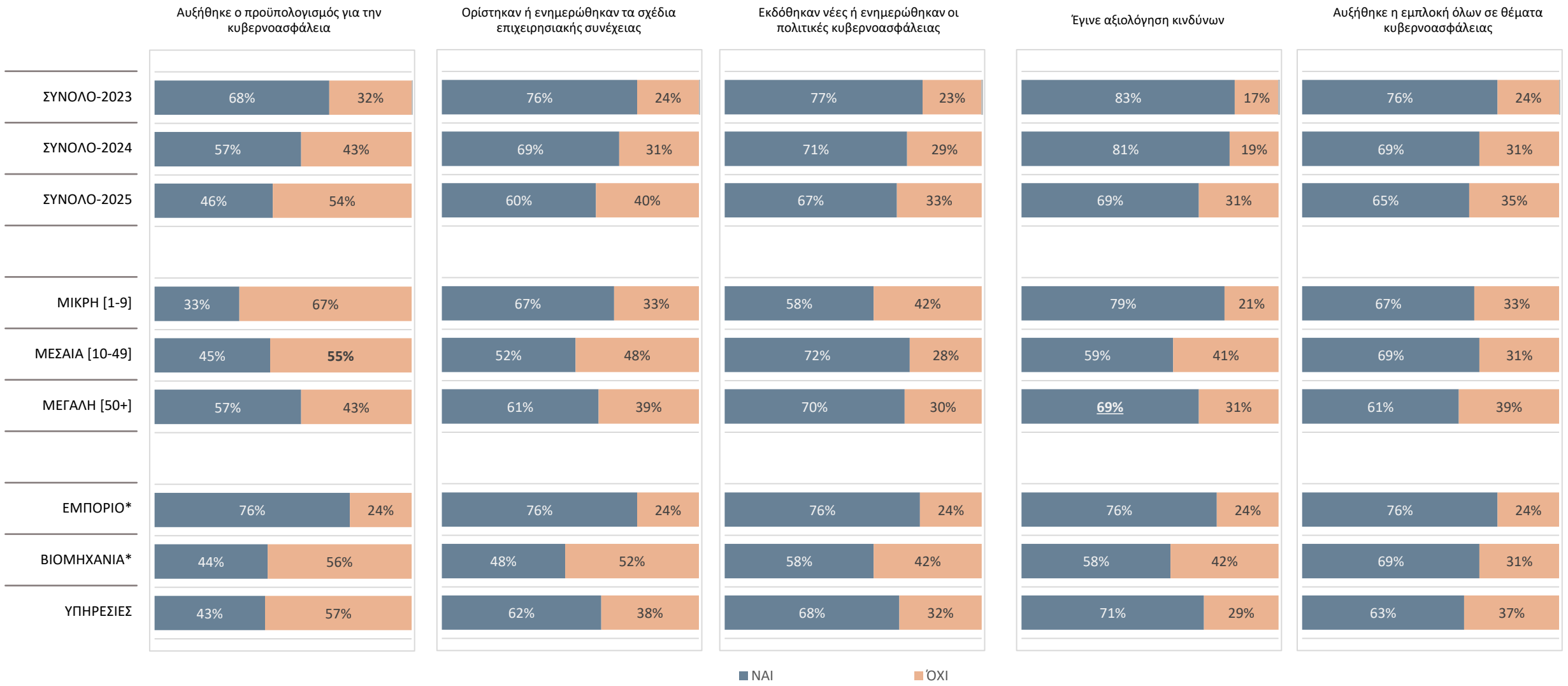
Τι από τα ακόλουθα έχετε αλλάξει σε θέματα κυβερνοασφάλειας, εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι ΣΥΜΜΕΤΕΙΧΑΝ 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;

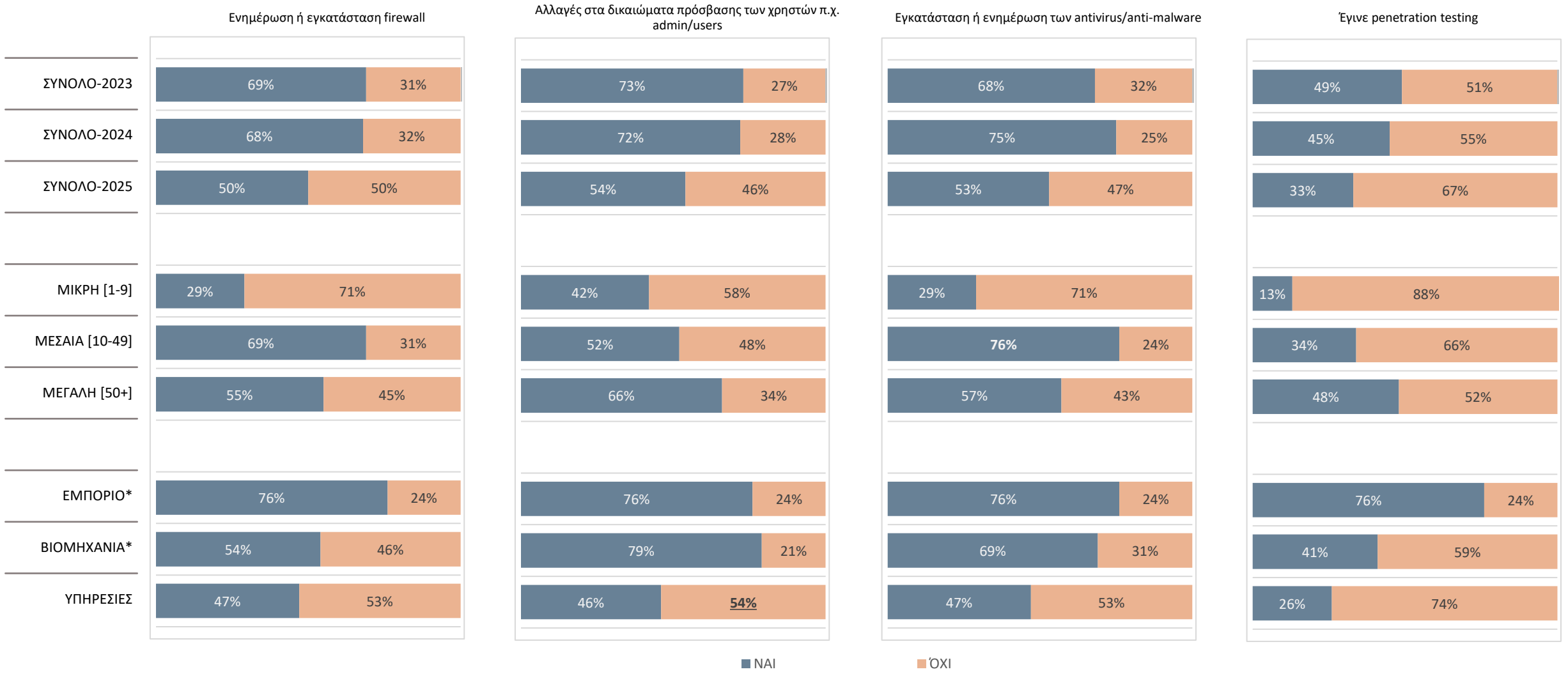
Βάση: Όλοι όσοι ΣΥΜΜΕΤΕΙΧΑΝ σε σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια



** Πολύ μικρός αριθμός ατόμων | στατιστικά μη σημαντικό*

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

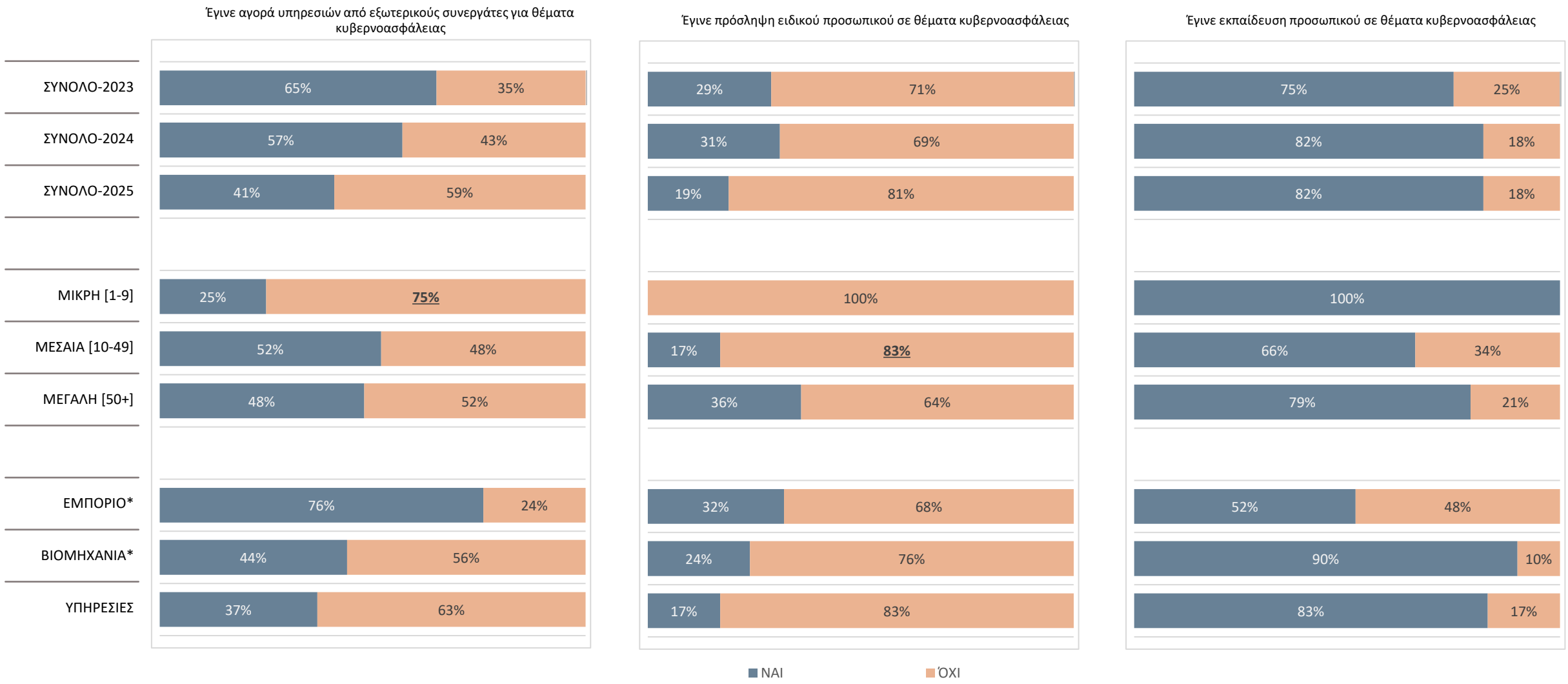
Βάση: Όλοι όσοι ΣΥΜΜΕΤΕΙΧΑΝ σε σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια



** Πολύ μικρός αριθμός ατόμων | στατιστικά μη σημαντικό*

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

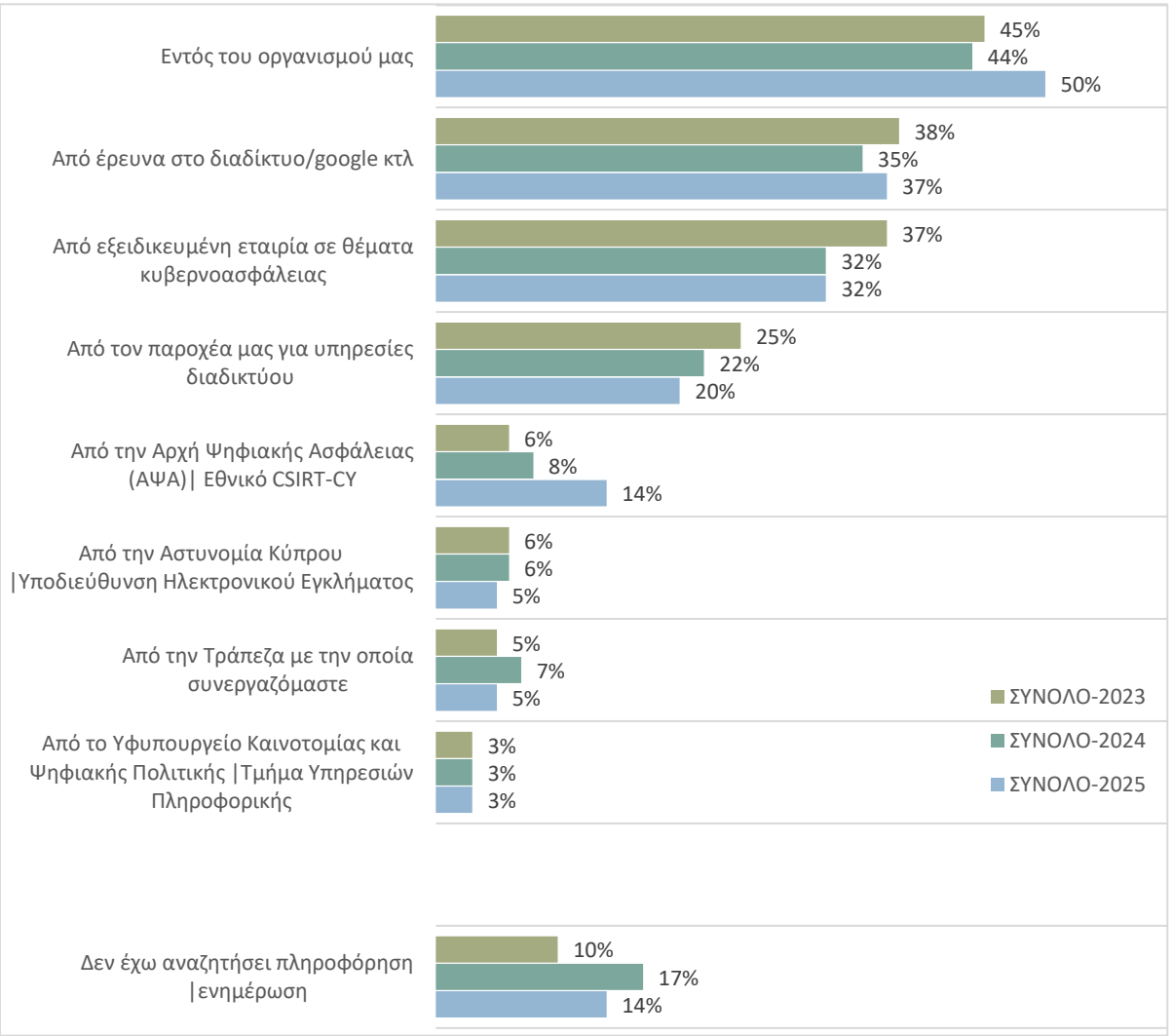
Βάση: Όλοι όσοι ΣΥΜΜΕΤΕΙΧΑΝ σε σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια



** Πολύ μικρός αριθμός ατόμων | στατιστικά μη σημαντικό*

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

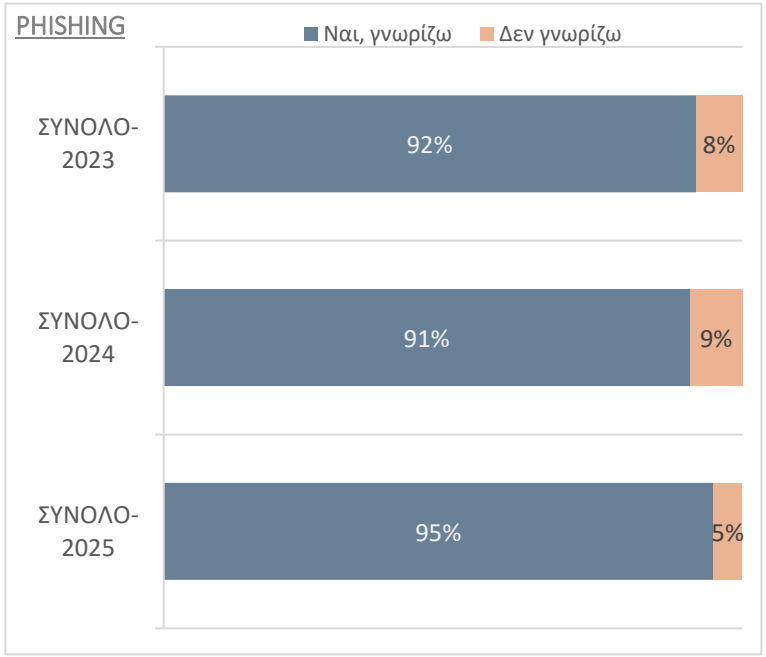
Βάση: Όλοι οι ερωτώμενοι

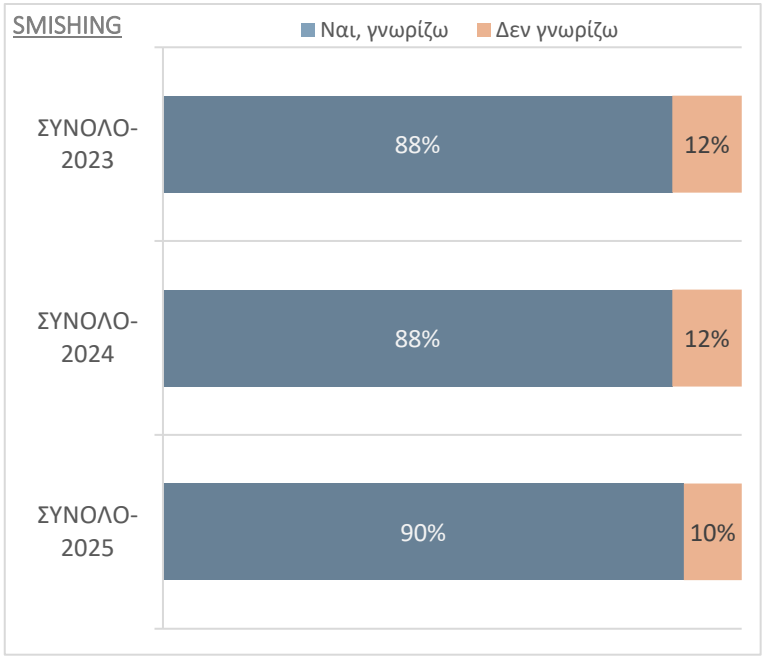


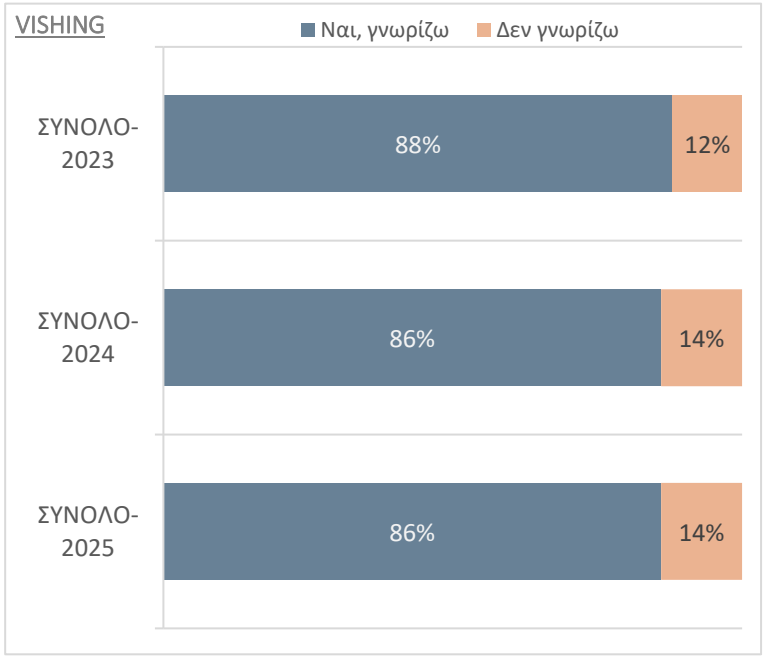
	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Εντός του οργανισμού μας	47%	51%	55%	**67%**	42%	51%
Από έρευνα στο διαδίκτυο/google κτλ	41%	35%	33%	**44%**	23%	**40%**
Από εξειδικευμένη εταιρία σε θέματα κυβερνοασφάλειας	22%	**33%**	**49%**	**44%**	25%	32%
Από τον παροχέα μας για υπηρεσίες διαδικτύου	17%	22%	19%	**39%**	19%	17%
Από την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)| Εθνικό CSIRT-CY	14%	8%	**23%**	5%	10%	15%
Από την Αστυνομία Κύπρου |Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος	4%	7%	6%	5%	3%	6%
Από την Τράπεζα με την οποία συνεργαζόμαστε	5%	3%	8%	**17%**	5%	4%
Από το Υφυπουργείο Καινοτομίας και Ψηφιακής Πολιτικής |Τμήμα Υπηρεσιών Πληροφορικής	1%	2%	**7%**	0%	4%	3%
Δεν έχω αναζητήσει πληροφόρηση |ενημέρωση	17%	12%	10%	8%	**21%**	12%

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

Βάση: Όλοι οι ερωτώμενοι



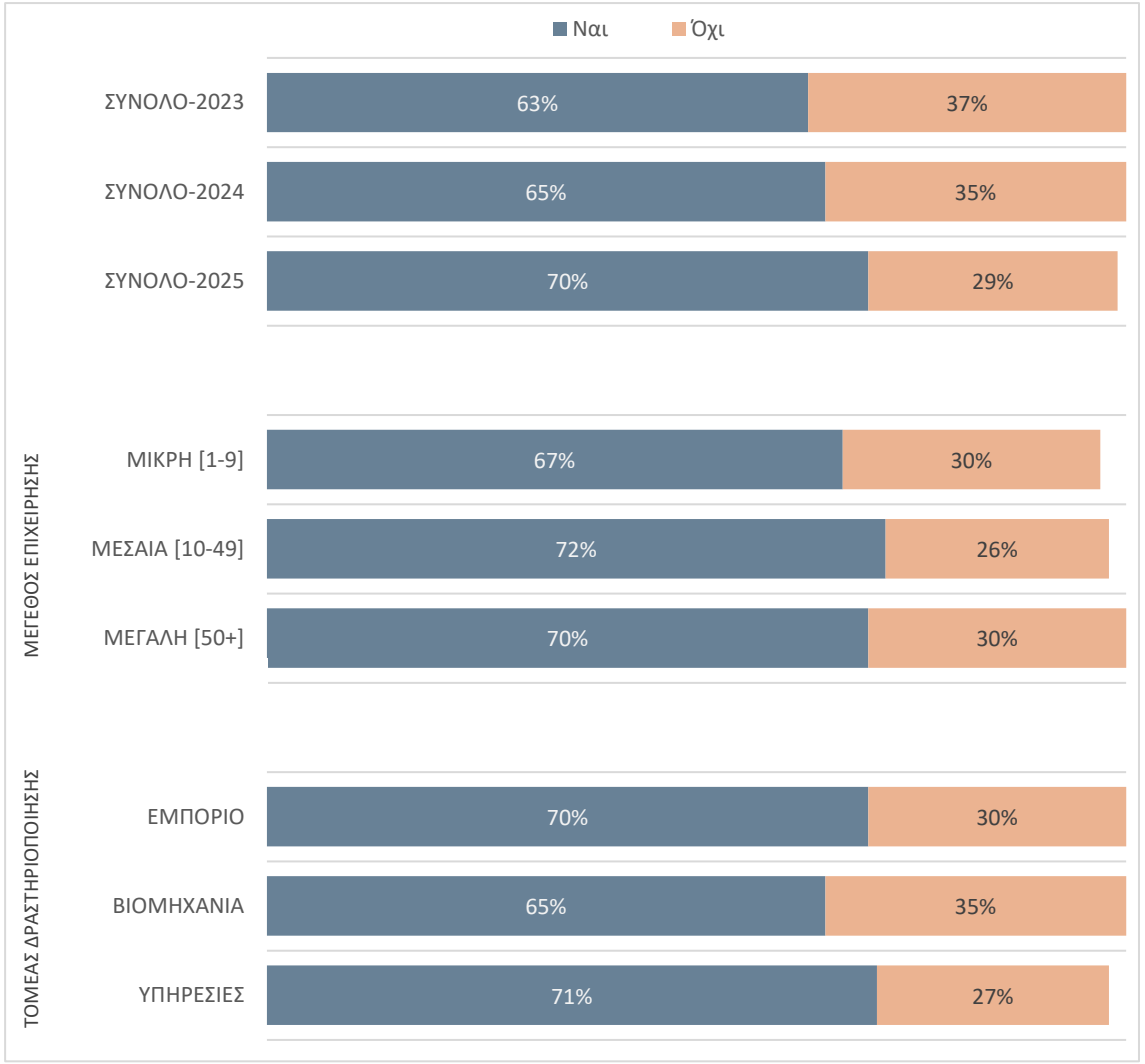


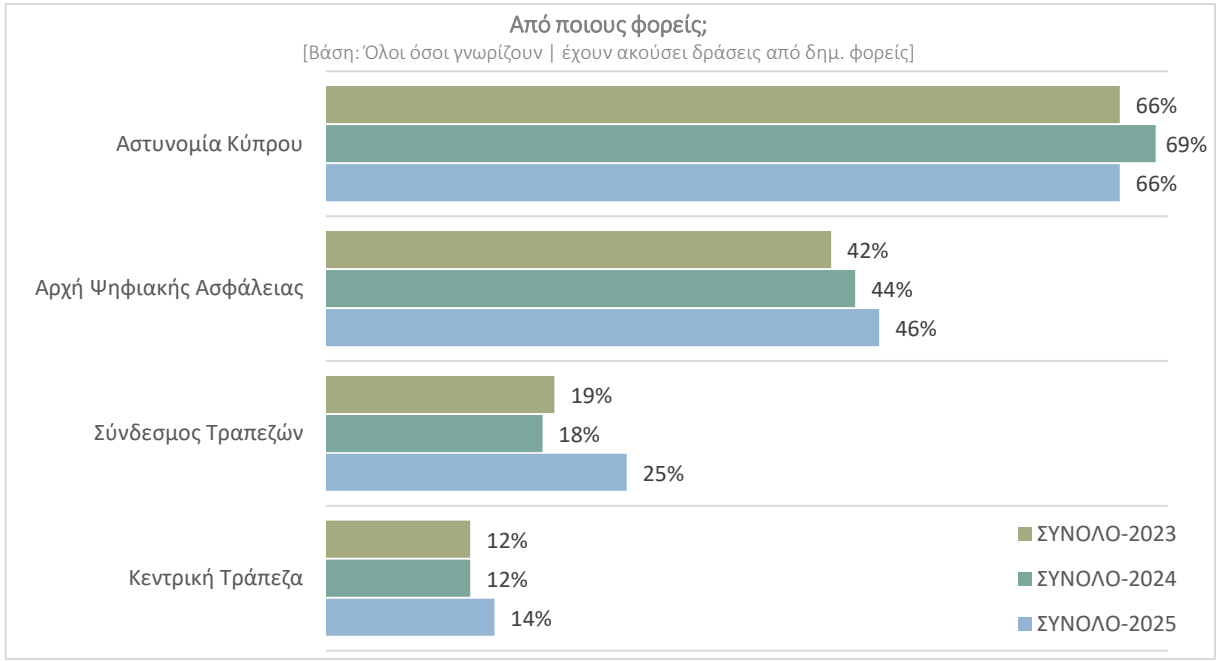


		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
PHISHING	Ναι, γνωρίζω	**96%**	90%	**98%**	100%	98%	93%
	Δεν γνωρίζω	1%	**10%**	2%	0%	2%	6%
SMISHING	Ναι, γνωρίζω	91%	85%	**96%**	97%	92%	89%
	Δεν γνωρίζω	9%	**15%**	4%	3%	8%	11%
VISHING	Ναι, γνωρίζω	83%	86%	**92%**	**97%**	88%	85%
	Δεν γνωρίζω	**17%**	14%	8%	3%	12%	**15%**

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

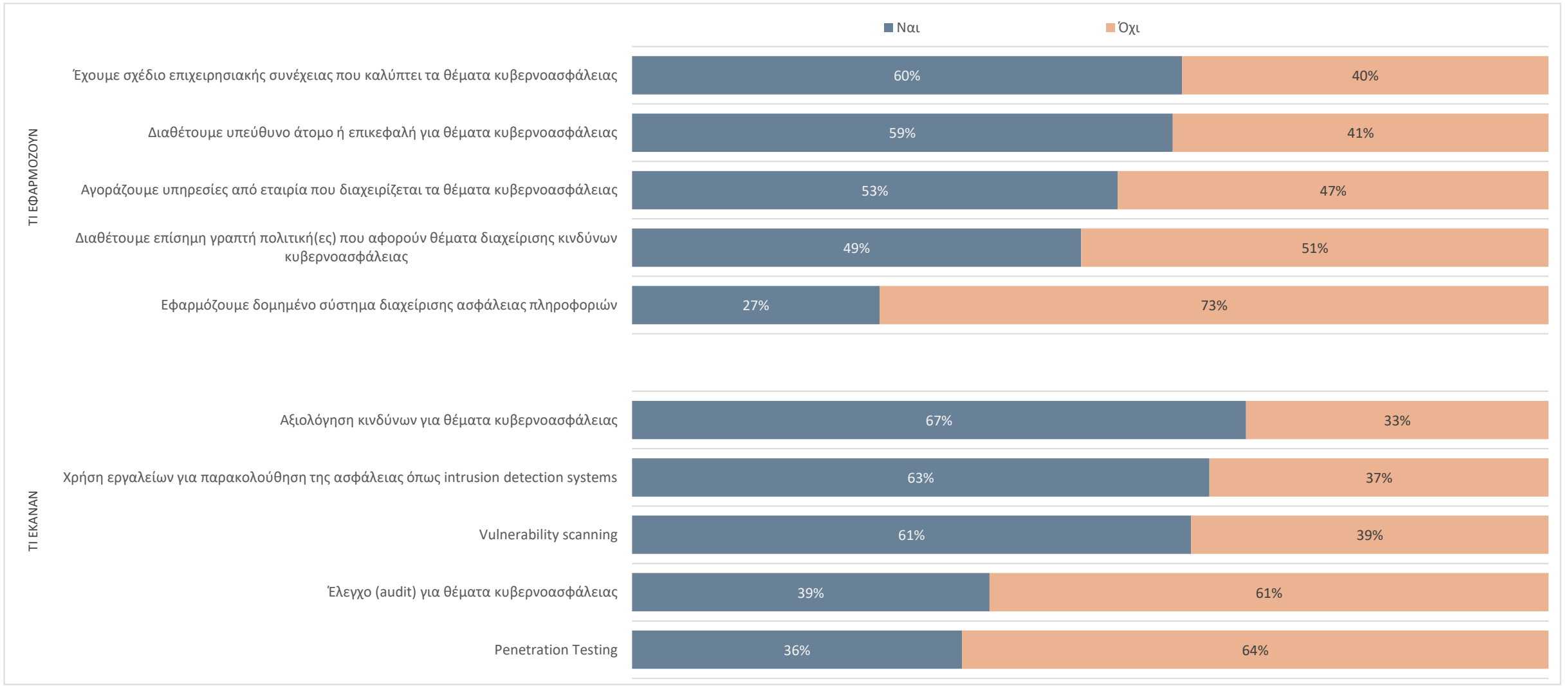




	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Αστυνομία Κύπρου	**72%**	66%	55%	58%	**82%**	63%
Αρχή Ψηφιακής Ασφάλειας	39%	46%	**61%**	51%	35%	49%
Σύνδεσμος Τραπεζών	**28%**	**29%**	14%	36%	32%	23%
Κεντρική Τράπεζα	16%	12%	14%	13%	9%	16%

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

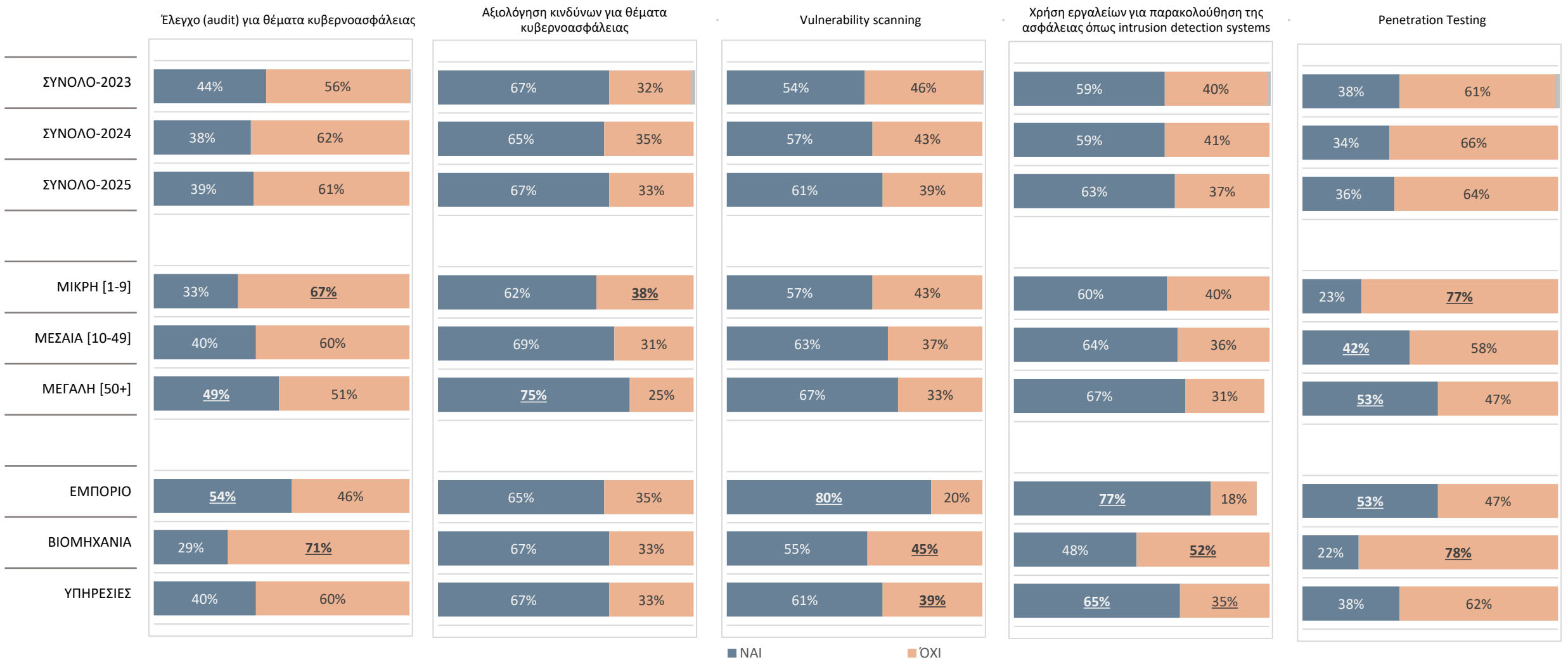


Ποιες από τις ακόλουθες αρχές διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας εφαρμόζετε στην εταιρεία;

Βάση: Όλοι οι ερωτώμενοι

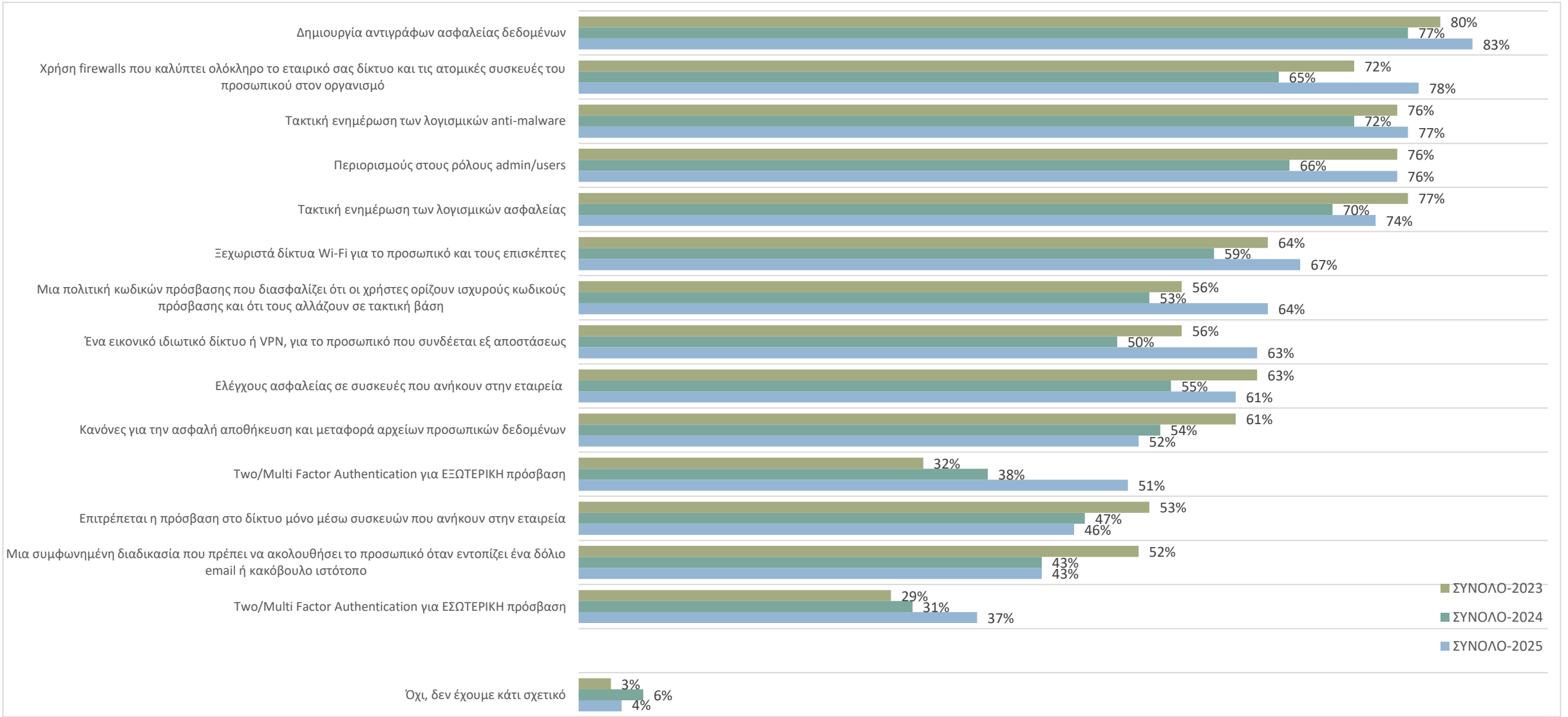
Και ποια από τα ακόλουθα έχετε κάνει τους τελευταίους 12 μήνες για να εντοπίσετε κινδύνους που αφορούν την κυβερνοασφάλεια της εταιρίας;

Βάση: Όλοι οι ερωτώμενοι



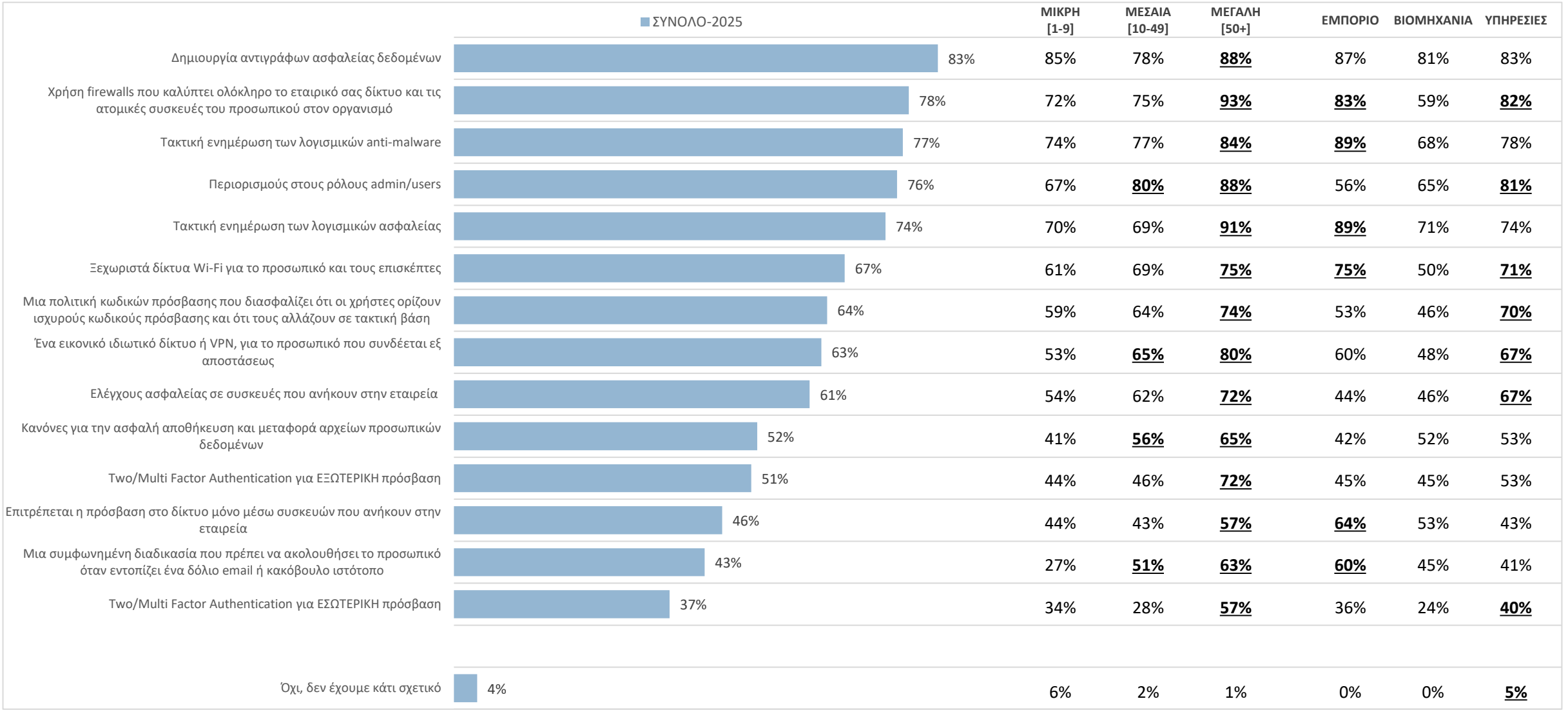
Ποιους από τους ακόλουθους κανόνες ή ελέγχους εφαρμόζετε στην επιχείρηση | εταιρεία σας;

Βάση: Όλοι οι ερωτώμενοι



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

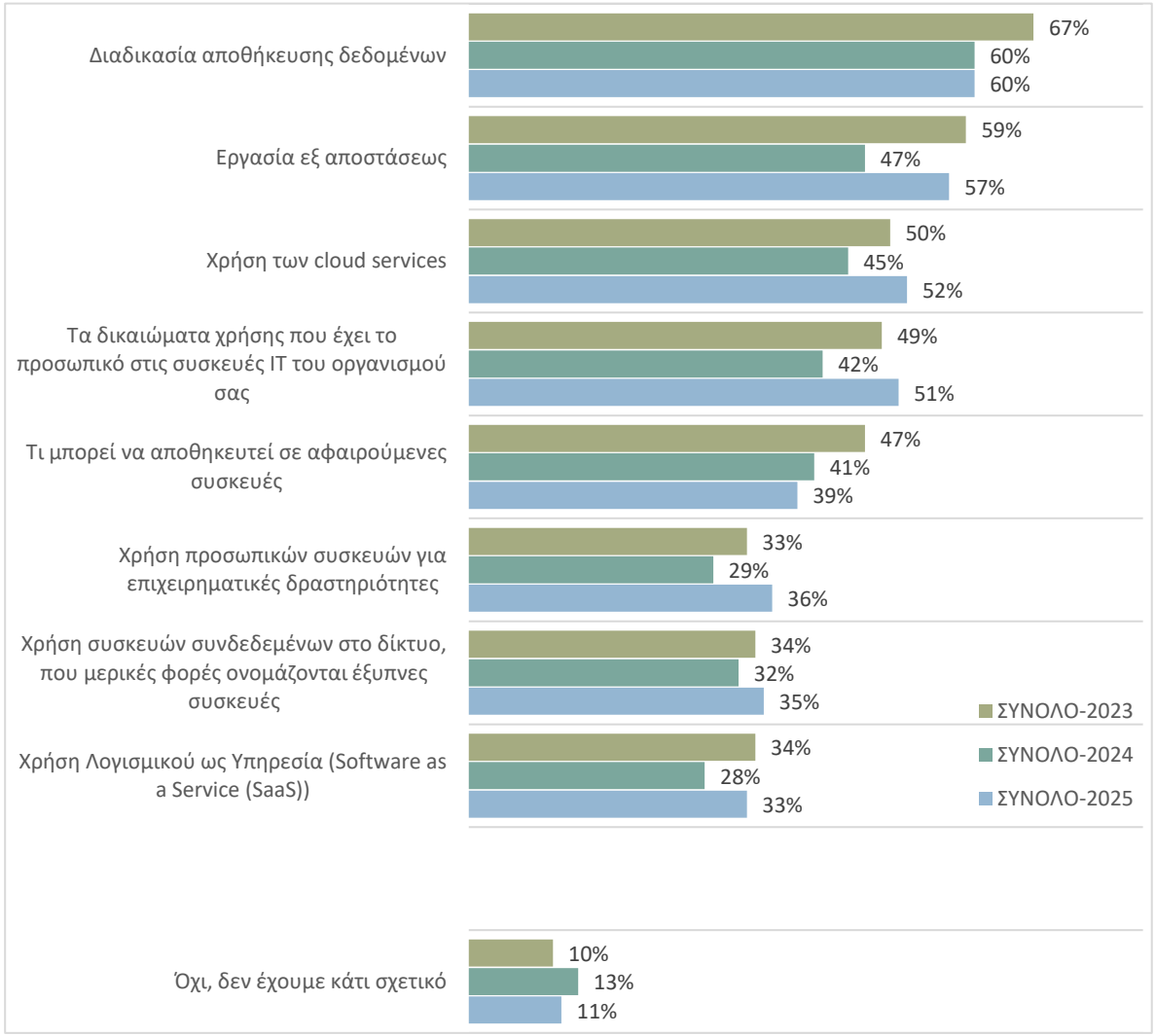
Βάση: Όλοι οι ερωτώμενοι



	ΣΥΝΟΛΟ-2025	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Δημιουργία αντιγράφων ασφαλείας δεδομένων	83%	85%	78%	**88%**	87%	81%	83%
Χρήση firewalls που καλύπτει ολόκληρο το εταιρικό σας δίκτυο και τις ατομικές συσκευές του προσωπικού στον οργανισμό	78%	72%	75%	**93%**	**83%**	59%	**82%**
Τακτική ενημέρωση των λογισμικών anti-malware	77%	74%	77%	**84%**	**89%**	68%	78%
Περιορισμούς στους ρόλους admin/users	76%	67%	**80%**	**88%**	56%	65%	**81%**
Τακτική ενημέρωση των λογισμικών ασφαλείας	74%	70%	69%	**91%**	**89%**	71%	74%
Ξεχωριστά δίκτυα Wi-Fi για το προσωπικό και τους επισκέπτες	67%	61%	69%	**75%**	**75%**	50%	**71%**
Μια πολιτική κωδικών πρόσβασης που διασφαλίζει ότι οι χρήστες ορίζουν ισχυρούς κωδικούς πρόσβασης και ότι τους αλλάζουν σε τακτική βάση	64%	59%	64%	**74%**	53%	46%	**70%**
Ένα εικονικό ιδιωτικό δίκτυο ή VPN, για το προσωπικό που συνδέεται εξ αποστάσεως	63%	53%	**65%**	**80%**	60%	48%	**67%**
Ελέγχους ασφαλείας σε συσκευές που ανήκουν στην εταιρεία	61%	54%	62%	**72%**	44%	46%	**67%**
Κανόνες για την ασφαλή αποθήκευση και μεταφορά αρχείων προσωπικών δεδομένων	52%	41%	**56%**	**65%**	42%	52%	53%
Two/Multi Factor Authentication για ΕΞΩΤΕΡΙΚΗ πρόσβαση	51%	44%	46%	**72%**	45%	45%	53%
Επιτρέπεται η πρόσβαση στο δίκτυο μόνο μέσω συσκευών που ανήκουν στην εταιρεία	46%	44%	43%	**57%**	**64%**	53%	43%
Μια συμφωνημένη διαδικασία που πρέπει να ακολουθήσει το προσωπικό όταν εντοπίζει ένα δόλιο email ή κακόβουλο ιστότοπο	43%	27%	**51%**	**63%**	**60%**	45%	41%
Two/Multi Factor Authentication για ΕΣΩΤΕΡΙΚΗ πρόσβαση	37%	34%	28%	**57%**	36%	24%	**40%**
Όχι, δεν έχουμε κάτι σχετικό	4%	6%	2%	1%	0%	0%	**5%**

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

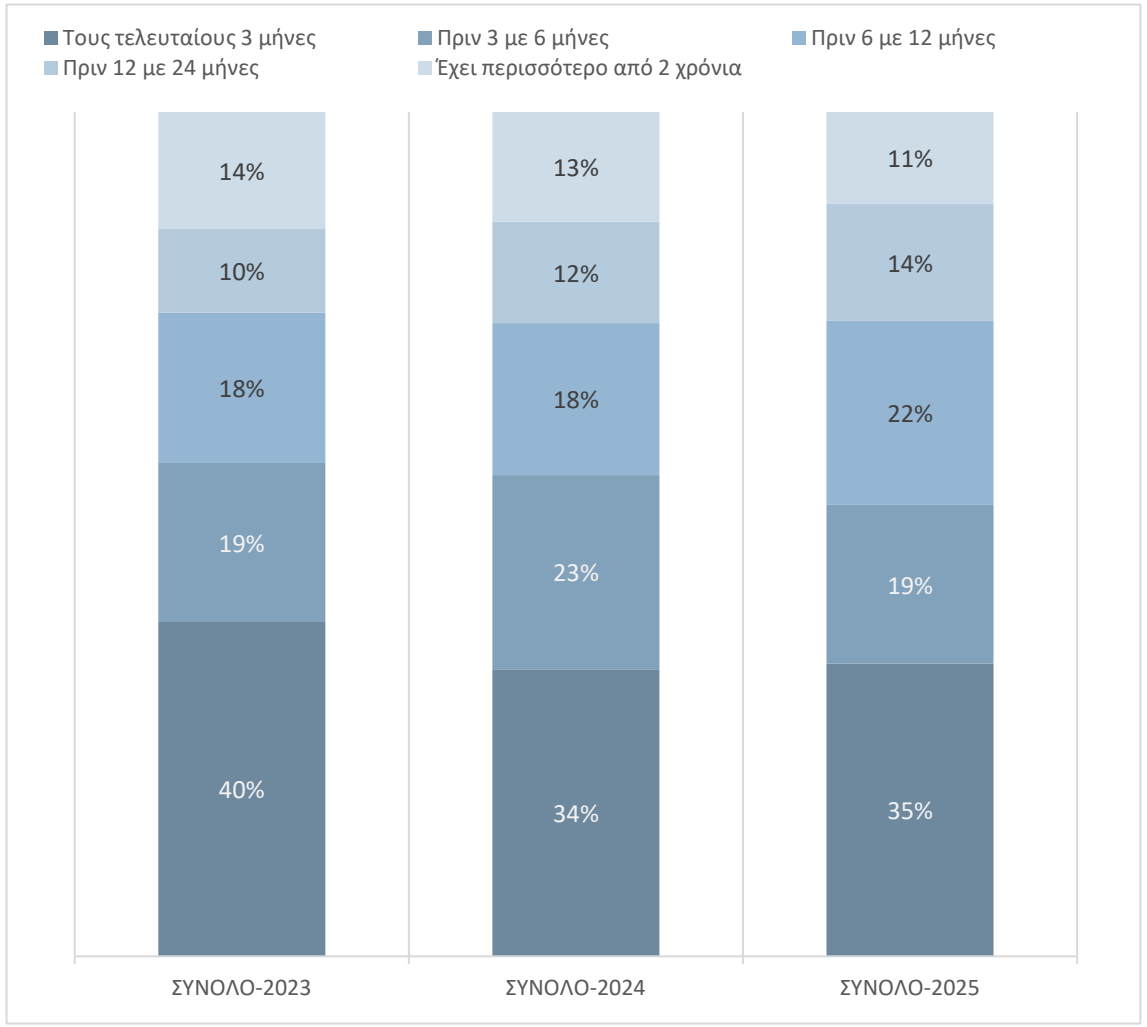
Βάση: Όλοι οι ερωτώμενοι

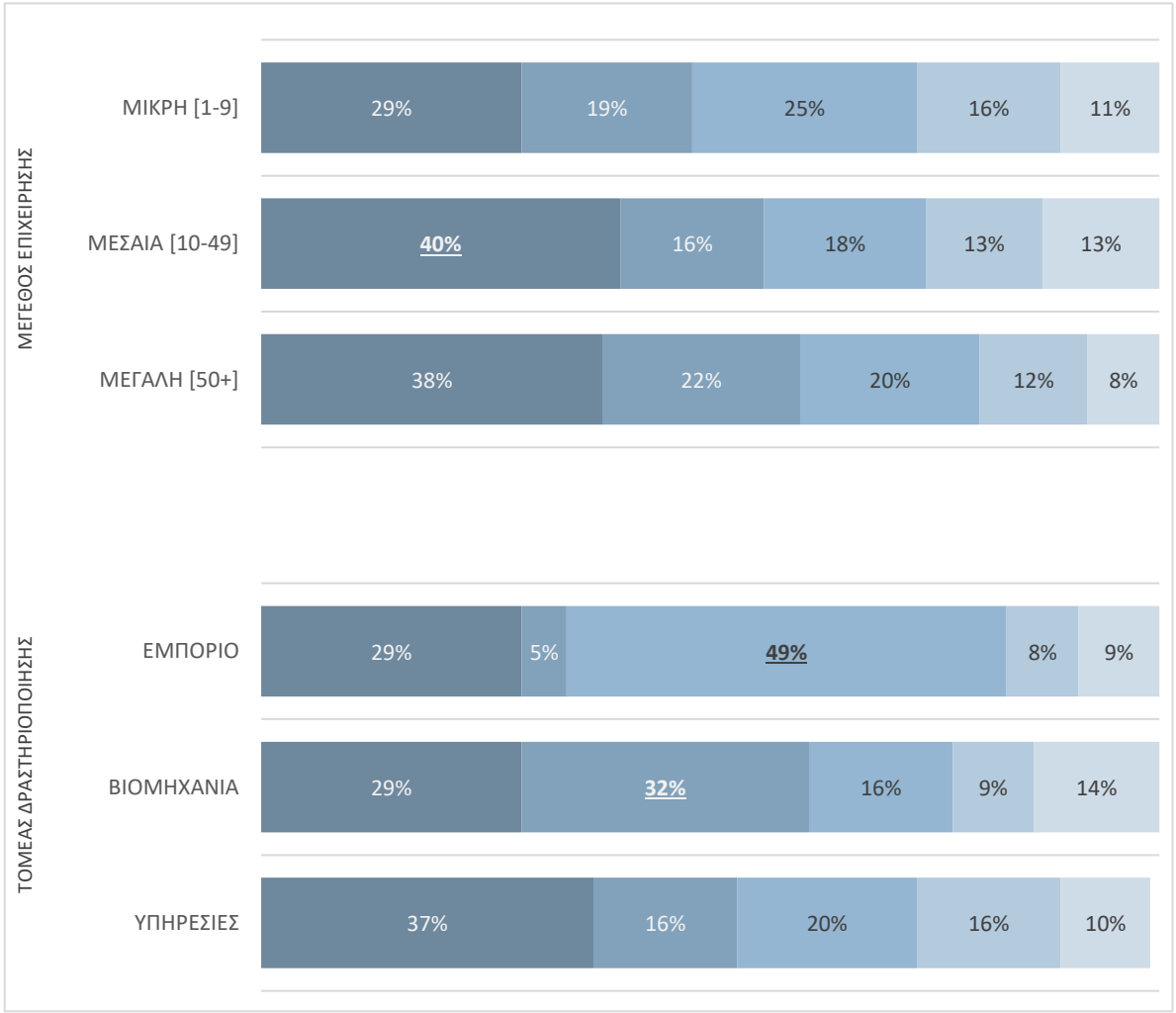


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Διαδικασία αποθήκευσης δεδομένων	56%	64%	62%	42%	55%	**64%**
Εργασία εξ αποστάσεως	52%	53%	**72%**	43%	50%	**60%**
Χρήση των cloud services	49%	56%	54%	55%	43%	55%
Τα δικαιώματα χρήσης που έχει το προσωπικό στις συσκευές IT του οργανισμού σας	41%	**53%**	**68%**	44%	43%	54%
Τι μπορεί να αποθηκευτεί σε αφαιρούμενες συσκευές	25%	**46%**	**54%**	**71%**	27%	**38%**
Χρήση προσωπικών συσκευών για επιχειρηματικές δραστηριότητες	29%	38%	**45%**	**46%**	23%	**38%**
Χρήση συσκευών συνδεδεμένων στο δίκτυο, που μερικές φορές ονομάζονται έξυπνες συσκευές	34%	31%	**43%**	**44%**	26%	36%
Χρήση Λογισμικού ως Υπηρεσία (Software as a Service (SaaS))	25%	34%	**46%**	**34%**	17%	**37%**
Όχι, δεν έχουμε κάτι σχετικό	14%	10%	8%	7%	16%	11%

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;

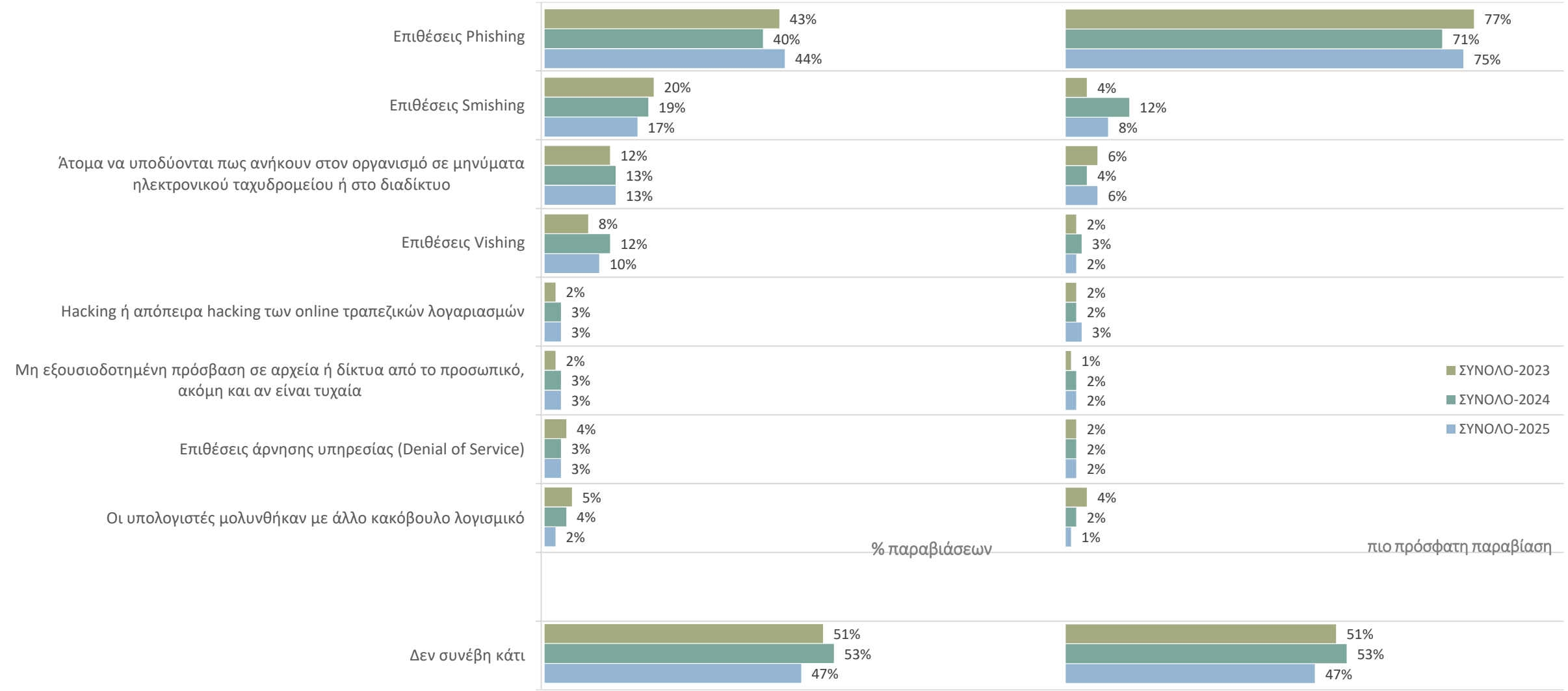
Βάση: Όλοι οι ερωτώμενοι





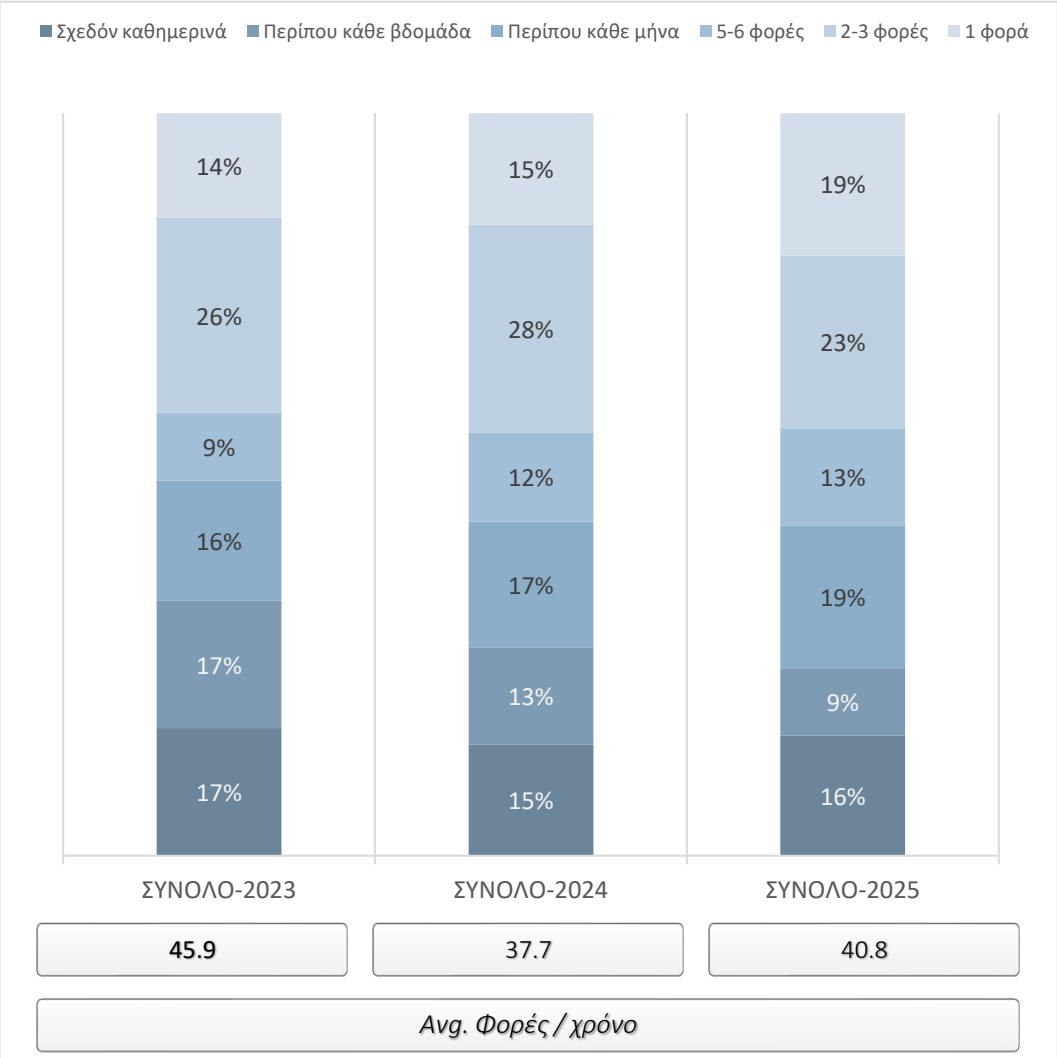
Τους τελευταίους 12 μήνες, τι από τα παρακάτω συνέβη στην εταιρεία |επιχείρηση |οργανισμό; Και ποια ήταν η πιο πρόσφατη παραβίαση κυβερνοασφάλειας |επίθεση, που δεχτήκατε;

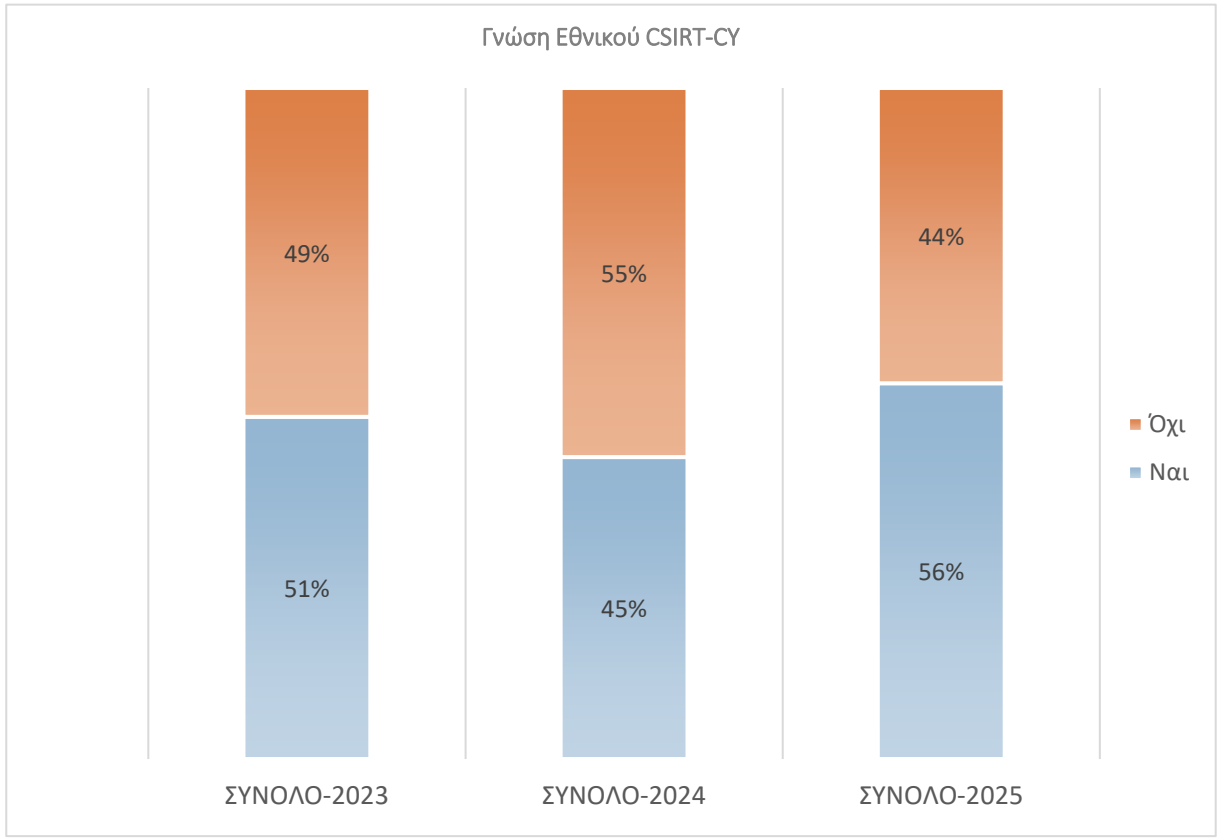
Βάση: Όλοι οι ερωτώμενοι



Πόσο συχνά αντιμετωπίσατε κάποια από τις παραβιάσεις ή τις επιθέσεις αυτές; | Γνωρίζετε για το Εθνικό CSIRT-CY και το ρόλο του σε περιστατικά κυβερνοεπιθέσεων;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση

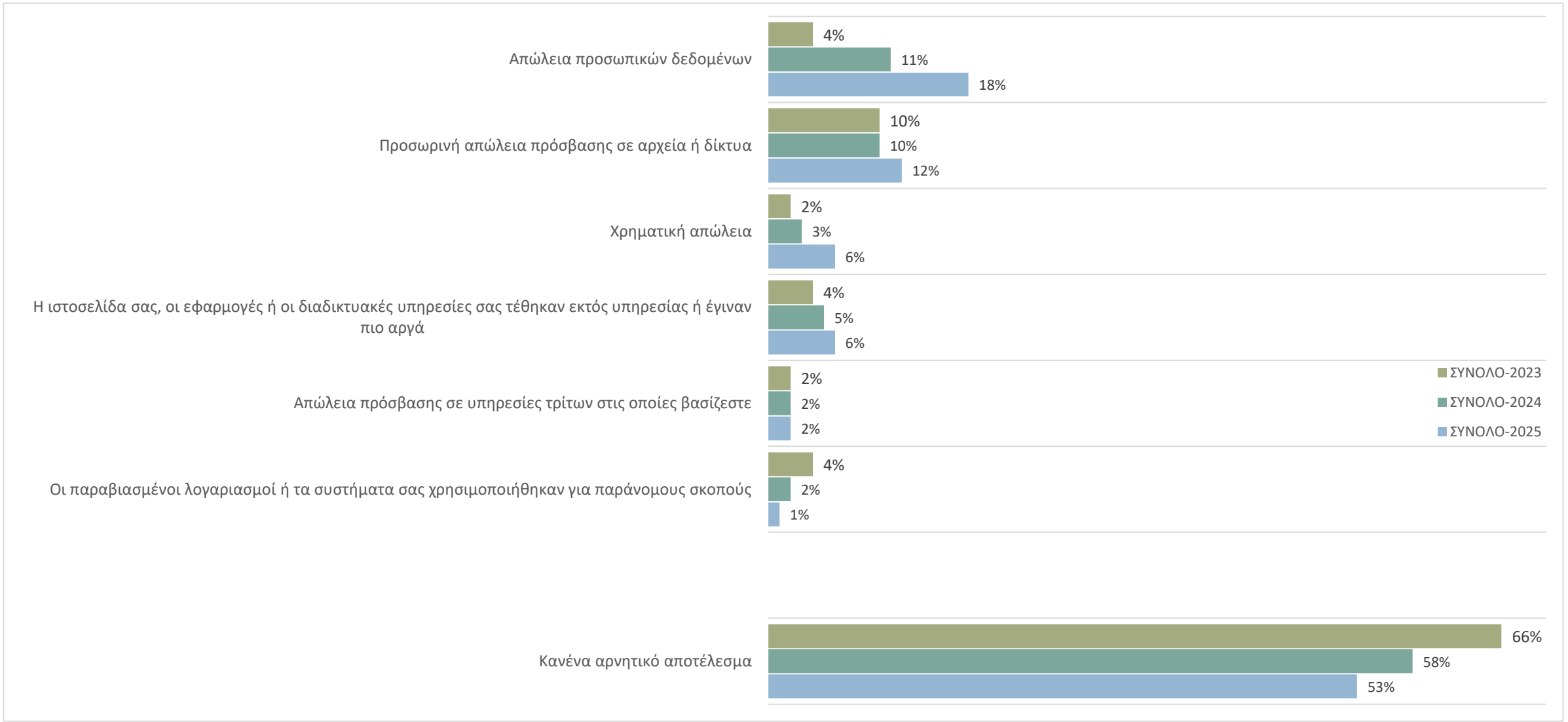




	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Ναι	47%	**67%**	57%	27%	39%	**66%**
Όχι	**53%**	33%	43%	73%	**61%**	34%

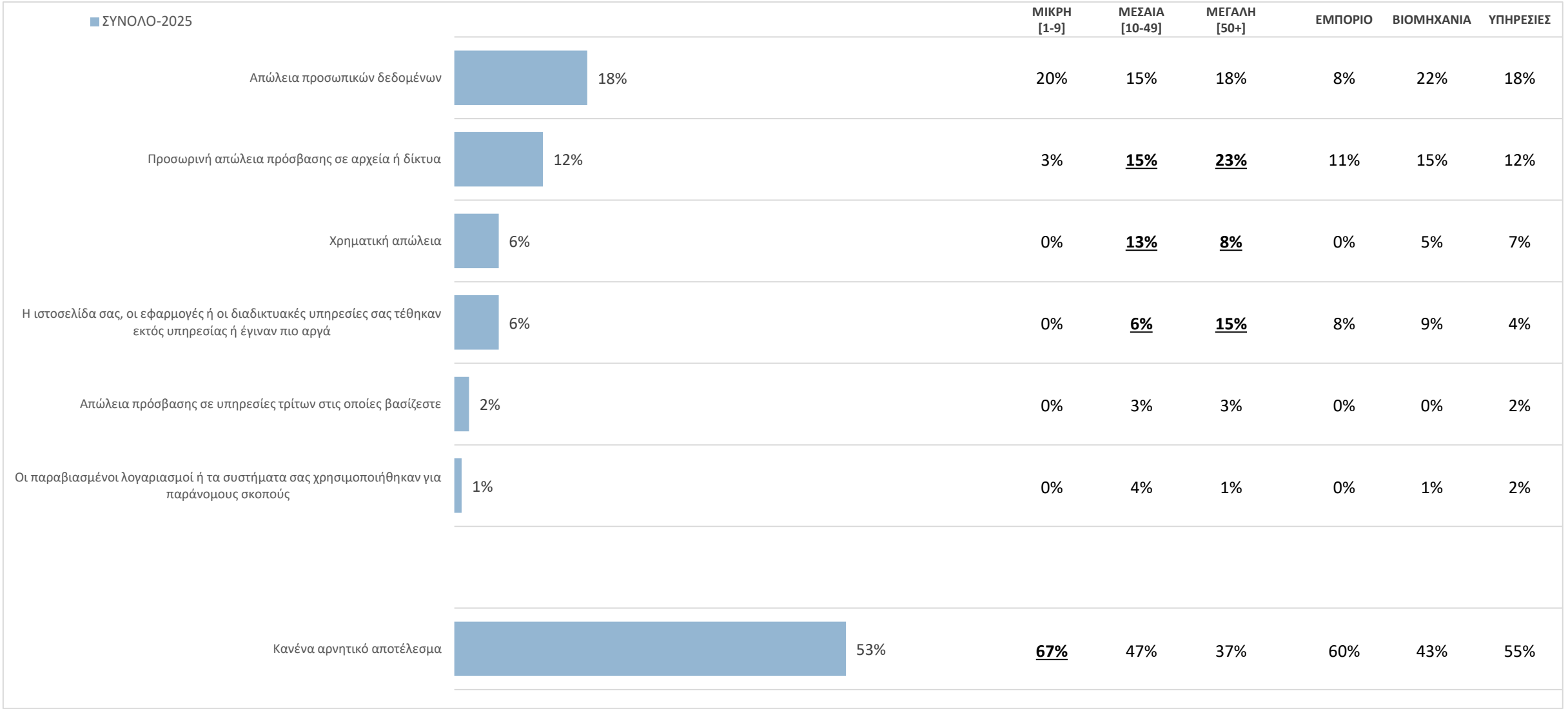
Λαμβάνοντας υπόψιν όλες τις παραβιάσεις /κυβερνοεπιθέσεις που αντιμετωπίσατε τους τελευταίους 12 μήνες, ποια από τα ακόλουθα συνέβησαν ως αποτέλεσμα τους;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

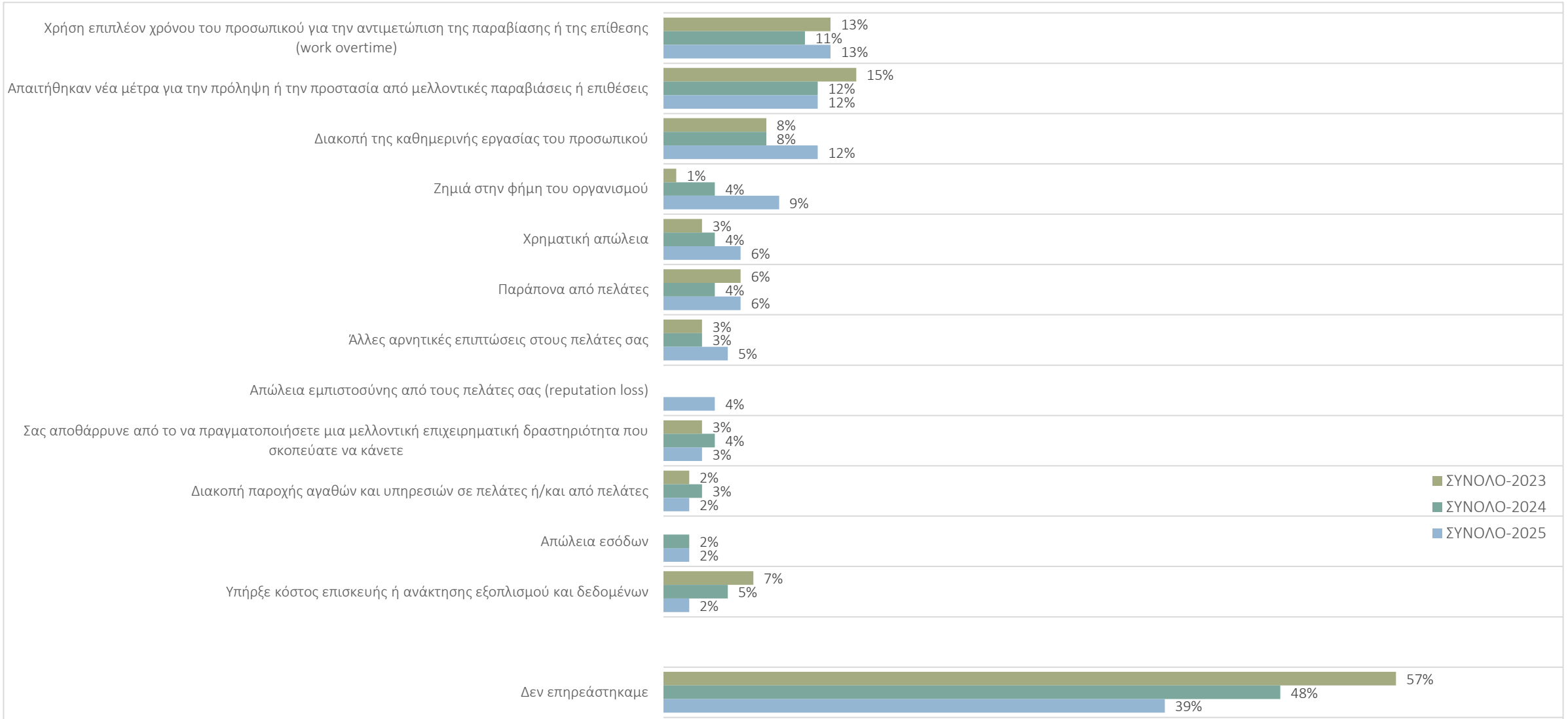
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



	ΣΥΝΟΛΟ-2025	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Απώλεια προσωπικών δεδομένων	18%	20%	15%	18%	8%	22%	18%
Προσωρινή απώλεια πρόσβασης σε αρχεία ή δίκτυα	12%	3%	**15%**	**23%**	11%	15%	12%
Χρηματική απώλεια	6%	0%	**13%**	**8%**	0%	5%	7%
Η ιστοσελίδα σας, οι εφαρμογές ή οι διαδικτυακές υπηρεσίες σας τέθηκαν εκτός υπηρεσίας ή έγιναν πιο αργά	6%	0%	**6%**	**15%**	8%	9%	4%
Απώλεια πρόσβασης σε υπηρεσίες τρίτων στις οποίες βασίζεστε	2%	0%	3%	3%	0%	0%	2%
Οι παραβιασμένοι λογαριασμοί ή τα συστήματα σας χρησιμοποιήθηκαν για παράνομους σκοπούς	1%	0%	4%	1%	0%	1%	2%
Κανένα αρνητικό αποτέλεσμα	53%	**67%**	47%	37%	60%	43%	55%

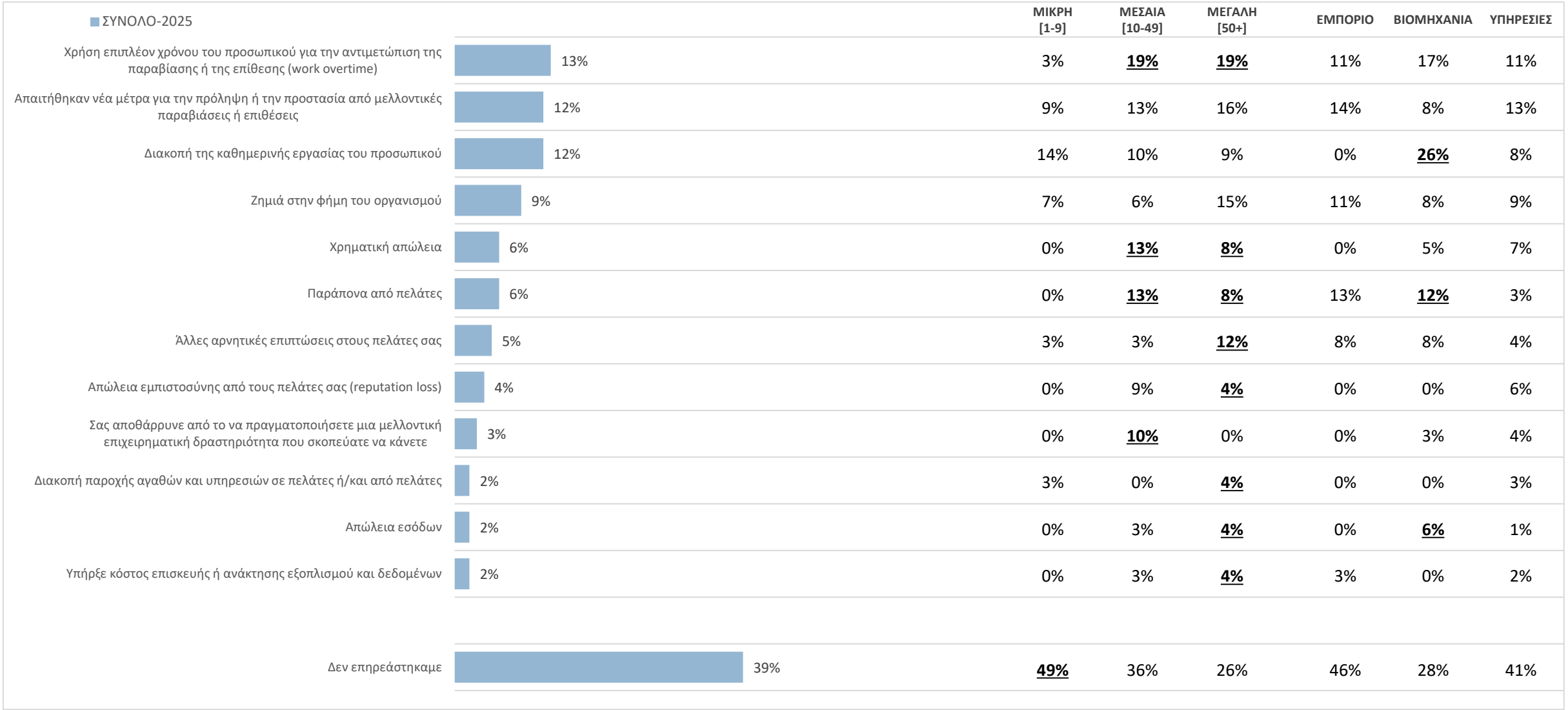
Πως έχουν επηρεάσει την εταιρεία/ επιχείρηση /τον οργανισμό αυτές οι παραβιάσεις ή επιθέσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

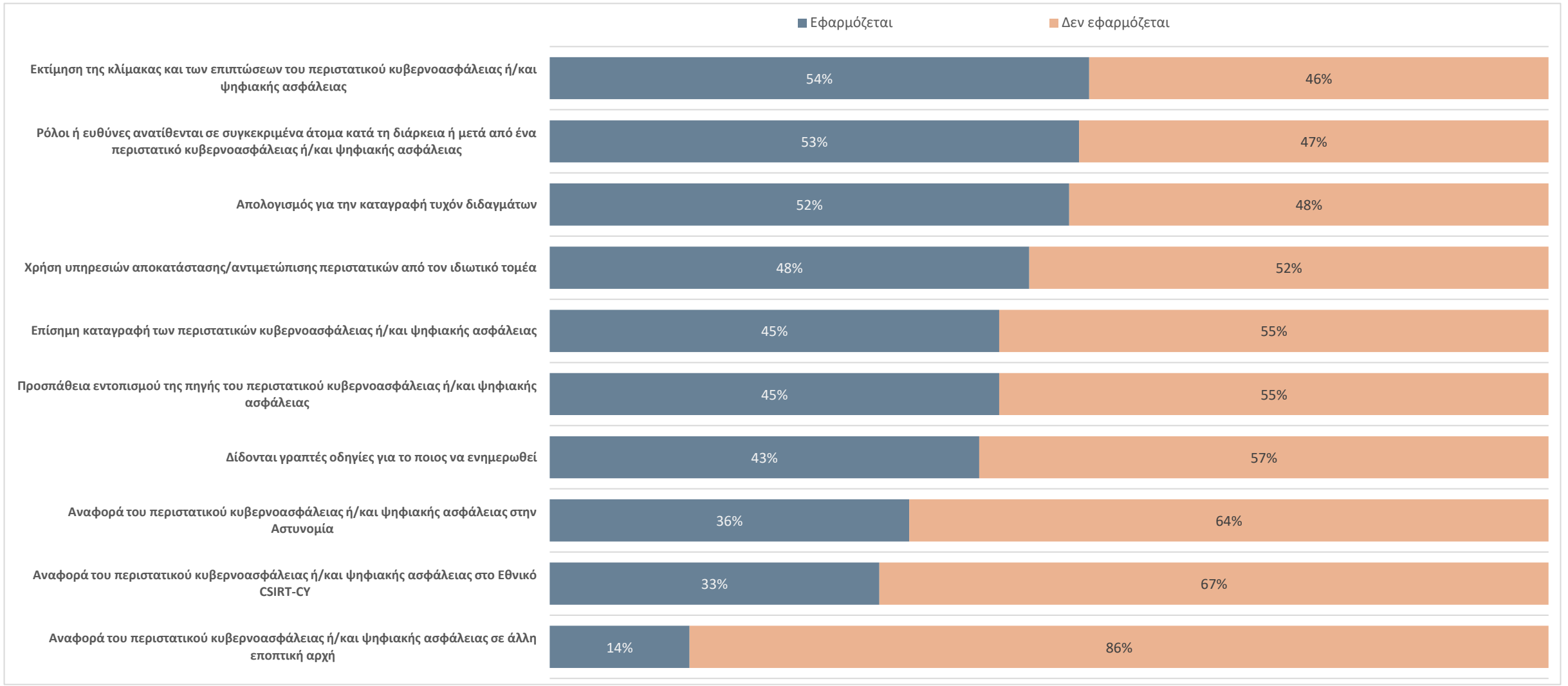
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



	ΣΥΝΟΛΟ-2025	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Χρήση επιπλέον χρόνου του προσωπικού για την αντιμετώπιση της παραβίασης ή της επίθεσης (work overtime)	13%	3%	**19%**	**19%**	11%	17%	11%
Απαιτήθηκαν νέα μέτρα για την πρόληψη ή την προστασία από μελλοντικές παραβιάσεις ή επιθέσεις	12%	9%	13%	16%	14%	8%	13%
Διακοπή της καθημερινής εργασίας του προσωπικού	12%	14%	10%	9%	0%	**26%**	8%
Ζημιά στην φήμη του οργανισμού	9%	7%	6%	15%	11%	8%	9%
Χρηματική απώλεια	6%	0%	**13%**	**8%**	0%	5%	7%
Παράπονα από πελάτες	6%	0%	**13%**	**8%**	13%	**12%**	3%
Άλλες αρνητικές επιπτώσεις στους πελάτες σας	5%	3%	3%	**12%**	8%	8%	4%
Απώλεια εμπιστοσύνης από τους πελάτες σας (reputation loss)	4%	0%	9%	**4%**	0%	0%	6%
Σας αποθάρρυνε από το να πραγματοποιήσετε μια μελλοντική επιχειρηματική δραστηριότητα που σκοπεύατε να κάνετε	3%	0%	**10%**	0%	0%	3%	4%
Διακοπή παροχής αγαθών και υπηρεσιών σε πελάτες ή/και από πελάτες	2%	3%	0%	**4%**	0%	0%	3%
Απώλεια εσόδων	2%	0%	3%	**4%**	0%	**6%**	1%
Υπήρξε κόστος επισκευής ή ανάκτησης εξοπλισμού και δεδομένων	2%	0%	3%	**4%**	3%	0%	2%
Δεν επηρεάστηκαμε	39%	**49%**	36%	26%	46%	28%	41%

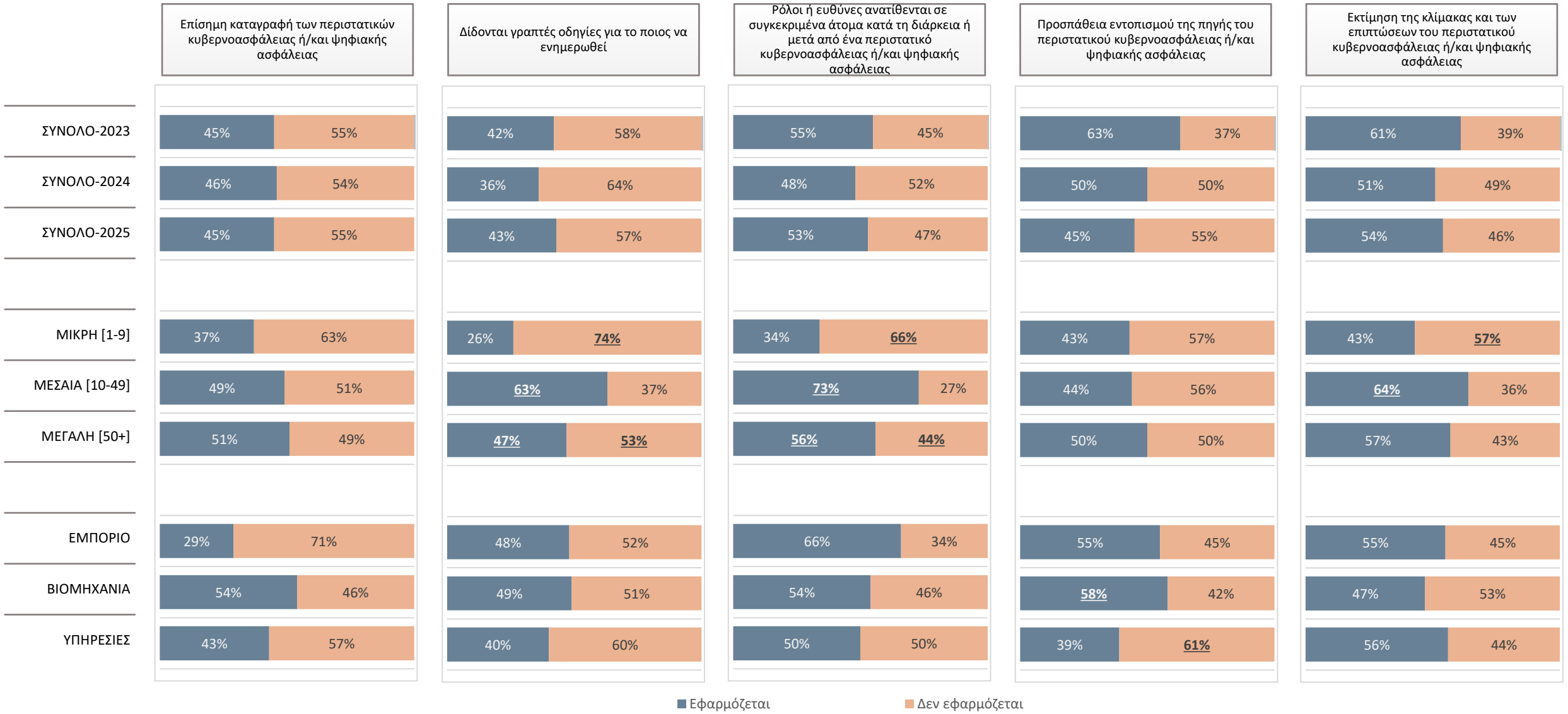
Ποια από τα παρακάτω κάνετε ή εφαρμόζετε, όταν αντιμετωπίζετε ένα περιστατικό κυβερνοασφάλειας;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση (2025)



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

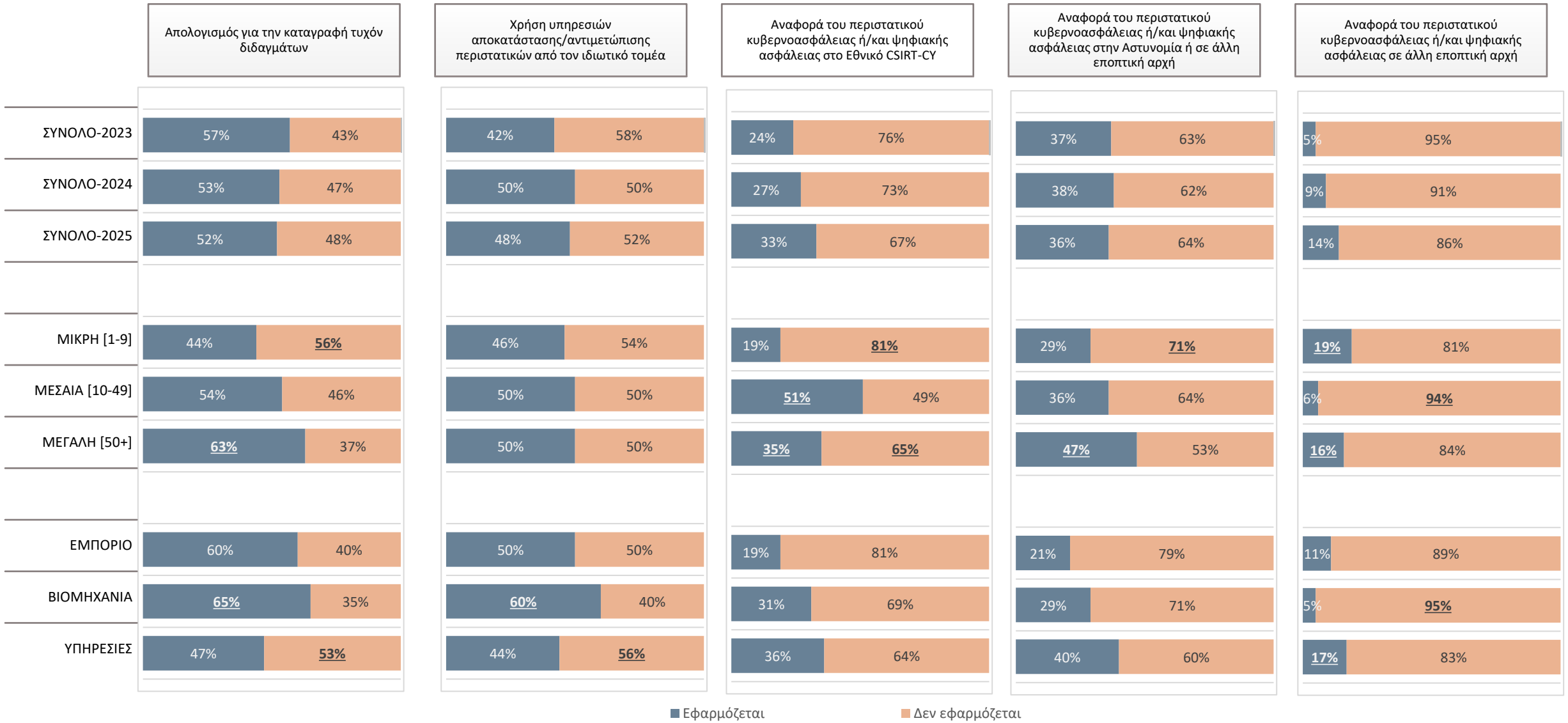
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

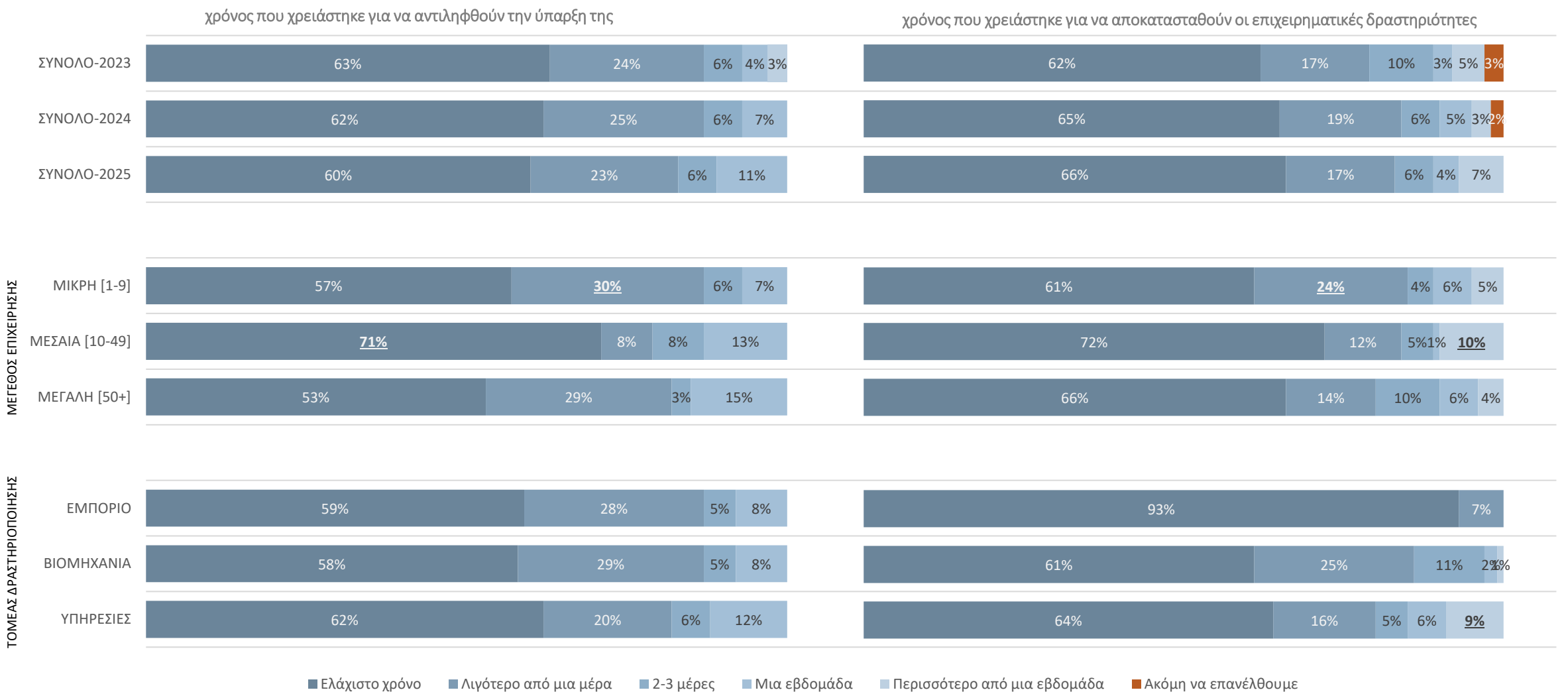
... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



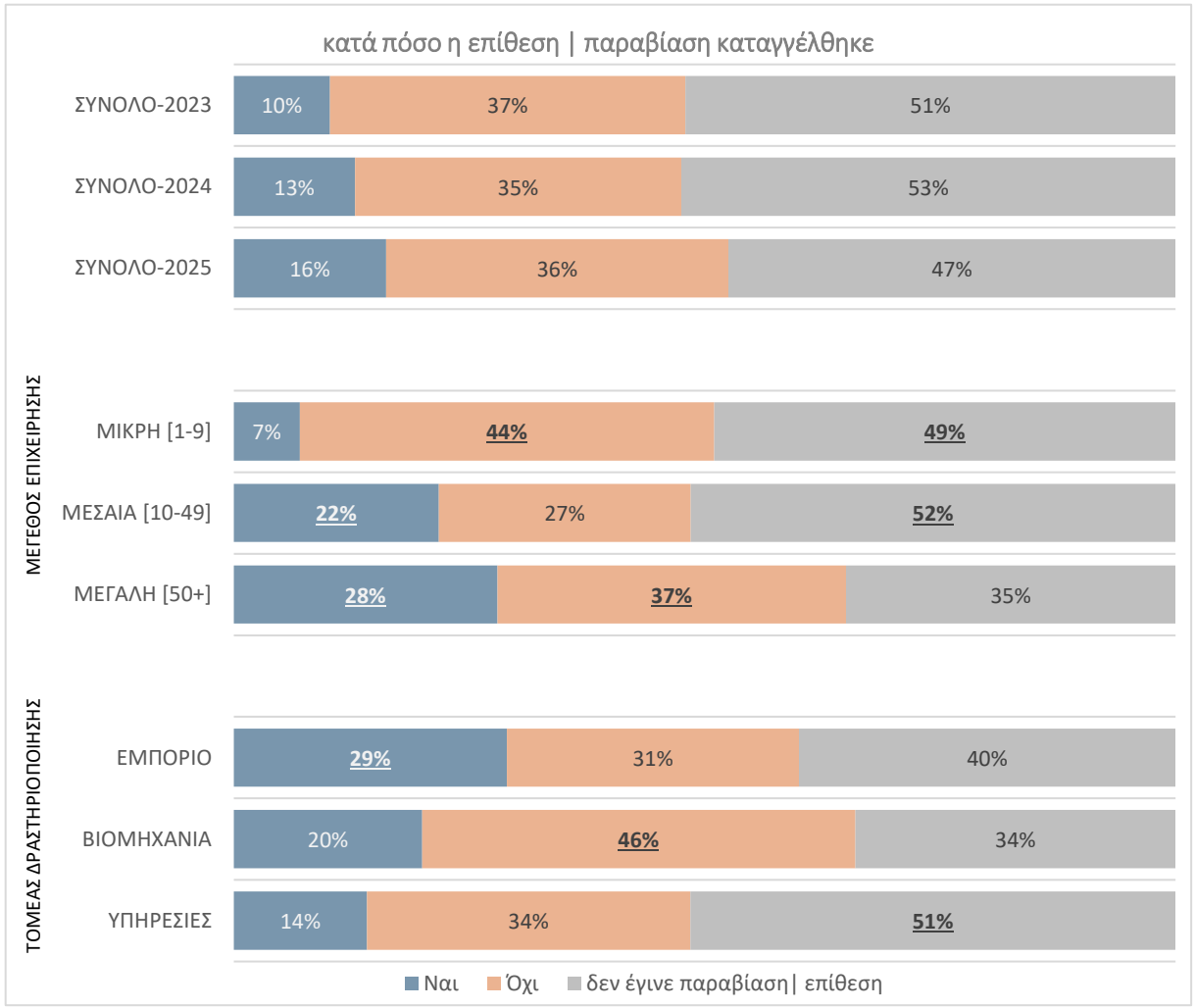
Σκεπτόμενοι την πιο πρόσφατη παραβίαση κυβερνοασφάλειας, που δεχτήκατε, πόσος χρόνος χρειάστηκε για να αντιληφθείτε την ύπαρξη της; | Και πόσος χρόνος χρειάστηκε για να αποκατασταθούν οι επιχειρηματικές σας δραστηριότητες;

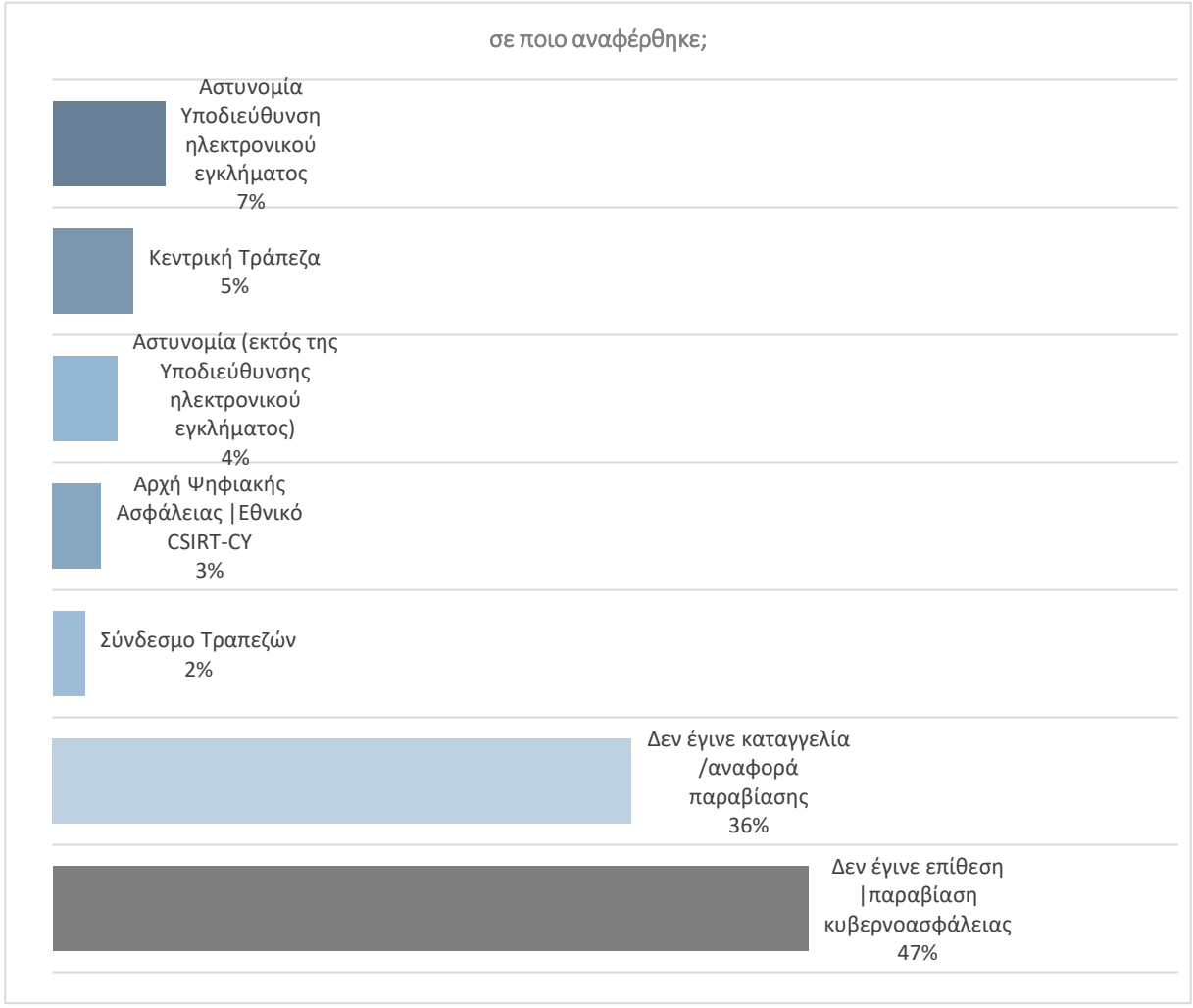
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

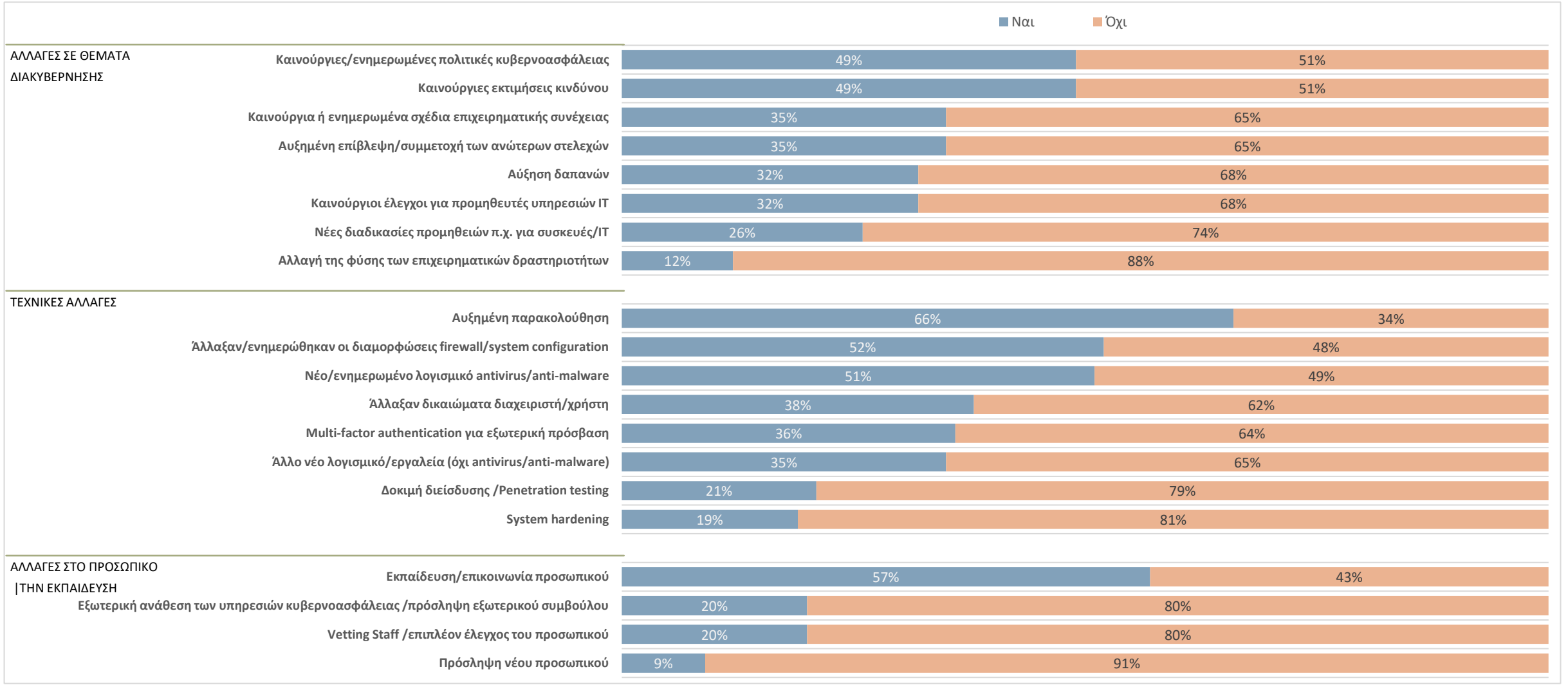
Βάση: Όλοι οι ερωτώμενοι





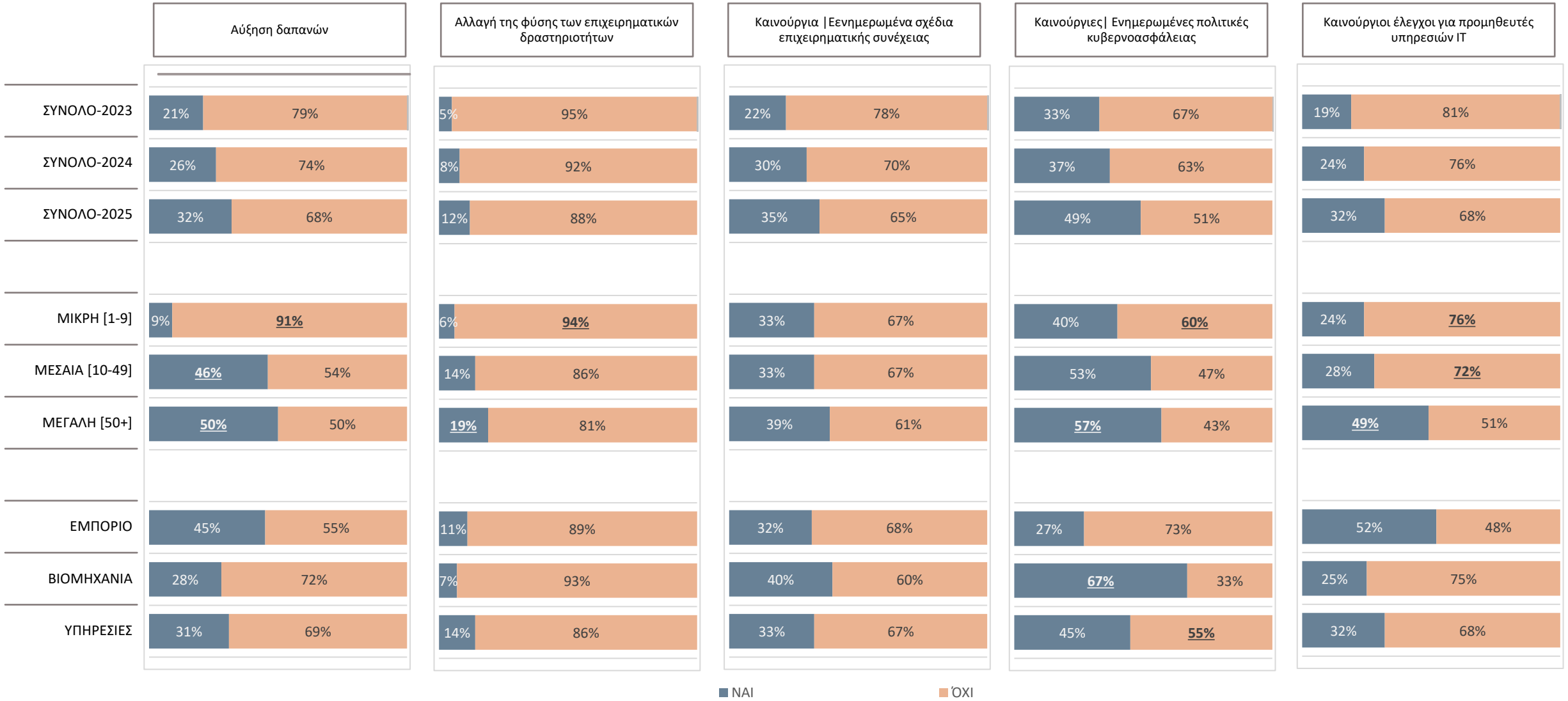
Μετά από αυτήν την παραβίαση| επίθεση, τι από τα ακόλουθα έχετε κάνει για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

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;

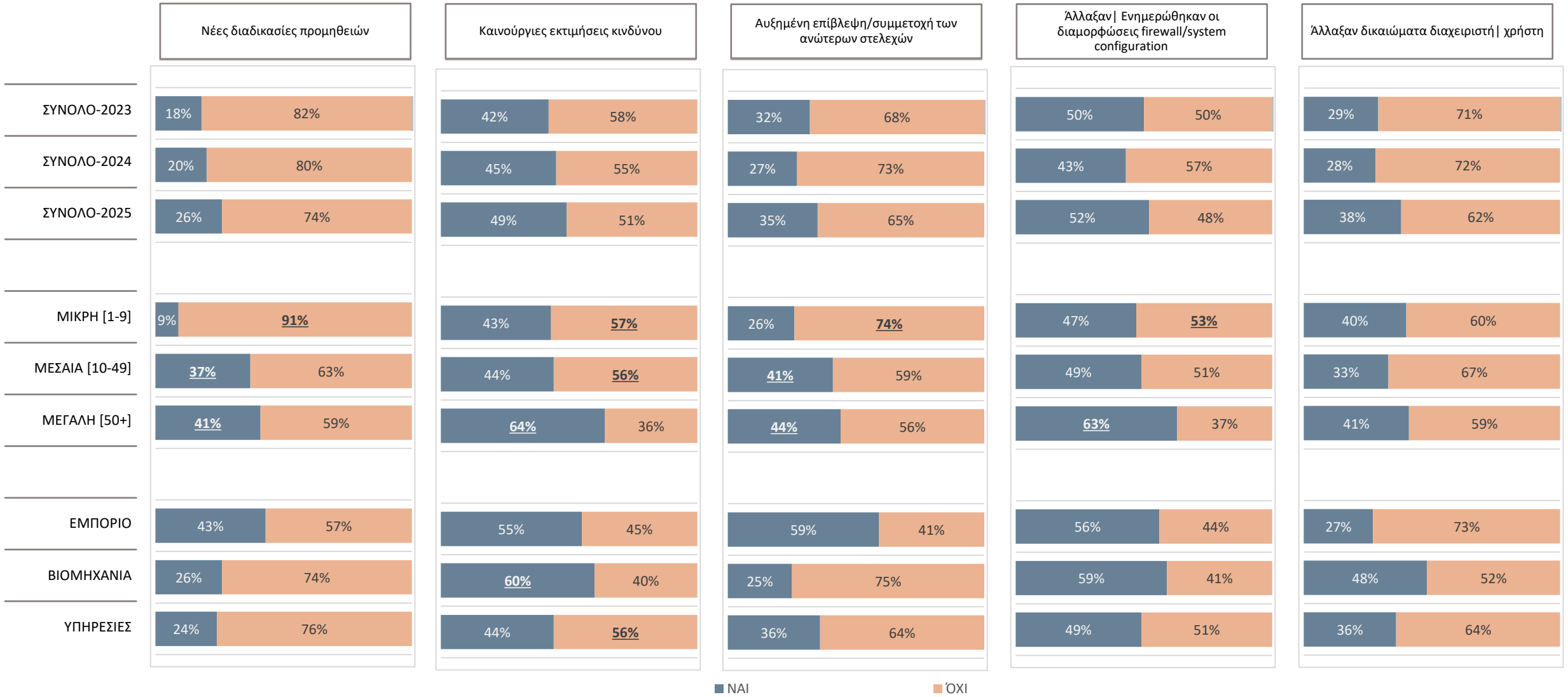
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

... συνέχεια

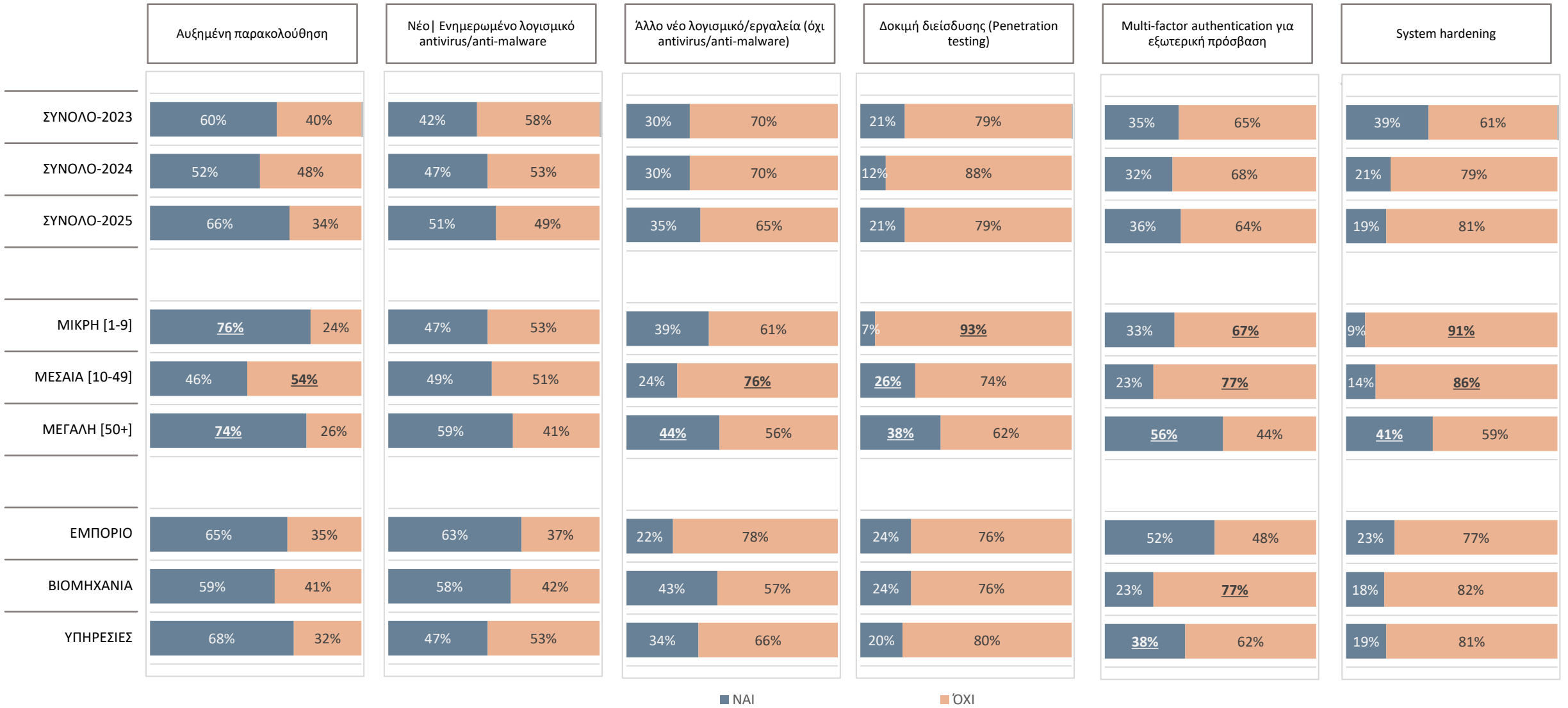
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

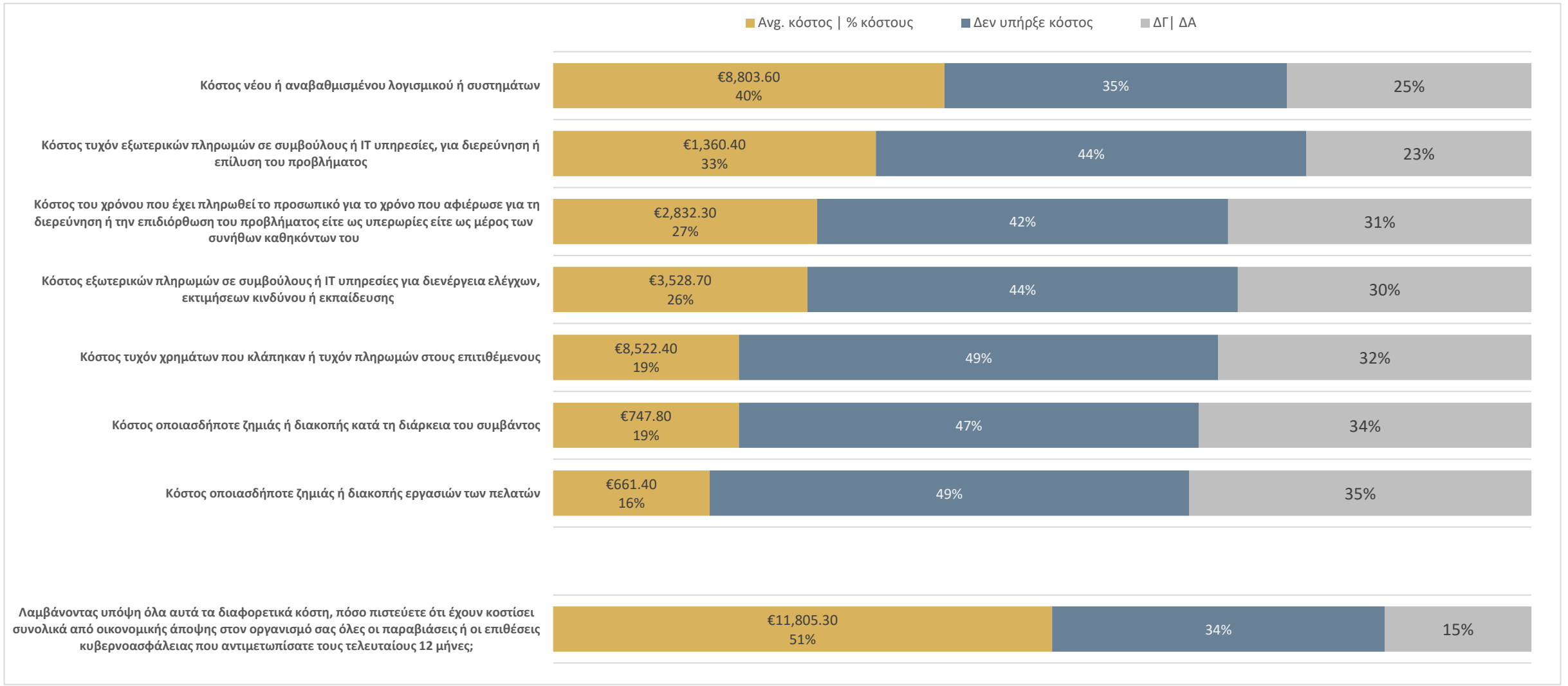


Μετά από αυτήν την παραβίαση/επίθεση, τι *αλλαγές κάνατε σε σχέση με την εκπαίδευση και το προσωπικό*, για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση

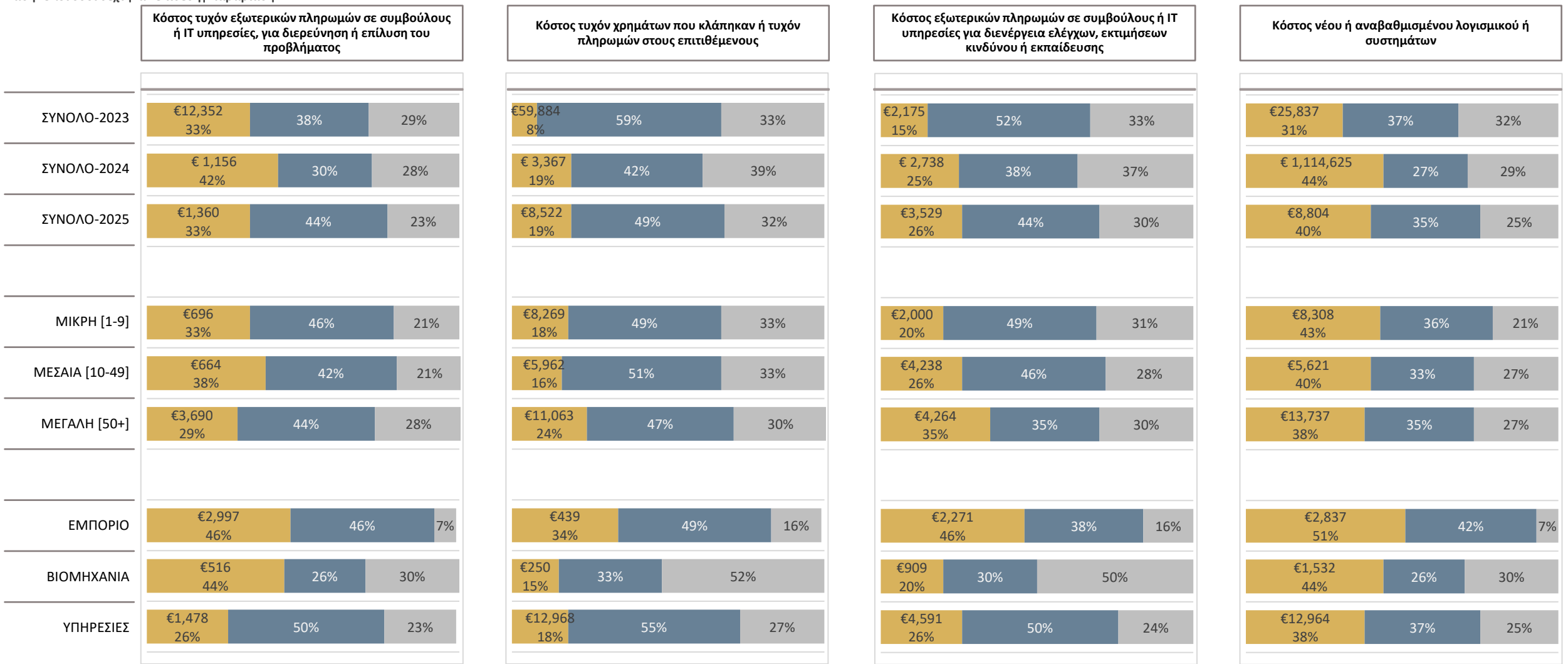
Ποια είναι, τα κατά προσέγγιση, κόστη, της πιο πρόσφατης παραβίασης| επίθεσης, που δεχτήκατε στην εταιρεία σας;

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

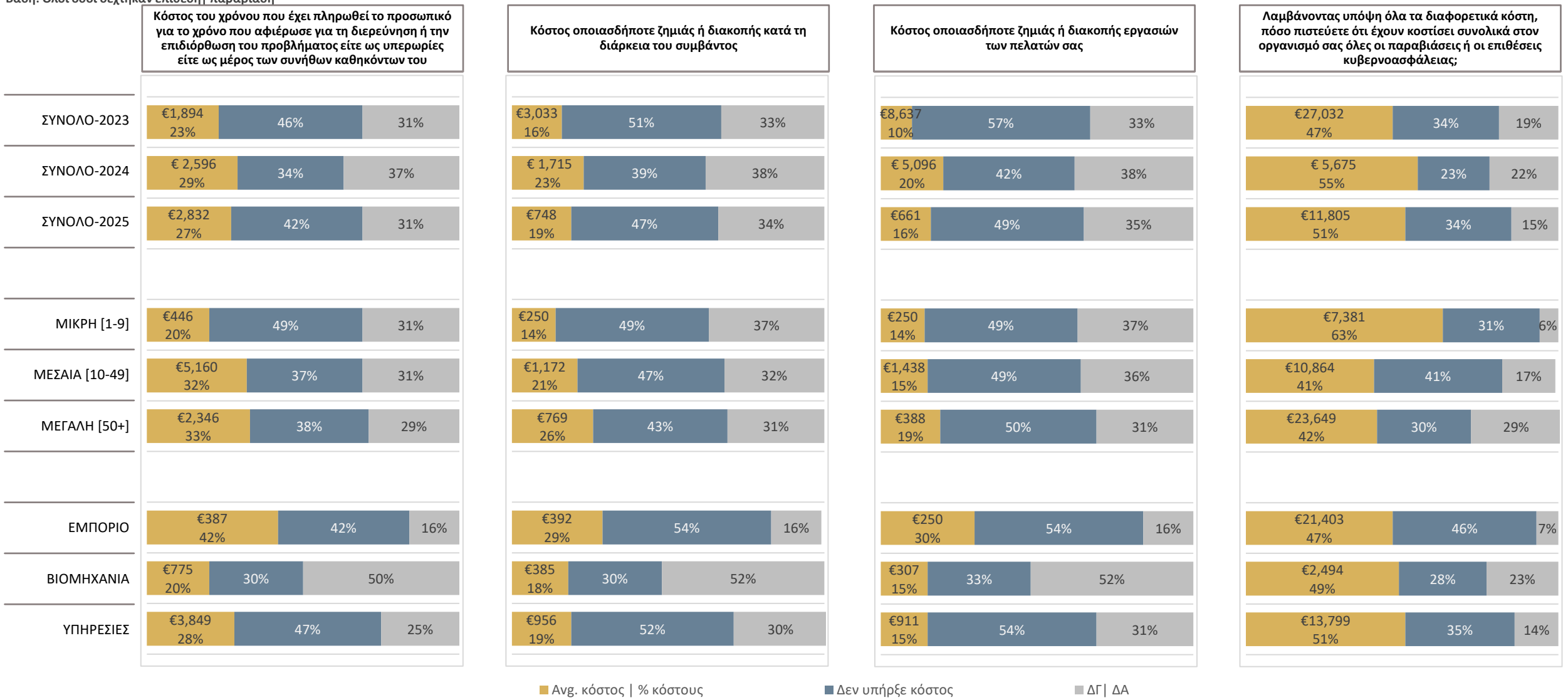
Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

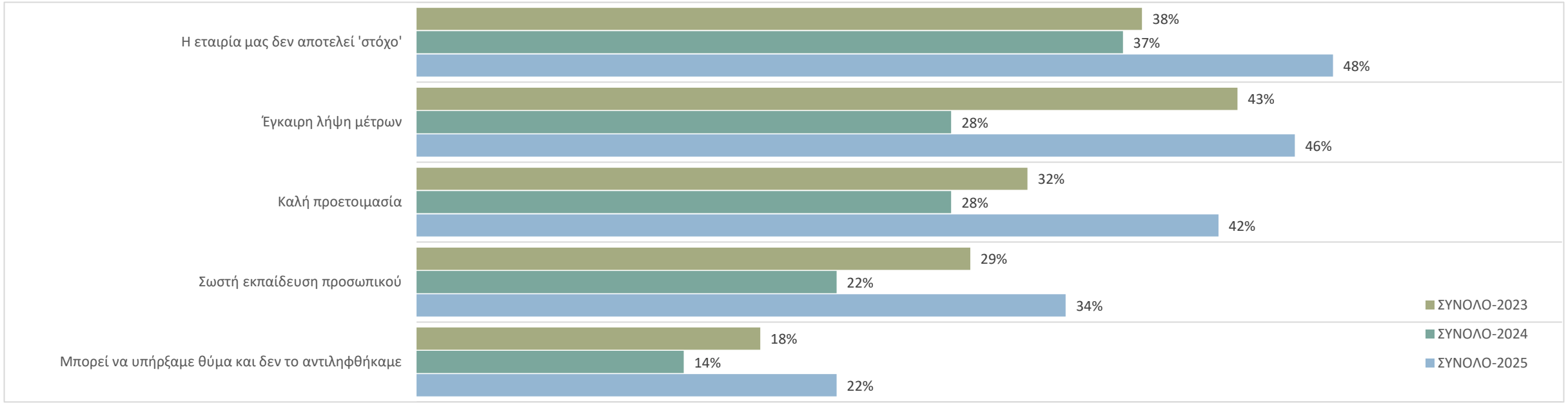
... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση| παραβίαση



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

Βάση: : Όλοι όσοι δεν δέχτηκαν επίθεση| παραβίαση

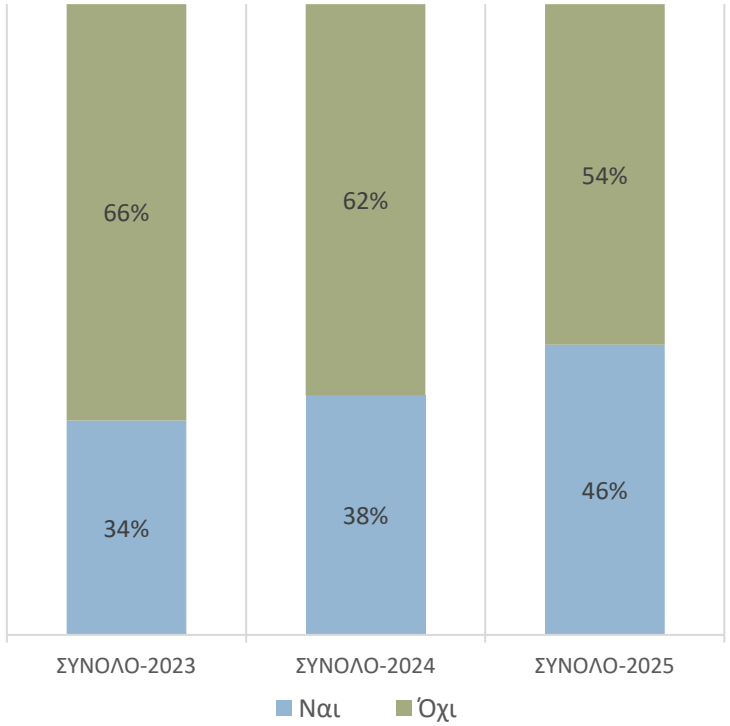


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Η εταιρία μας δεν αποτελεί στόχο	**63%**	38%	29%	83%	62%	42%
Έγκαιρη λήψη μέτρων	51%	37%	54%	65%	12%	**50%**
Καλή προετοιμασία	40%	39%	**57%**	21%	34%	46%
Σωστή εκπαίδευση προσωπικού	31%	32%	**50%**	13%	34%	36%
Μπορεί να υπήρξαμε θύμα και δεν το αντιληφθήκαμε	26%	21%	13%	48%	**45%**	16%

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

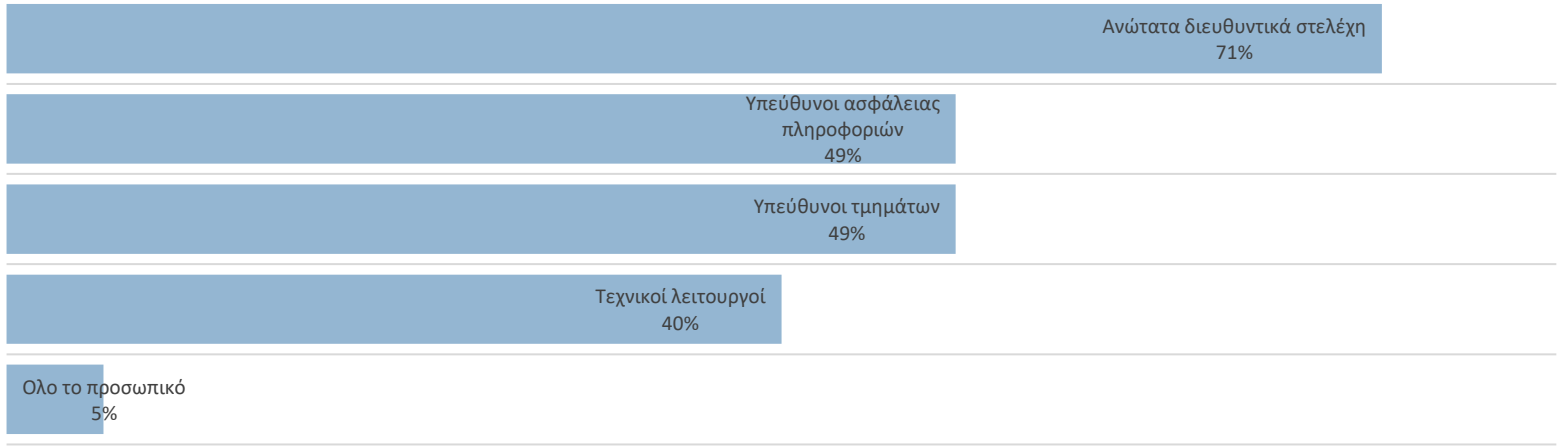
έχετε πραγματοποιήσει κάποια εκπαίδευση ή ενημέρωση για θέματα κυβερνοασφάλειας, για το προσωπικό;



	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Ναι	36%	43%	**68%**	43%	46%	46%
Όχι	**64%**	**57%**	32%	57%	54%	54%

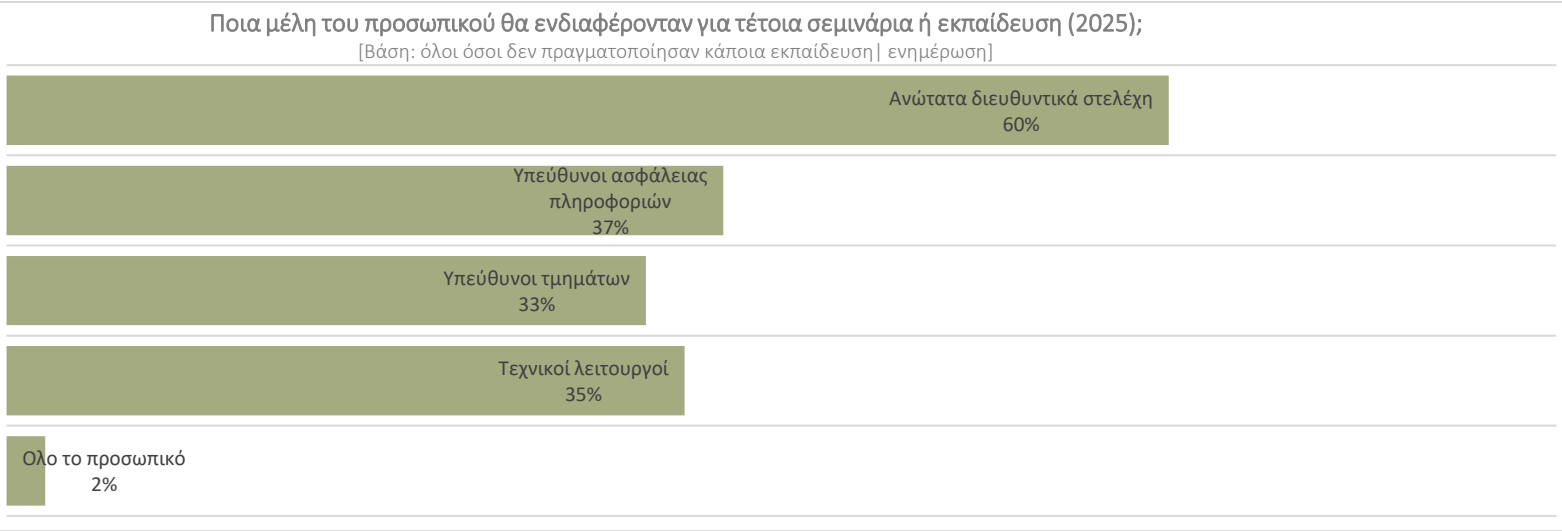
Ποια μέλη του προσωπικού έλαβαν μέρος στα σεμινάρια/εκπαίδευση (2025);

[Βάση: όλοι όσοι πραγματοποίησαν κάποια εκπαίδευση| ενημέρωση]



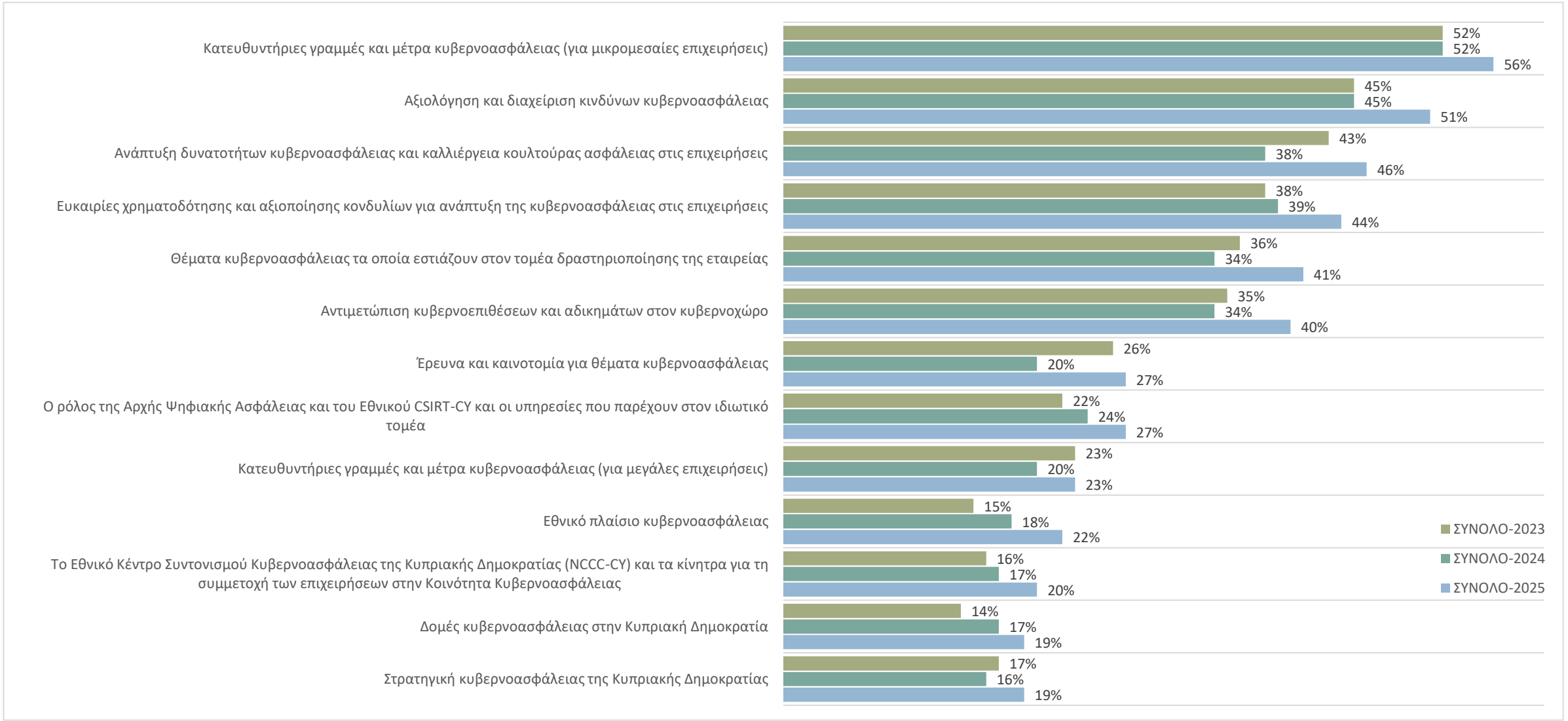
Ποια μέλη του προσωπικού θα ενδιαφέρονταν για τέτοια σεμινάρια ή εκπαίδευση (2025);

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



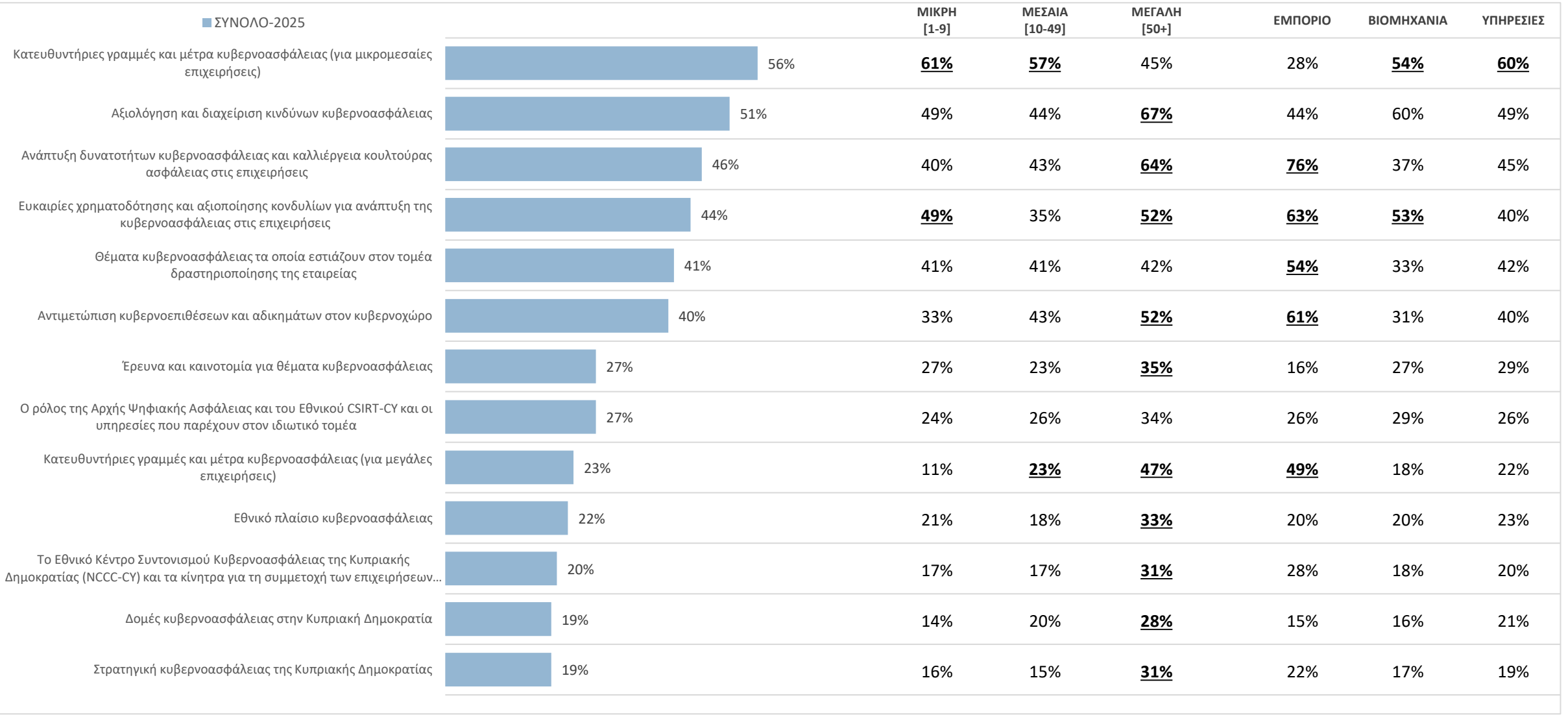
Σε ποια από τα παρακάτω θέματα θα προτιμούσατε να εστιάζουν τα σεμινάρια κατάρτισης;

Βάση: Όλοι οι ερωτώμενοι



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

Βάση: Όλοι οι ερωτώμενοι



	ΣΥΝΟΛΟ-2025	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Κατευθυντήριες γραμμές και μέτρα κυβερνοασφάλειας (για μικρομεσαίες επιχειρήσεις)	56%	**61%**	**57%**	45%	28%	**54%**	**60%**
Αξιολόγηση και διαχείριση κινδύνων κυβερνοασφάλειας	51%	49%	44%	**67%**	44%	60%	49%
Ανάπτυξη δυνατοτήτων κυβερνοασφάλειας και καλλιέργεια κουλτούρας ασφάλειας στις επιχειρήσεις	46%	40%	43%	**64%**	**76%**	37%	45%
Ευκαιρίες χρηματοδότησης και αξιοποίησης κονδυλίων για ανάπτυξη της κυβερνοασφάλειας στις επιχειρήσεις	44%	**49%**	35%	**52%**	**63%**	**53%**	40%
Θέματα κυβερνοασφάλειας τα οποία εστιάζουν στον τομέα δραστηριοποίησης της εταιρείας	41%	41%	41%	42%	**54%**	33%	42%
Αντιμετώπιση κυβερνοεπιθέσεων και αδικημάτων στον κυβερνοχώρο	40%	33%	43%	**52%**	**61%**	31%	40%
Έρευνα και καινοτομία για θέματα κυβερνοασφάλειας	27%	27%	23%	**35%**	16%	27%	29%
Ο ρόλος της Αρχής Ψηφιακής Ασφάλειας και του Εθνικού CSIRT-CY και οι υπηρεσίες που παρέχουν στον ιδιωτικό τομέα	27%	24%	26%	34%	26%	29%	26%
Κατευθυντήριες γραμμές και μέτρα κυβερνοασφάλειας (για μεγάλες επιχειρήσεις)	23%	11%	**23%**	**47%**	**49%**	18%	22%
Εθνικό πλαίσιο κυβερνοασφάλειας	22%	21%	18%	**33%**	20%	20%	23%
Το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (NCCC-CY) και τα κίνητρα για τη συμμετοχή των επιχειρήσεων...	20%	17%	17%	**31%**	28%	18%	20%
Δομές κυβερνοασφάλειας στην Κυπριακή Δημοκρατία	19%	14%	20%	**28%**	15%	16%	21%
Στρατηγική κυβερνοασφάλειας της Κυπριακής Δημοκρατίας	19%	16%	15%	**31%**	22%	17%	19%

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

ΕΤΟΙΜΑΣΤΗΚΕ ΓΙΑ ΤΗΝ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΝΟΕΜΒΡΙΟΣ 2025

RAI Consultants Ltd

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ