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

ΕΤΟΙΜΑΣΤΗΚΕ ΓΙΑ ΤΗΝ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΟΚΤΩΒΡΙΟΣ 2024

RAI Consultants Ltd

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

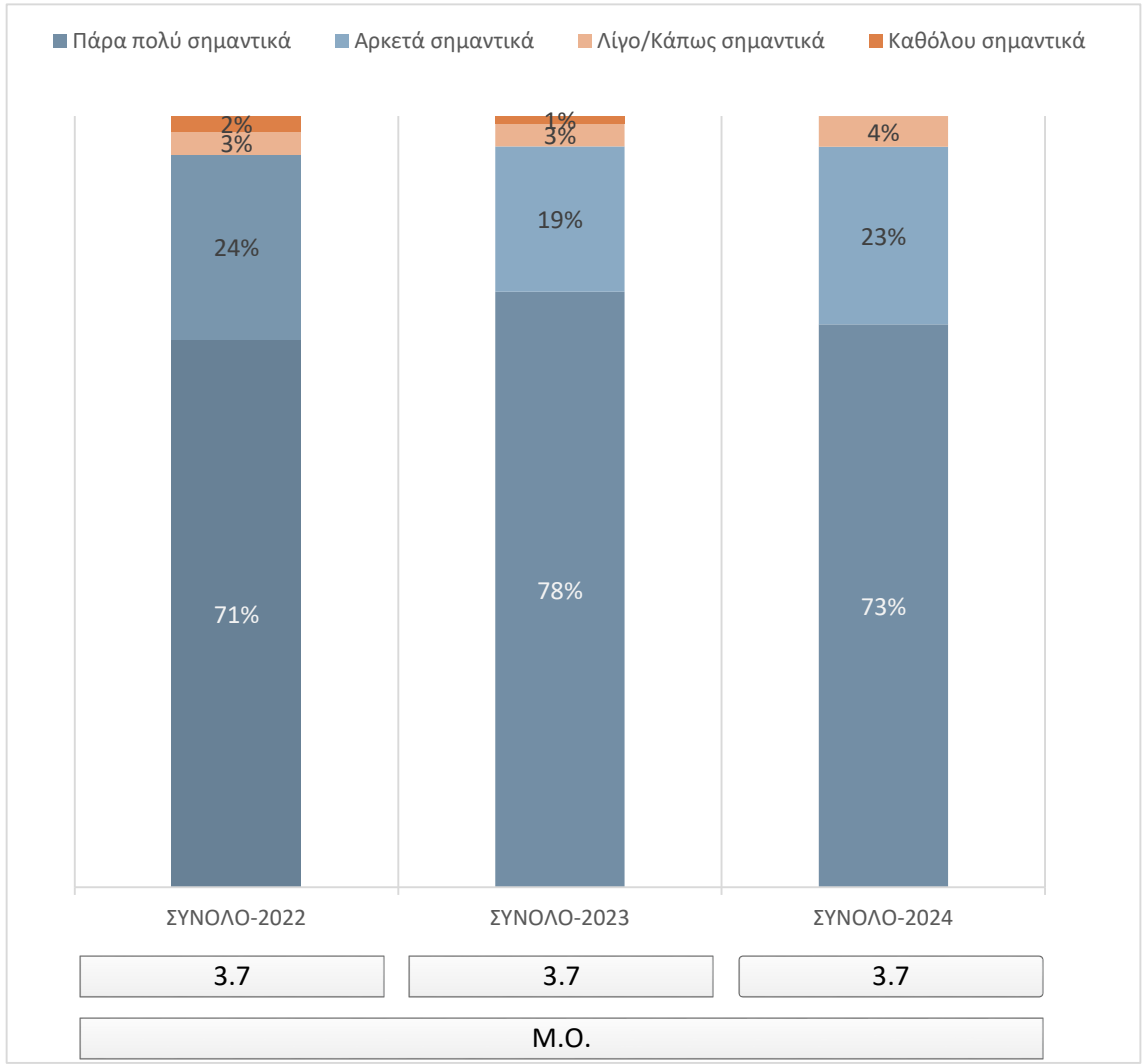
Εισαγωγή & Μεθοδολογία

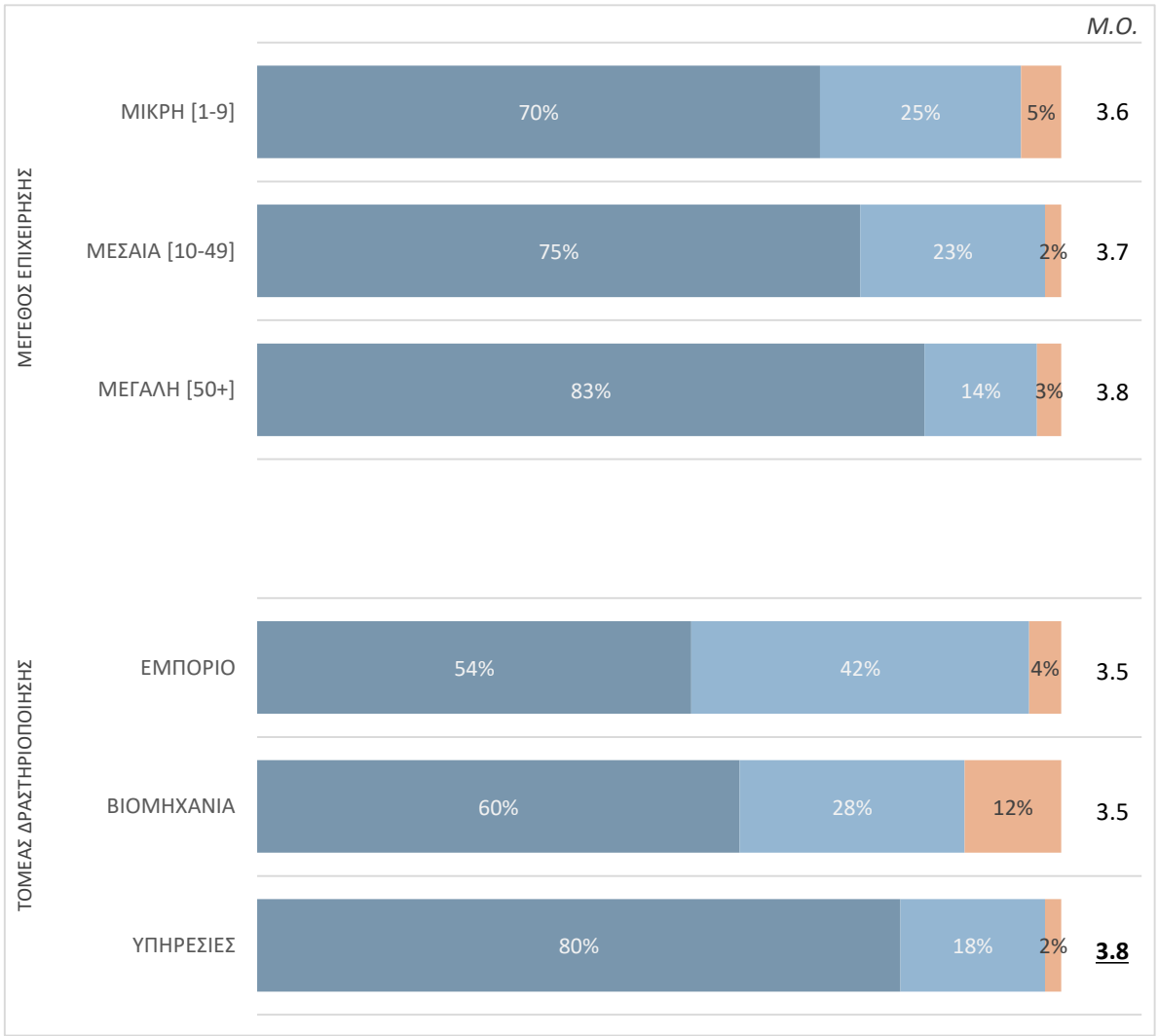
Αντικείμενο Μελέτης	Αντικείμενο της Σύμβασης αποτελεί η Παροχή Υπηρεσιών διεξαγωγής έρευνας σε επιχειρήσεις, σε σχέση με τον τρόπο χειρισμού θεμάτων κυβερνοασφάλειας, αποτίμησης της σημαντικότητας που αποδίδεται στα θέματα κυβερνοασφάλειας, τον τρόπο αντιμετώπισης περιστατικών κυβερνοασφάλειας ή/και 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** ολοκληρωμένα ερωτηματολόγια εκ των οποίων:	243 επιχειρήσεις είχαν συνολικό αριθμό απασχολουμένων μέχρι 9 άτομα (Μικρή) 144 επιχειρήσεις είχαν συνολικό αριθμό απασχολουμένων 10-49 άτομα (Μεσαία) 63 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	12 Σεπτεμβρίου – 11 Οκτωβρίου 2024	
Σύγκριση αποτελεσμάτων	Τα αποτελέσματα του έργου συγκρίνονται με τα αποτελέσματα της ίδιας έρευνας που διεξάχθηκαν τον Οκτώβριο 2022 & τον Νοέμβριο 2023	

ΑΝΑΛΥΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

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

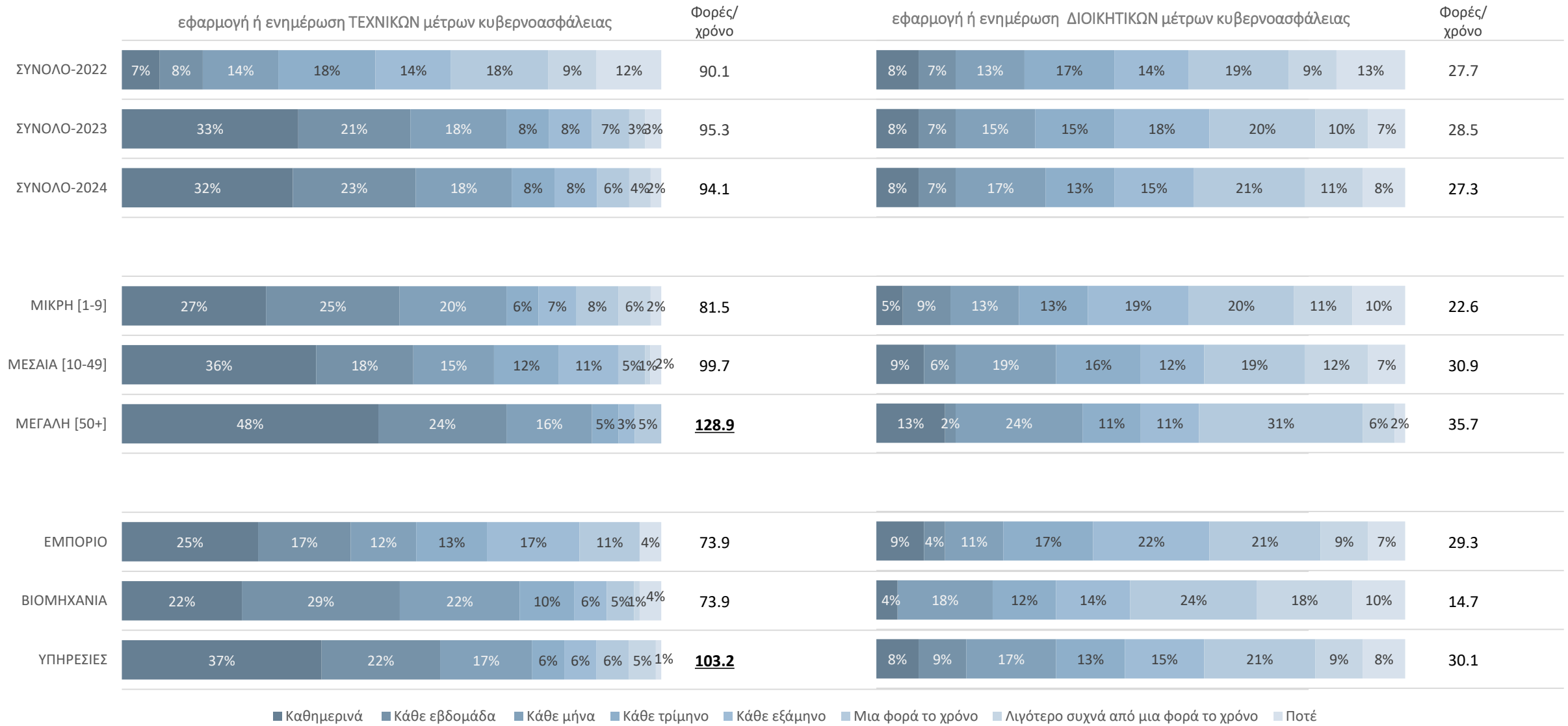
Βάση: Όλοι οι ερωτώμενοι





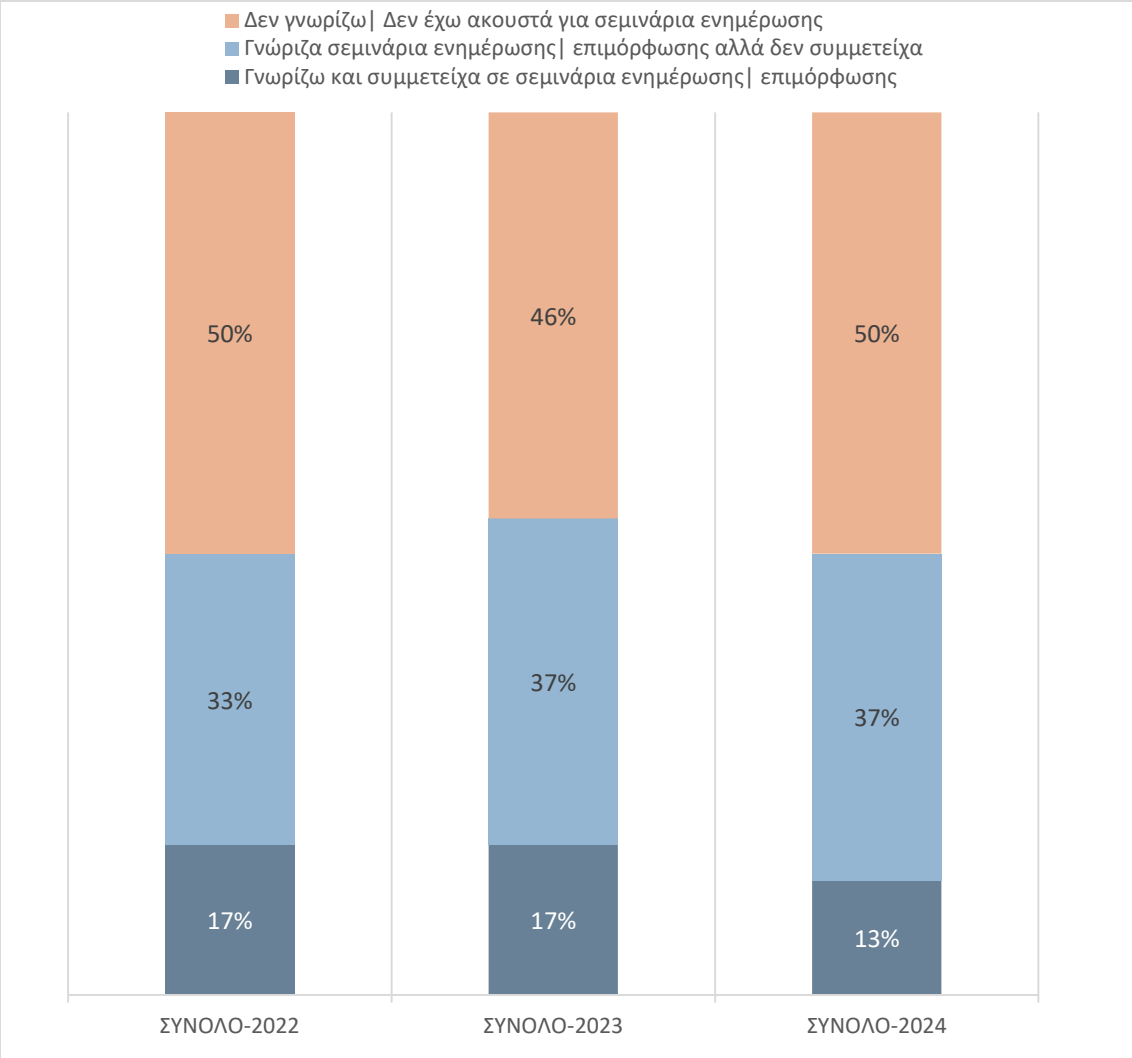
Πόσο συχνά προβαίνει η εταιρία σας σε εφαρμογή ή ενημέρωση ΤΕΧΝΙΚΩΝ | ΔΙΟΙΚΗΤΙΚΩΝ μέτρων κυβερνοασφάλειας;

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;

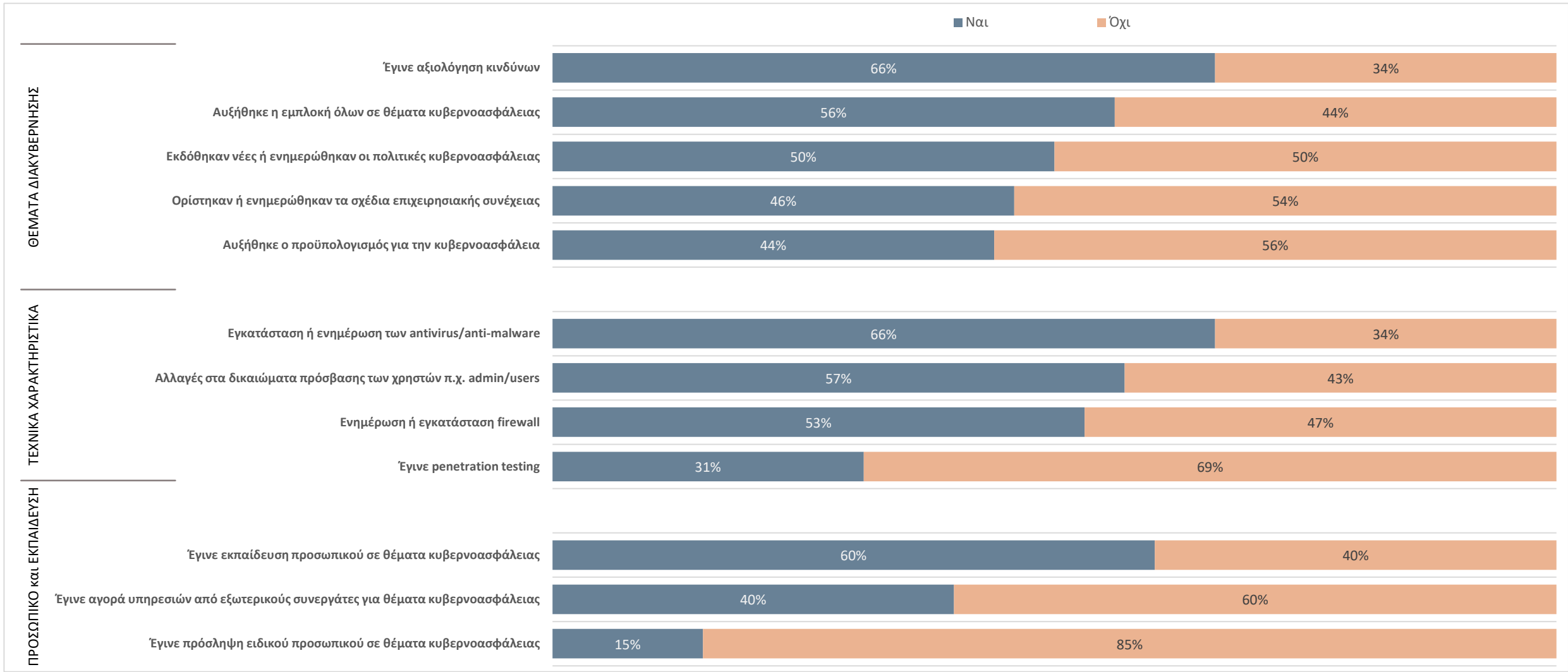
Βάση: Όλοι οι ερωτώμενοι



	Γνώση	Συμμετοχή
Σερφάρω στο Διαδίκτυο με Ασφάλεια (ΚΕΠΑ)	24%	3%
Cyberbullying - Εκφοβισμός μέσω Διαδικτύου (CYTA)	18%	4%
Ημερίδα για τη Διεθνή Ημέρα Ασφαλούς Διαδικτύου	15%	3%
DIGITAL SECURITY STAKEHOLDERS CONFERENCE (ΑΨΑ| Εθνικό CSIRT-CY)	12%	5%
CyberSafety: Ένα Καλύτερο Διαδίκτυο για τα Παιδιά στην Κύπρο (ΣΧΟΛΗ ΓΟΝΕΩΝ)	11%	2%
Course on Cybersecurity Organisational and Defensive Capabilities (ΑΨΑ|Εθνικό CSIRT-CY ESDC)	8%	3%
Μαθητική Ημερίδα "Ασφαλές διαδίκτυο για όλους" (ΥΠ.ΠΑΙΔΕΙΑΣ)	6%	1%
ITU Cyber Drill - ALERT (Applied Learning for Emergency Response Teams)	4%	1%
"Together for a better internet"	3%	1%

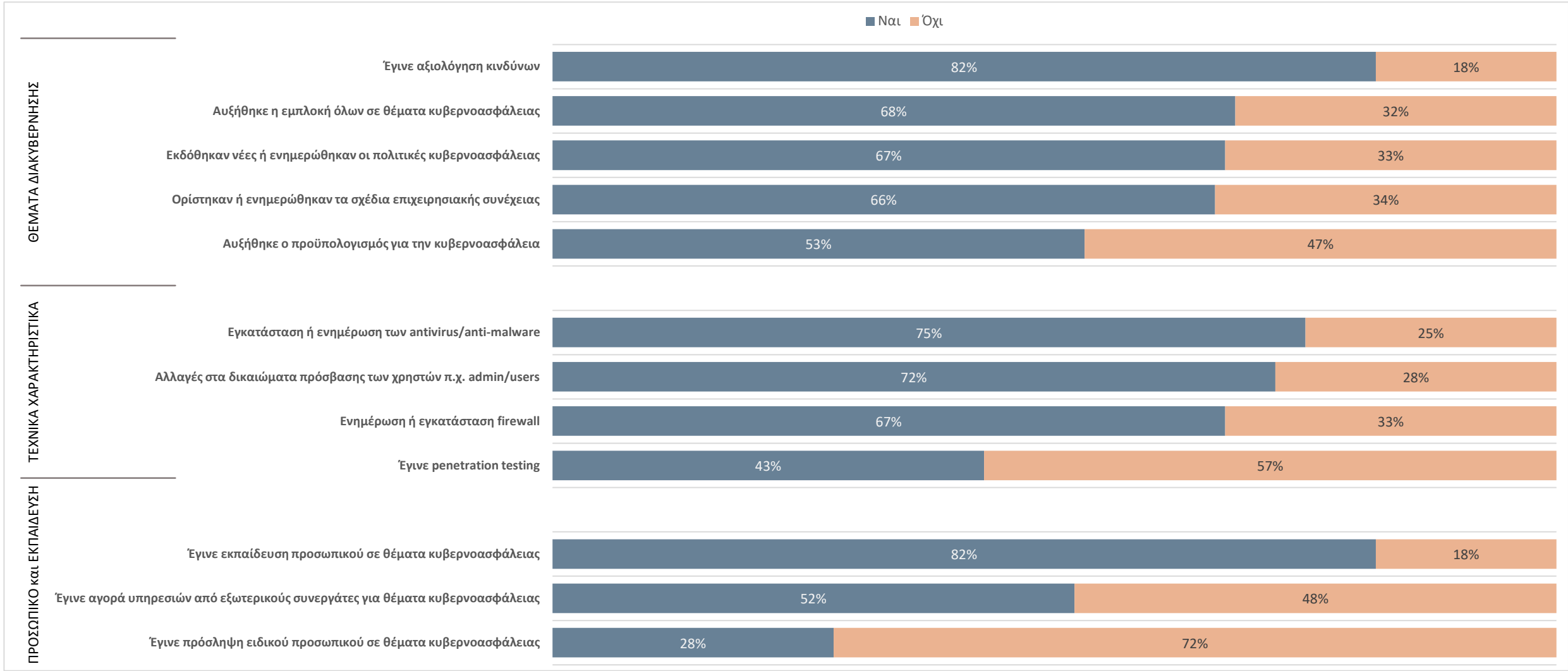
Τι από τα ακόλουθα έχετε αλλάξει σε θέματα κυβερνοασφάλειας, εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι ΓΝΩΡΙΖΟΥΝ σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια (225)



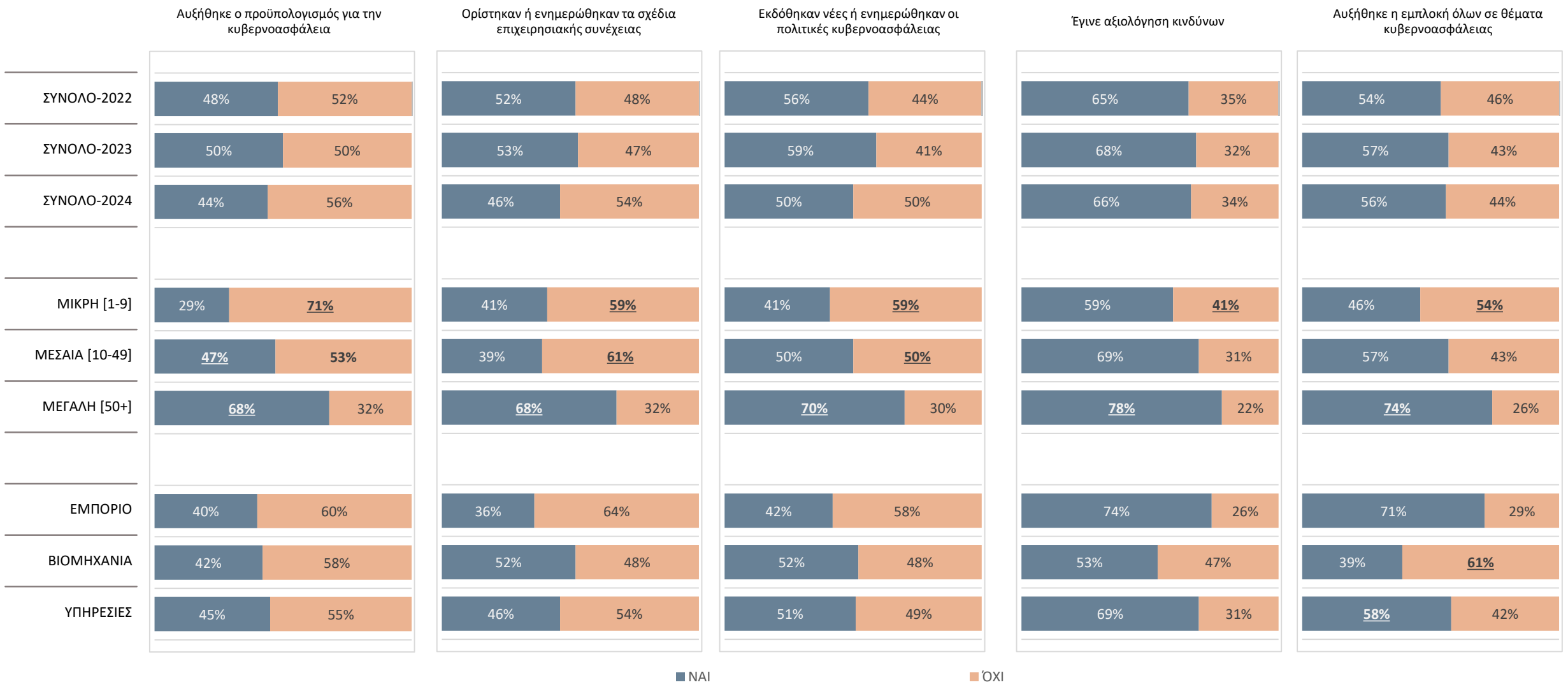
Τι από τα ακόλουθα έχετε αλλάξει σε θέματα κυβερνοασφάλειας, εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι ΣΥΜΜΕΤΕΙΧΑΝ σε σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια (58)



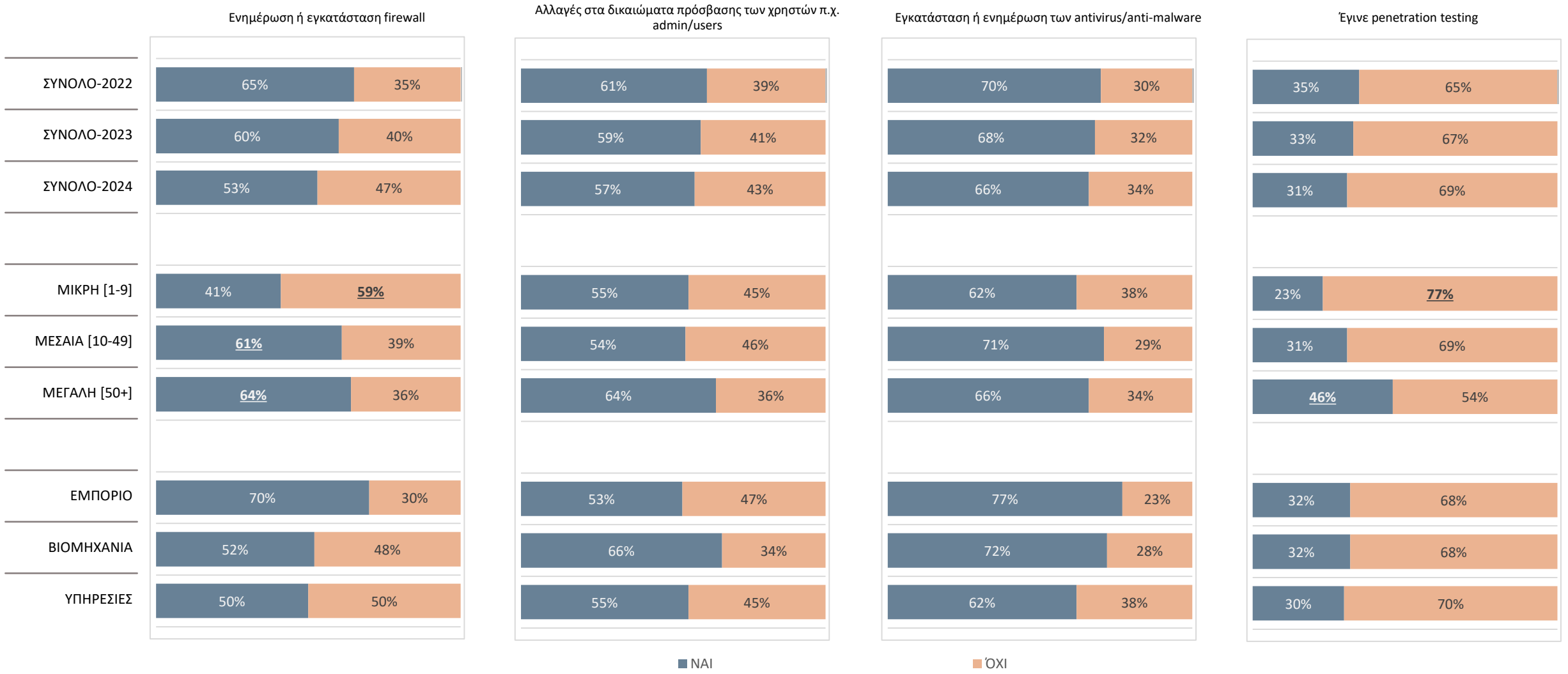
Τι από τα ακόλουθα έχετε αλλάξει σε σχέση με την ΔΙΑΚΥΒΕΡΝΗΣΗ στον οργανισμό, εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι ΓΝΩΡΙΖΟΥΝ σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια (225)



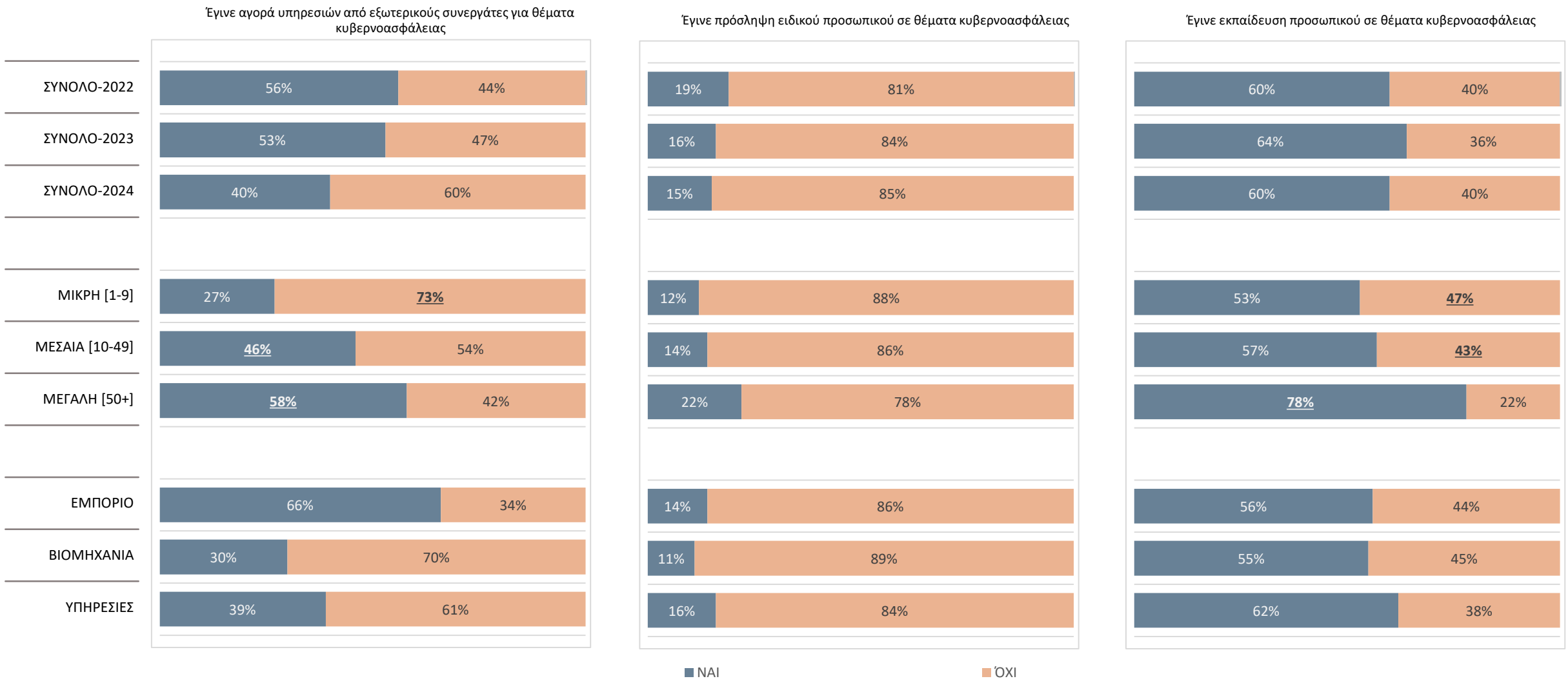
Τι από τα ακόλουθα ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ, έχετε αλλάξει εξαιτίας αυτών των σεμιναρίων;

Βάση: Όλοι όσοι ΓΝΩΡΙΖΟΥΝ σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια (225)



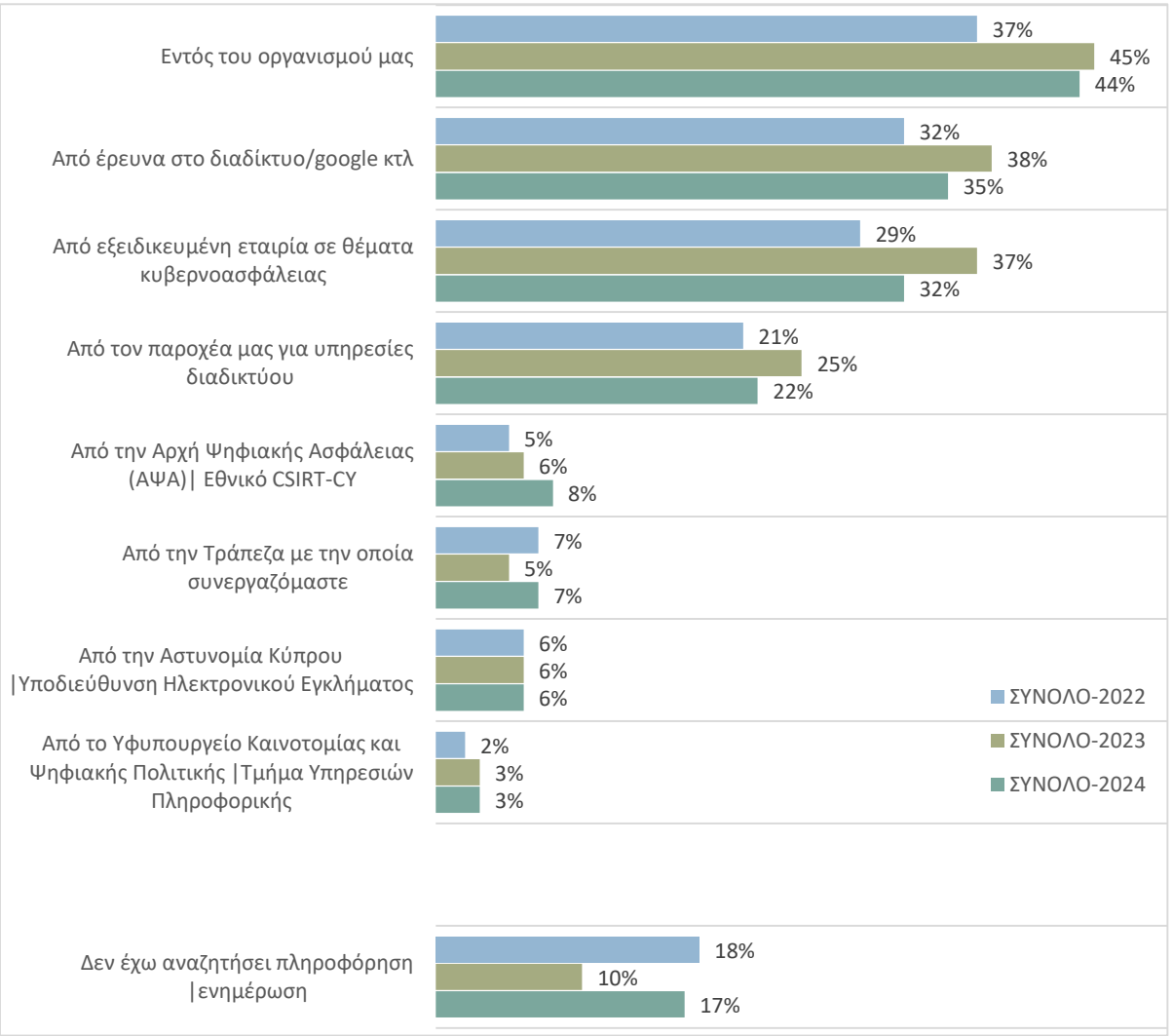
Και τι από τα ακόλουθα έχετε αλλάξει όσον αφορά στο ΠΡΟΣΩΠΙΚΟ και ΕΚΠΑΙΔΕΥΣΗ του προσωπικού;

Βάση: Όλοι όσοι ΓΝΩΡΙΖΟΥΝ σεμινάρια ενημέρωσης και εκπαίδευσης για την κυβερνοασφάλεια (225)



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

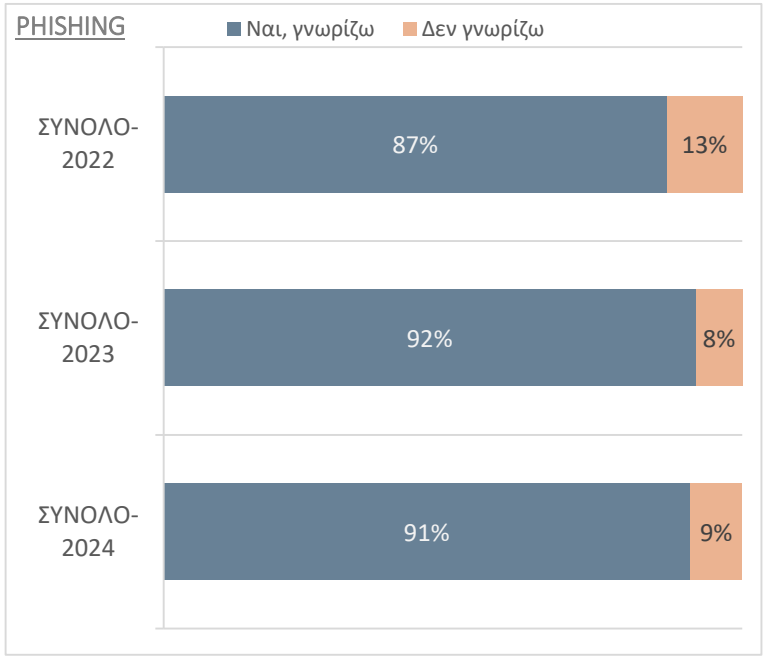
Βάση: Όλοι οι ερωτώμενοι

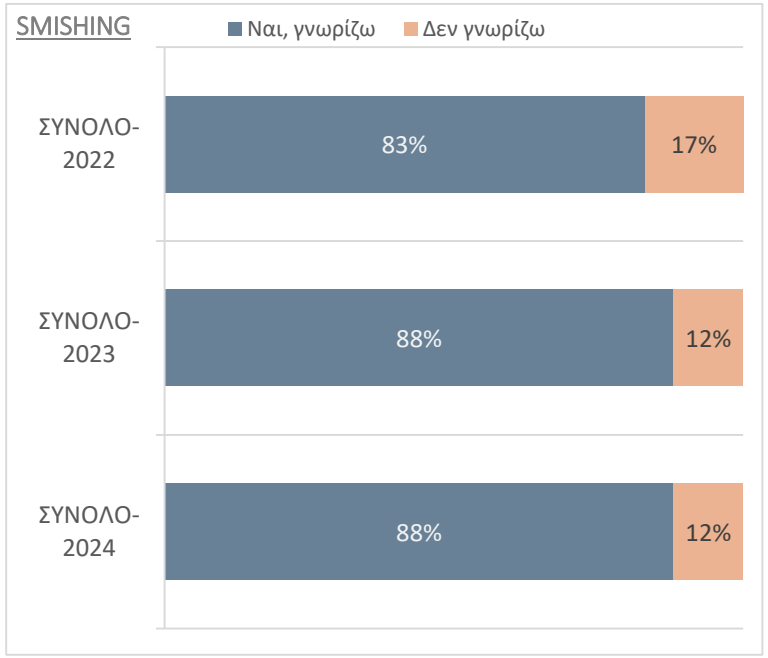


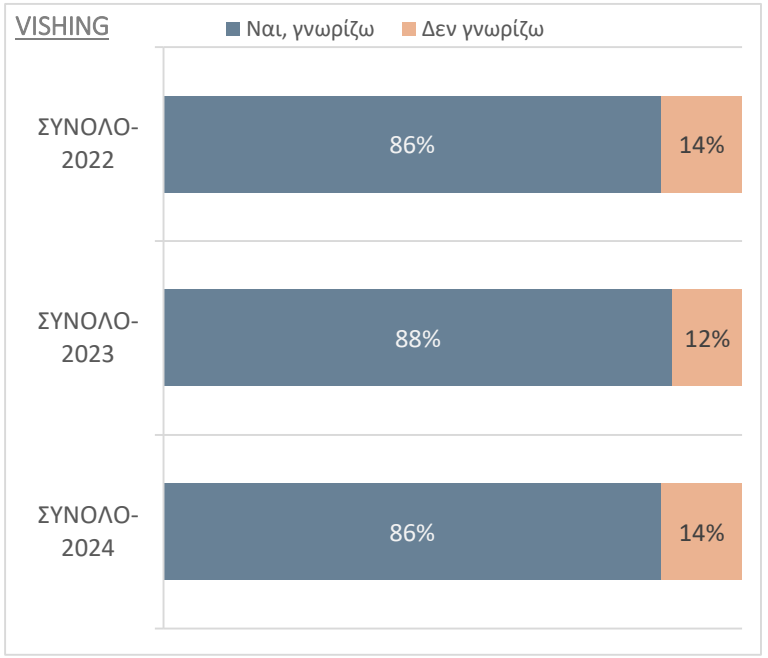
	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Εντός του οργανισμού μας	37%	**50%**	**54%**	40%	33%	**47%**
Από έρευνα στο διαδίκτυο/google κτλ	35%	36%	35%	35%	21%	**39%**
Από εξειδικευμένη εταιρία σε θέματα κυβερνοασφάλειας	23%	30%	**67%**	19%	32%	**34%**
Από τον παροχέα μας για υπηρεσίες διαδικτύου	25%	17%	21%	**36%**	22%	19%
Από την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)| Εθνικό CSIRT-CY	8%	5%	**14%**	2%	1%	**11%**
Από την Τράπεζα με την οποία συνεργαζόμαστε	**10%**	2%	5%	**17%**	4%	5%
Από την Αστυνομία Κύπρου |Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος	6%	6%	5%	3%	3%	7%
Από το Υφυπουργείο Καινοτομίας και Ψηφιακής Πολιτικής |Τμήμα Υπηρεσιών Πληροφορικής	3%	4%	3%	0%	0%	5%
Δεν έχω αναζητήσει πληροφόρηση |ενημέρωση	21%	13%	11%	11%	**27%**	16%

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

Βάση: Όλοι οι ερωτώμενοι



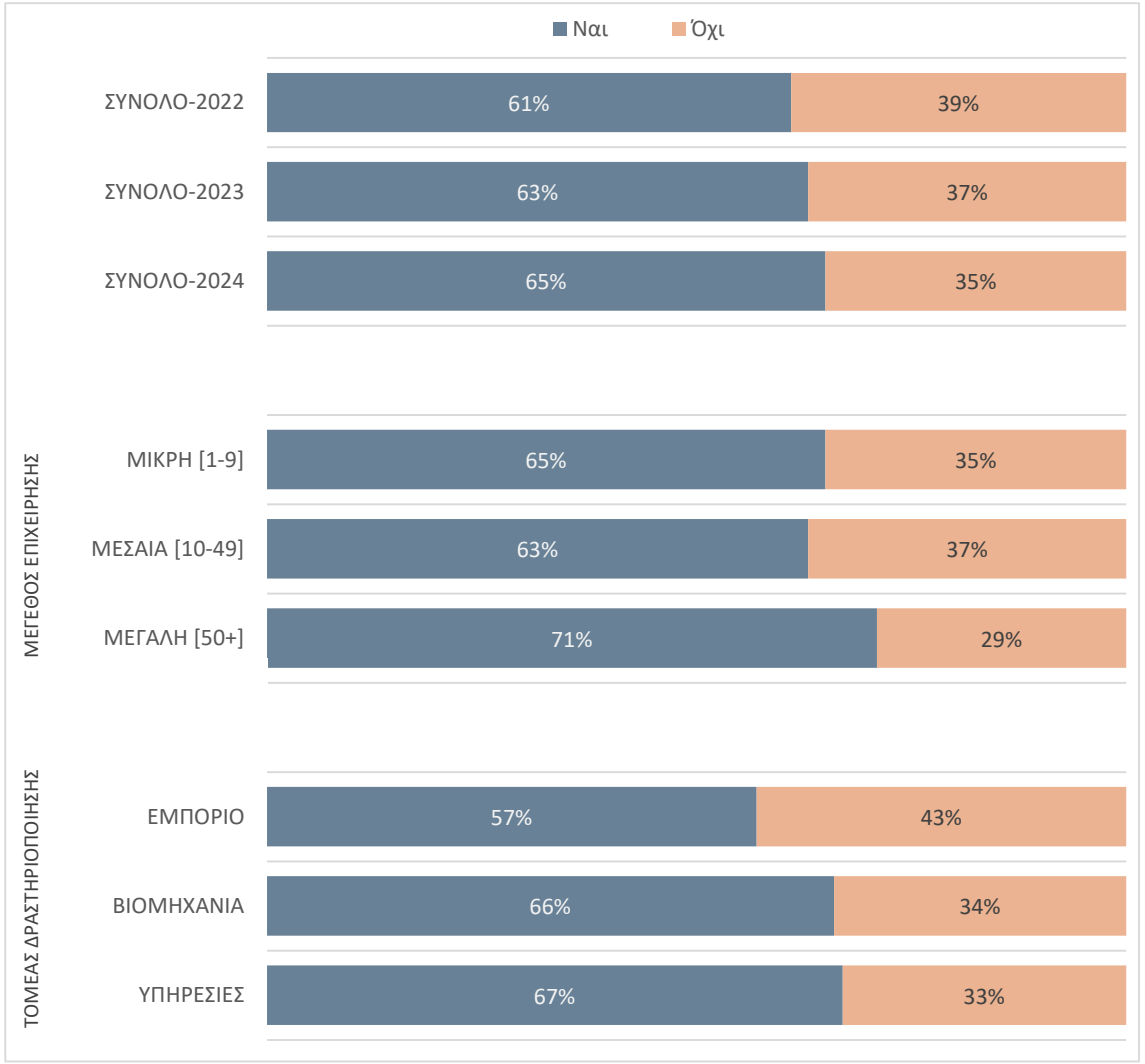


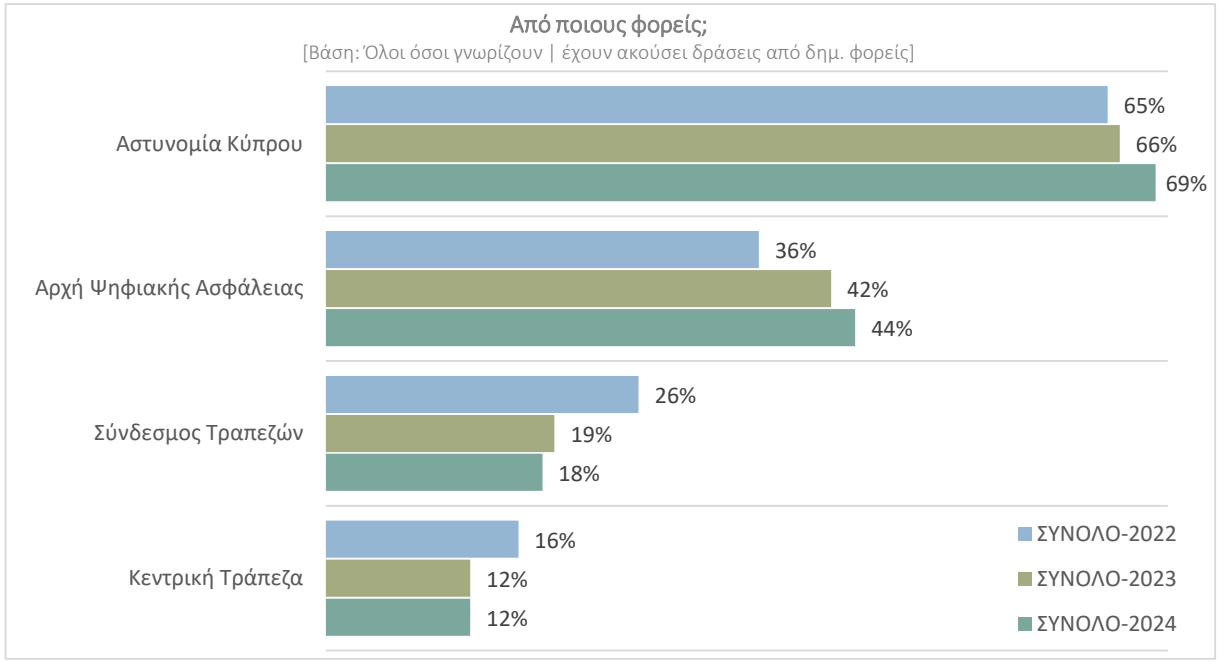


		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
PHISHING	Ναι, γνωρίζω	**93%**	84%	**100%**	92%	91%	91%
	Δεν γνωρίζω	**7%**	**16%**	0%	8%	9%	9%
SMISHING	Ναι, γνωρίζω	89%	83%	**95%**	92%	89%	87%
	Δεν γνωρίζω	11%	**17%**	5%	8%	11%	13%
VISHING	Ναι, γνωρίζω	85%	84%	**95%**	**96%**	86%	84%
	Δεν γνωρίζω	**15%**	**16%**	5%	4%	14%	**16%**

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

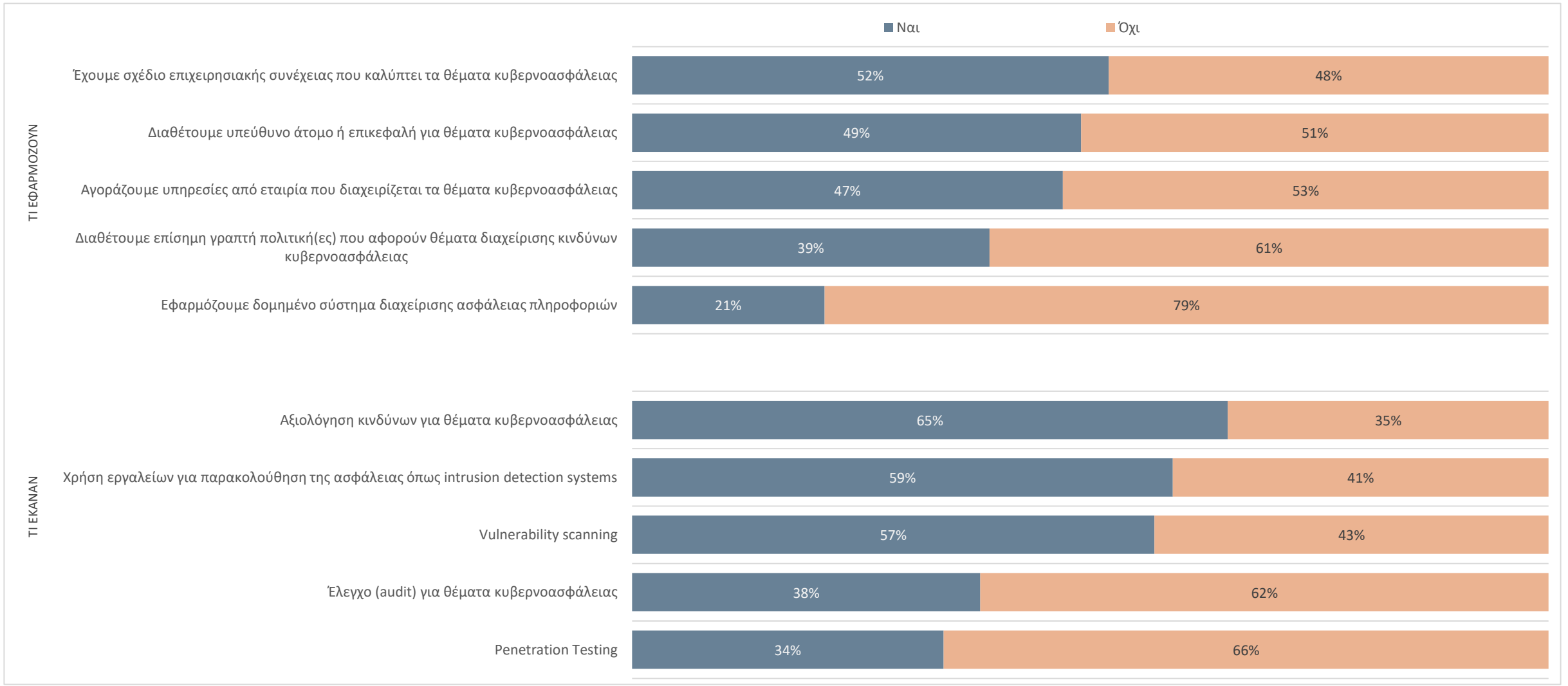




	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Αστυνομία Κύπρου	73%	64%	62%	64%	75%	68%
Αρχή Ψηφιακής Ασφάλειας	34%	**51%**	**64%**	35%	31%	**49%**
Σύνδεσμος Τραπεζών	13%	**27%**	16%	24%	25%	15%
Κεντρική Τράπεζα	11%	11%	16%	10%	15%	11%

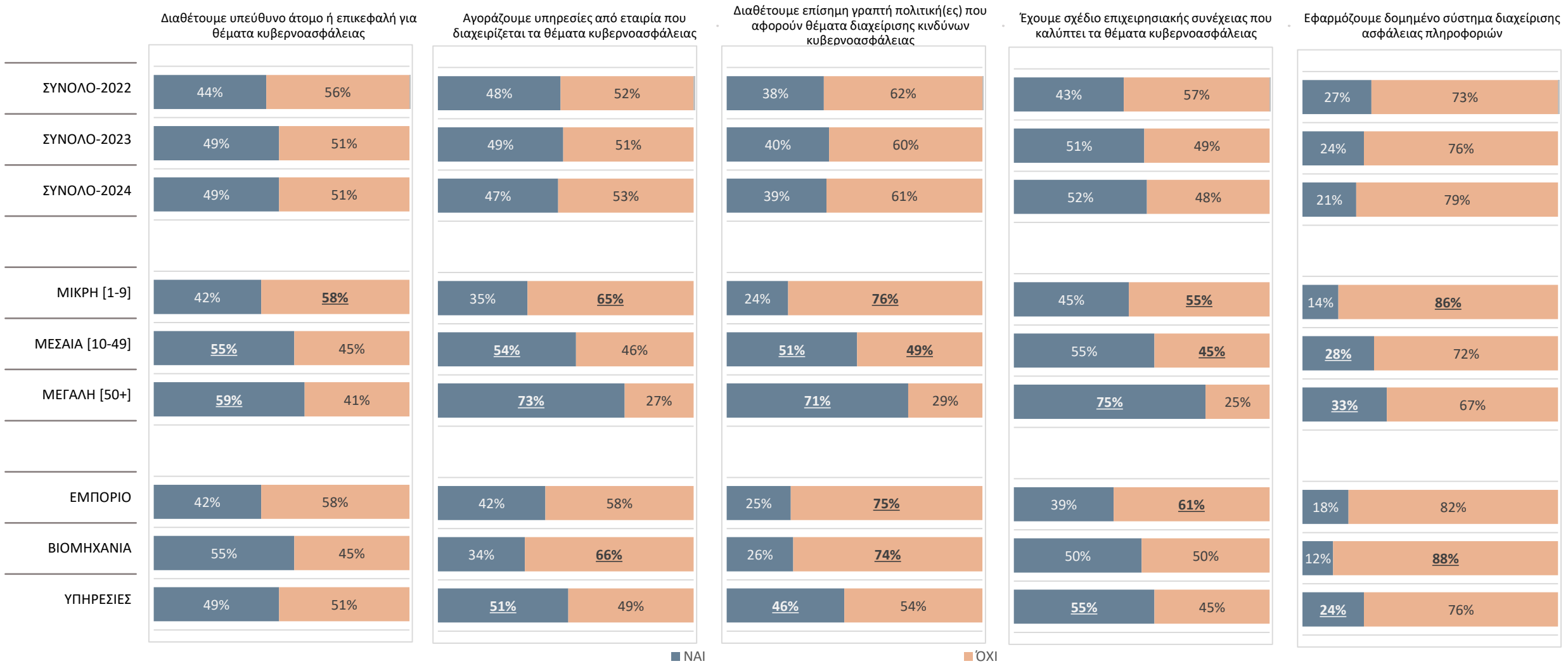
Ποιες από τις ακόλουθες αρχές διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας εφαρμόζετε στην εταιρεία; | Και ποια από τα ακόλουθα έχετε κάνει τους τελευταίους 12 μήνες για να εντοπίσετε κινδύνους;

Βάση: Όλοι οι ερωτώμενοι



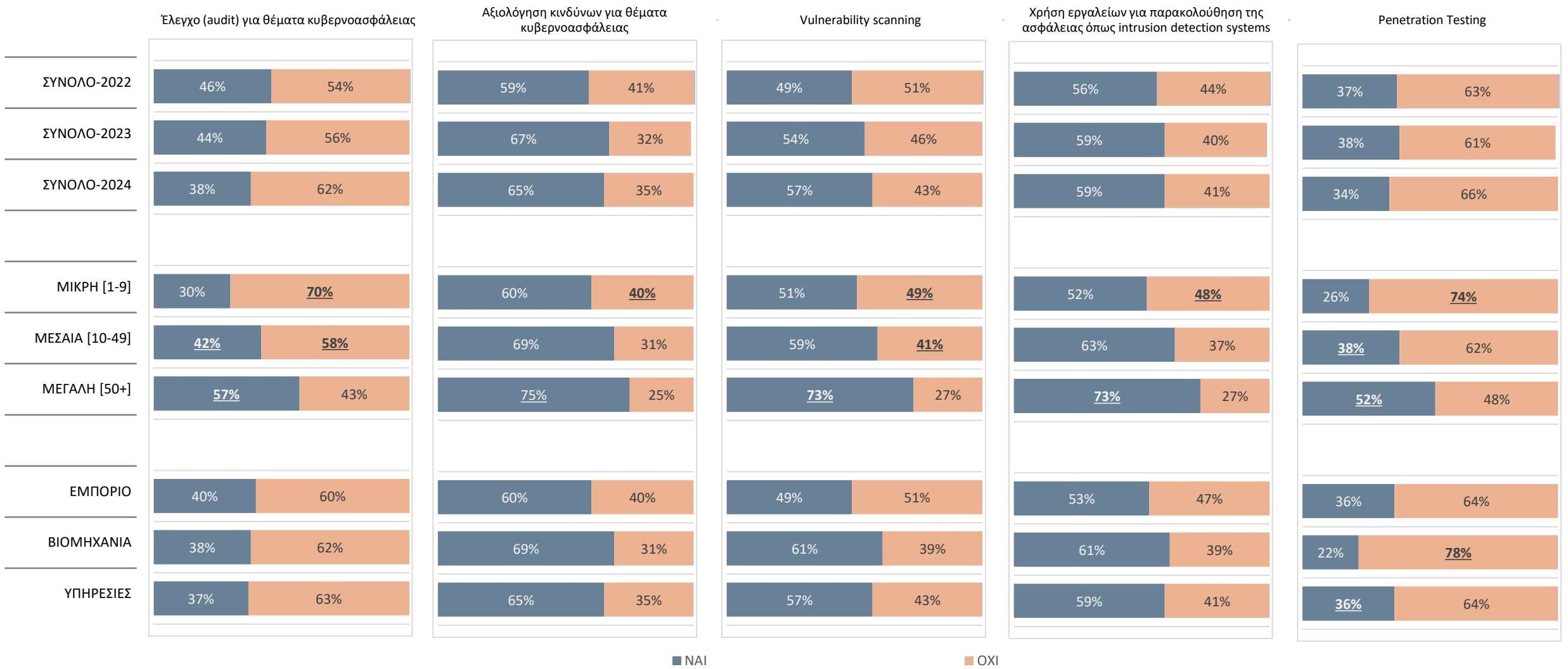
Ποιες από τις ακόλουθες αρχές διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας εφαρμόζετε στην εταιρεία;

Βάση: Όλοι οι ερωτώμενοι



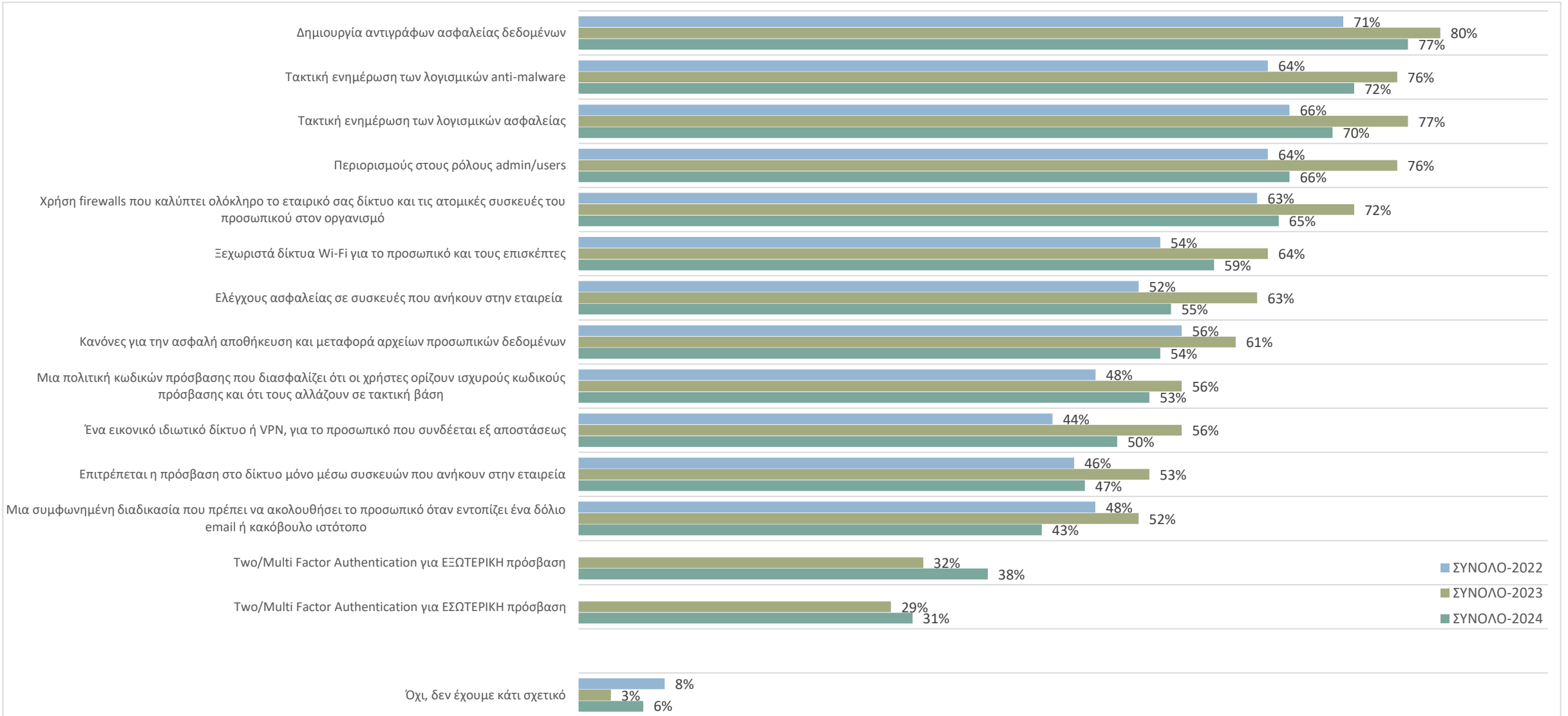
Και ποια από τα ακόλουθα έχετε κάνει τους τελευταίους 12 μήνες για να εντοπίσετε κινδύνους που αφορούν την κυβερνοασφάλεια της εταιρίας;

Βάση: Όλοι οι ερωτώμενοι



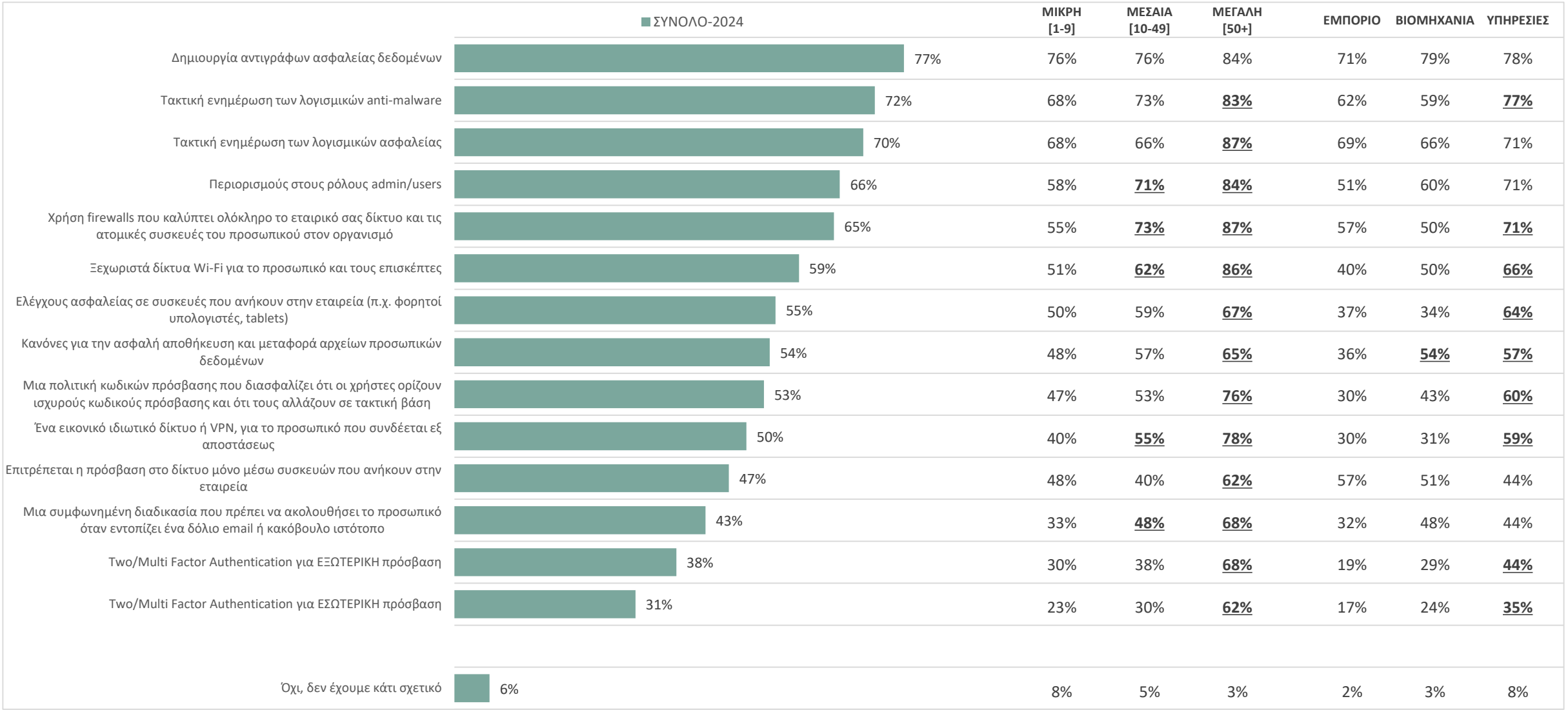
Ποιους από τους ακόλουθους κανόνες ή ελέγχους εφαρμόζετε στην επιχείρηση | εταιρεία σας;

Βάση: Όλοι οι ερωτώμενοι



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

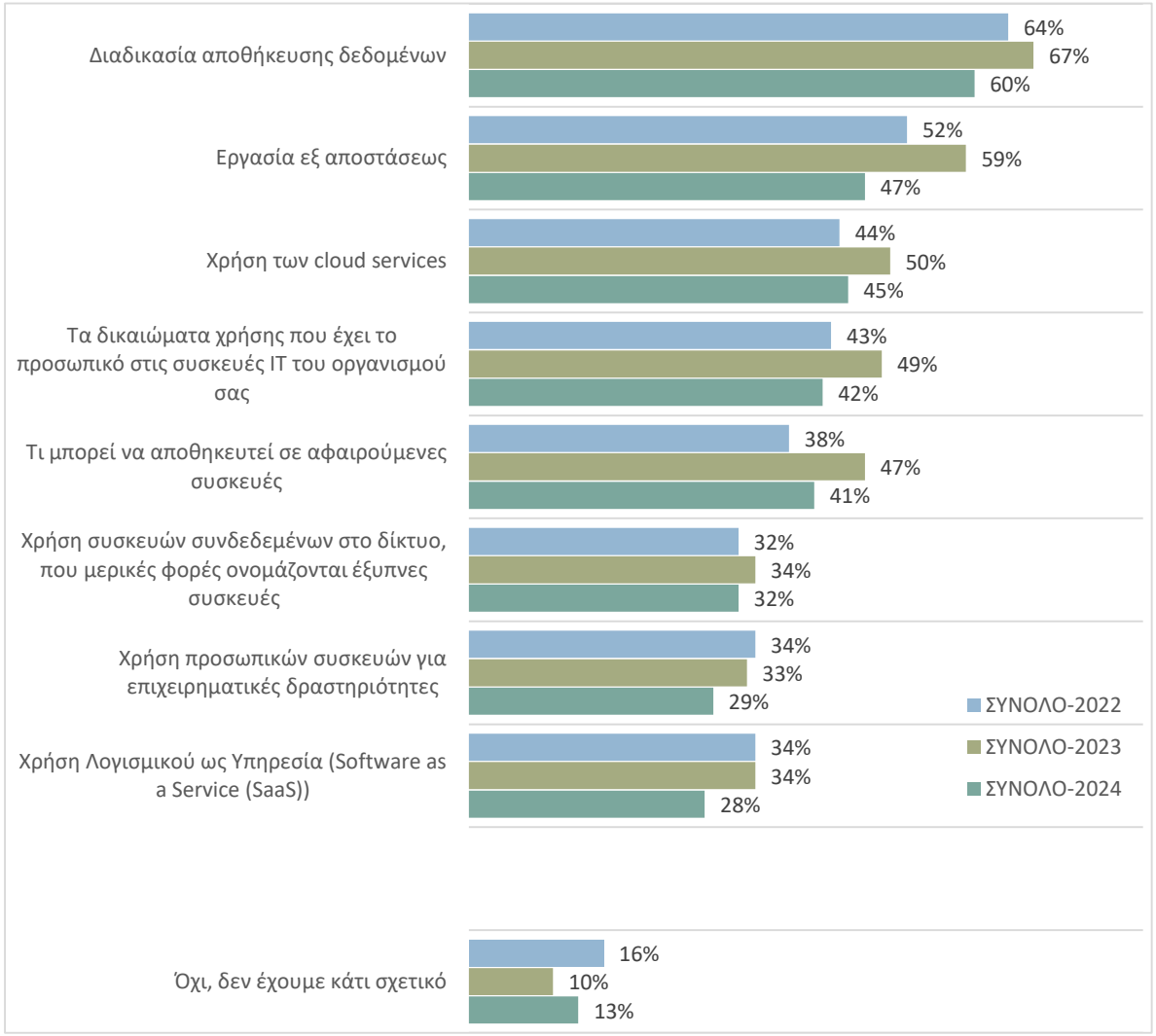
Βάση: Όλοι οι ερωτώμενοι



	ΣΥΝΟΛΟ-2024	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Δημιουργία αντιγράφων ασφαλείας δεδομένων	77%	76%	76%	84%	71%	79%	78%
Τακτική ενημέρωση των λογισμικών anti-malware	72%	68%	73%	**83%**	62%	59%	**77%**
Τακτική ενημέρωση των λογισμικών ασφαλείας	70%	68%	66%	**87%**	69%	66%	71%
Περιορισμούς στους ρόλους admin/users	66%	58%	**71%**	**84%**	51%	60%	71%
Χρήση firewalls που καλύπτει ολόκληρο το εταιρικό σας δίκτυο και τις ατομικές συσκευές του προσωπικού στον οργανισμό	65%	55%	**73%**	**87%**	57%	50%	**71%**
Ξεχωριστά δίκτυα Wi-Fi για το προσωπικό και τους επισκέπτες	59%	51%	**62%**	**86%**	40%	50%	**66%**
Ελέγχους ασφαλείας σε συσκευές που ανήκουν στην εταιρεία (π.χ. φορητοί υπολογιστές, tablets)	55%	50%	59%	**67%**	37%	34%	**64%**
Κανόνες για την ασφαλή αποθήκευση και μεταφορά αρχείων προσωπικών δεδομένων	54%	48%	57%	**65%**	36%	**54%**	**57%**
Μια πολιτική κωδικών πρόσβασης που διασφαλίζει ότι οι χρήστες ορίζουν ισχυρούς κωδικούς πρόσβασης και ότι τους αλλάζουν σε τακτική βάση	53%	47%	53%	**76%**	30%	43%	**60%**
Ένα εικονικό ιδιωτικό δίκτυο ή VPN, για το προσωπικό που συνδέεται εξ αποστάσεως	50%	40%	**55%**	**78%**	30%	31%	**59%**
Επιτρέπεται η πρόσβαση στο δίκτυο μόνο μέσω συσκευών που ανήκουν στην εταιρεία	47%	48%	40%	**62%**	57%	51%	44%
Μια συμφωνημένη διαδικασία που πρέπει να ακολουθήσει το προσωπικό όταν εντοπίζει ένα δόλιο email ή κακόβουλο ιστότοπο	43%	33%	**48%**	**68%**	32%	48%	44%
Two/Multi Factor Authentication για ΕΞΩΤΕΡΙΚΗ πρόσβαση	38%	30%	38%	**68%**	19%	29%	**44%**
Two/Multi Factor Authentication για ΕΣΩΤΕΡΙΚΗ πρόσβαση	31%	23%	30%	**62%**	17%	24%	**35%**
Όχι, δεν έχουμε κάτι σχετικό	6%	8%	5%	3%	2%	3%	8%

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

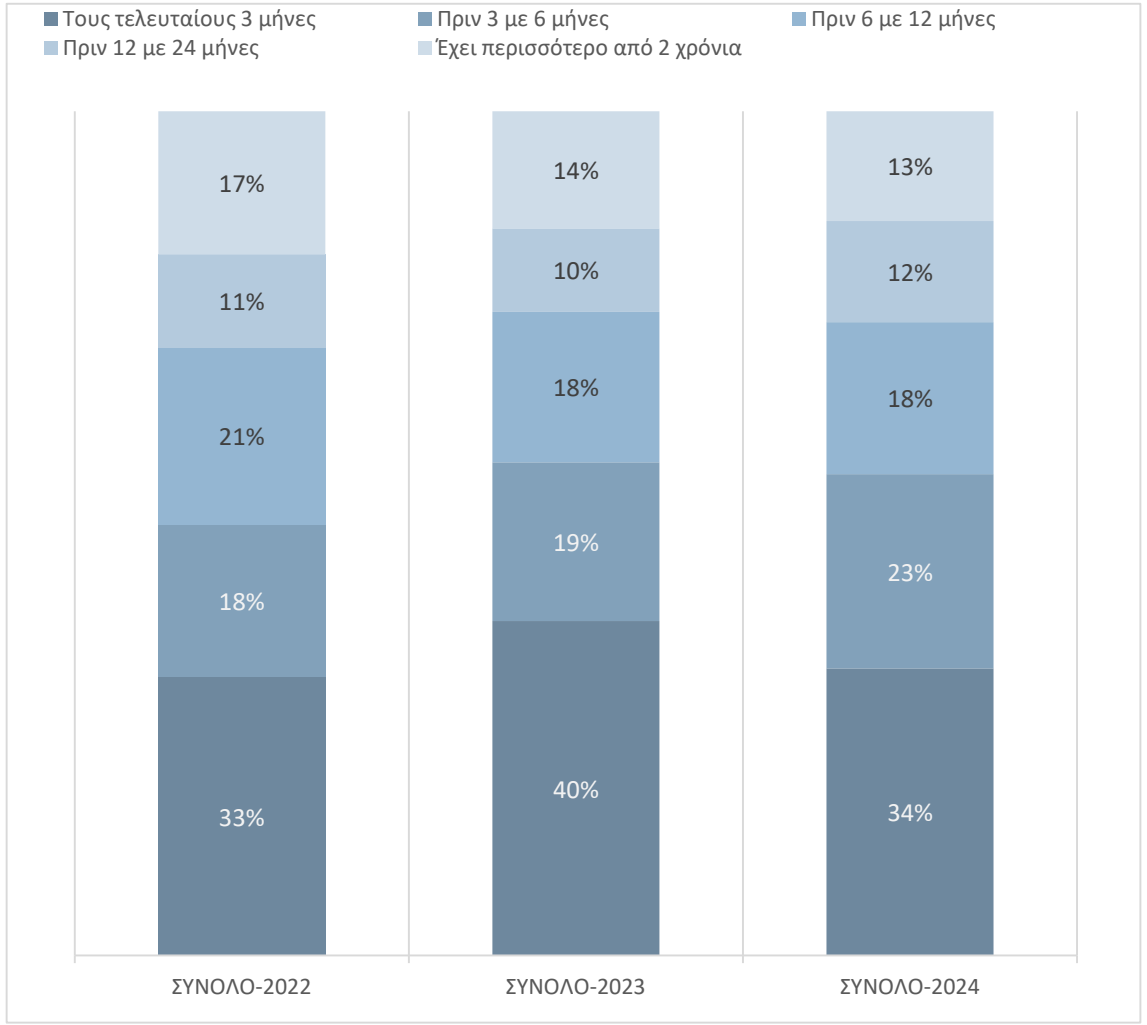
Βάση: Όλοι οι ερωτώμενοι

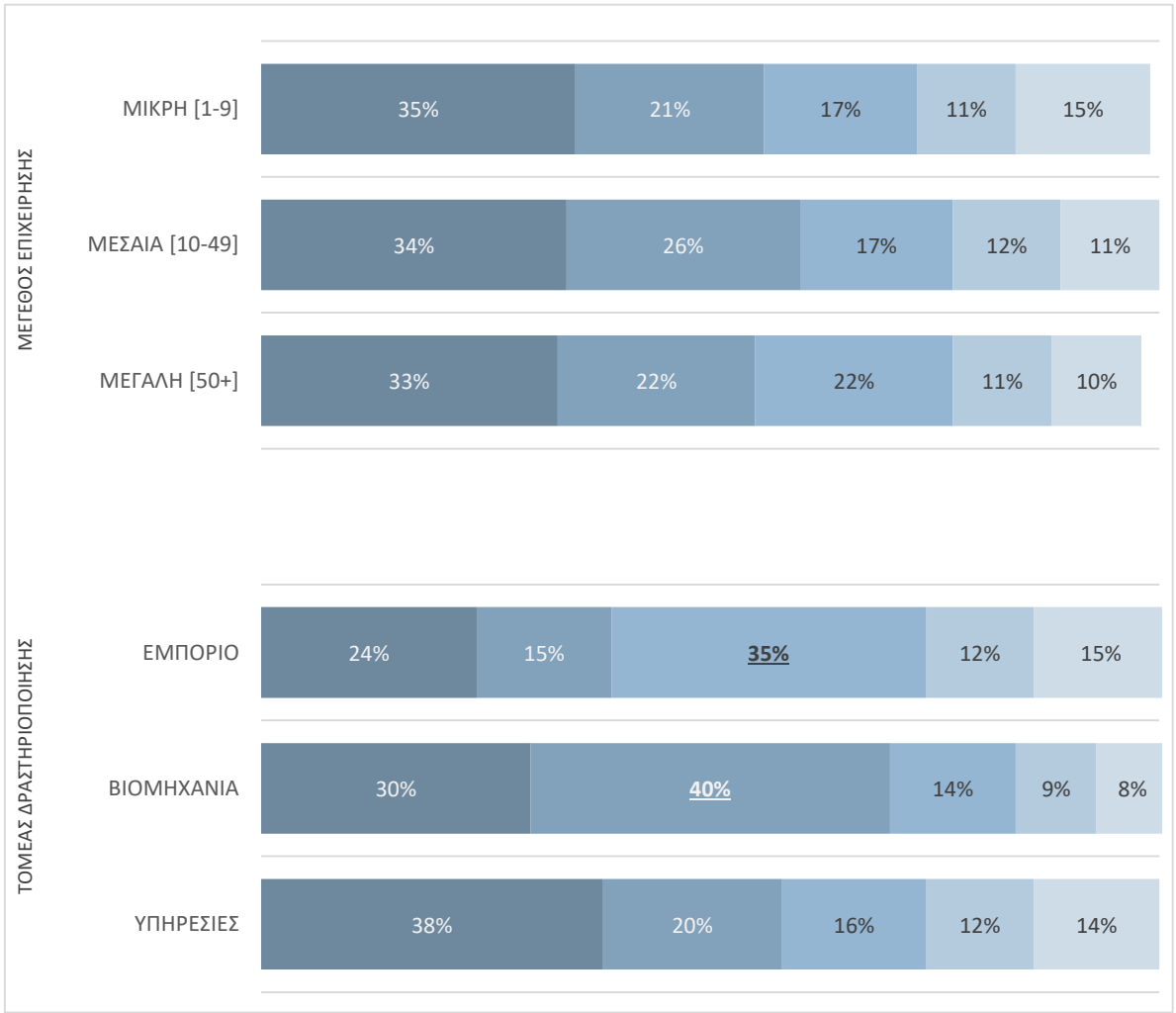


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Διαδικασία αποθήκευσης δεδομένων	58%	64%	62%	44%	55%	**65%**
Εργασία εξ αποστάσεως	42%	46%	**68%**	23%	**47%**	**52%**
Χρήση των cloud services	37%	**54%**	**56%**	29%	41%	**49%**
Τα δικαιώματα χρήσης που έχει το προσωπικό στις συσκευές IT του οργανισμού σας	32%	**47%**	**67%**	20%	33%	**48%**
Τι μπορεί να αποθηκευτεί σε αφαιρούμενες συσκευές	32%	**49%**	**60%**	**59%**	28%	**41%**
Χρήση συσκευών συνδεδεμένων στο δίκτυο, που μερικές φορές ονομάζονται έξυπνες συσκευές	31%	29%	43%	19%	**36%**	**34%**
Χρήση προσωπικών συσκευών για επιχειρηματικές δραστηριότητες	25%	26%	**52%**	28%	20%	32%
Χρήση Λογισμικού ως Υπηρεσία (Software as a Service (SaaS))	22%	31%	**44%**	15%	25%	**32%**
Όχι, δεν έχουμε κάτι σχετικό	**17%**	10%	5%	11%	11%	14%

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

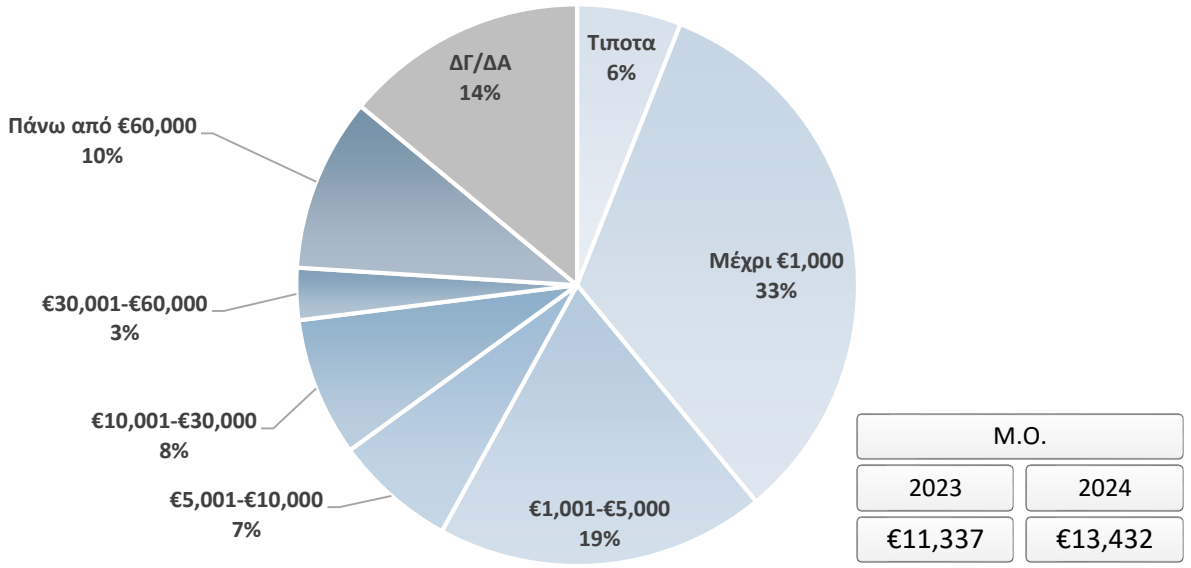




Τι ποσό επενδύει σε ετήσια βάση, ενεργά η επιχείρηση σας, σε εργαλεία και υπηρεσίες κυβερνοασφάλειας; | Τι ποσοστό του προϋπολογισμού των δαπανών σας αποτελεί περίπου το πιο πάνω ποσό;

Βάση: Όλοι οι ερωτώμενοι

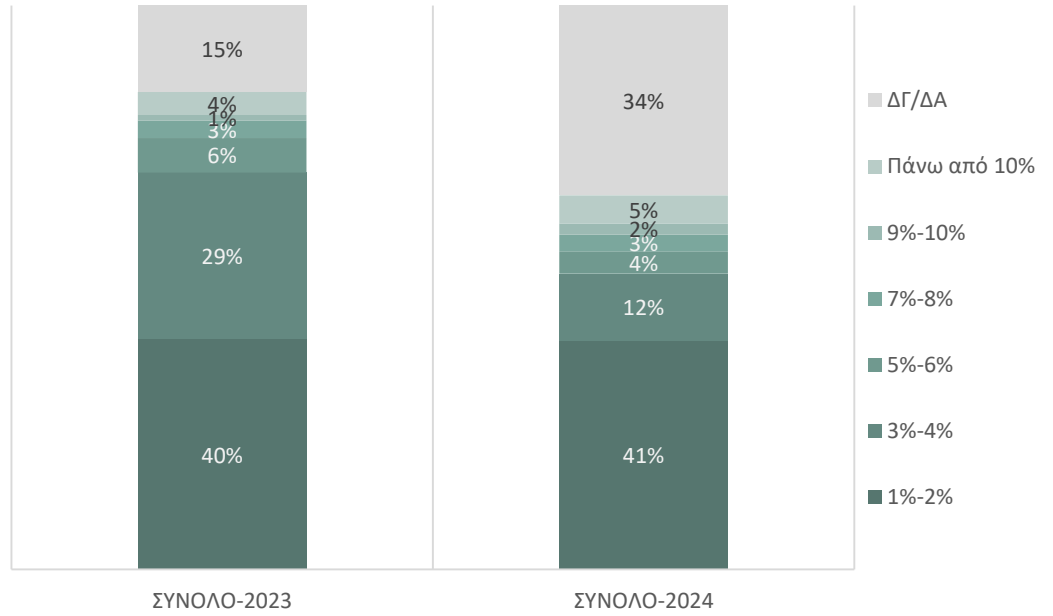
Τι ποσό επενδύει σε ετήσια βάση, ενεργά η επιχείρηση σας, σε εργαλεία και υπηρεσίες κυβερνοασφάλειας;



M.O.	
2023	2024
€11,337	€13,432

	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Τίποτα	7%	4%	3%	6%	13%	4%
Μέχρι €1,000	47%	22%	5%	36%	29%	33%
€1,001-€5,000	13%	28%	21%	14%	26%	18%
€5,001-€10,000	3%	13%	11%	8%	5%	7%
€10,001-€30,000	4%	11%	16%	0%	4%	11%
€30,001-€60,000	1%	0%	17%	3%	2%	3%
Πάνω από €60,000	7%	9%	22%	5%	1%	13%
ΔΓ/ΔΑ	18%	13%	5%	27%	20%	11%
M.O.	€8,683	€12,643	**€30,633**	€8,799	€5,093	**€16,184**

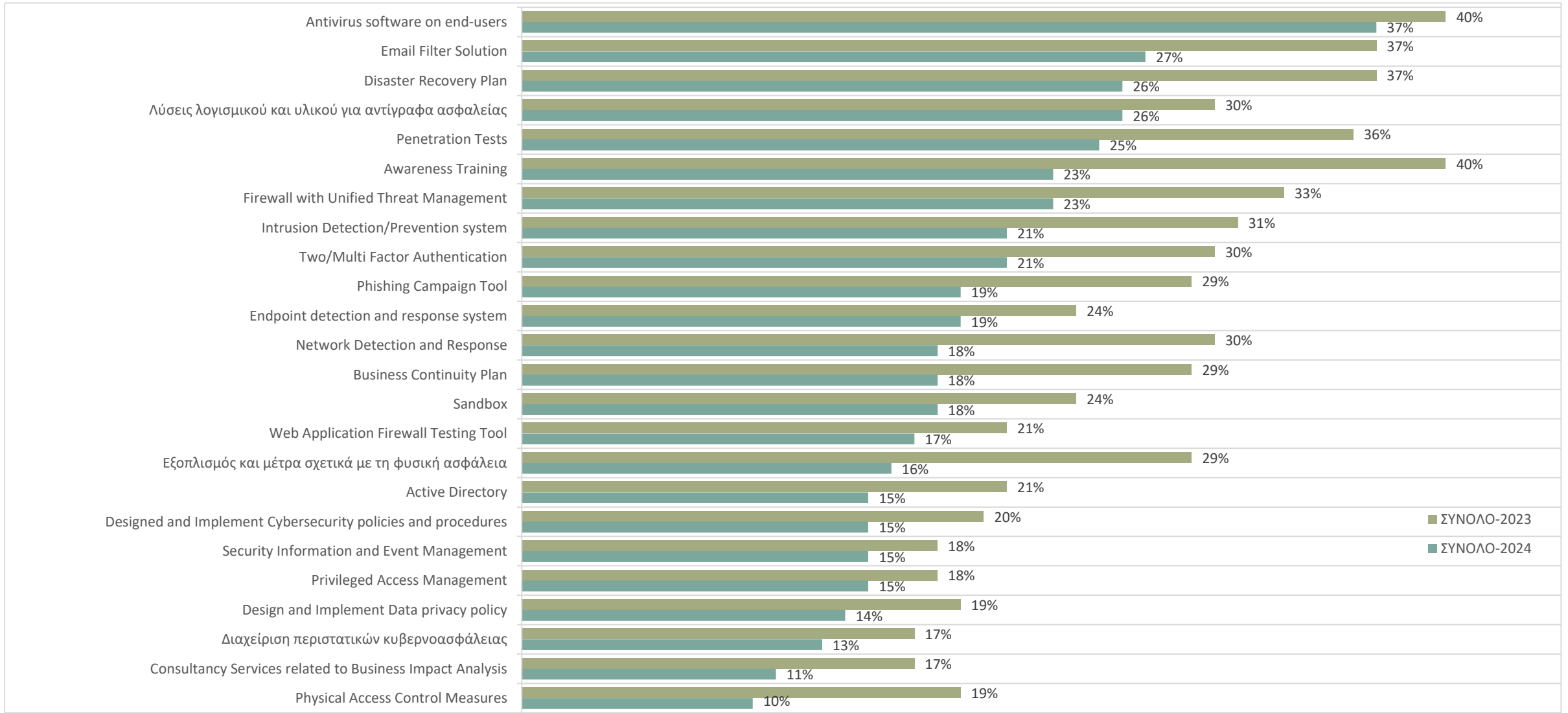
τι ποσοστό του προϋπολογισμού των δαπανών σας αποτελεί περίπου το πιο πάνω ποσό;



	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
1%-2%	44%	40%	33%	45%	**54%**	37%
3%-4%	3%	**24%**	**14%**	5%	6%	14%
5%-6%	3%	3%	7%	0%	7%	4%
7%-8%	1%	4%	3%	2%	2%	3%
9%-10%	1%	2%	**7%**	0%	2%	3%
Πάνω από 10%	3%	5%	9%	2%	2%	6%
NA	**45%**	22%	28%	45%	28%	34%

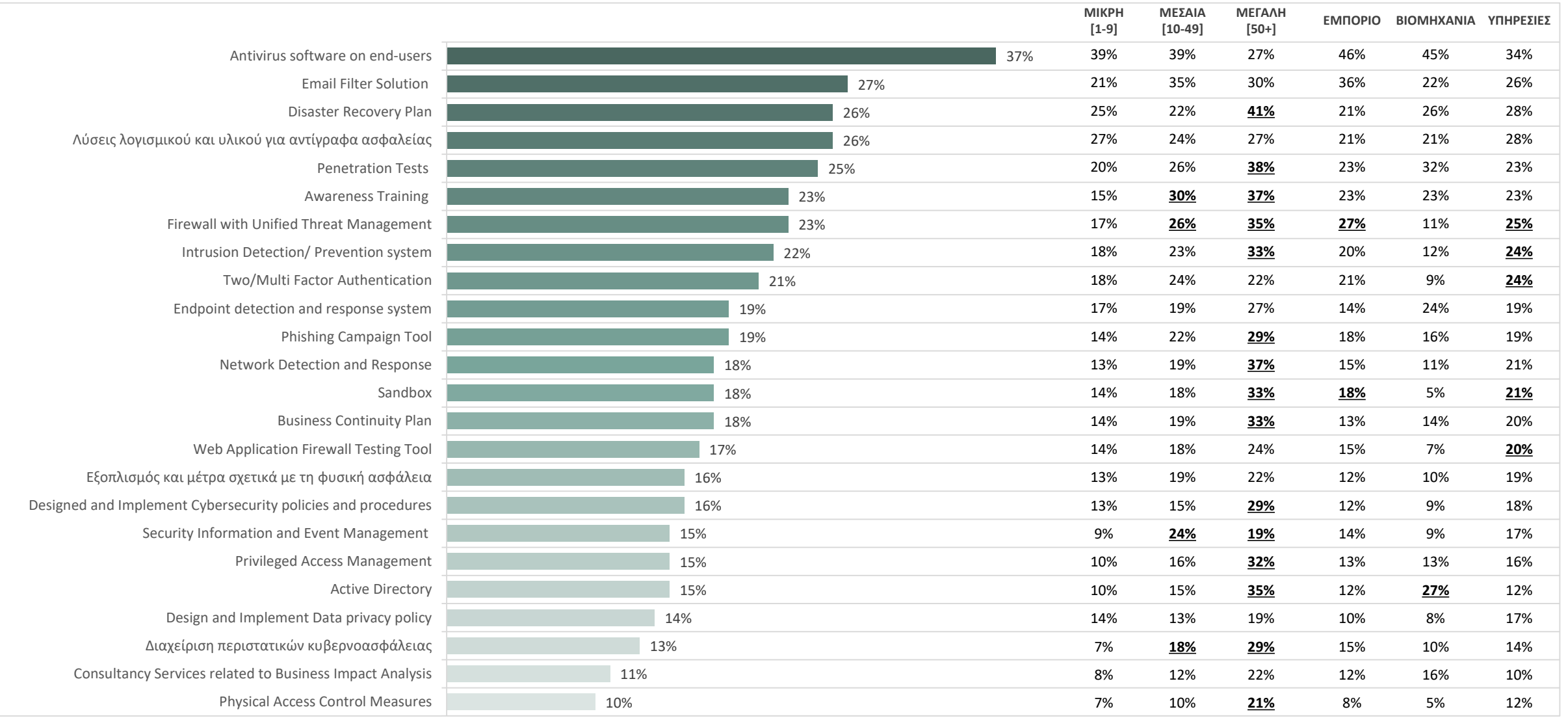
Σε ποια εργαλεία και υπηρεσίες κυβερνοασφάλειας θα σας ενδιέφερε να επενδύσετε;

Βάση: Όλοι οι ερωτώμενοι



Σε ποια εργαλεία και υπηρεσίες κυβερνοασφάλειας θα σας ενδιέφερε να επενδύσετε;

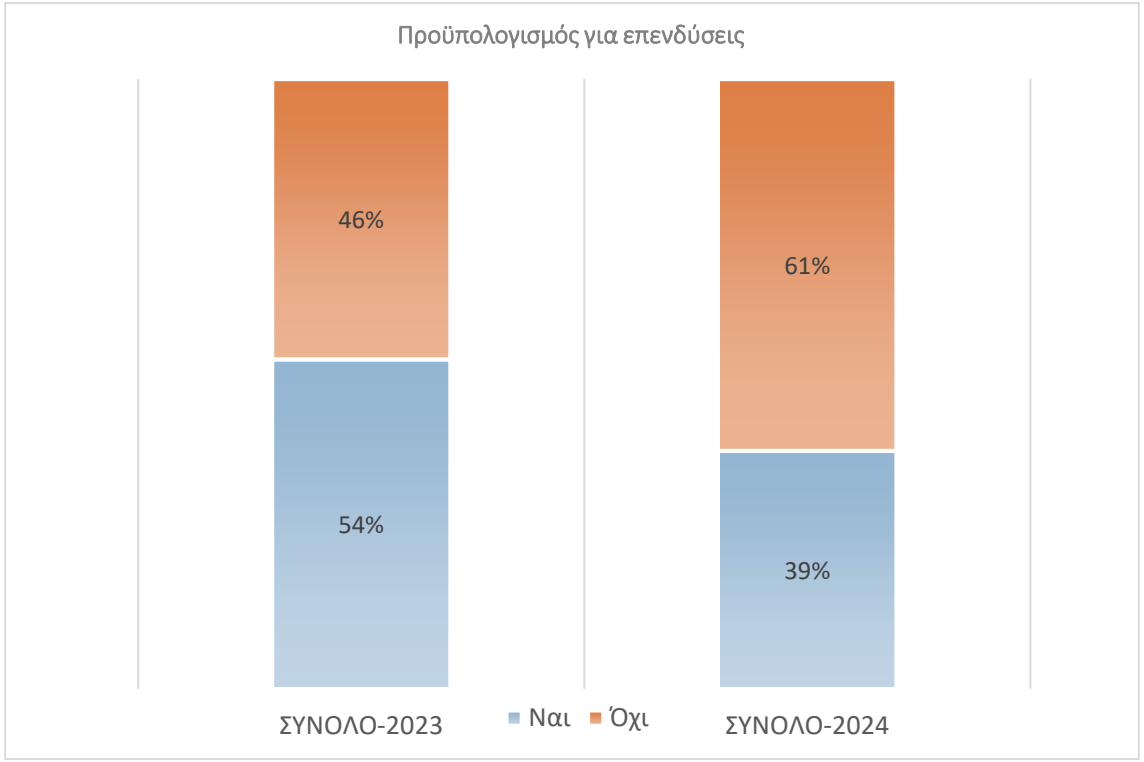
Βάση: Όλοι οι ερωτώμενοι

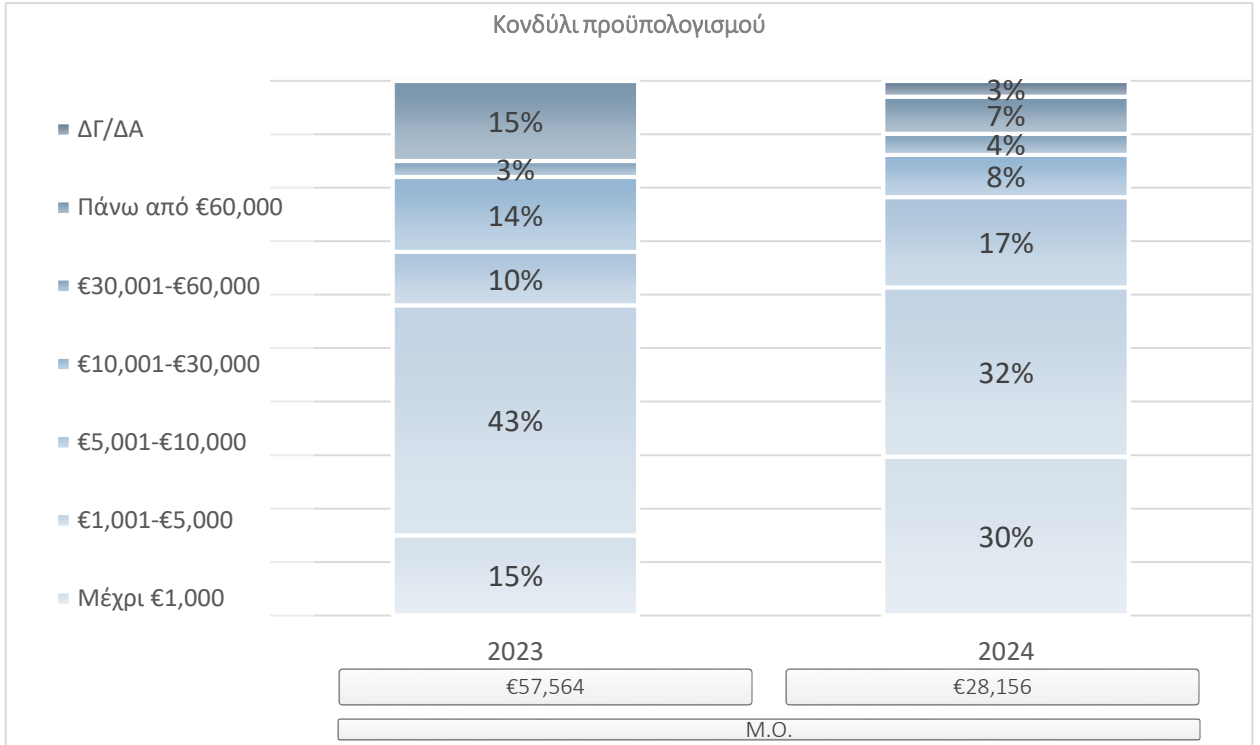


		ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Antivirus software on end-users	37%	39%	39%	27%	46%	45%	34%
Email Filter Solution	27%	21%	35%	30%	36%	22%	26%
Disaster Recovery Plan	26%	25%	22%	**41%**	21%	26%	28%
Λύσεις λογισμικού και υλικού για αντίγραφα ασφαλείας	26%	27%	24%	27%	21%	21%	28%
Penetration Tests	25%	20%	26%	**38%**	23%	32%	23%
Awareness Training	23%	15%	**30%**	**37%**	23%	23%	23%
Firewall with Unified Threat Management	23%	17%	**26%**	**35%**	**27%**	11%	**25%**
Intrusion Detection/ Prevention system	22%	18%	23%	**33%**	20%	12%	**24%**
Two/Multi Factor Authentication	21%	18%	24%	22%	21%	9%	**24%**
Endpoint detection and response system	19%	17%	19%	27%	14%	24%	19%
Phishing Campaign Tool	19%	14%	22%	**29%**	18%	16%	19%
Network Detection and Response	18%	13%	19%	**37%**	15%	11%	21%
Sandbox	18%	14%	18%	**33%**	**18%**	5%	**21%**
Business Continuity Plan	18%	14%	19%	**33%**	13%	14%	20%
Web Application Firewall Testing Tool	17%	14%	18%	24%	15%	7%	**20%**
Εξοπλισμός και μέτρα σχετικά με τη φυσική ασφάλεια	16%	13%	19%	22%	12%	10%	19%
Designed and Implement Cybersecurity policies and procedures	16%	13%	15%	**29%**	12%	9%	18%
Security Information and Event Management	15%	9%	**24%**	**19%**	14%	9%	17%
Privileged Access Management	15%	10%	16%	**32%**	13%	13%	16%
Active Directory	15%	10%	15%	**35%**	12%	**27%**	12%
Design and Implement Data privacy policy	14%	14%	13%	19%	10%	8%	17%
Διαχείριση περιστατικών κυβερνοασφάλειας	13%	7%	**18%**	**29%**	15%	10%	14%
Consultancy Services related to Business Impact Analysis	11%	8%	12%	22%	12%	16%	10%
Physical Access Control Measures	10%	7%	10%	**21%**	8%	5%	12%

Έχετε προϋπολογισμό για επένδυση σε εργαλεία και υπηρεσίες κυβερνοασφάλειας; | Τι κονδύλι;

Βάση: Όλοι οι ερωτώμενοι



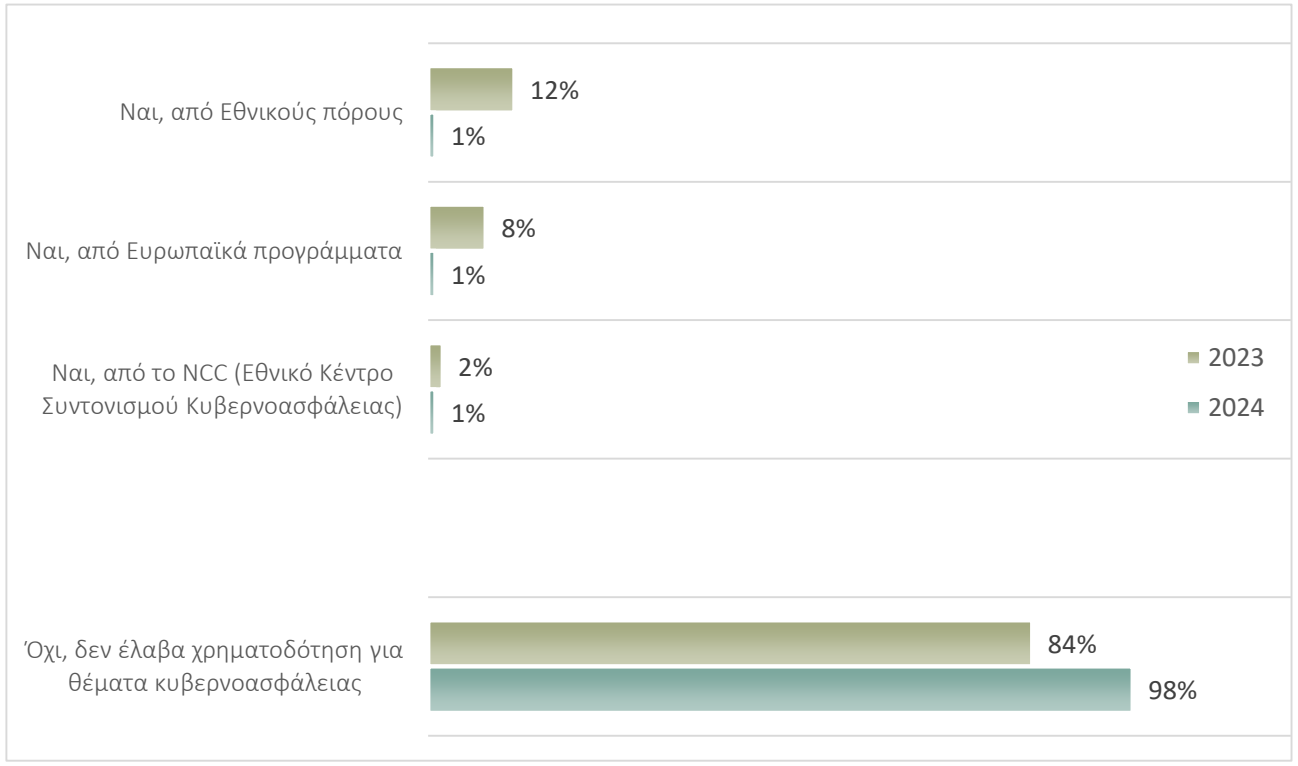


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Ναι	35%	40%	**52%**	21%	31%	**45%**
Όχι	65%	60%	48%	79%	69%	55%

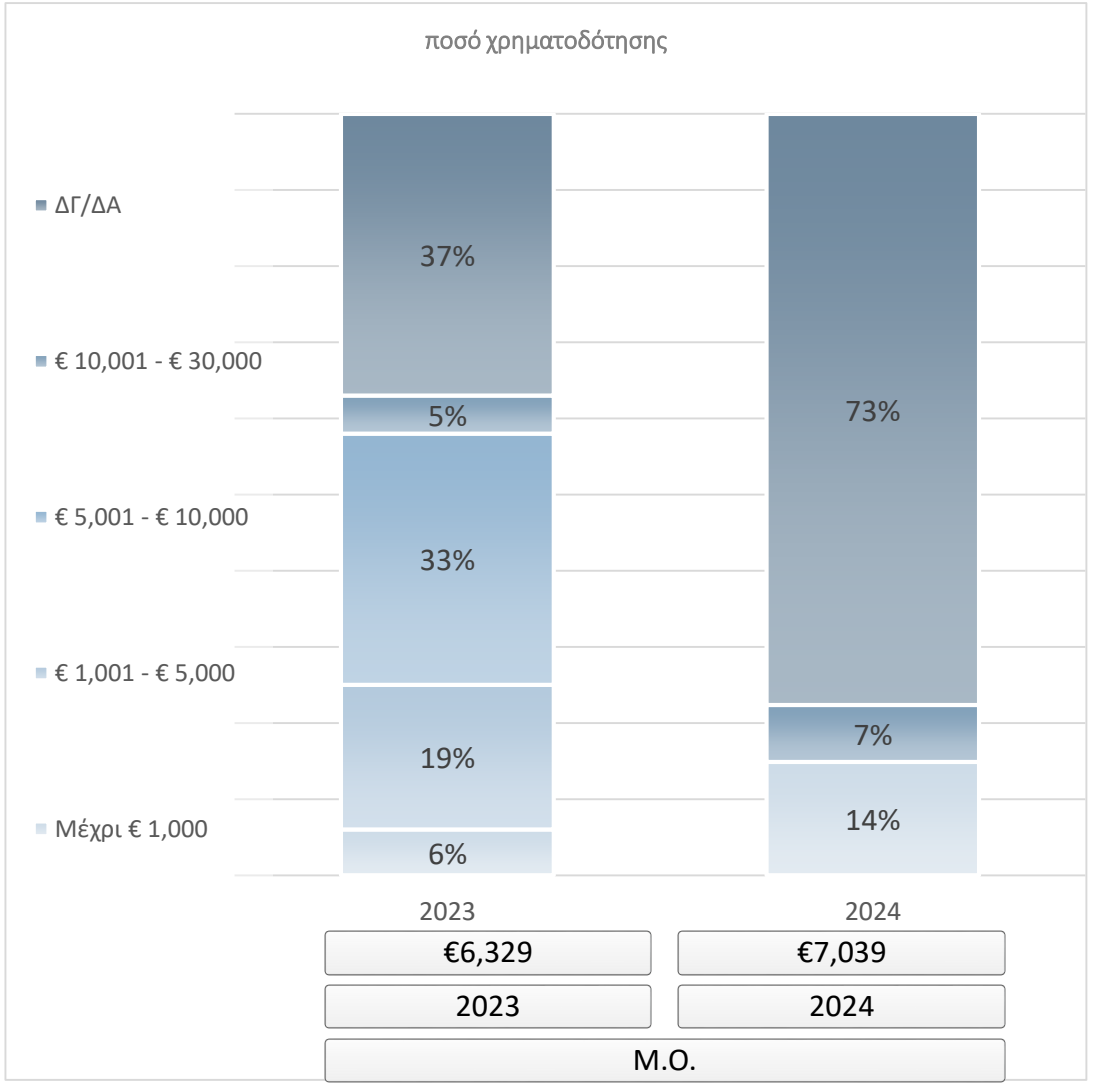
	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Μέχρι €1,000	48%	20%	3%	31%	9%	34%
€1,001-€5,000	37%	37%	6%	21%	28%	33%
€5,001-€10,000	8%	21%	30%	32%	40%	11%
€10,001-€30,000	0%	9%	27%	0%	4%	10%
€30,001-€60,000	0%	5%	12%	8%	4%	4%
Πάνω από €60,000	3%	4%	21%	8%	0%	8%
ΔΓ/ΔΑ	3%	4%	0%	0%	15%	1%
Μ.Ο.	**€7,237**	**€19,113**	**€94,758**	**€87,422**	**€8,807**	**€25,707**

Έχετε λάβει χρηματοδότηση για θέματα κυβερνοασφάλειας τους τελευταίους 12 μήνες; | Τι ποσό λάβατε;

Βάση: Όλοι οι ερωτώμενοι

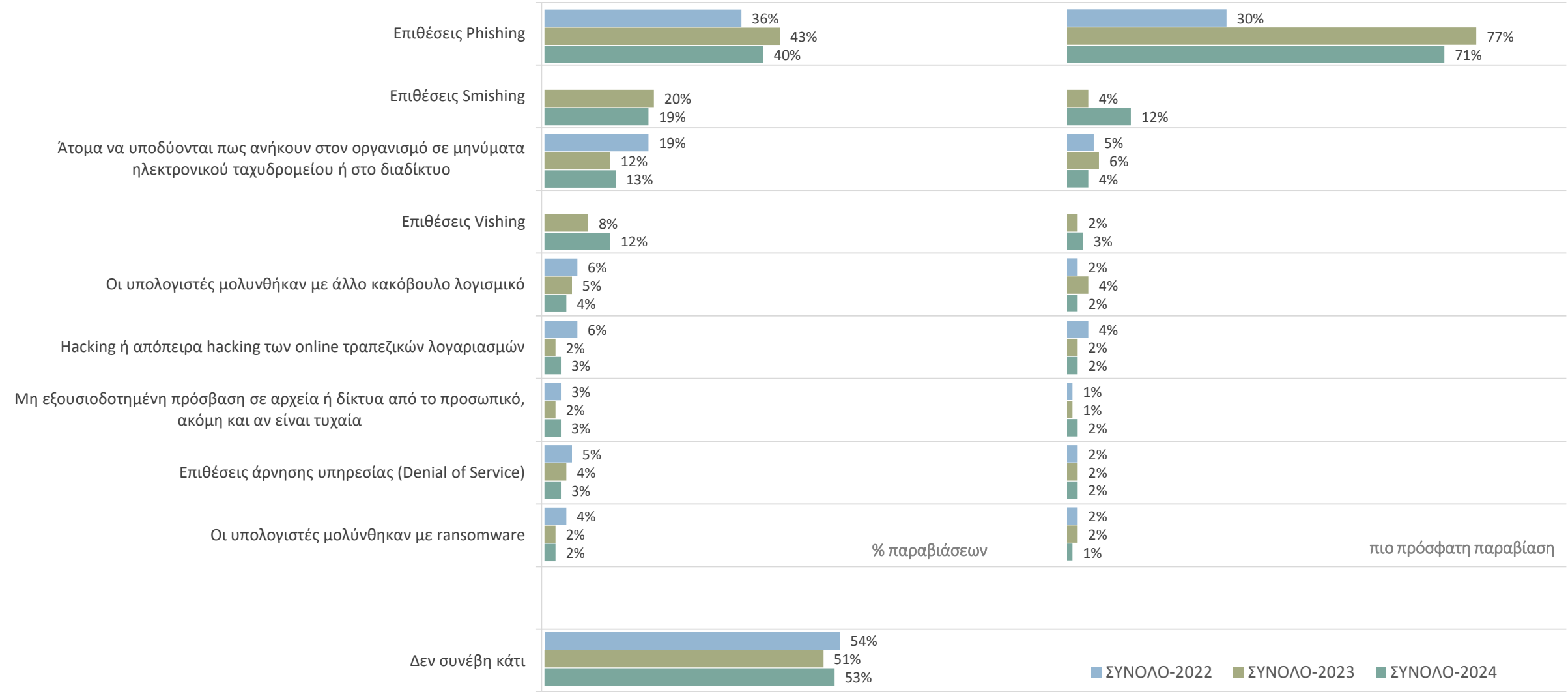


	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Ναι, από Εθνικούς πόρους	0%	1%	3%	0%	0%	1%
Ναι, από Ευρωπαϊκά προγράμματα	0%	2%	3%	0%	0%	2%
Ναι, από το NCC	1%	1%	3%	0%	0%	2%
Όχι, δεν έλαβα χρηματοδότηση	99%	98%	94%	100%	100%	97%



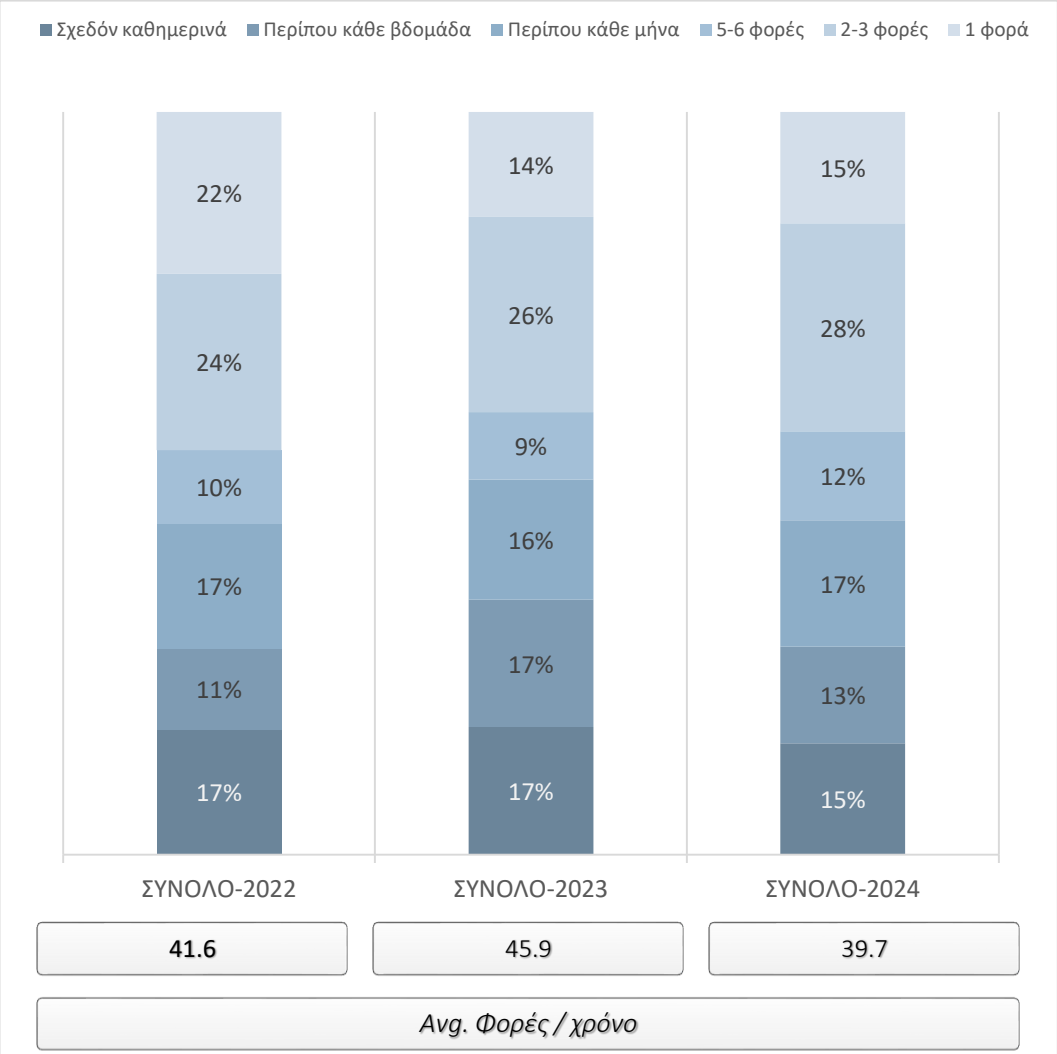
Τους τελευταίους 12 μήνες, τι από τα παρακάτω συνέβη στην εταιρεία |επιχείρηση |οργανισμό; Και ποια ήταν η πιο πρόσφατη παραβίαση κυβερνοασφάλειας |επίθεση, που δεχτήκατε;

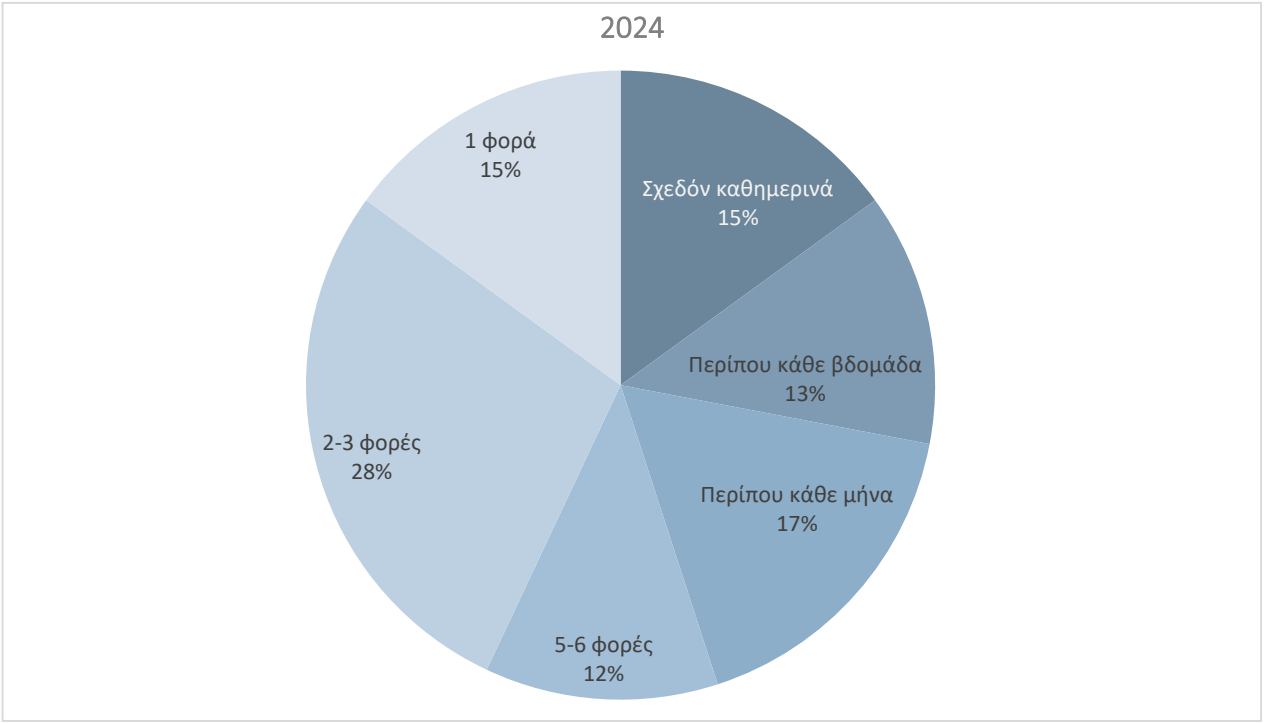
Βάση: Όλοι οι ερωτώμενοι



Πόσο συχνά αντιμετωπίσατε κάποια από τις παραβιάσεις ή τις επιθέσεις αυτές;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)

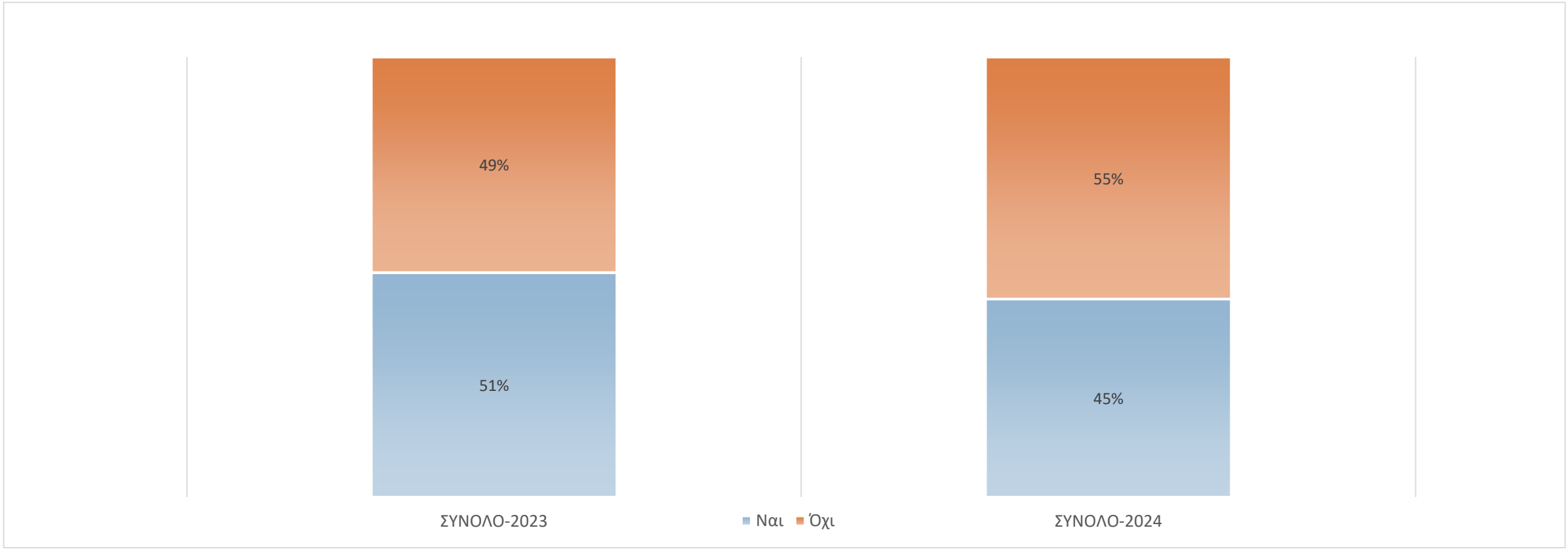




	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
1 φορά (1.0)	14%	16%	19%	28%	11%	14%
2 3 φορές (2.5)	20%	39%	35%	33%	28%	26%
5-6 φορές (5.5)	14%	5%	16%	4%	29%	7%
Περίπου κάθε μήνα (11.0)	17%	21%	10%	17%	27%	14%
Περίπου κάθε βδομάδα (50.0)	17%	11%	3%	13%	4%	17%
Σχεδόν καθημερινά (200.0)	18%	7%	16%	5%	2%	22%
Μ.Ο. (Φορές / χρόνο)	**48**	**23**	**37**	**20**	**11**	**54**

Γνωρίζετε για το Εθνικό CSIRT-CY και το ρόλο του σε περιστατικά κυβερνοεπιθέσεων;

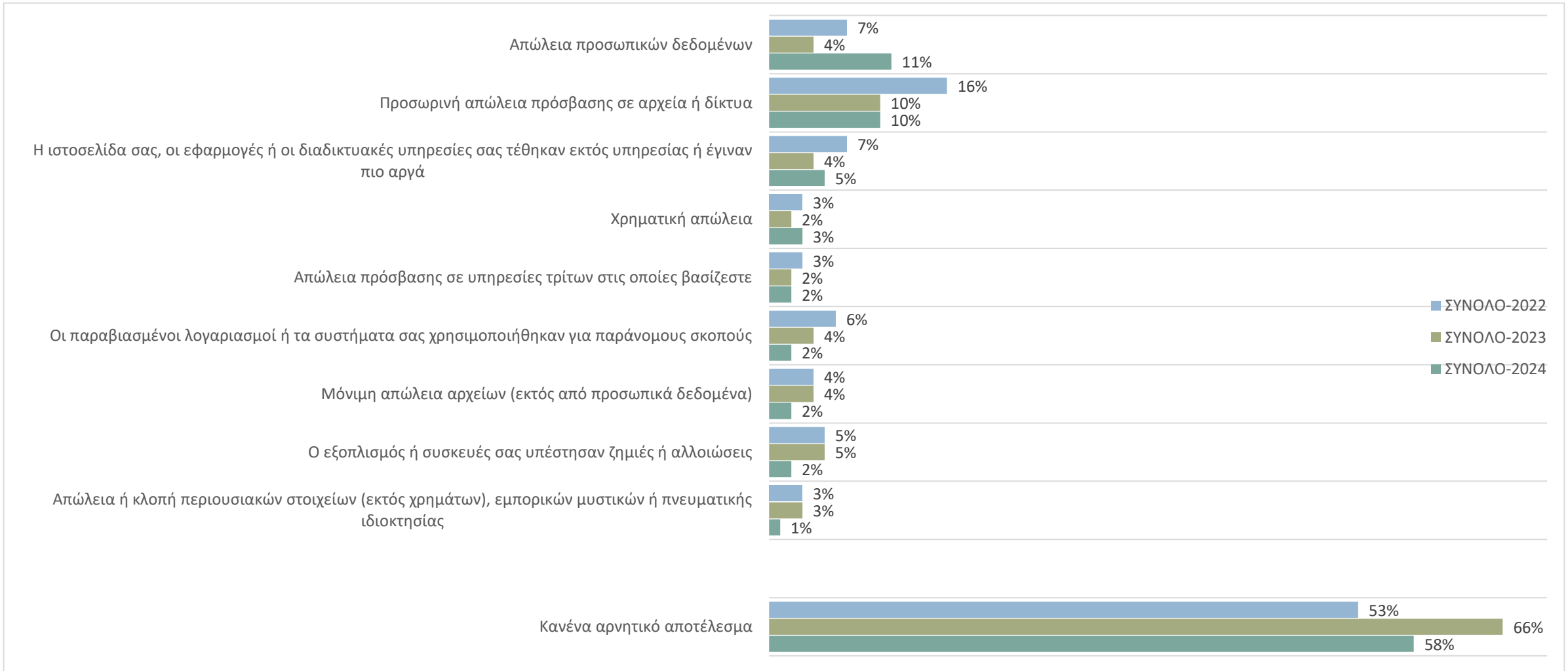
Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Ναι	37%	50%	**65%**	24%	26%	**56%**
Όχι	63%	50%	35%	76%	74%	45%

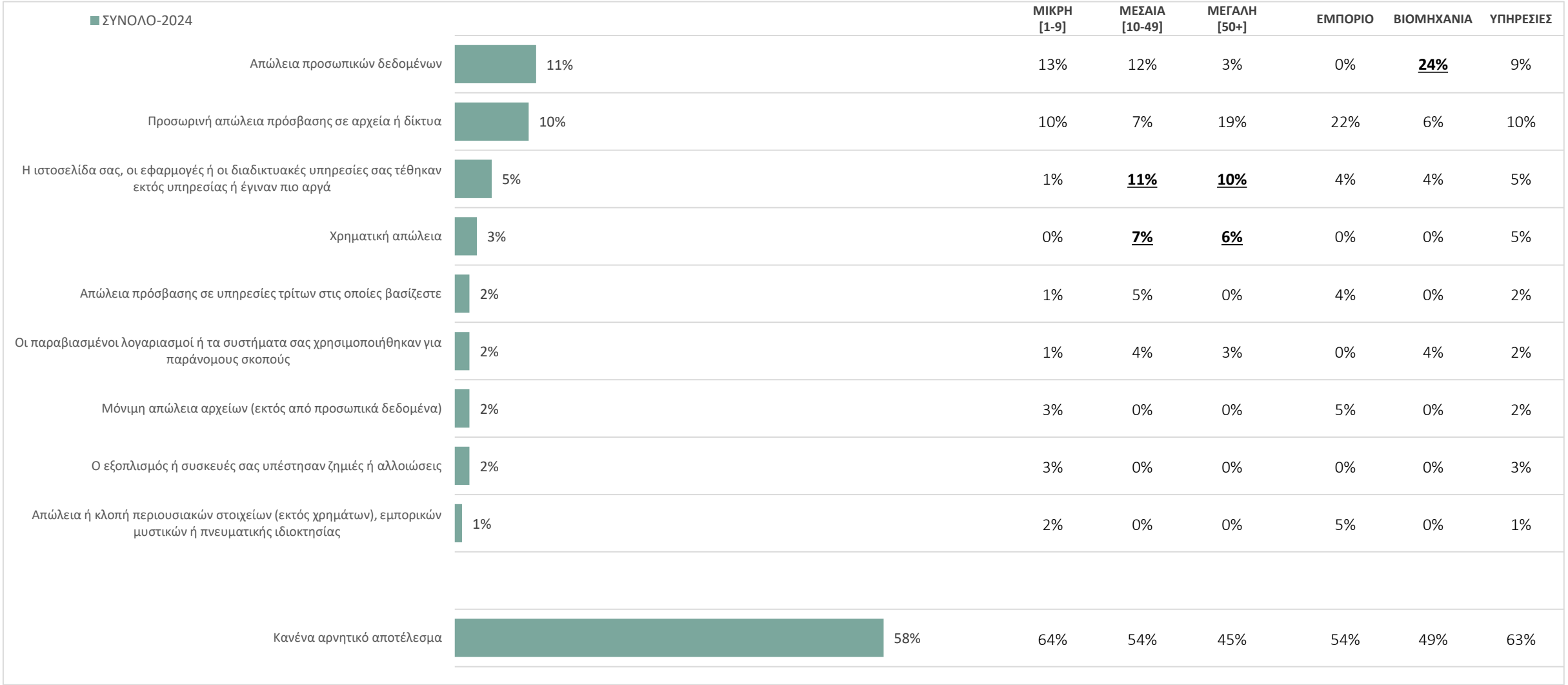
Λαμβάνοντας υπόψιν όλες τις παραβιάσεις /κυβερνοεπιθέσεις που αντιμετωπίσατε τους τελευταίους 12 μήνες, ποια από τα ακόλουθα συνέβησαν ως αποτέλεσμα τους;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

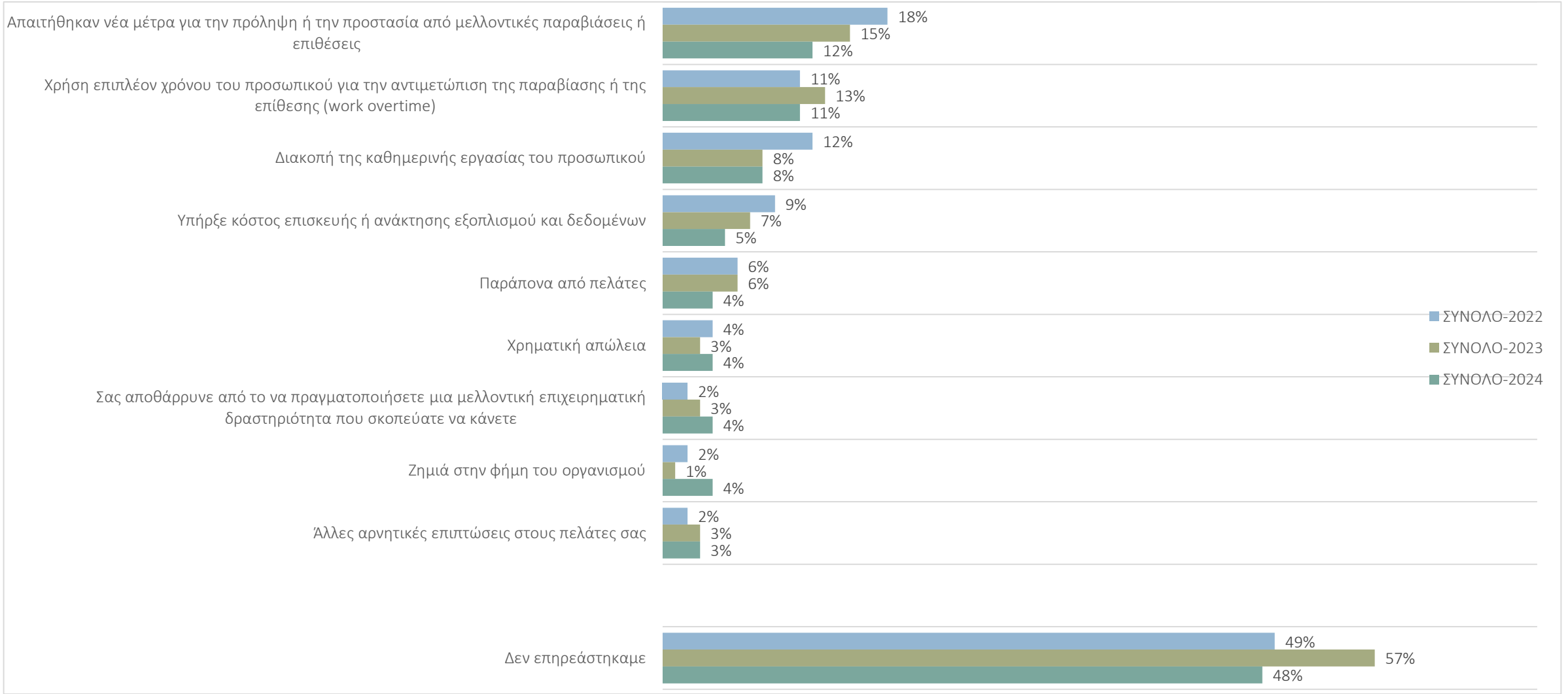
Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



	ΣΥΝΟΛΟ-2024	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Απώλεια προσωπικών δεδομένων	11%	13%	12%	3%	0%	**24%**	9%
Προσωρινή απώλεια πρόσβασης σε αρχεία ή δίκτυα	10%	10%	7%	19%	22%	6%	10%
Η ιστοσελίδα σας, οι εφαρμογές ή οι διαδικτυακές υπηρεσίες σας τέθηκαν εκτός υπηρεσίας ή έγιναν πιο αργά	5%	1%	**11%**	**10%**	4%	4%	5%
Χρηματική απώλεια	3%	0%	**7%**	**6%**	0%	0%	5%
Απώλεια πρόσβασης σε υπηρεσίες τρίτων στις οποίες βασίζεστε	2%	1%	5%	0%	4%	0%	2%
Οι παραβιασμένοι λογαριασμοί ή τα συστήματα σας χρησιμοποιήθηκαν για παράνομους σκοπούς	2%	1%	4%	3%	0%	4%	2%
Μόνιμη απώλεια αρχείων (εκτός από προσωπικά δεδομένα)	2%	3%	0%	0%	5%	0%	2%
Ο εξοπλισμός ή συσκευές σας υπέστησαν ζημιές ή αλλοιώσεις	2%	3%	0%	0%	0%	0%	3%
Απώλεια ή κλοπή περιουσιακών στοιχείων (εκτός χρημάτων), εμπορικών μυστικών ή πνευματικής ιδιοκτησίας	1%	2%	0%	0%	5%	0%	1%
Κανένα αρνητικό αποτέλεσμα	58%	64%	54%	45%	54%	49%	63%

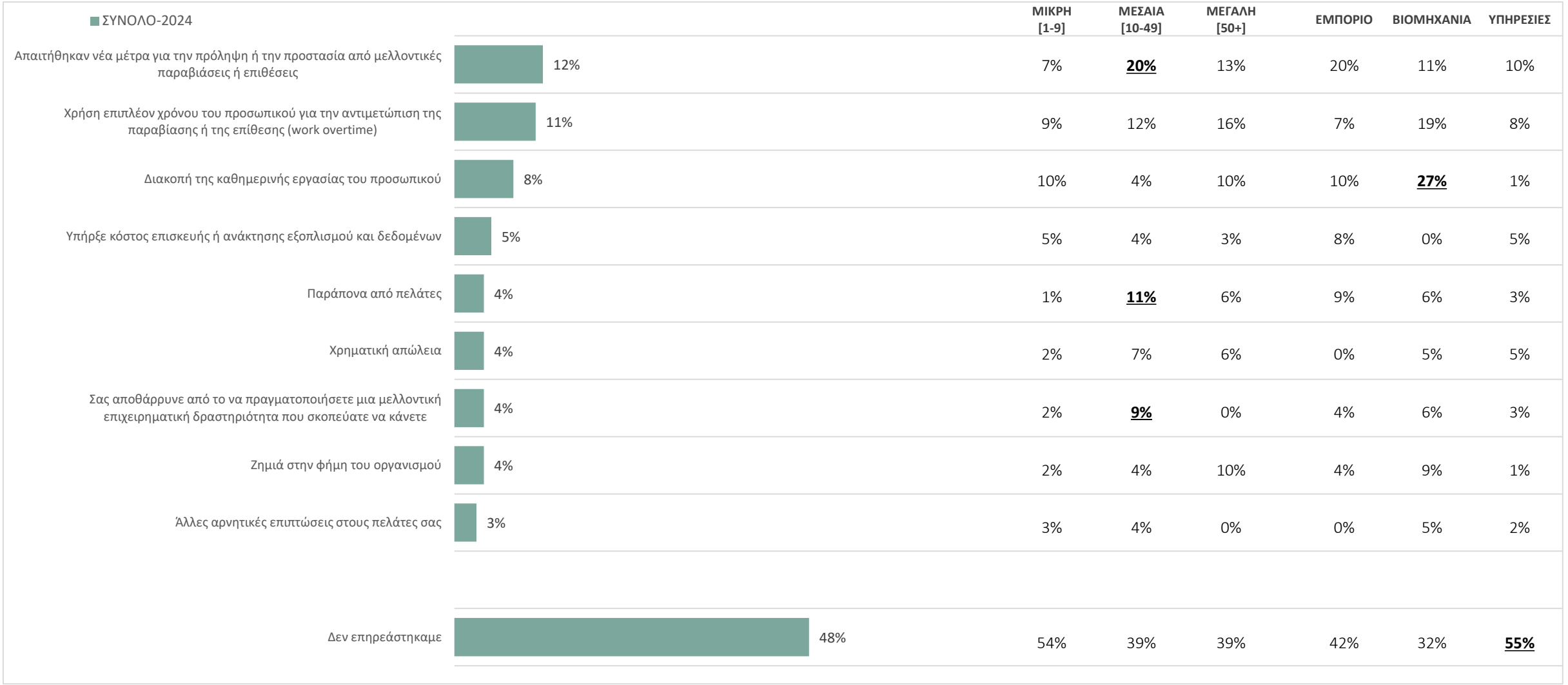
Πως έχουν επηρεάσει την εταιρεία/ επιχείρηση /τον οργανισμό αυτές οι παραβιάσεις ή επιθέσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

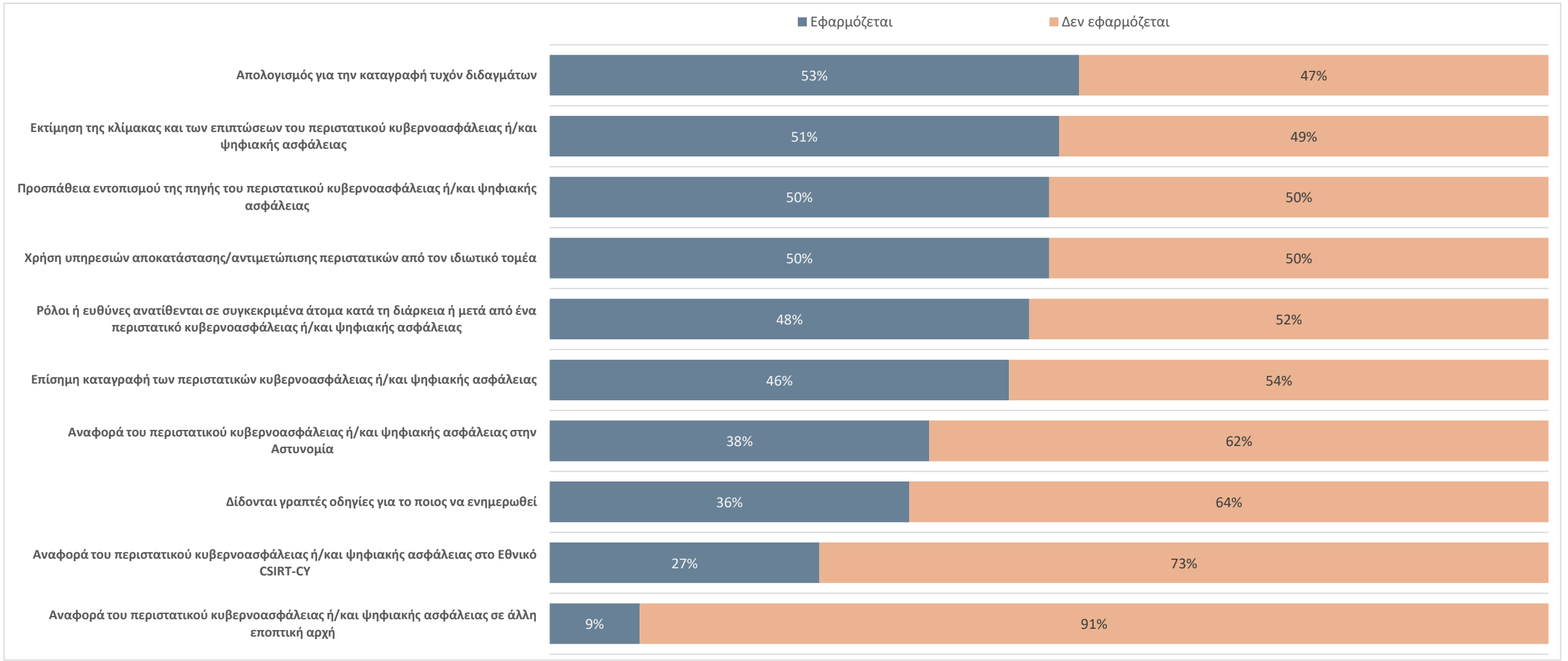
Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



	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	7%	**20%**	13%	20%	11%	10%
Χρήση επιπλέον χρόνου του προσωπικού για την αντιμετώπιση της παραβίασης ή της επίθεσης (work overtime)	9%	12%	16%	7%	19%	8%
Διακοπή της καθημερινής εργασίας του προσωπικού	10%	4%	10%	10%	**27%**	1%
Υπήρξε κόστος επισκευής ή ανάκτησης εξοπλισμού και δεδομένων	5%	4%	3%	8%	0%	5%
Παράπονα από πελάτες	1%	**11%**	6%	9%	6%	3%
Χρηματική απώλεια	2%	7%	6%	0%	5%	5%
Σας αποθάρρυνε από το να πραγματοποιήσετε μια μελλοντική επιχειρηματική δραστηριότητα που σκοπεύατε να κάνετε	2%	**9%**	0%	4%	6%	3%
Ζημιά στην φήμη του οργανισμού	2%	4%	10%	4%	9%	1%
Άλλες αρνητικές επιπτώσεις στους πελάτες σας	3%	4%	0%	0%	5%	2%
Δεν επηρεάστηκαμε	54%	39%	39%	42%	32%	**55%**

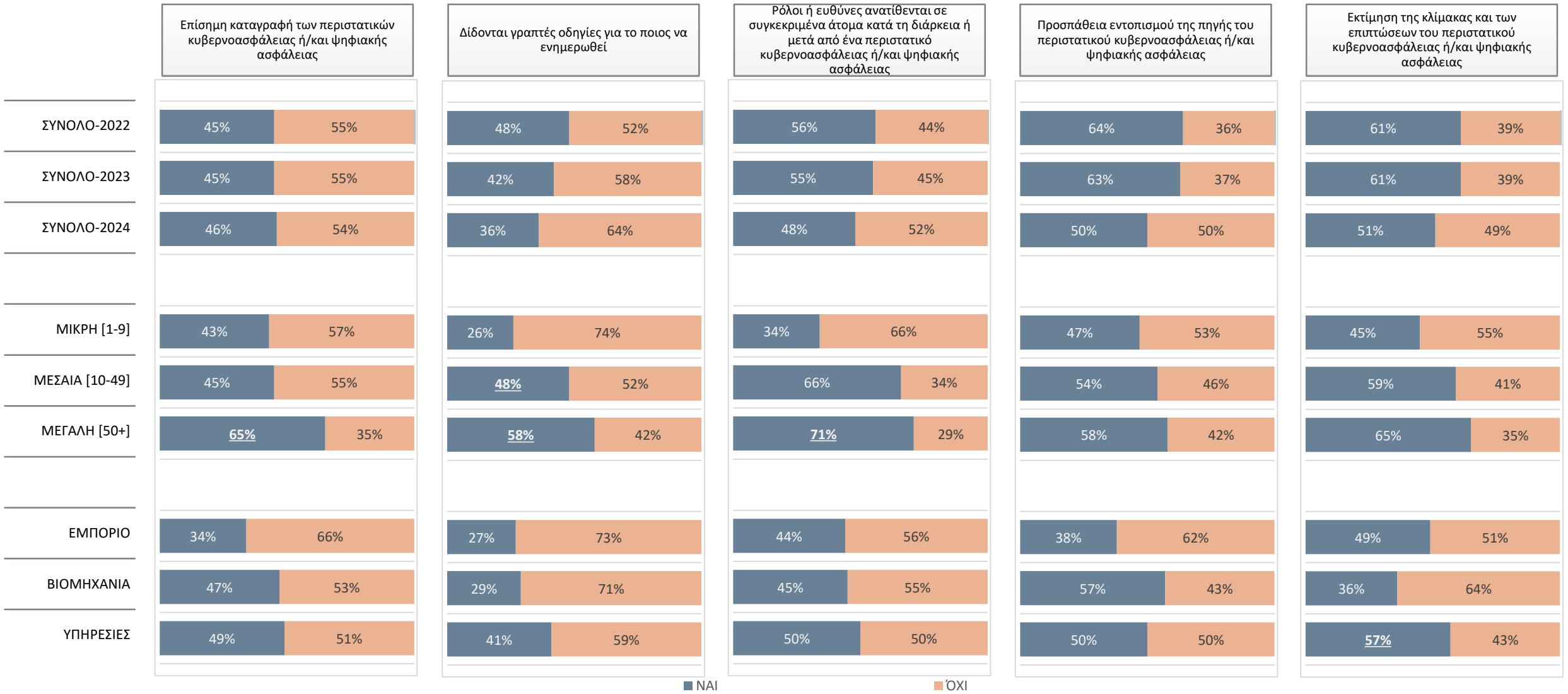
Ποια από τα παρακάτω κάνετε ή εφαρμόζετε, όταν αντιμετωπίζετε ένα περιστατικό κυβερνοασφάλειας;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

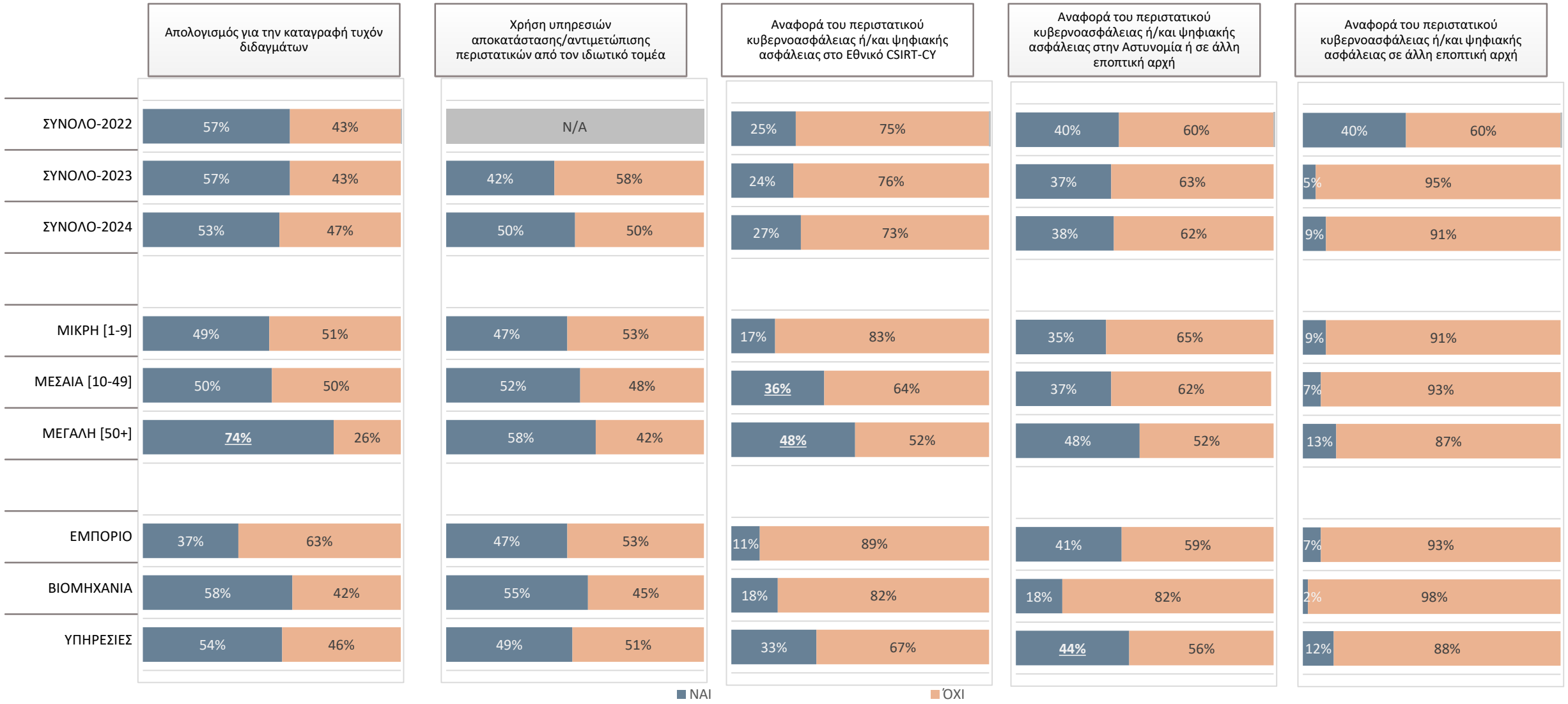
Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

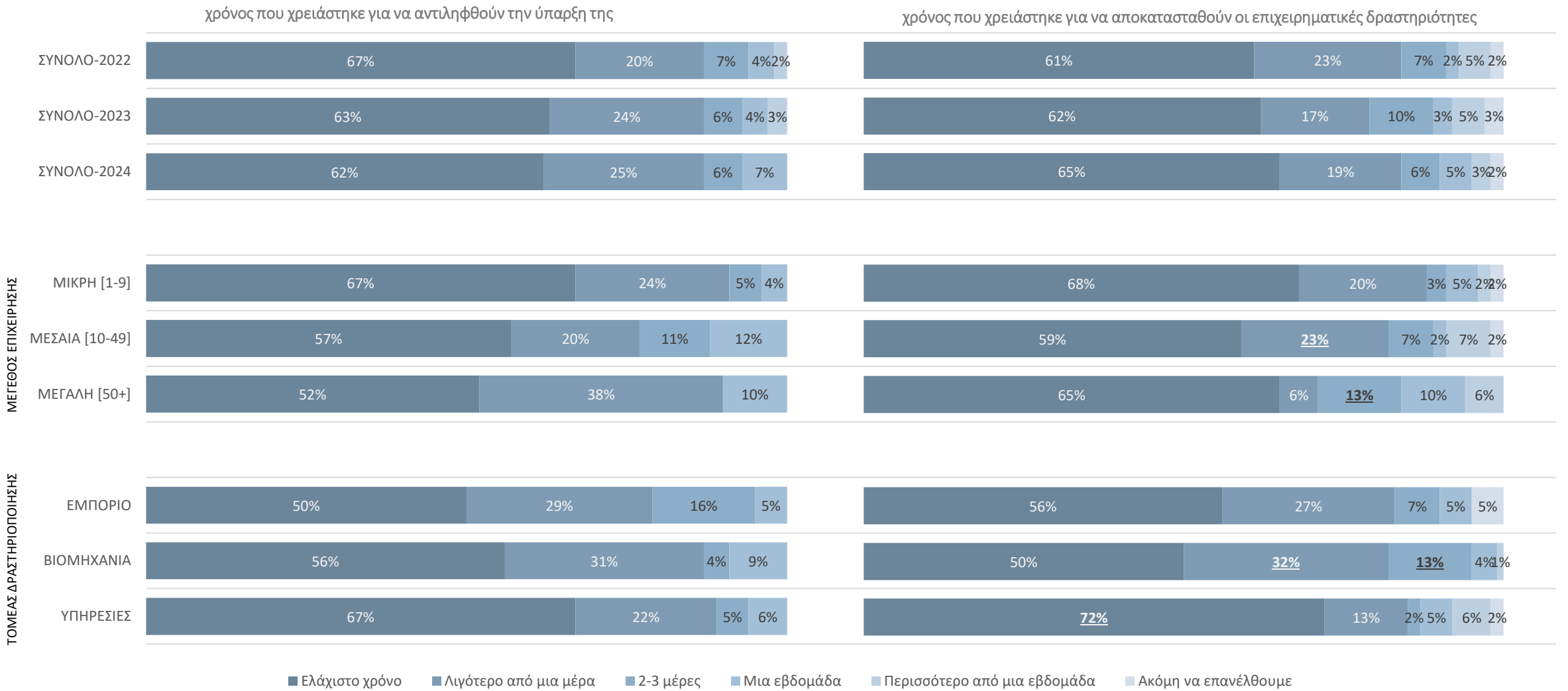
... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



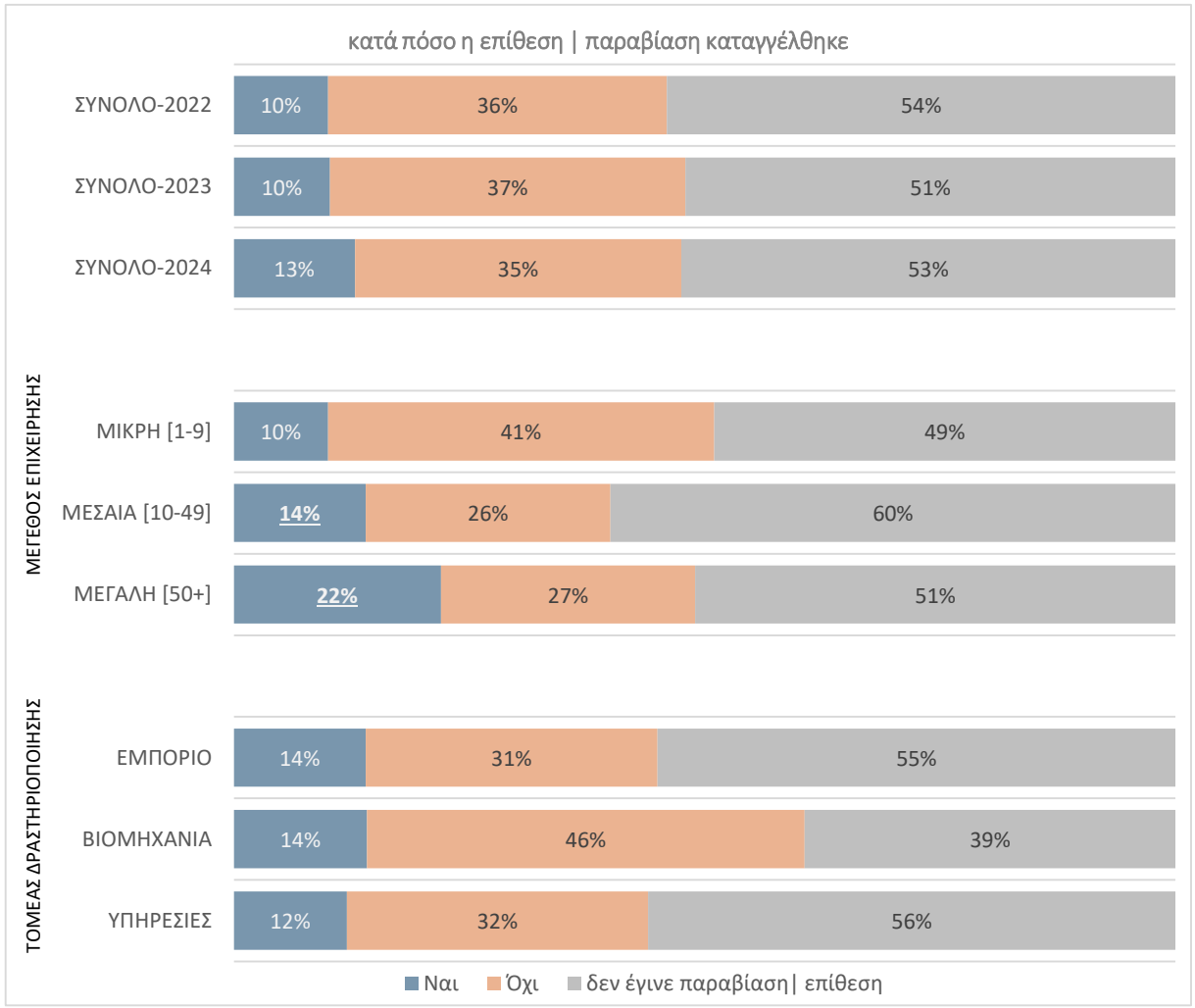
Σκεπτόμενοι την πιο πρόσφατη παραβίαση κυβερνοασφάλειας, που δεχτήκατε, πόσος χρόνος χρειάστηκε για να αντιληφθείτε την ύπαρξη της; | Και πόσος χρόνος χρειάστηκε για να αποκατασταθούν οι επιχειρηματικές σας δραστηριότητες;

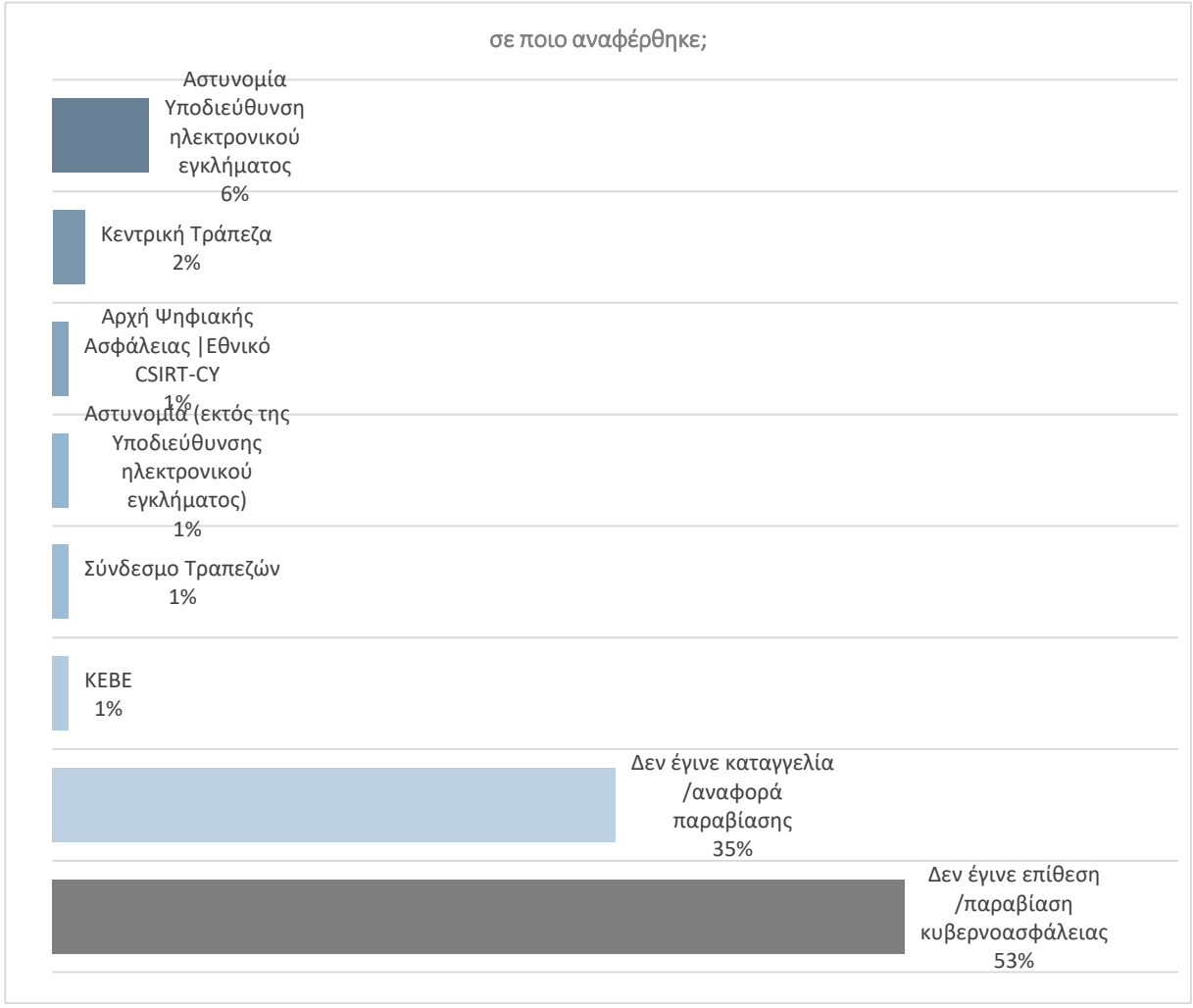
Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

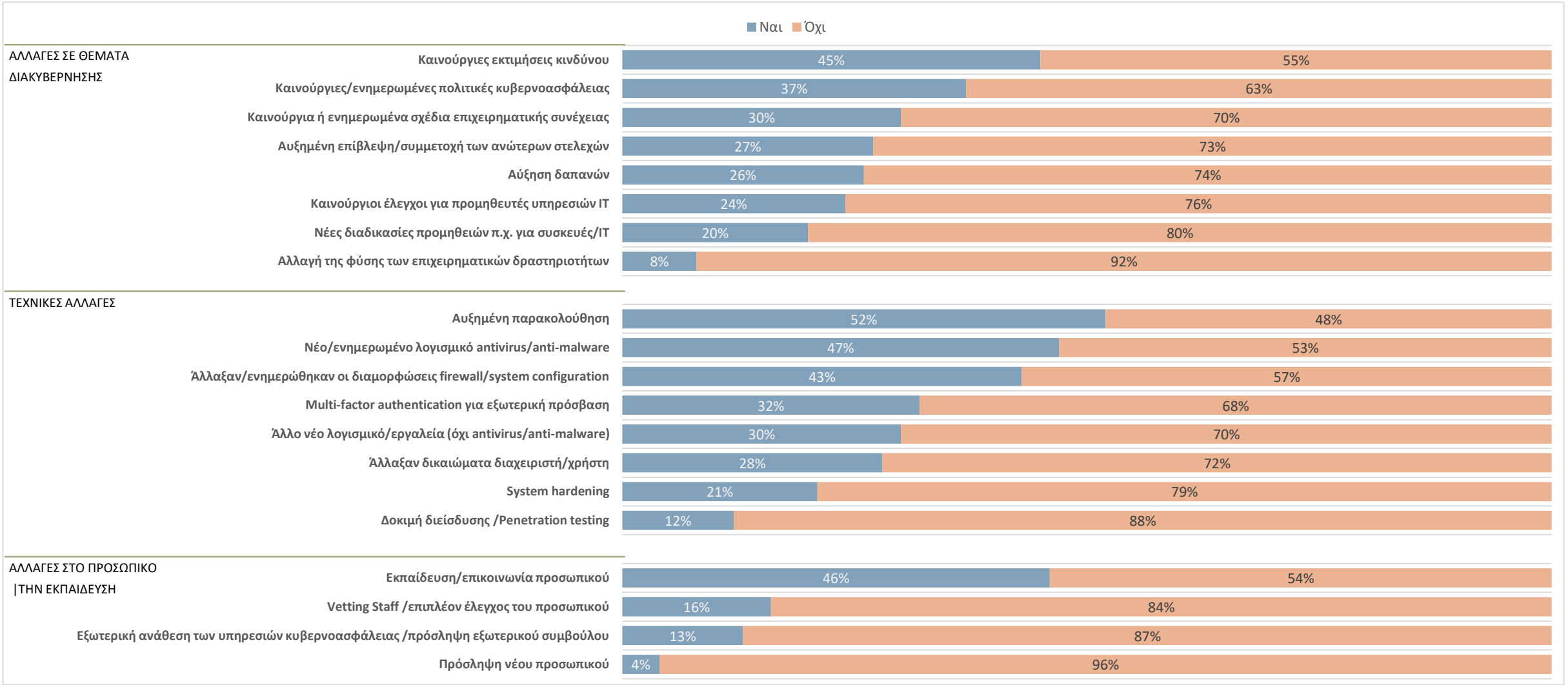
Βάση: Όλοι οι ερωτώμενοι





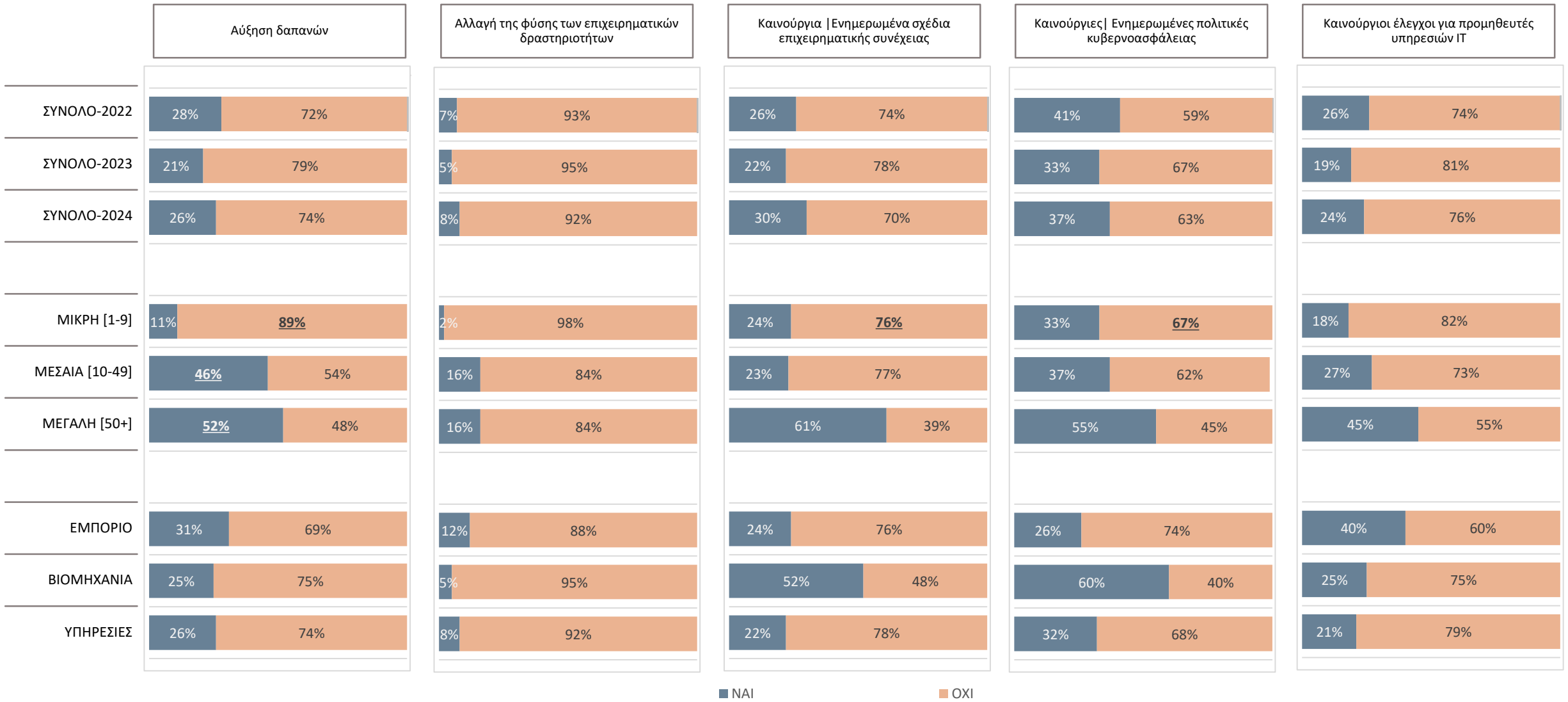
Μετά από αυτήν την παραβίαση| επίθεση, τι από τα ακόλουθα έχετε κάνει για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

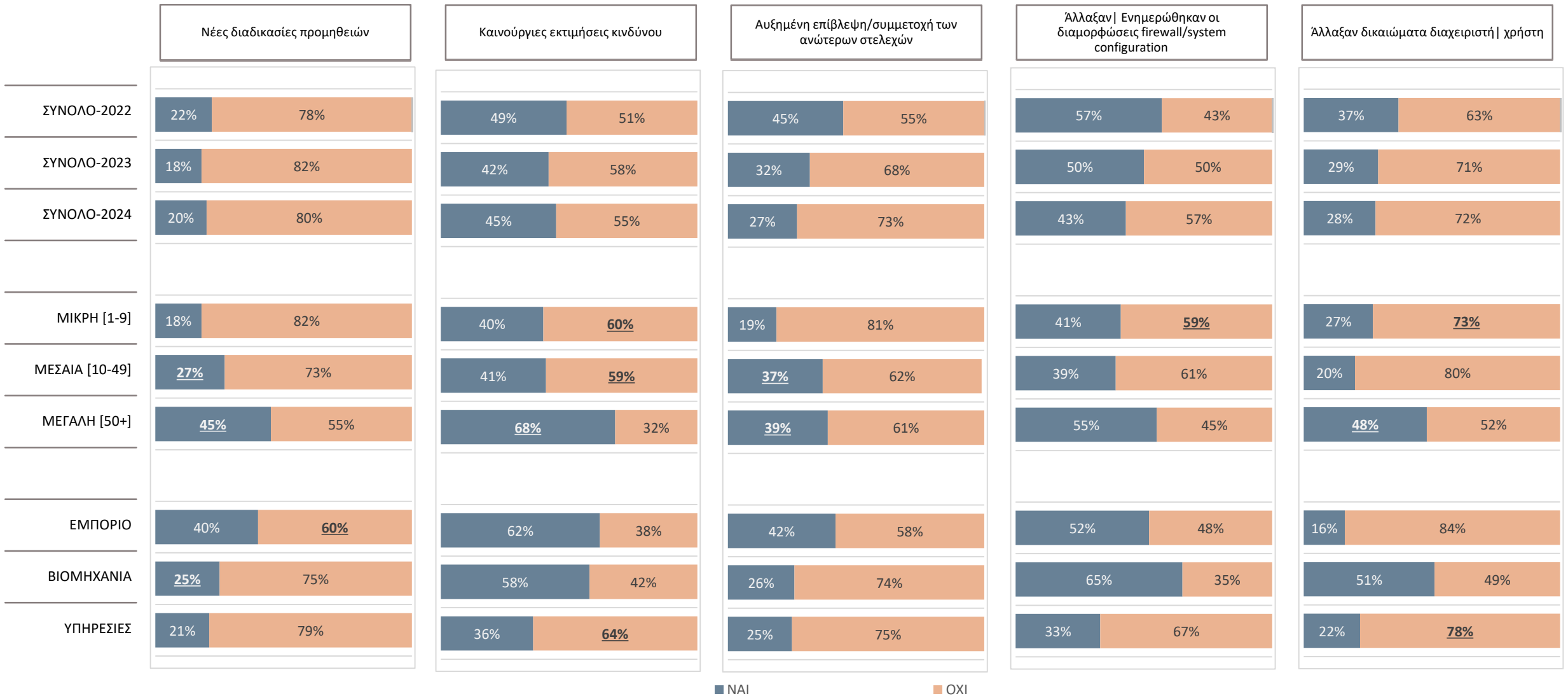
Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

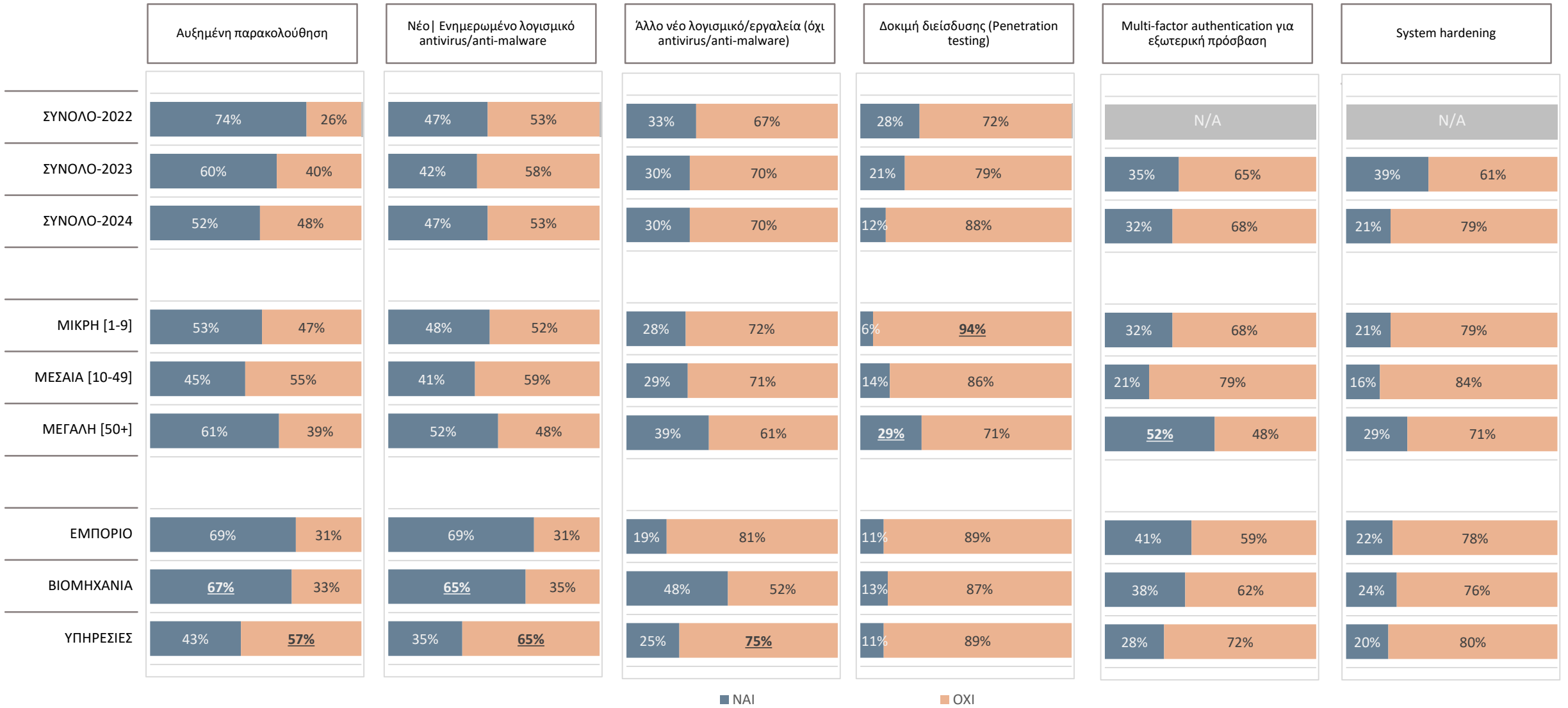
... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



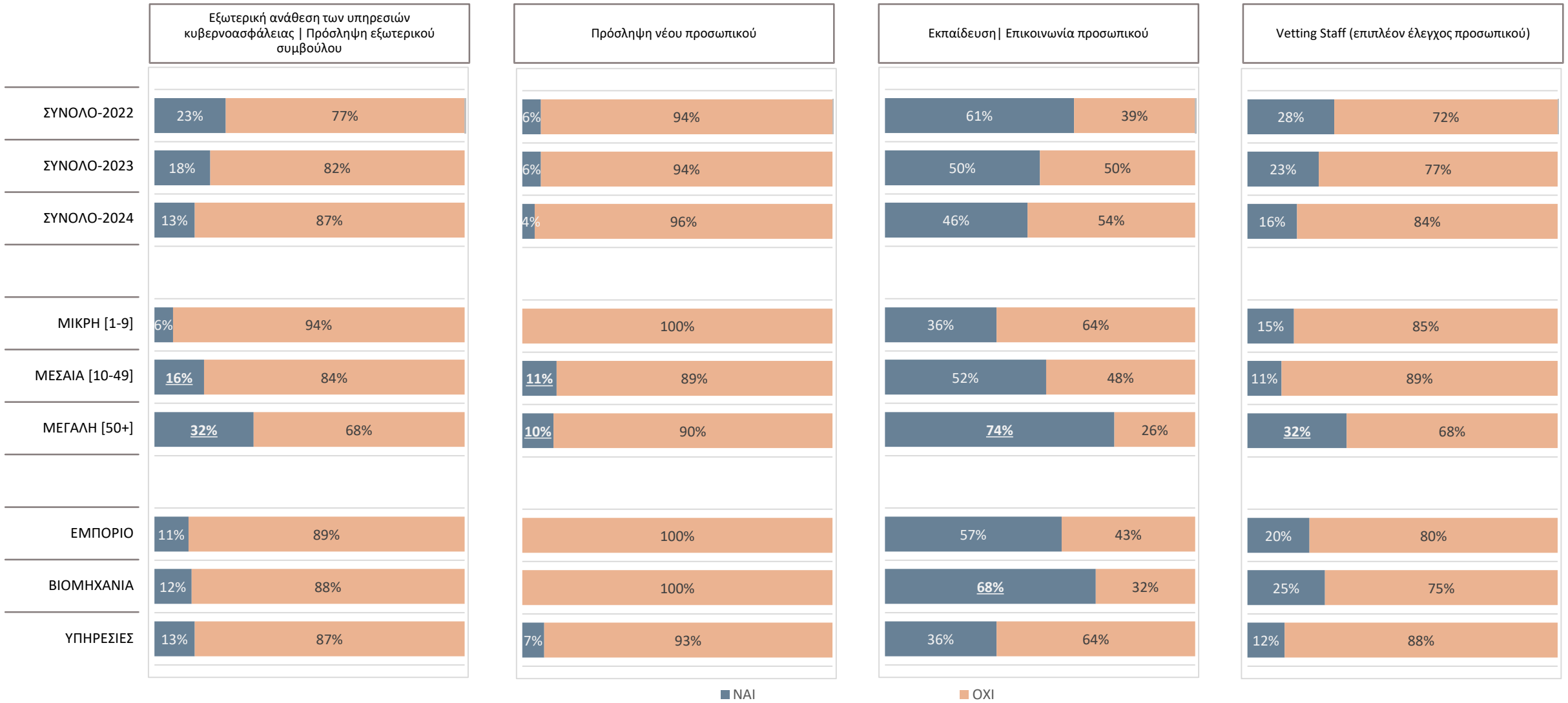
Μετά από αυτήν την παραβίαση/επίθεση, τι *τεχνικές αλλαγές κάνατε*, για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



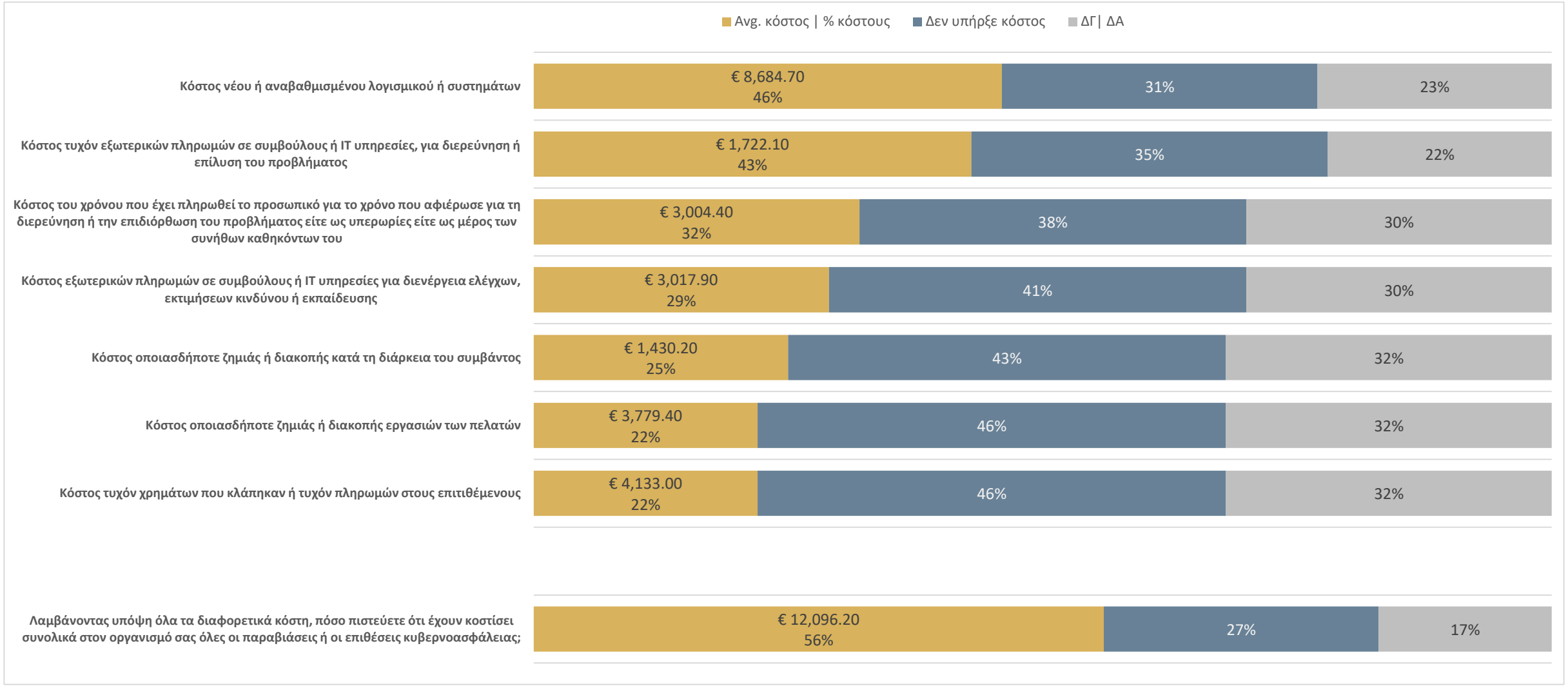
Μετά από αυτήν την παραβίαση/επίθεση, τι *αλλαγές κάνατε σε σχέση με την εκπαίδευση και το προσωπικό*, για να προστατέψετε τον οργανισμό σας από περαιτέρω παραβιάσεις;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



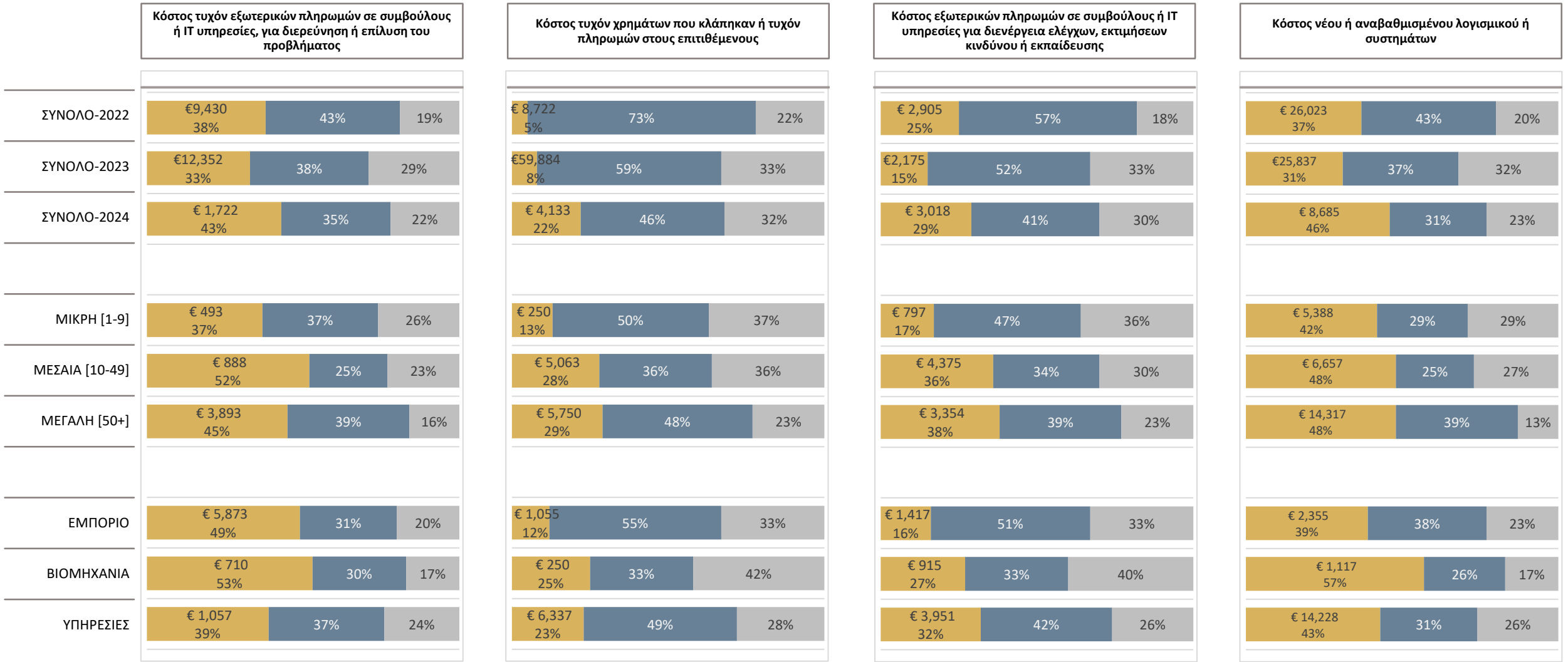
Ποια είναι, τα κατά προσέγγιση, κόστη, της πιο πρόσφατης παραβίασης| επίθεσης, που δεχτήκατε στην εταιρεία σας;

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



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

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



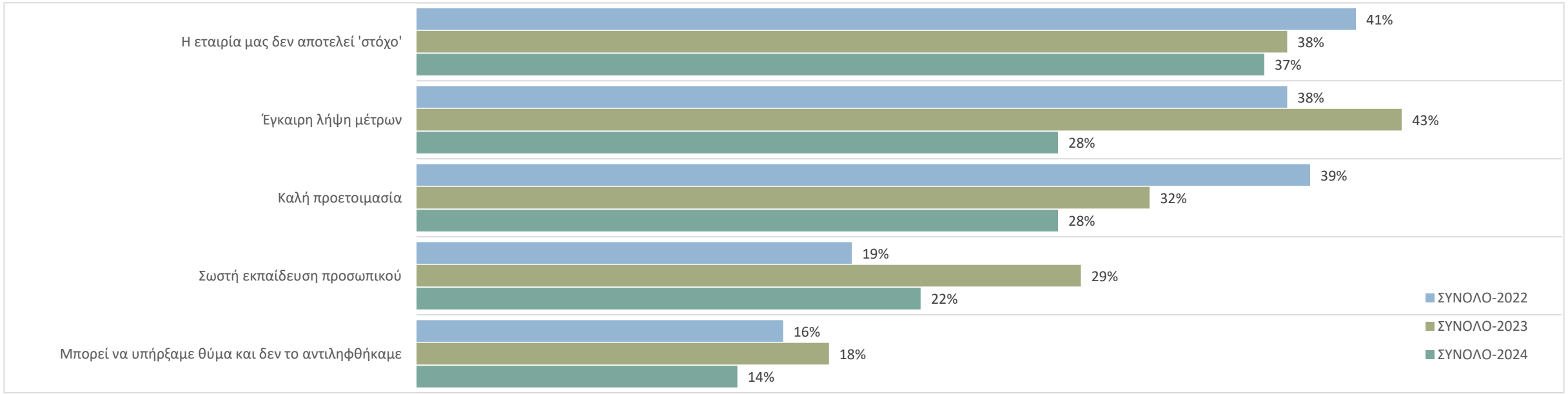
Ποια είναι, τα κατά προσέγγιση, κόστη, της πιο πρόσφατης παραβίασης| επίθεσης, που δεχτήκατε στην εταιρεία σας;

... συνέχεια

Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)

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

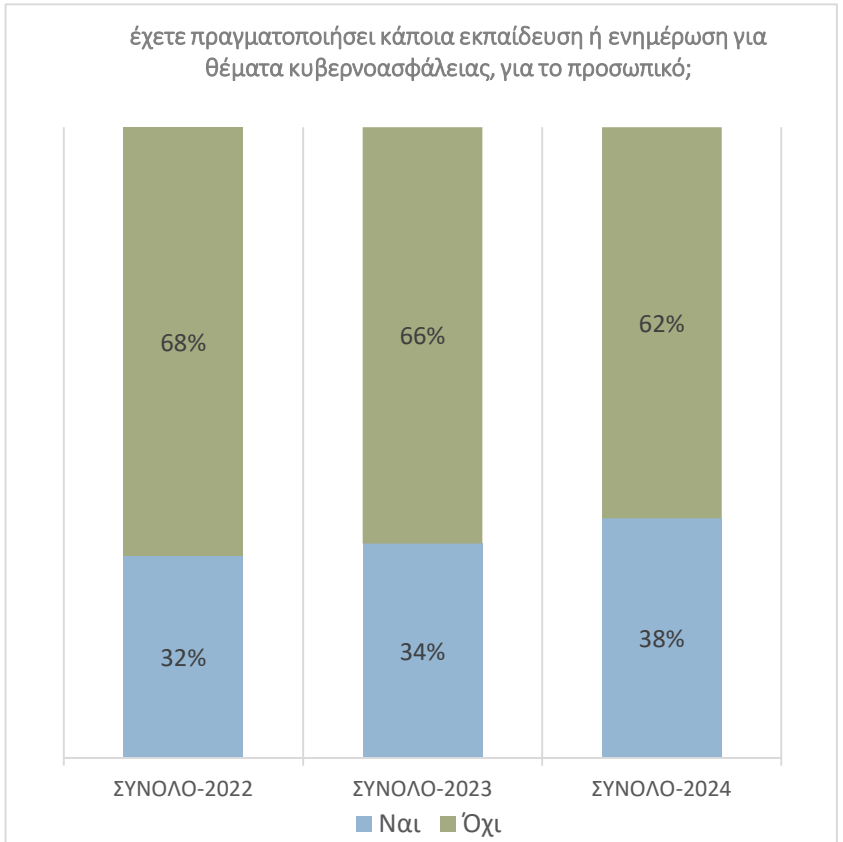
Βάση: Όλοι όσοι δέχτηκαν επίθεση/ παραβίαση (213)



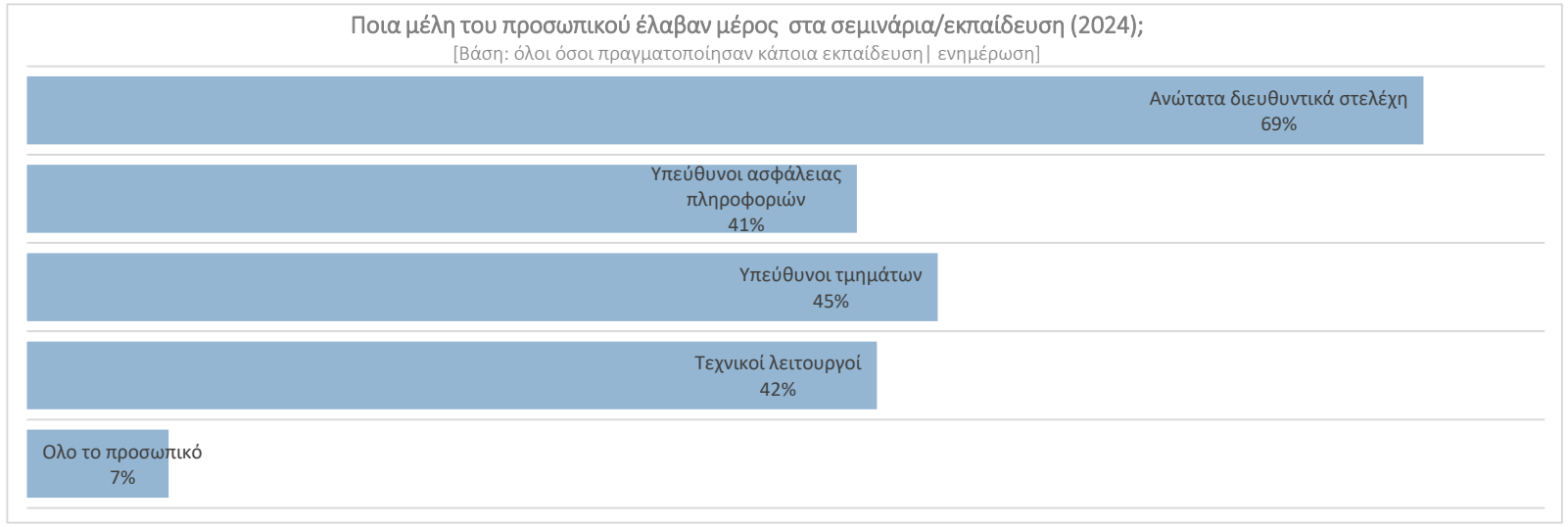
	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Η εταιρία μας δεν αποτελεί στόχο	**49%**	27%	22%	63%	31%	34%
Έγκαιρη λήψη μέτρων	27%	20%	**56%**	36%	9%	30%
Καλή προετοιμασία	24%	23%	**53%**	14%	26%	31%
Σωστή εκπαίδευση προσωπικού	12%	20%	**59%**	21%	25%	21%
Μπορεί να υπήρξαμε θύμα και δεν το αντιληφθήκαμε	17%	12%	13%	24%	19%	12%

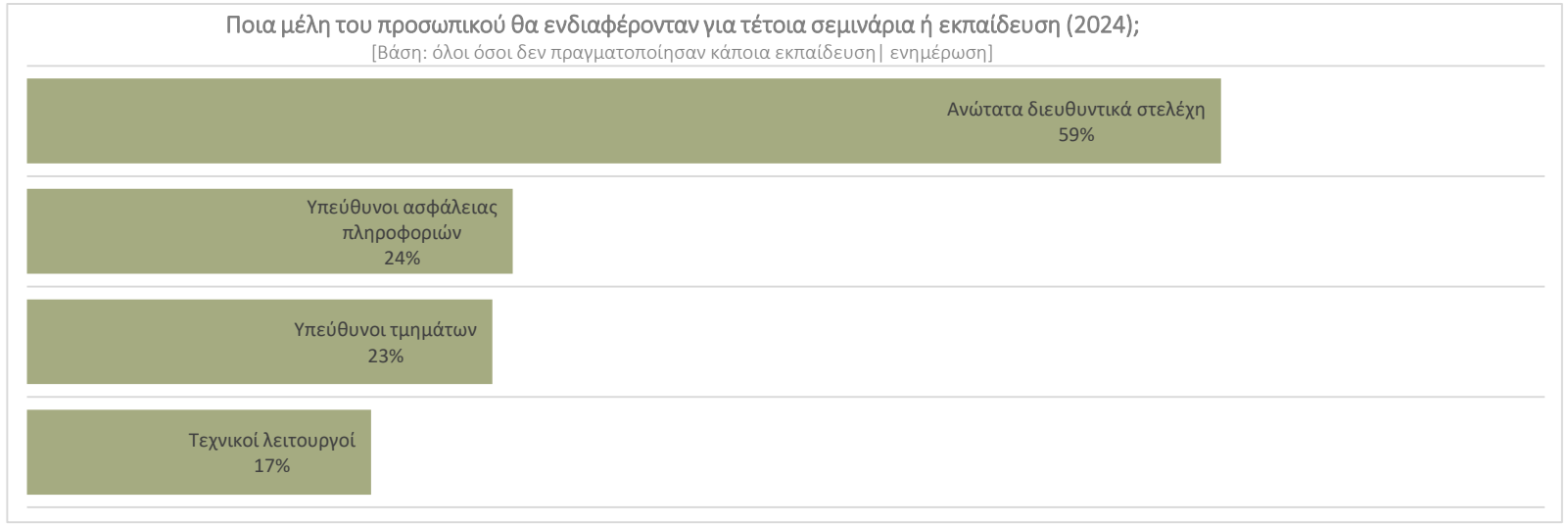
Τους τελευταίους 12 μήνες, έχετε πραγματοποιήσει κάποια εκπαίδευση ή ενημέρωση για θέματα κυβερνοασφάλειας, για το προσωπικό, που ΔΕΝ εμπλέκεται άμεσα στα θέματα αυτά; | Σε ποια μέλη του προσωπικού;

Βάση: Όλοι οι ερωτώμενοι



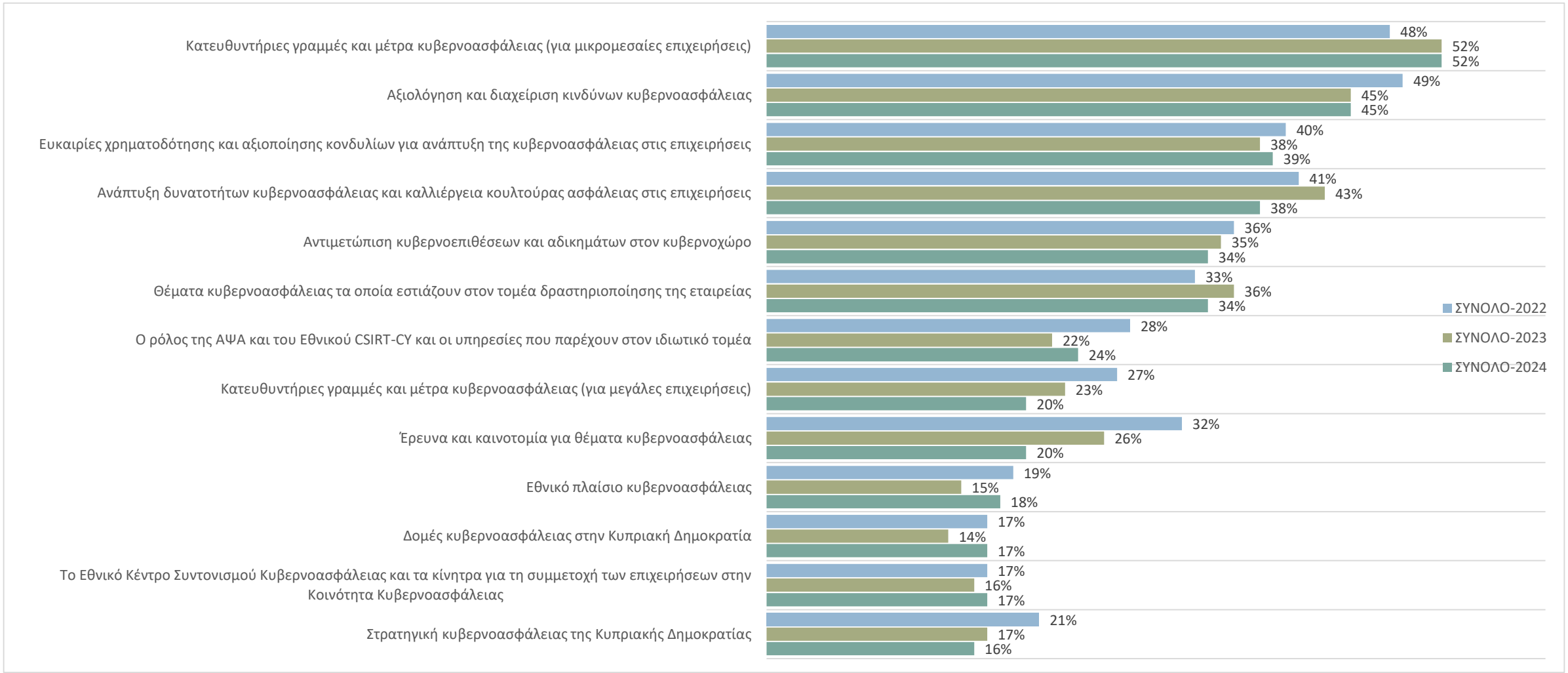
	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Ναι	30%	**41%**	**62%**	18%	**38%**	**42%**
Όχι	70%	59%	38%	**82%**	62%	58%





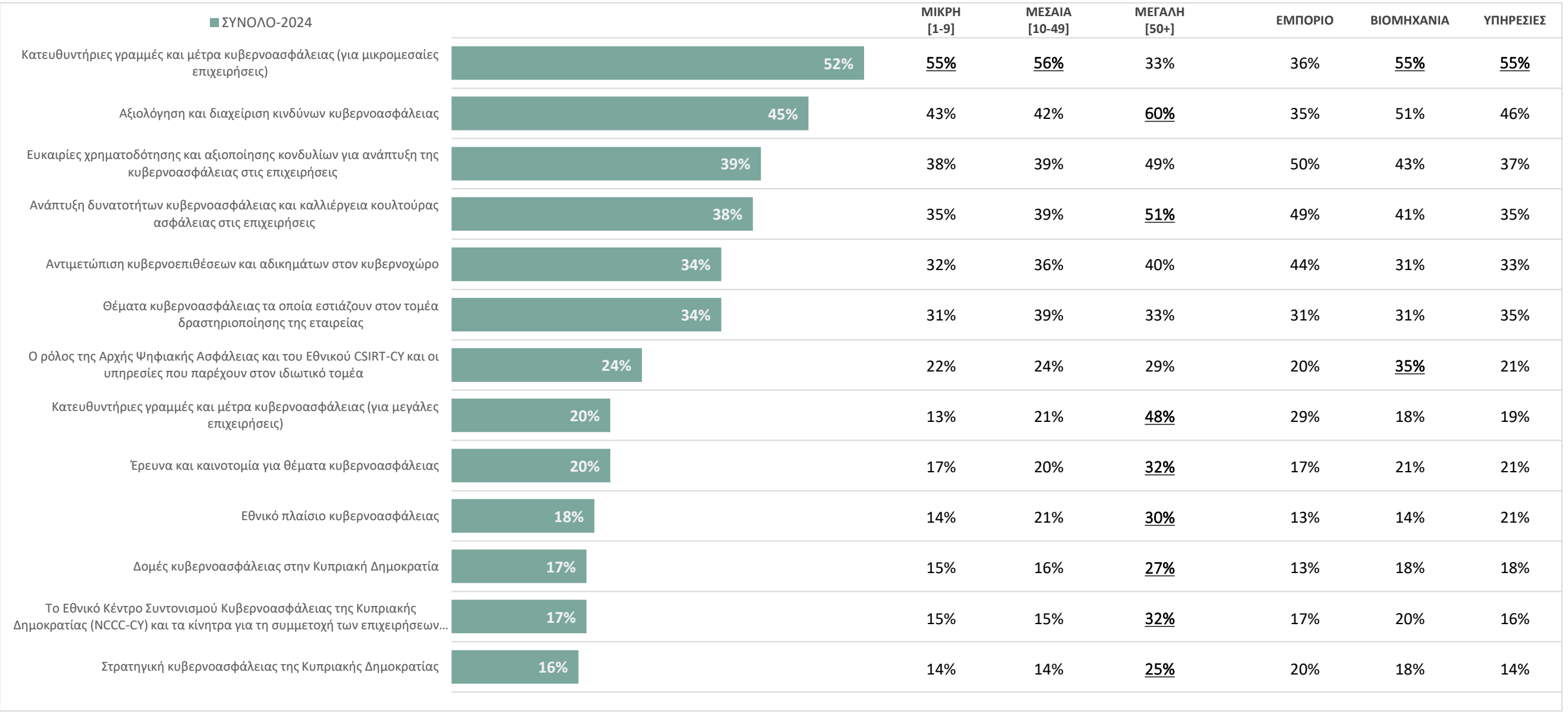
Σε ποια από τα παρακάτω θέματα θα προτιμούσατε να εστιάζουν τα σεμινάρια κατάρτισης;

Βάση: Όλοι οι ερωτώμενοι



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

Βάση: Όλοι οι ερωτώμενοι



	ΣΥΝΟΛΟ-2024	ΜΙΚΡΗ [1-9]	ΜΕΣΑΙΑ [10-49]	ΜΕΓΑΛΗ [50+]	ΕΜΠΟΡΙΟ	ΒΙΟΜΗΧΑΝΙΑ	ΥΠΗΡΕΣΙΕΣ
Κατευθυντήριες γραμμές και μέτρα κυβερνοασφάλειας (για μικρομεσαίες επιχειρήσεις)	52%	55%	56%	33%	36%	55%	55%
Αξιολόγηση και διαχείριση κινδύνων κυβερνοασφάλειας	45%	43%	42%	60%	35%	51%	46%
Ευκαιρίες χρηματοδότησης και αξιοποίησης κονδυλίων για ανάπτυξη της κυβερνοασφάλειας στις επιχειρήσεις	39%	38%	39%	49%	50%	43%	37%
Ανάπτυξη δυνατοτήτων κυβερνοασφάλειας και καλλιέργεια κουλτούρας ασφάλειας στις επιχειρήσεις	38%	35%	39%	51%	49%	41%	35%
Αντιμετώπιση κυβερνοεπιθέσεων και αδικημάτων στον κυβερνοχώρο	34%	32%	36%	40%	44%	31%	33%
Θέματα κυβερνοασφάλειας τα οποία εστιάζουν στον τομέα δραστηριοποίησης της εταιρείας	34%	31%	39%	33%	31%	31%	35%
Ο ρόλος της Αρχής Ψηφιακής Ασφάλειας και του Εθνικού CSIRT-CY και οι υπηρεσίες που παρέχουν στον ιδιωτικό τομέα	24%	22%	24%	29%	20%	35%	21%
Κατευθυντήριες γραμμές και μέτρα κυβερνοασφάλειας (για μεγάλες επιχειρήσεις)	20%	13%	21%	48%	29%	18%	19%
Έρευνα και καινοτομία για θέματα κυβερνοασφάλειας	20%	17%	20%	32%	17%	21%	21%
Εθνικό πλαίσιο κυβερνοασφάλειας	18%	14%	21%	30%	13%	14%	21%
Δομές κυβερνοασφάλειας στην Κυπριακή Δημοκρατία	17%	15%	16%	27%	13%	18%	18%
Το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (NCCC-CY) και τα κίνητρα για τη συμμετοχή των επιχειρήσεων...	17%	15%	15%	32%	17%	20%	16%
Στρατηγική κυβερνοασφάλειας της Κυπριακής Δημοκρατίας	16%	14%	14%	25%	20%	18%	14%

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

ΕΤΟΙΜΑΣΤΗΚΕ ΓΙΑ ΤΗΝ ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΟΚΤΩΒΡΙΟΣ 2024

RAI Consultants Ltd

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ