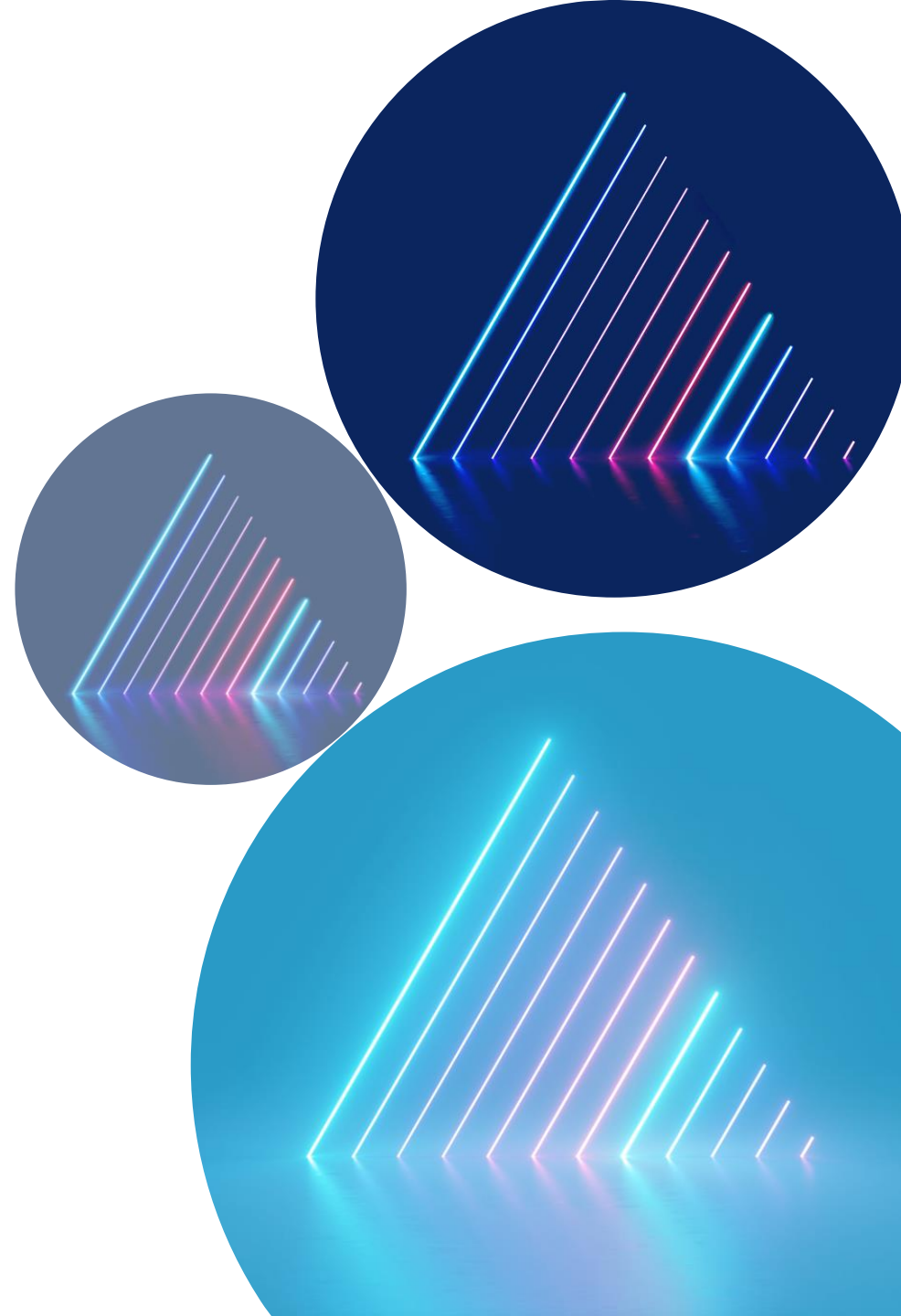


Πανελλαδική Έρευνα B2B για την Ασφάλεια στο Διαδίκτυο

Δεκέμβριος 2023



Η ταυτότητα της έρευνας

Εταιρεία: Metron Analysis (Α.Μ. ΕΣΡ 4 - Αρ. Γ.Ε.ΜΗ 002305501000)

Ανάθεση: ΤΣΟΜΩΚΟΣ ΔΗΜΟΣΙΕΣ ΣΧΕΣΕΙΣ ΑΕ

Τύπος Έρευνας: Τηλεφωνικές και online συνεντεύξεις με χρήση δομημένου ερωτηματολογίου

Περιοχή Έρευνας Πανελλαδική

Μέθοδος Δειγματοληψίας: Τυχαία επιλογή ανώτερων διοικητικών στελεχών επιχειρήσεων με προσωπικό τουλάχιστον 10 άτομα πανελλαδικά

Χρόνος Διεξαγωγής: 20/11-10/12/2023

Μέγεθος Δείγματος: 171 συνεντεύξεις, 111 online και 60 τηλεφωνικά

Προσωπικό field/Ελεγχοι: Για τις τηλεφωνικές συνεντεύξεις εργάστηκαν 3 επόπτες και 2 συνεντευκτές. Το 34% των τηλεφωνικών συνεντεύξεων ελέγχθηκαν με τη μέθοδο της συνακρόασης και το 100% ηλεκτρονικά.

Επισήμανση: Λόγω στρογγυλοποίησης ενδέχεται κάποιες κατανομές να μην αθροίζουν στο 100%

Η METRON ANALYSIS είναι μέλος της ESOMAR και του ΣΕΔΕΑ και τηρεί τους κώδικες δεοντολογίας και διεξαγωγής ερευνών και επαγγελματικής πρακτικής της ESOMAR και του ΣΕΔΕΑ.

Προφίλ Εταιρειών

Αντιλήψεις & Αντιλαμβανόμενες Απειλές από τη Χρήση του Διαδικτύου

Περιπτώσεις Κυβερνοεπιθέσεων και Αντιμετώπιση

Μέτρα Πρόληψης

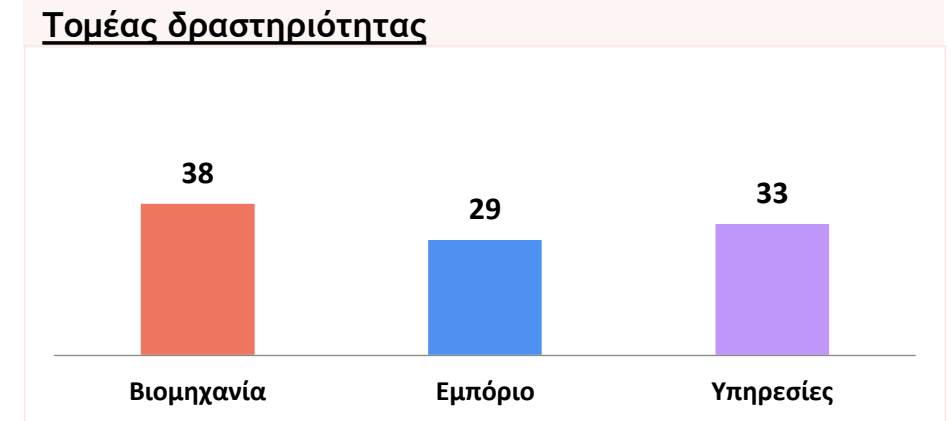
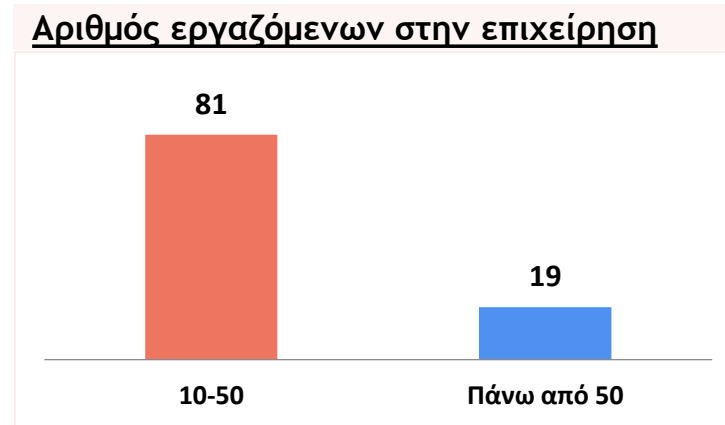
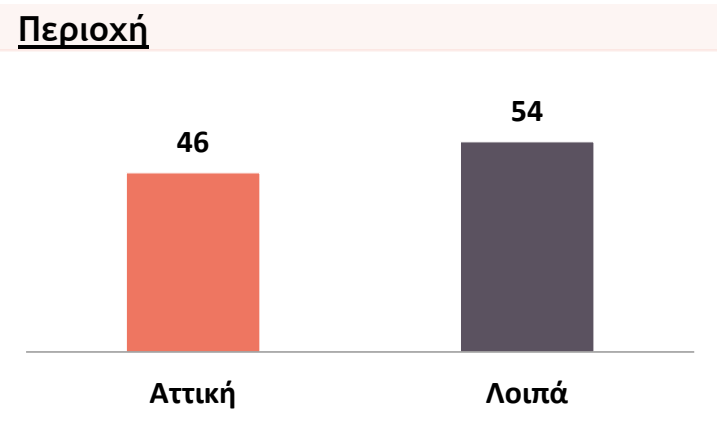
Πολιτικές Προστασίας Προσωπικών Δεδομένων & Πληροφοριών

Σύνοψη αποτελεσμάτων



Προφίλ Εταιρειών

Προφίλ εταιρειών

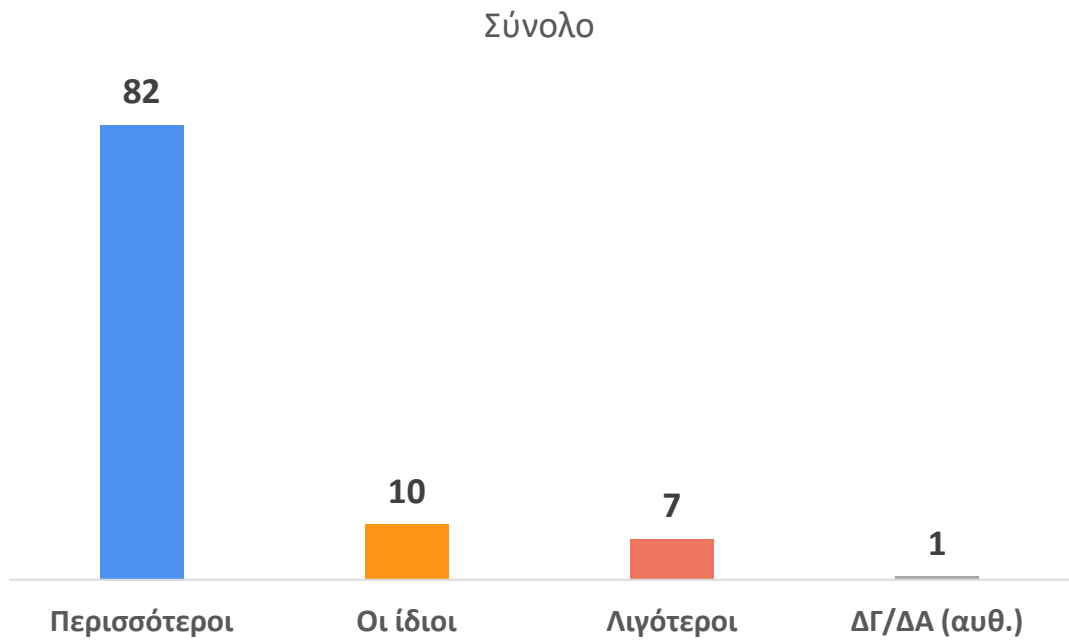




Αντιλήψεις & Αντιλαμβανόμενες Απειλές από τη Χρήση του Διαδικτύου

Για τη μεγάλη πλειονότητα των ερωτώμενων οι κίνδυνοι κυβερνοασφάλειας γενικά για τις επιχειρήσεις αυξάνονται με την πάροδο του χρόνου ...

Συγκριτικά με 5 χρόνια πριν, αισθάνεστε ότι οι κίνδυνοι κυβερνοασφάλειας για τις επιχειρήσεις είναι...



		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Περισσότεροι	82	85	79	80	88	77	84	86
Οι ίδιοι	10	8	12	10	9	14	6	9
Λιγότεροι	7	6	9	9	3	9	10	4
ΔΓ/ΔΑ (αυθ.)	1	1	*	1	*	*	*	2

...ειδικότερα όμως όσον αφορά τα προσωπικά δεδομένα, καταγράφεται μια αίσθηση σχετικής ασφάλειας (σε σχέση και με το γενικό κοινό), ιδίως σε μεγαλύτερες επιχειρήσεις και στην Αττική.

Συγκριτικά με 5 χρόνια πριν, αισθάνεστε ότι τα προσωπικά δεδομένα και πληροφορίες των πολιτών είναι...

Σύνολο

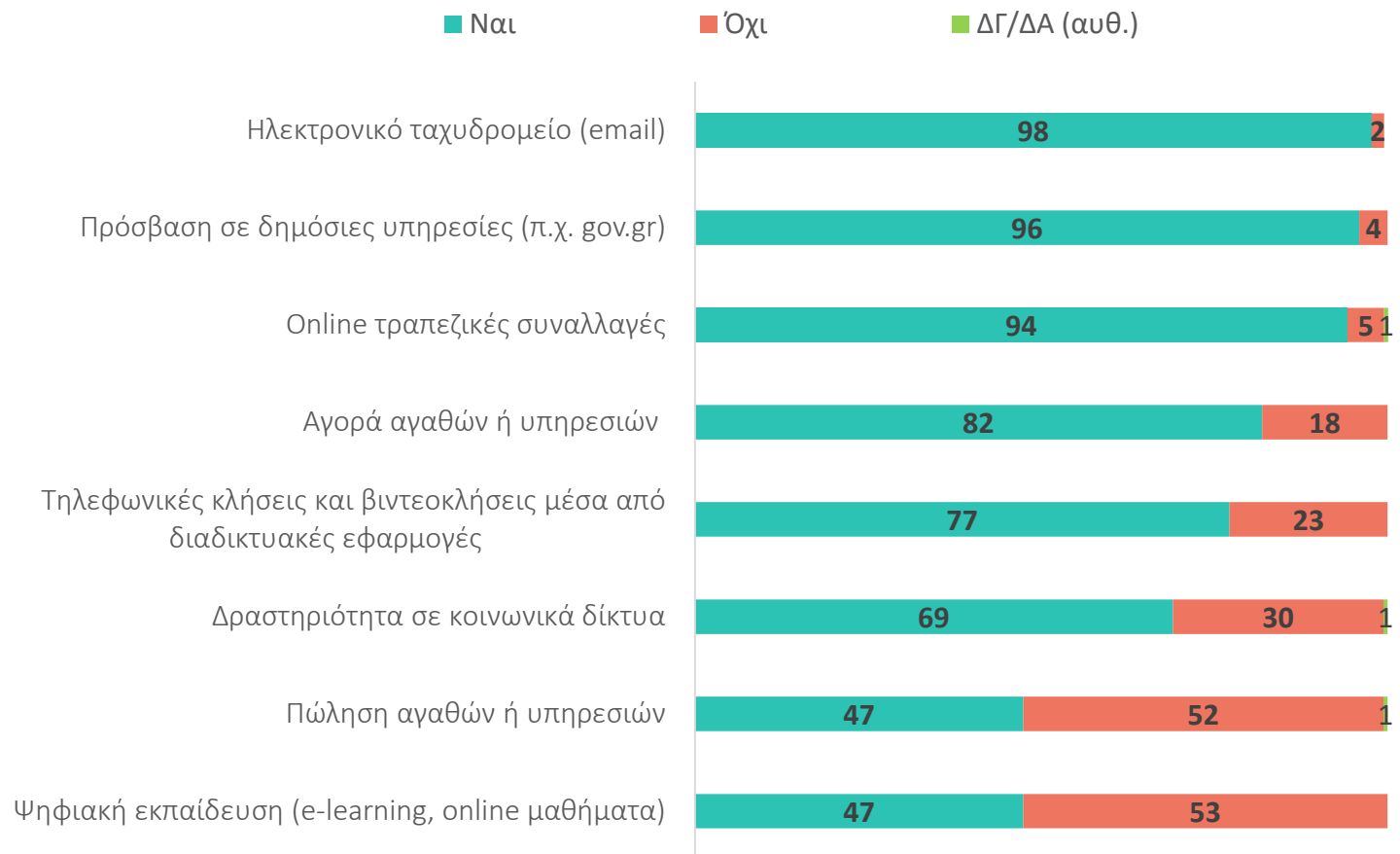


- ✓ Περισσότερο ασφαλή 17%
 - ✓ Το ίδιο ασφαλή 27%
 - ✓ Λιγότερο ασφαλή 51%
- Έρευνα γενικού κοινού (Απρίλιος 2023)

	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Περισσότερο ασφαλή	41	53	32	38	58	40	38	46
Το ίδιο ασφαλή	25	20	28	27	15	23	28	23
Λιγότερο ασφαλή	33	27	38	34	27	37	34	27
ΔΓ/ΔΑ (αυθ.)	1	*	2	1	*	*	*	4

Οι επιχειρήσεις παρέχουν/χρησιμοποιούν κατά κανόνα περισσότερο online υπηρεσίες απ' ό,τι το γενικό κοινό

Ποιες από τις παρακάτω υπηρεσίες παρέχει ή χρησιμοποιεί online η εταιρεία σας;



- ✓ Ηλεκτρονικό ταχυδρομείο (email) 82%
- ✓ Πρόσβαση σε δημόσιες υπηρεσίες (π.χ. gov.gr) 75%
- ✓ Online τραπεζικές συναλλαγές 71%
- ✓ Αγορά αγαθών ή υπηρεσιών 58%
- ✓ Τηλεφωνικές κλήσεις και βιντεοκλήσεις μέσα από διαδικτυακές εφαρμογές 83%
- ✓ Δραστηριότητα σε κοινωνικά δίκτυα 82%
- ✓ Πώληση αγαθών ή υπηρεσιών 22%
- ✓ Ψηφιακή εκπαίδευση (e-learning, online μαθήματα) 33%

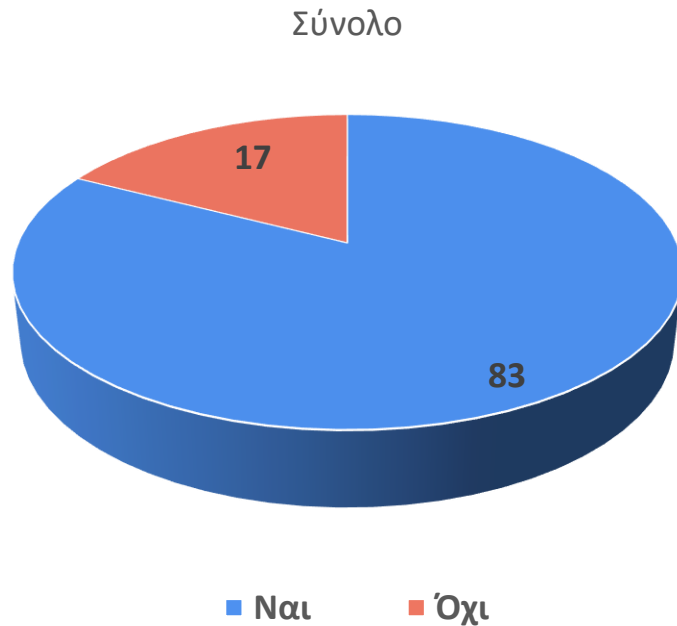
Έρευνα γενικού κοινού (Απρίλιος 2023)

Υπηρεσίες που παρέχει ή χρησιμοποιεί online η εταιρεία

Ναι	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ηλεκτρονικό ταχυδρομείο (email)	98	98	98	99	94	99	96	98
Πρόσβαση σε δημόσιες υπηρεσίες (π.χ. gov.gr)	96	95	97	96	97	95	96	96
Online τραπεζικές συναλλαγές	94	92	96	97	82	94	96	93
Αγορά αγαθών ή υπηρεσιών	82	86	78	86	67	82	78	86
Τηλεφωνικές κλήσεις και βιντεοκλήσεις μέσα από διαδικτυακές εφαρμογές	77	79	76	75	85	79	68	84
Δραστηριότητα σε κοινωνικά δίκτυα	69	76	63	71	61	65	62	80
Πώληση αγαθών ή υπηρεσιών	47	48	47	48	46	43	48	52
Ψηφιακή εκπαίδευση (e-learning, online μαθήματα)	47	49	46	44	64	45	32	64

Και πάνω από 8 στους 10 θεωρούν ότι η χρήση του διαδικτύου εγκυμονεί κινδύνους – ακόμη περισσότερο στις μεγαλύτερες επιχειρήσεις

Κατά την άποψή σας η χρήση του διαδικτύου εγκυμονεί κινδύνους για τις επιχειρήσεις ή όχι;



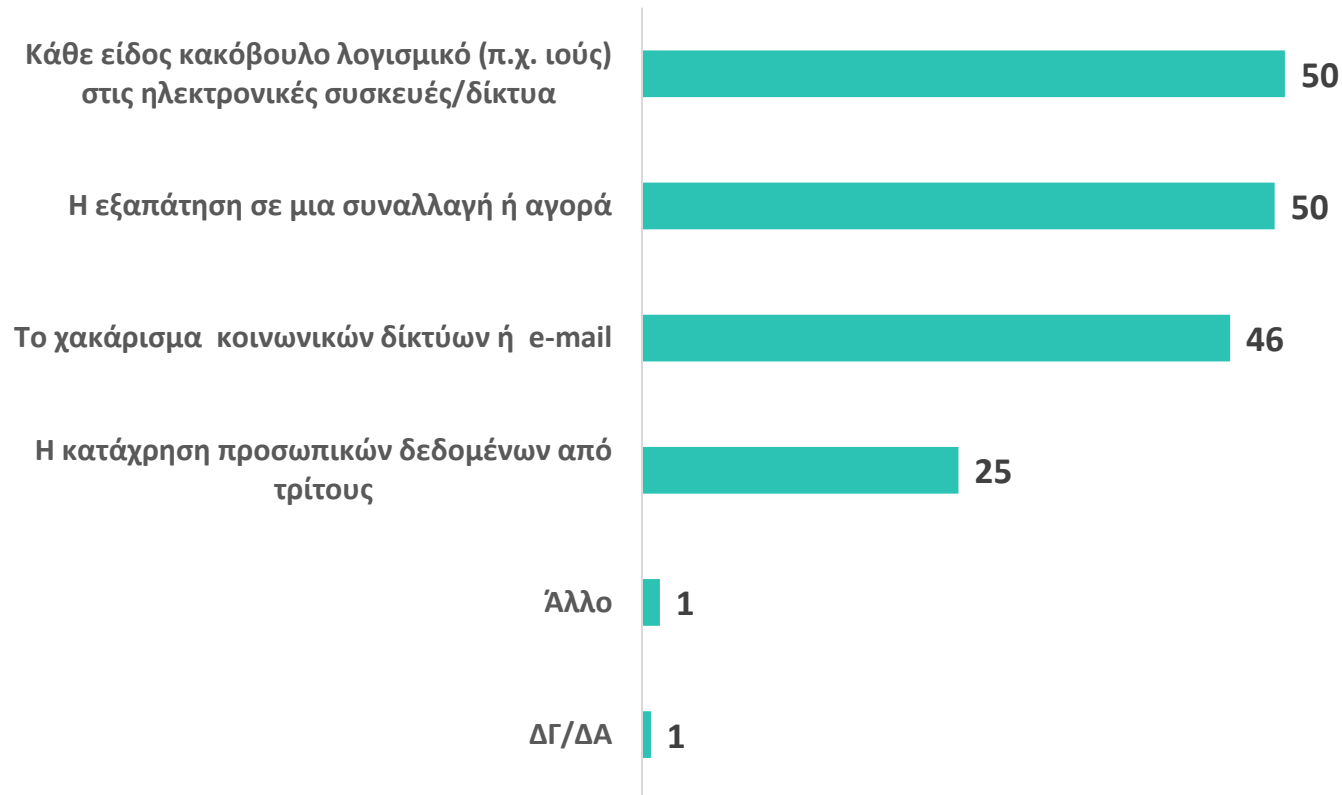
		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	83	84	82	80	94	86	82	79
Όχι	17	17	19	20	6	14	18	21

84% στην έρευνα γενικού κοινού θεωρεί πως η χρήση του διαδικτύου εγκυμονεί κινδύνους για τους χρήστες (Απρίλιος 2023)

Σε όσους θεωρούν ότι η χρήση του διαδικτύου εγκυμονεί κινδύνους, οι αντιλαμβανόμενοι κίνδυνοι αφορούν κυρίως το κακόβουλο λογισμικό, την εξαπάτηση σε συναλλαγές και το χακάρισμα – ενώ στο γενικό κοινό βαραίνουν η εξαπάτηση σε συναλλαγές και η κατάχρηση προσωπικών δεδομένων

Ποιοι θεωρείτε πως είναι οι σημαντικότεροι κίνδυνοι που μπορεί να αντιμετωπίσει μια επιχείρηση στο διαδίκτυο;
(αυθόρμητα – έως 2 απαντήσεις)

Βάση: το 83% που πιστεύει ότι η χρήση του διαδικτύου εγκυμονεί κινδύνους για τις επιχειρήσεις



- ✓ Κάθε είδος κακόβουλο λογισμικό (π.χ. ιούς) στις ηλεκτρονικές συσκευές/δίκτυα 14%
- ✓ Η εξαπάτηση σε μια συναλλαγή ή αγορά 48%
- ✓ Το χακάρισμα κοινωνικών δικτύων ή e-mail 14%
- ✓ Η κατάχρηση προσωπικών δεδομένων από τρίτους 32%

Έρευνα γενικού κοινού (Απρίλιος 2023)

Σημαντικότεροι κίνδυνοι που μπορεί να αντιμετωπίσει μια εταιρεία στο διαδίκτυο

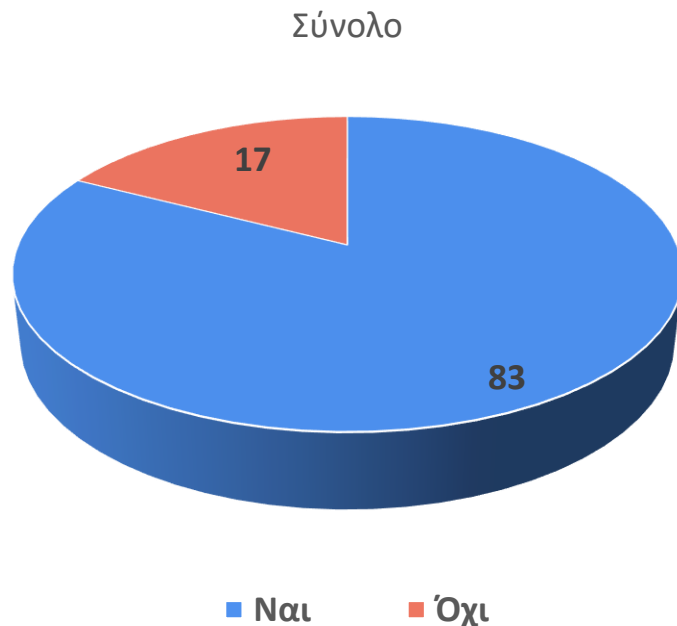
Αυθόρμητα-ως 2 απαντήσεις

Βάση: το 83% που πιστεύει ότι η χρήση του διαδικτύου εγκυμονεί κινδύνους για τις επιχειρήσεις

		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Κάθε είδος κακόβουλο λογισμικό (π.χ. ιούς) στις ηλεκτρονικές συσκευές/δίκτυα	50	52	49	50	52	46	56	50
Η εξαπάτηση σε μια συναλλαγή ή αγορά	50	55	45	49	52	59	44	43
Το χακάρισμα κοινωνικών δικτύων ή e-mail	46	49	44	48	39	43	49	48
Η κατάχρηση προσωπικών δεδομένων από τρίτους	25	21	28	24	29	23	24	27
Άλλο	1	2	1	1	3	2	*	2
ΔΓ/ΔΑ	1	*	1	1	*	*	*	2

Η επίδραση της πανδημίας είναι εμφανής ως προς την περαιτέρω ψηφιοποίηση των υπηρεσιών για τις περισσότερες επιχειρήσεις...

Η υγειονομική κρίση και η πανδημία έκανε την εταιρεία σας να προχωρήσει σε μεγαλύτερη ψηφιοποίηση των υπηρεσιών της;

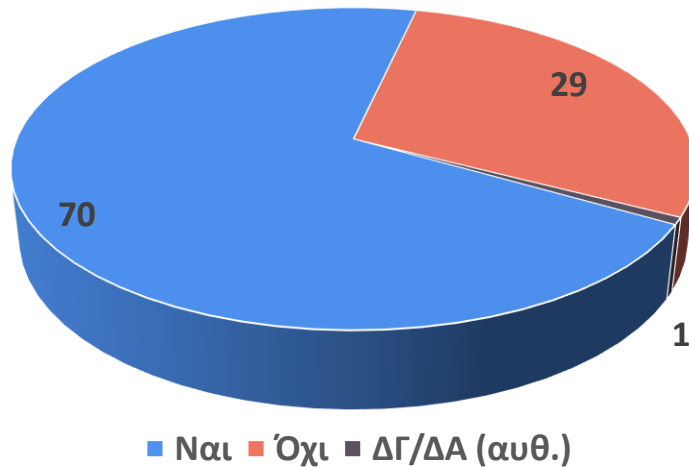


		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	83	87	78	83	82	82	80	86
Όχι	17	13	22	17	18	19	20	14

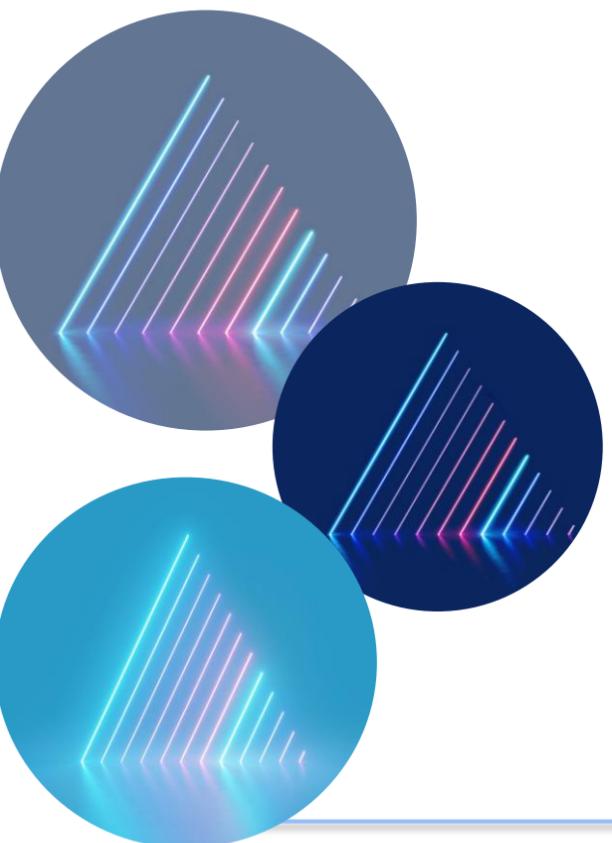
...εξέλιξη που όμως συνεπάγεται και περαιτέρω ενίσχυση των αντιλαμβανόμενων κινδύνων κυβερνοασφάλειας – περισσότερο στις μικρότερες επιχειρήσεις παρά στις μεγαλύτερες

Αυτό πιστεύετε ότι αύξησε τους κινδύνους κυβερνοασφάλειας στην εταιρεία σας;

Βάση: το 83% που αναφέρει ότι η υγειονομική κρίση και η πανδημία έκανε την εταιρεία τους να προχωρήσει σε μεγαλύτερη ψηφιοποίηση των υπηρεσιών της



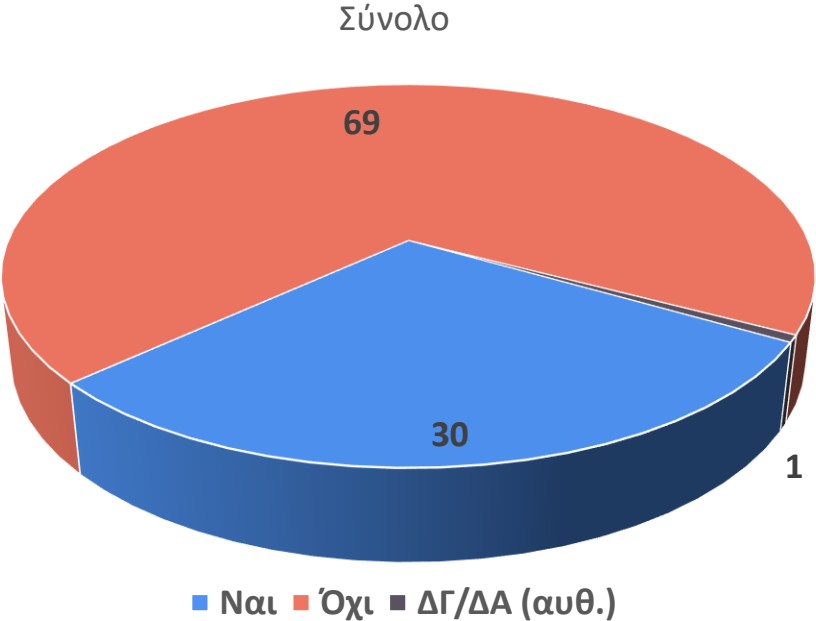
	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	70	65	75	74	56	74	70	67
Όχι	29	35	24	25	44	25	30	33
ΔΓ/ΔΑ (αυθ.)	1	*	1	1	*	2	*	*



Περιπτώσεις
Κυβερνοεπιθέσεων και
Αντιμετώπιση

Όσον αφορά συγκεκριμένες εμπειρίες κυβερνοεπίθεσης/κυβερνοεγκλήματος, σχεδόν το 1/3 των εν λόγω επιχειρήσεων αναφέρουν σχετικά περιστατικά – έναντι 11% στο γενικό κοινό...

Έχει πέσει ποτέ η εταιρεία σας θύμα κυβερνοεπίθεσης/κυβερνοεγκλήματος;



		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	30	32	28	31	24	32	24	32
Όχι	69	67	72	69	73	66	76	68
ΔΓ/ΔΑ (αυθ.)	1	1	*	*	3	2	*	*

11% στην έρευνα γενικού κοινού έχει πέσει θύμα κυβερνοεπίθεσης/κυβερνοεγκλήματος (Απρίλιος 2023)

...και ειδικότερα, αναφέρονται κατά κύριο λόγο παραπλανητικά emails και δευτερευόντως κακόβουλο λογισμικό ή χακάρισμα κοινωνικών δικτύων/emails – αλλά ελάχιστα περιπτώσεις παραβίασης προσωπικών δεδομένων πελατών

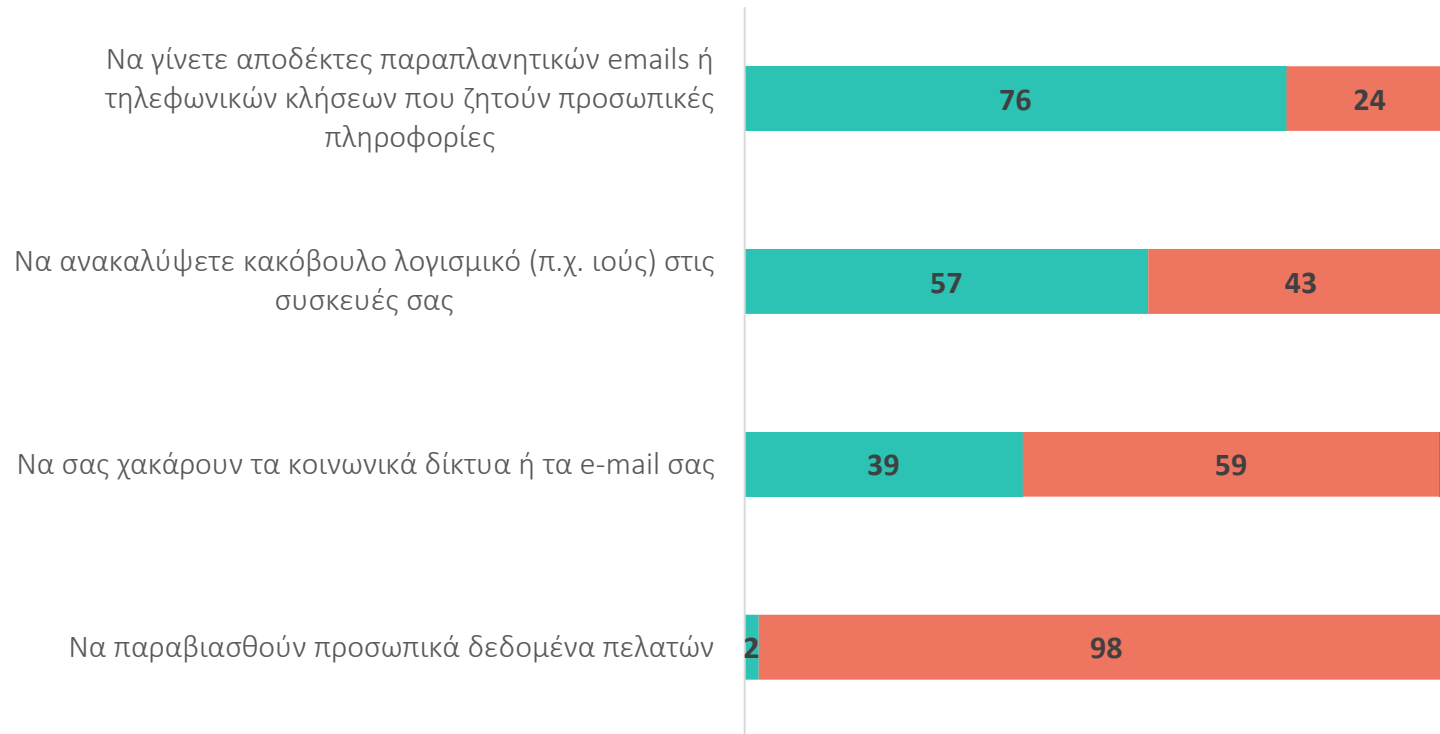
Και ποια από τις παρακάτω περιπτώσεις κυβερνοεπίθεσης/κυβερνοεγκλήματος σας έχει συμβεί;

Βάση: το 30% που έχουν πέσει θύματα κυβερνοεπίθεσης/κυβερνοεγκλήματος

■ Ναι

■ Όχι

■ ΔΓ/ΔΑ (αυθ.)



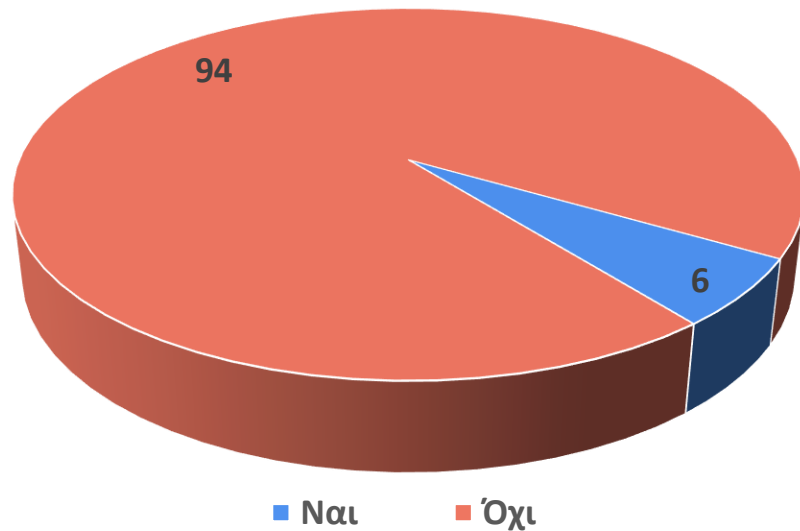
- ✓ Να γίνετε αποδέκτες παραπλανητικών emails ή τηλεφωνικών κλήσεων που ζητούν προσωπικές πληροφορίες 62%
- ✓ Να ανακαλύψετε κακόβουλο λογισμικό (π.χ. ιούς) στις συσκευές σας 65%
- ✓ Να σας χακάρουν τα κοινωνικά δίκτυα ή τα e-mail σας 44%

Έρευνα γενικού κοινού (Απρίλιος 2023)

Σε αυτό το πλαίσιο, αναφέρονται επίσης και περιπτώσεις χακαρίσματος server ή «κλειδώματος» αρχείων με στόχο την εκβίαση

Υπάρχει κάποια άλλη περίπτωση κυβερνοεπίθεσης/κυβερνοεγκλήματος που έχει συμβεί στην εταιρεία σας;

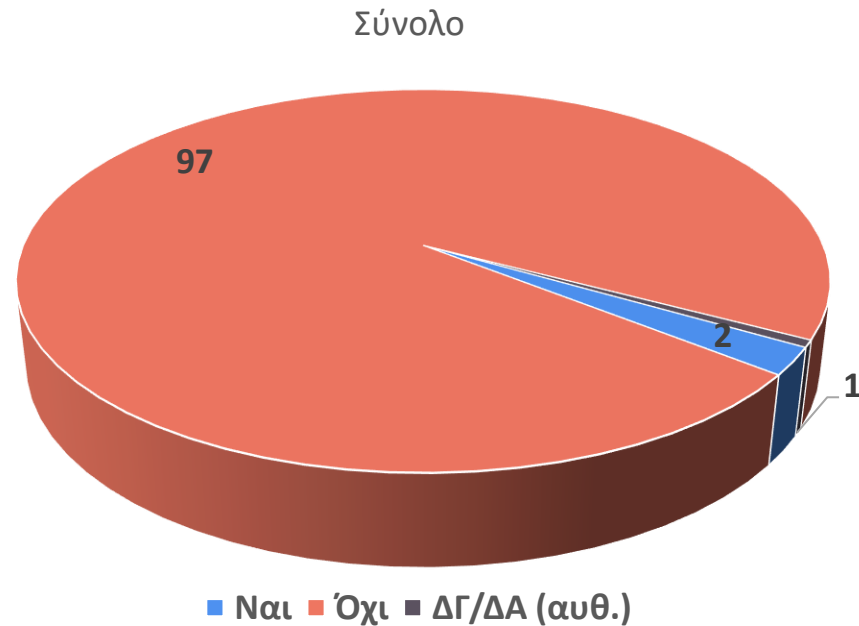
Βάση: το 30% που έχουν πέσει θύματα κυβερνοεπίθεσης/κυβερνοεγκλήματος



- ✓ Χάκαραν τον server
- ✓ Κλειδώθηκαν τα αρχεία και ζητούσαν χρήματα για να τα ξεκλειδώσουν

Ελάχιστα όμως αναφέρονται περιπτώσεις πελατών που διαμαρτυρήθηκαν για ελλιπή προστασία προσωπικών δεδομένων – όπως, αντίστοιχα, ελάχιστα αναφέρθηκαν περιπτώσεις παραβίασης προσωπικών δεδομένων πελατών

Έχουν υπάρξει περιπτώσεις πελατών που διαμαρτυρήθηκαν για ελλιπή προστασία προσωπικών δεδομένων από την εταιρεία σας;

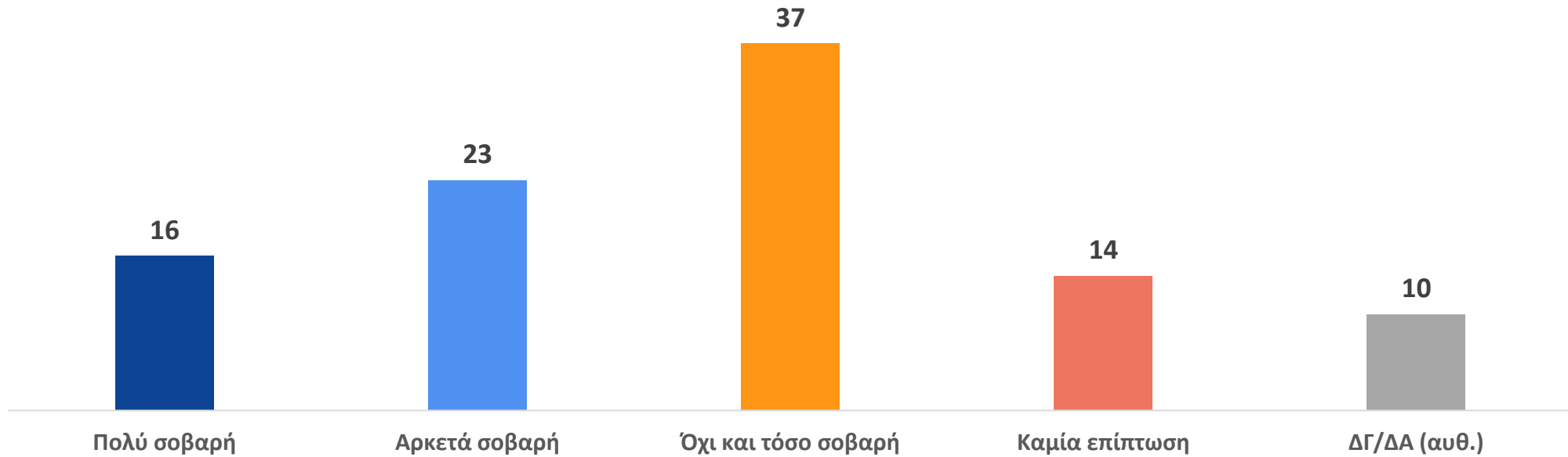


		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	2	1	3	1	6	3	*	4
Όχι	97	98	97	99	91	95	100	96
ΔΓ/ΔΑ (αυθ.)	1	1	*	*	3	2	*	*

Όσον αφορά πάντως την επίπτωση των περιστατικών αυτών στην επιχείρηση, σχεδόν 4 στους 10 θεωρούν ότι ήταν πολύ/αρκετά σοβαρή, αλλά και 1 στους 2 ότι ήταν όχι τόσο σοβαρή ή ασήμαντη

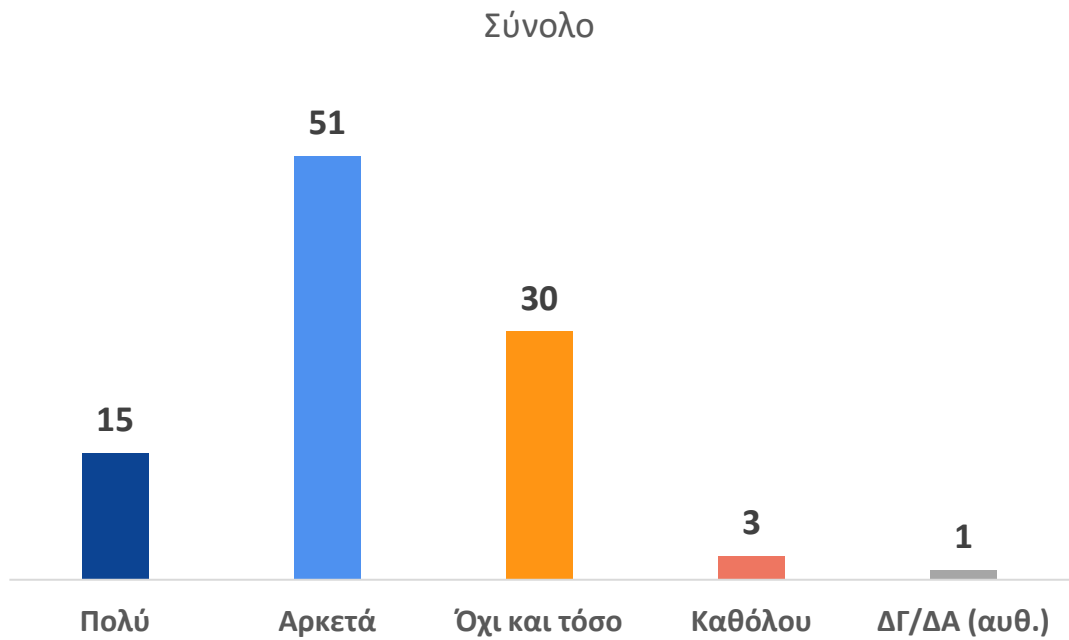
Και πόσο σοβαρή επίπτωση είχε/είχαν στην εταιρεία σας;

Βάση: το 30% που έχουν πέσει θύματα κυβερνοεπίθεσης/κυβερνοεγκλήματος



Η αίσθηση κινδύνου πάντως παραμένει, καθώς 2 στους 3 θεωρούν ότι είναι πολύ/αρκετά πιθανό να επαναληφθεί στο μέλλον κάποιου είδους κυβερνοεπίθεση

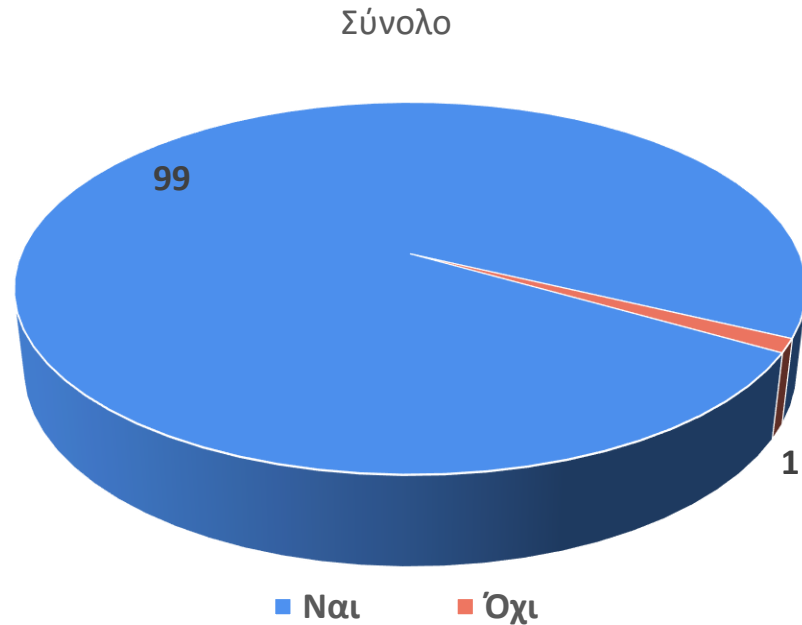
Και πόσο πιθανό θεωρείτε η εταιρεία σας να δεχτεί κυβερνοεπίθεση στο μέλλον;



		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Πολύ	15	14	16	15	18	15	22	9
Αρκετά	51	54	48	53	42	57	44	50
Όχι και τόσο	30	25	34	30	30	26	32	32
Καθόλου	3	5	1	2	6	*	2	7
ΔΓ/ΔΑ (αυθ.)	1	1	1	1	3	2	*	2

Όσον αφορά τους φορείς συνδρομής σε περίπτωση κυβερνοεπίθεσης, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος φαίνεται να είναι απολύτως οικεία στους ενδιαφερόμενους (όπως και στο γενικό κοινό)...

Έχετε ακούσει για την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος;

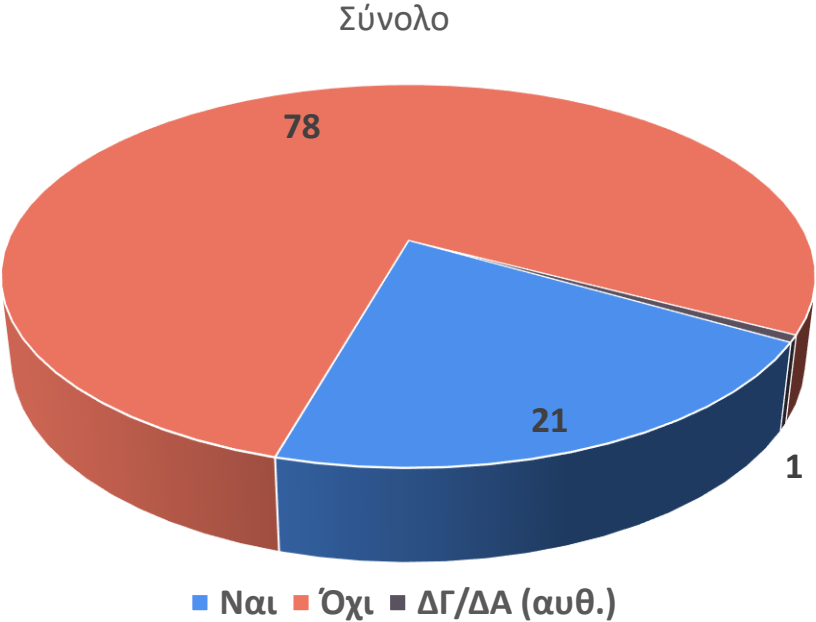


		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	99	99	99	99	100	100	98	98
Όχι	1	1	1	1	*	*	2	2

95% στην έρευνα γενικού κοινού έχουν ακούσει για την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (Απρίλιος 2023)

...και 1 στους 5 δηλώνει ότι έχει απευθυνθεί σε αυτήν για θέματα ασφάλειας στο διαδίκτυο (1 στους 10 στο γενικό κοινό)

Έχετε απευθυνθεί ποτέ σε αυτήν για θέματα ασφάλειας στο διαδίκτυο;

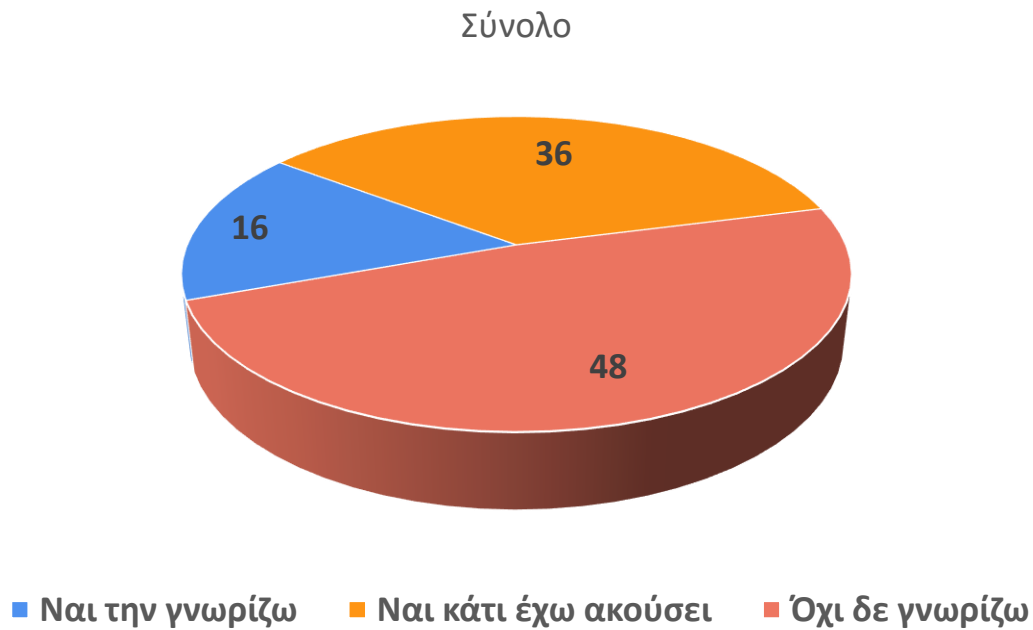


		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	21	17	25	20	24	15	16	32
Όχι	78	82	75	80	73	83	84	68
ΔΓ/ΔΑ (αυθ.)	1	1	*	*	3	2	*	*

9% στην έρευνα γενικού κοινού έχουν απευθυνθεί σε αυτήν για θέματα ασφάλειας στο διαδίκτυο (Απρίλιος 2023)

Συναφώς, 1 στους 2 δηλώνει ότι γνωρίζει ή έχει ακούσει για την σχεδιαζόμενη σύσταση Εθνικής Αρχής Κυβερνοασφάλειας

Γνωρίζετε ή έχετε ακούσει κάτι για την Εθνική Αρχή Κυβερνοασφάλειας που πρόκειται να συσταθεί με σκοπό την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα και την αποτελεσματική πρόληψη και διαχείριση των κυβερνοεπιθέσεων;



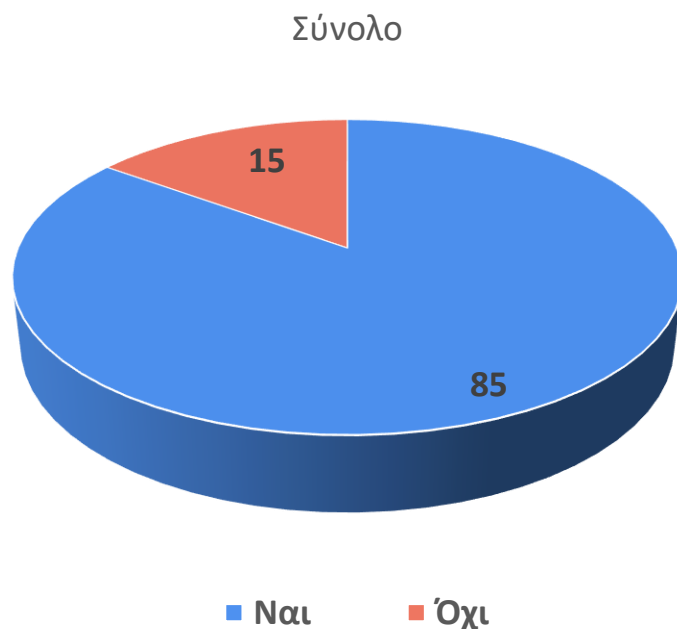
	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι την γνωρίζω	18	27	11	15	33	15	14	25
Ναι κάτι έχω ακούσει	34	27	40	36	24	39	32	30
Όχι δε γνωρίζω	48	47	49	49	42	46	54	45



Μέτρα Πρόληψης

Αναφορικά με τα μέτρα πρόληψης, στη μεγάλη τους πλειονότητα (85%) οι επιχειρήσεις δηλώνουν ότι παίρνουν μέτρα διαφύλαξης της ασφάλειας σε ηλεκτρονικές αγορές/συναλλαγές – και ακόμα περισσότερο οι μεγαλύτερες επιχειρήσεις (94%)

Η εταιρεία σας λαμβάνει κάποια μέτρα προκειμένου να διαφυλάξει την ασφάλειά της σε ηλεκτρονικές αγορές ή online τραπεζικές συναλλαγές;



	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	85	91	79	83	94	86	86	82
Όχι	15	9	21	17	6	14	14	18

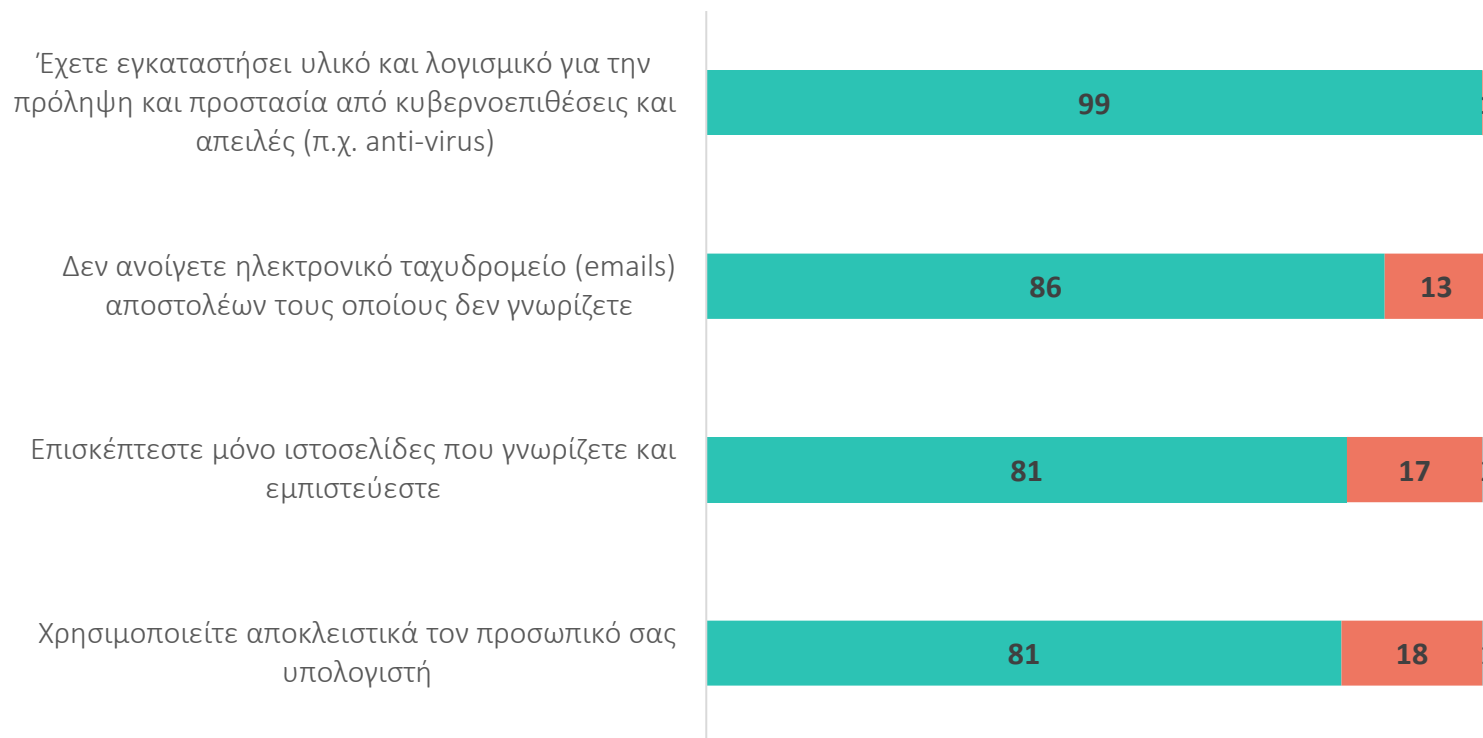
67% στην έρευνα γενικού κοινού λαμβάνουν κάποια μέτρα (Απρίλιος 2023)

Σε όλες σχεδόν τις περιπτώσεις αναφέρεται η εγκατάσταση λογισμικού προστασίας (ποσοστό μικρότερο στον γενικό πληθυσμό – 79%) και ακολούθως άλλα μέτρα που αφορούν κυρίως την ασφαλή πλοήγηση στο διαδίκτυο

Θα σας διαβάσω κάποια μέτρα διαφύλαξης της ασφάλειας συναλλαγών στο διαδίκτυο και θα ήθελα να μου πείτε για καθένα από αυτά εάν το κάνει η επιχείρησή σας και οι εργαζόμενοί της ή όχι;

Βάση: το 85% που λαμβάνουν κάποια μέτρα προκειμένου να διαφυλάξουν την ασφάλεια της εταιρείας σε ηλεκτρονικές αγορές ή online τραπεζικές συναλλαγές

■ Ναι ■ Όχι ■ ΔΓ/ΔΑ (αυθ.)



- ✓ Έχετε εγκαταστήσει υλικό και λογισμικό για την πρόληψη και προστασία από κυβερνοεπιθέσεις και απειλές (π.χ. anti-virus) 79%
- ✓ Δεν ανοίγετε ηλεκτρονικό ταχυδρομείο (emails) αποστολών τους οποίους δεν γνωρίζετε 88%
- ✓ Επισκέπτεστε μόνο ιστοσελίδες που γνωρίζετε και εμπιστεύεστε 90%
- ✓ Χρησιμοποιείτε αποκλειστικά τον προσωπικό σας υπολογιστή 84%

Έρευνα γενικού κοινού (Απρίλιος 2023)

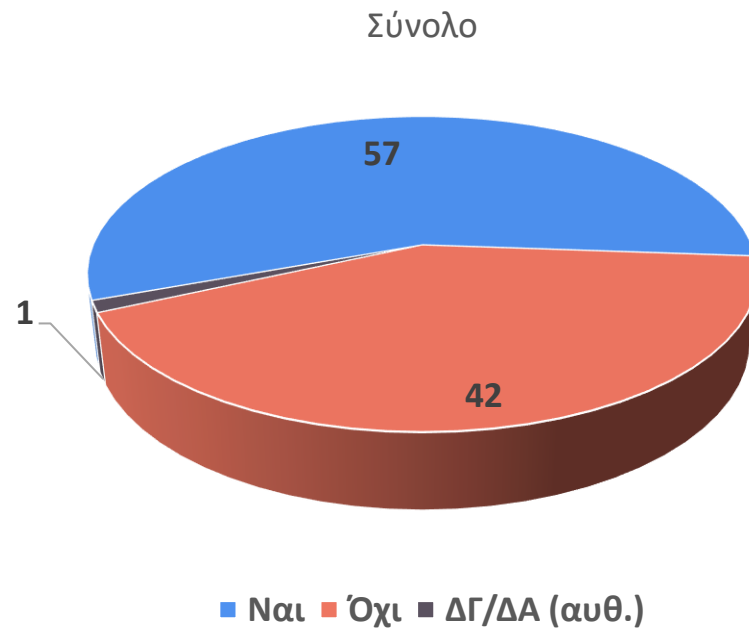
Μέτρα διαφύλαξης της ασφάλειας συναλλαγών στο διαδίκτυο

Βάση: το 85% που λαμβάνουν κάποια μέτρα προκειμένου να διαφυλάξουν την ασφάλεια της εταιρείας σε ηλεκτρονικές αγορές ή online τραπεζικές συναλλαγές

Ναι	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Έχετε εγκαταστήσει υλικό και λογισμικό για την πρόληψη και προστασία από κυβερνοεπιθέσεις και απειλές (π.χ. anti-virus)	99	99	99	98	100	98	100	98
Δεν ανοίγετε ηλεκτρονικό ταχυδρομείο (emails) αποστολών τους οποίους δεν γνωρίζετε	86	88	85	86	87	89	86	83
Επισκέπτεστε μόνο ιστοσελίδες που γνωρίζετε και εμπιστεύεστε	81	75	88	79	90	86	81	76
Χρησιμοποιείτε αποκλειστικά τον προσωπικό σας υπολογιστή	81	81	81	80	84	86	81	74

Πέρα από τα επιμέρους μέτρα, ωστόσο, είναι μικρότερο το ποσοστό των επιχειρήσεων που δηλώνει ότι διαθέτει σχέδιο πρόληψης/αντιμετώπισης κυβερνοεπιθέσεων (57%) – και σαφώς περισσότερο οι μεγαλύτερες επιχειρήσεις (85%)

Έχει η εταιρεία σας σχέδιο πρόληψης ή/και αντιμετώπισης κυβερνοεπιθέσεων;

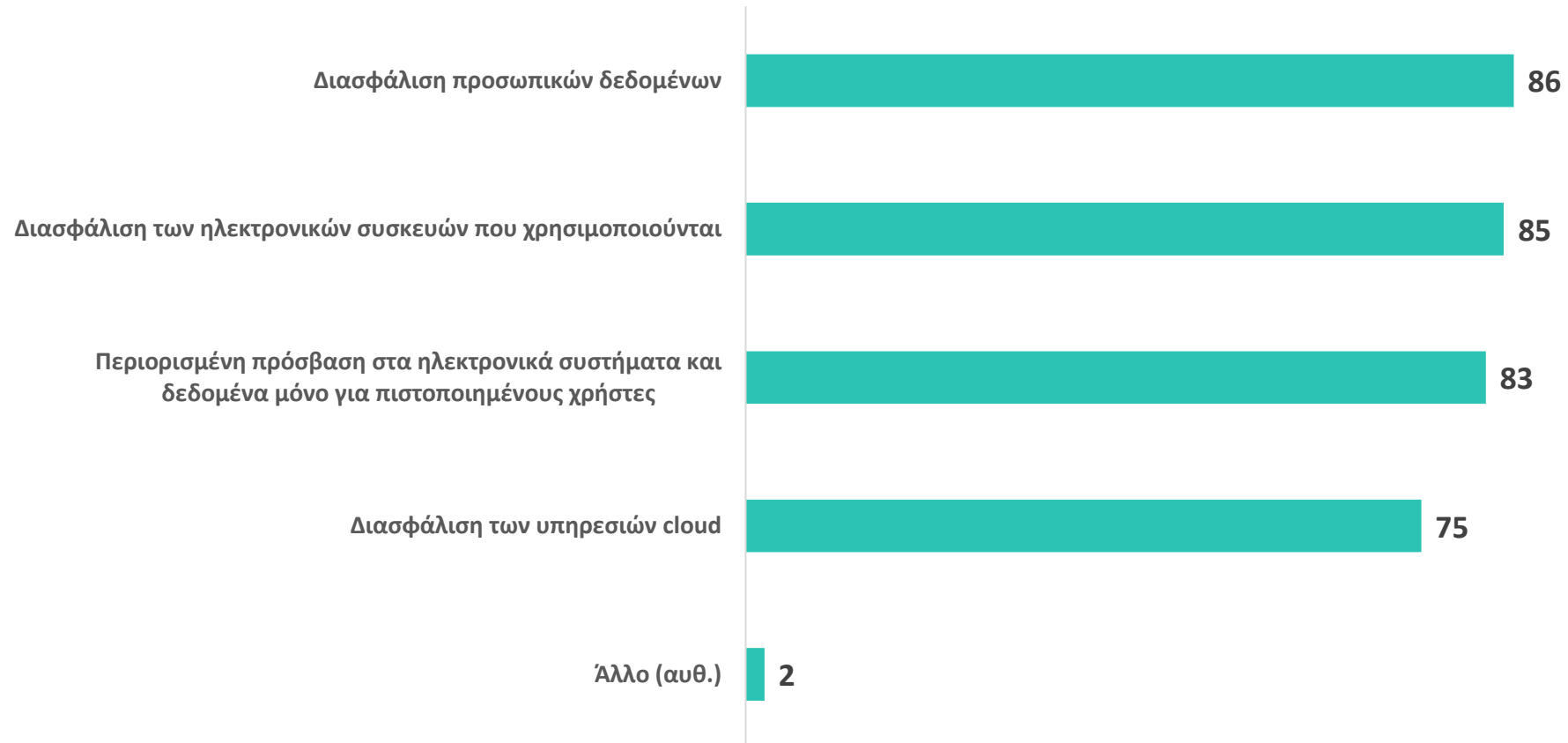


		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	57	68	47	50	85	55	54	61
Όχι	42	32	51	49	12	43	44	39
ΔΓ/ΔΑ (αυθ.)	1	*	2	1	3	2	2	*

Όταν υφίσταται σχέδιο πρόληψης/αντιμετώπισης, αυτό περιλαμβάνει κυρίως μέτρα διασφάλισης των προσωπικών δεδομένων και των χρησιμοποιούμενων συσκευών / ηλεκτρονικών συστημάτων

Και ποιες από τις παρακάτω ενέργειες περιλαμβάνει; (Πολλαπλές αναφορές)

Βάση: το 57% που έχει σχέδιο πρόληψης ή/και αντιμετώπισης κυβερνοεπιθέσεων



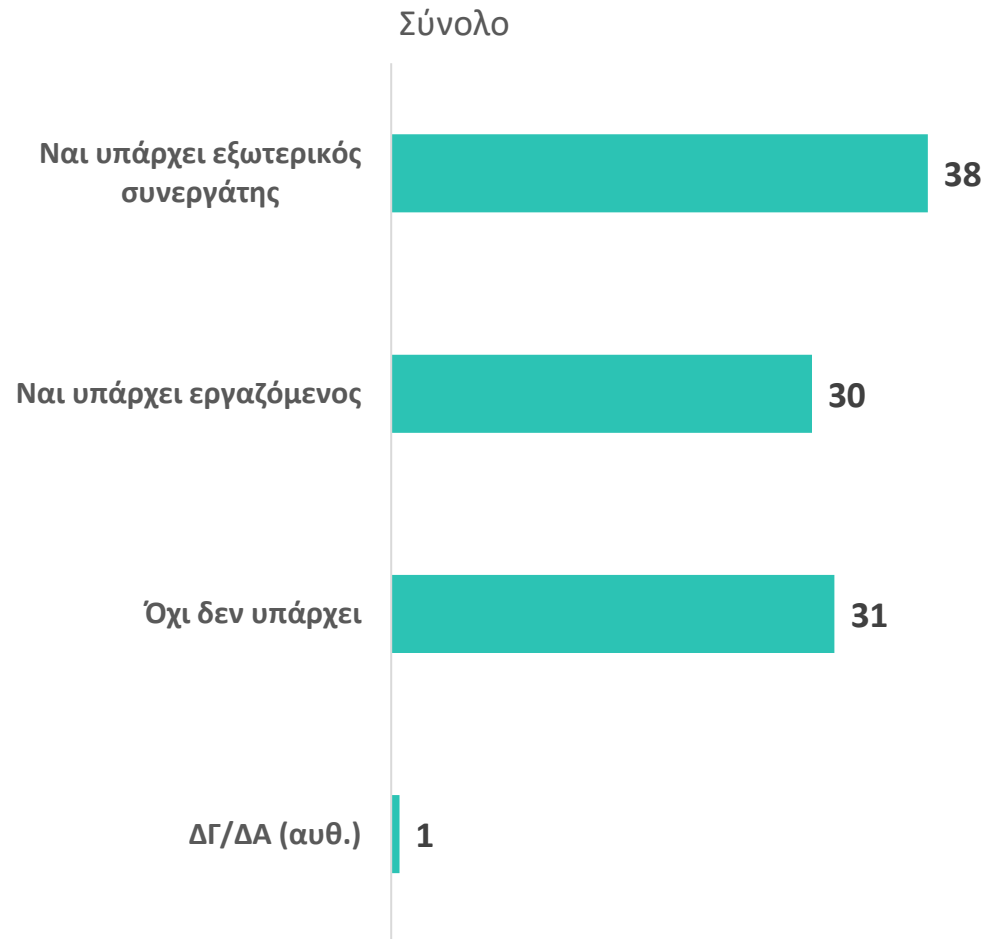
Ενέργειες πρόληψης ή/και αντιμετώπισης κυβερνοεπιθέσεων

Βάση: το 57% που έχει σχέδιο πρόληψης ή/και αντιμετώπισης κυβερνοεπιθέσεων

	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Διασφάλιση προσωπικών δεδομένων	86	85	86	81	96	81	82	94
Διασφάλιση των ηλεκτρονικών συσκευών που χρησιμοποιούνται	85	85	84	84	86	89	78	85
Περιορισμένη πρόσβαση στα ηλεκτρονικά συστήματα και δεδομένα μόνο για πιστοποιημένους χρήστες	83	82	84	81	86	81	82	85
Διασφάλιση των υπηρεσιών cloud	75	82	67	68	93	69	78	79
Άλλο (αυθ.)	2	2	2	3	*	*	4	3

Σε παραπάνω από το 1/3 των περιπτώσεων η σχετική ευθύνη έχει ανατεθεί σε εξωτερικό συνεργάτη (38%), σε λιγότερο από το 1/3 σε εργαζόμενο της επιχείρησης (30% - ιδίως σε μεγαλύτερες επιχειρήσεις) και σε άλλο 1/3 δεν έχει ανατεθεί σε συγκεκριμένο πρόσωπο

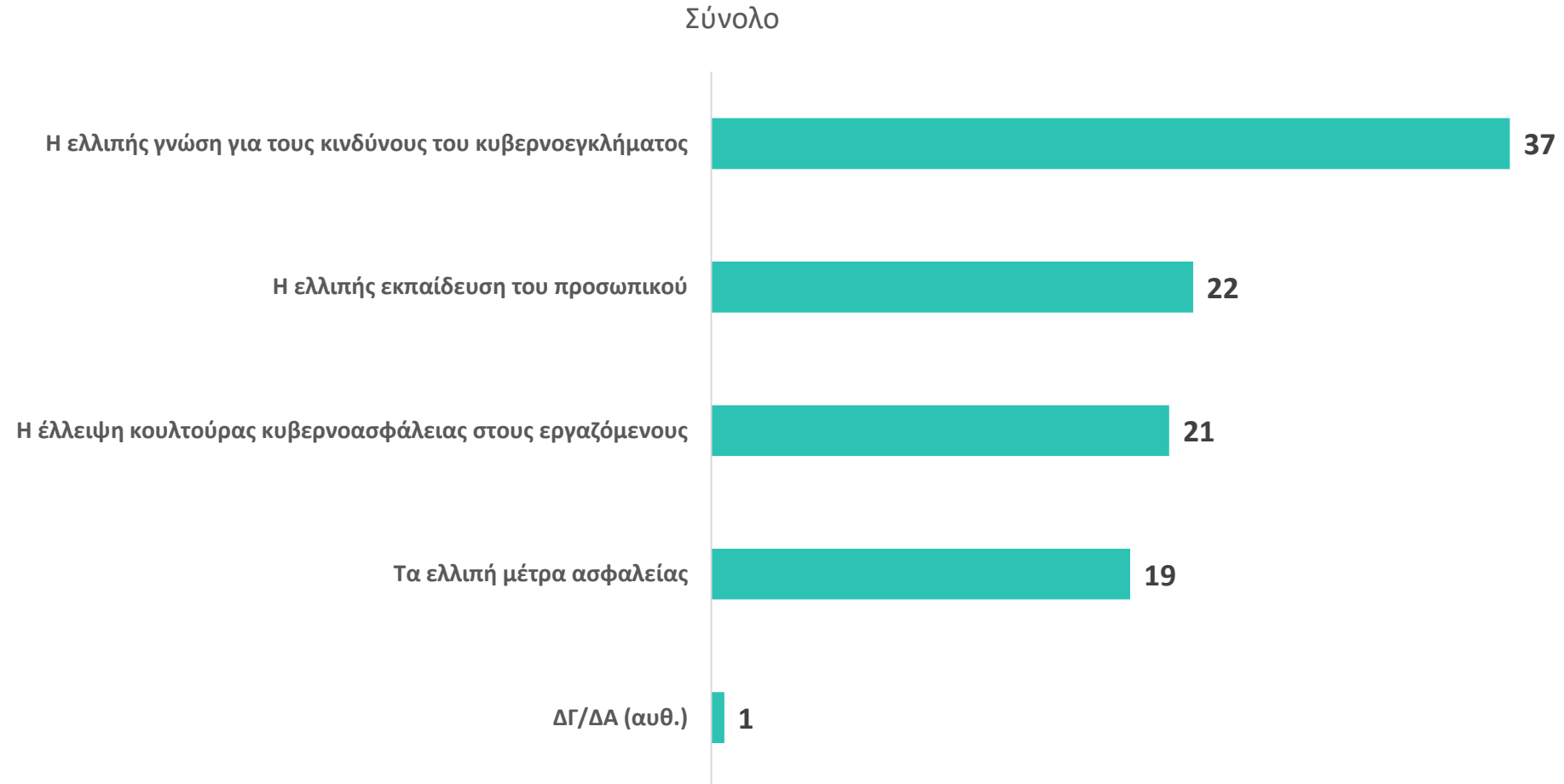
Έχει η εταιρεία σας κάποιον εργαζόμενο ή εξωτερικό συνεργάτη που να έχει επιφορτιστεί με την ευθύνη για την πρόληψη ή και αντιμετώπιση Κυβερνοεπιθέσεων;



	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι υπάρχει εξωτερικός συνεργάτης	38	39	37	43	18	37	50	29
Ναι υπάρχει εργαζόμενος	30	33	27	22	64	28	32	30
Όχι δεν υπάρχει	31	28	35	35	18	34	18	41
ΔΓ/ΔΑ (αυθ.)	1	*	1	1	*	2	*	*

Το αντιλαμβανόμενο ως πιο ευάλωτο σημείο των εταιρειών εν γένει σε θέματα κυβερνοασφάλειας είναι πρωτίστως η ελλιπής γνώση των συναφών κινδύνων, αλλά και η έλλειψη εκπαίδευσης/κουλτούρας, και σχετικά λιγότερο τα ελλιπή μέτρα ασφαλείας...

Ποιο είναι κατά τη γνώμη σας το πιο ευάλωτο σημείο των εταιρειών στη χώρα μας ως προς την πρόληψη και αντιμετώπιση κυβερνοεπιθέσεων;



Το πιο ευάλωτο σημείο των εταιρειών στη χώρα μας ως προς την πρόληψη και αντιμετώπιση κυβερνοεπιθέσεων

	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Η ελλιπής γνώση για τους κινδύνους του κυβερνοεγκλήματος	37	37	37	41	21	37	34	39
Η ελλιπής εκπαίδευση του προσωπικού	22	17	27	17	46	31	22	13
Η έλλειψη κουλτούρας κυβερνοασφάλειας στους εργαζόμενους	21	24	19	23	15	11	28	27
Τα ελλιπή μέτρα ασφαλείας	19	22	17	20	18	22	14	21
ΔΓ/ΔΑ (αυθ.)	1	1	*	1	*	*	2	*

...ωστόσο, 7 στις 10 επιχειρήσεις δεν έχουν οργανώσει τον τελευταίο χρόνο κάποια εκπαίδευση του προσωπικού τους σε θέματα κυβερνοασφάλειας – ενώ σχετικά σεμινάρια οργανώνουν περισσότερο οι μεγαλύτερες επιχειρήσεις

Τον τελευταίο χρόνο η εταιρεία σας έχει οργανώσει κάποια εκπαίδευση του προσωπικού ως προς την πρόληψη και αντιμετώπιση κυβερνοεπιθέσεων; (Πολλαπλές αναφορές)

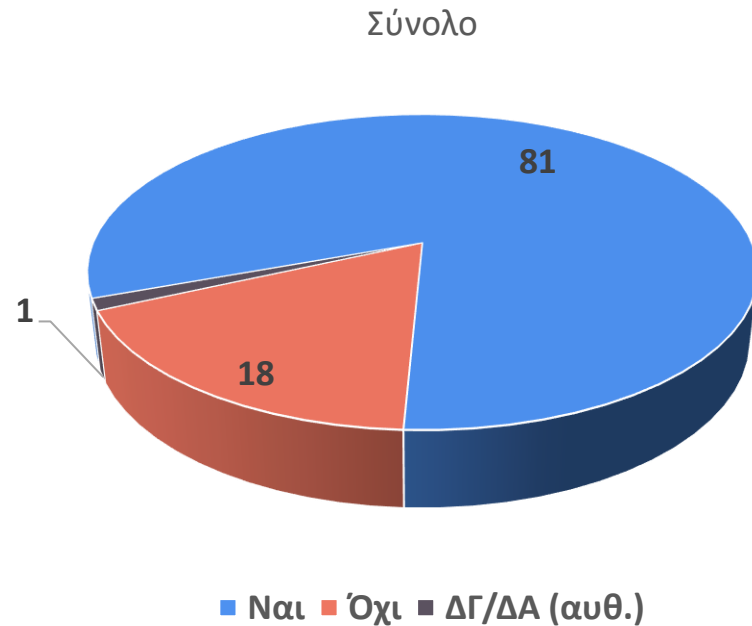


Εκπαίδευση του προσωπικού ως προς την πρόληψη και αντιμετώπιση κυβερνοεπιθέσεων

	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι, σεμινάριο στον χώρο εργασίας ή ηλεκτρονικά με οργάνωση της εταιρείας	23	25	21	17	46	23	8	36
Ναι, σεμινάρια στον χώρο εργασίας ή ηλεκτρονικά σε συνεργασία με κάποιον φορέα	10	10	10	9	15	11	6	13
Ναι, εκπαιδευτικά σενάρια για τον έλεγχο της ετοιμότητας των υπαλλήλων (security awareness scenarios)	9	13	5	8	12	8	8	11
Ναι, πιστοποιήσεις υπαλλήλων σε θέματα κυβερνοασφάλειας	7	13	2	5	15	5	4	13
Όχι, δεν έχει οργανώσει καμία εκπαίδευση	69	63	74	75	42	71	80	57

Ανεξάρτητα από την ύπαρξη σχεδίου πρόληψης/αντιμετώπισης κυβερνοεπιθέσεων, η μεγάλη πλειονότητα των επιχειρήσεων (81%) δηλώνουν ότι διαθέτουν πολιτική για την εφαρμογή του GDPR – και πάλι περισσότεροι οι μεγαλύτερες επιχειρήσεις

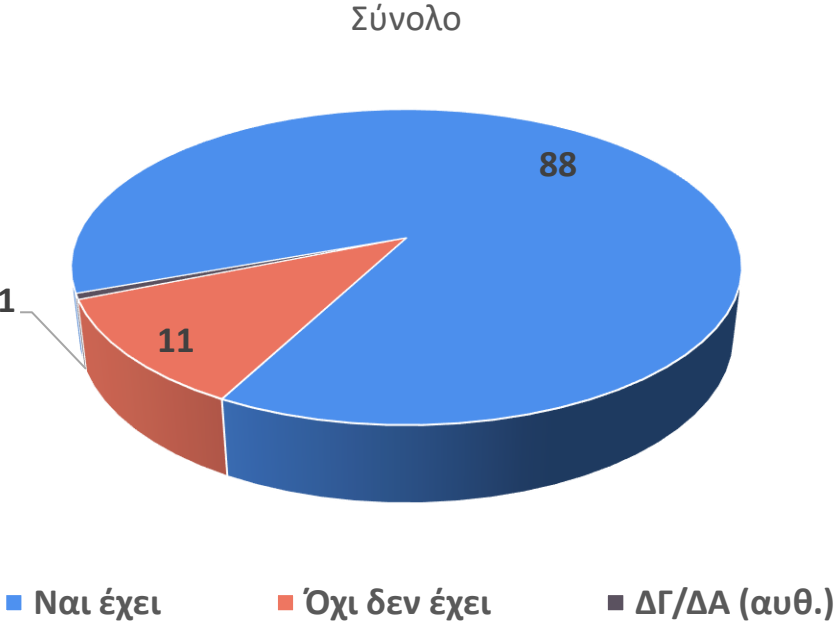
Έχει η εταιρεία σας πολιτική για την ορθή εφαρμογή του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR);



		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	81	84	79	78	94	71	90	86
Όχι	18	17	19	20	6	28	10	13
ΔΓ/ΔΑ (αυθ.)	1	*	2	1	*	2	*	2

Ενώ συνολικά, μικρότερες και μεγαλύτερες επιχειρήσεις θεωρούν ότι η θωράκιση μιας εταιρείας σε θέματα κυβερνοασφάλειας εν γένει έχει θετική επίδραση στους πελάτες και στη φήμη της

Πιστεύετε ότι η θωράκιση μιας εταιρείας σε θέματα κυβερνοασφάλειας έχει θετικό αντίκτυπο στους πελάτες της και στη φήμη της στην αγορά;



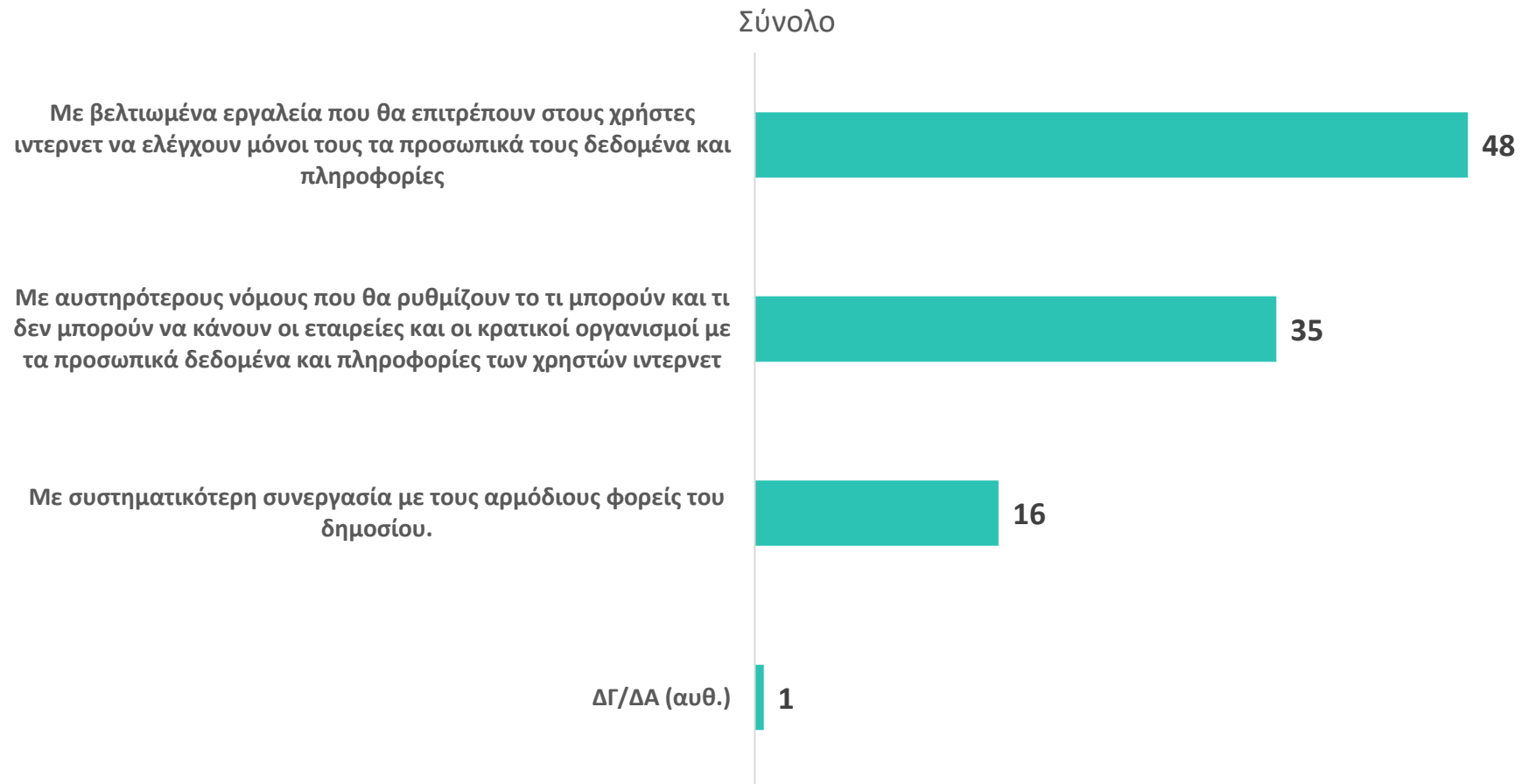
		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι έχει	88	87	89	88	88	88	86	91
Όχι δεν έχει	11	11	11	11	12	12	14	7
ΔΓ/ΔΑ (αυθ.)	1	1	*	1	*	*	*	2



Πολιτικές Προστασίας Προσωπικών Δεδομένων & Πληροφοριών

Στο σκέλος των μέτρων πολιτικής, η σχετική πλειονότητα (48%) φαίνεται να προκρίνει τα βελτιωμένα εργαλεία για εξατομικευμένη προστασία των χρηστών internet, και λιγότερο υιοθετείται μια προσέγγιση θεσμικής-νομοθετικής «ρύθμισης» (που προτιμούν όμως οι μεγαλύτερες επιχειρήσεις)

Ποιος από τους παρακάτω θα λέγατε ότι είναι περισσότερο αποτελεσματικός τρόπος να προστατεύονται τα προσωπικά δεδομένα και πληροφορίες;

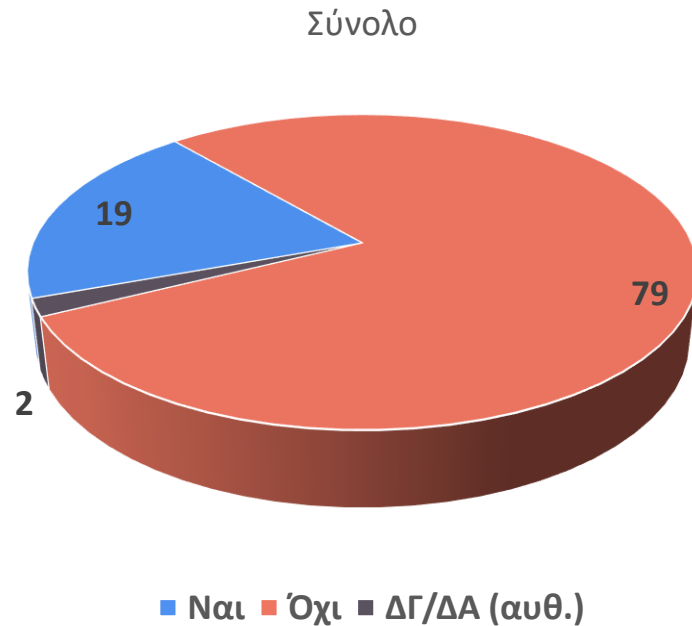


Περισσότερο αποτελεσματικός τρόπος προστασίας προσωπικών δεδομένων και πληροφοριών

		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Με βελτιωμένα εργαλεία που θα επιτρέπουν στους χρήστες ιντερνετ να ελέγχουν μόνοι τους τα προσωπικά τους δεδομένα και πληροφορίες	48	46	50	49	42	52	42	48
Με αυστηρότερους νόμους που θα ρυθμίζουν το τι μπορούν και τι δεν μπορούν να κάνουν οι εταιρείες και οι κρατικοί οργανισμοί με τα προσωπικά δεδομένα και πληροφορίες των χρηστών ιντερνετ	35	33	37	31	52	34	42	30
Με συστηματικότερη συνεργασία με τους αρμόδιους φορείς του δημοσίου.	16	20	13	19	6	14	14	21
ΔΓ/ΔΑ (αυθ.)	1	1	*	1	*	*	2	*

Ταυτόχρονα, μόνο ένα 19% των εν λόγω επιχειρήσεων έχει αξιοποιήσει εθνική ή ευρωπαϊκή χρηματοδότηση για τεχνολογική αναβάθμιση που αφορά την κυβερνοασφάλεια...

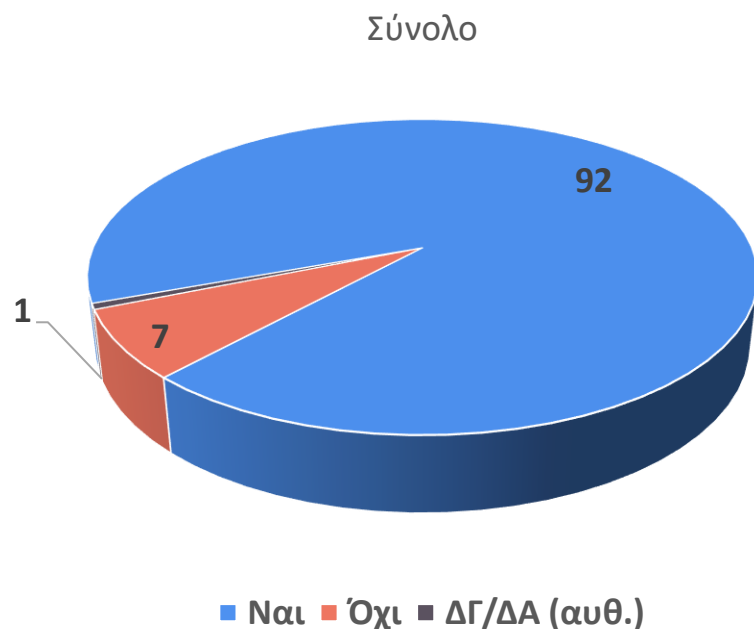
Έχει αξιοποιήσει ποτέ η εταιρεία σας κάποια κρατική ή ευρωπαϊκή επιδότηση για τεχνολογική αναβάθμιση που αφορά την κυβερνοασφάλεια;



	Σύνολο	Περιοχή		Αριθμός εργαζομένων		Κλάδος		
		Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	19	15	23	20	18	19	18	21
Όχι	79	84	75	80	76	82	78	77
ΔΓ/ΔΑ (αυθ.)	2	1	2	1	6	*	4	2

...ενώ η συντριπτική πλειονότητα τάσσεται υπέρ της ύπαρξης περισσότερων σχετικών κινήτρων

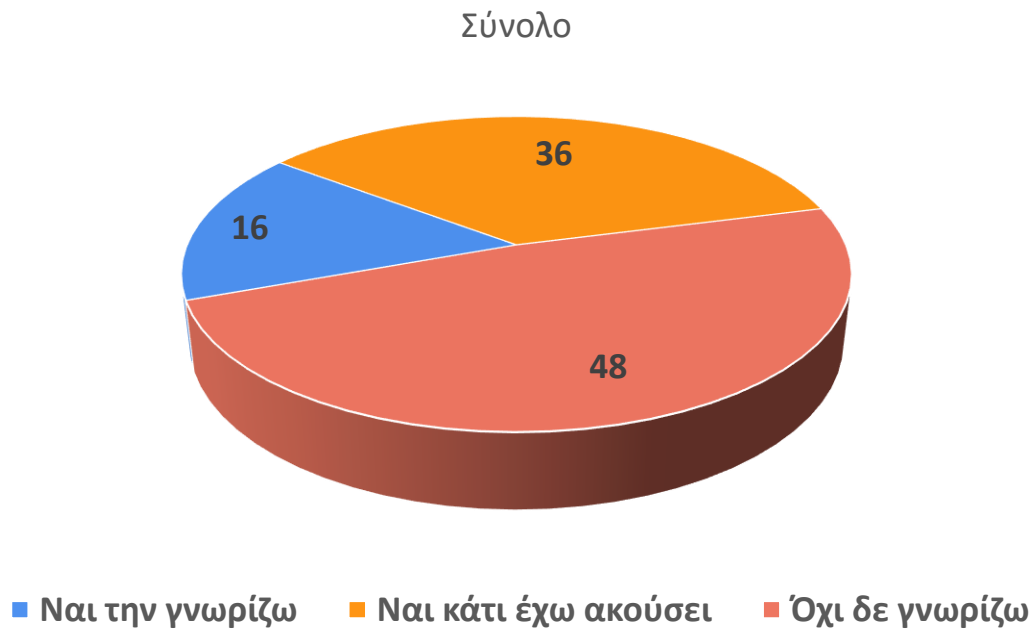
Πιστεύετε ότι θα έπρεπε το ελληνικό κράτος να δίνει περισσότερα κίνητρα στις εταιρείες ώστε να επενδύσουν στην κυβερνοασφάλεια;



		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι	92	91	94	91	97	94	88	95
Όχι	7	9	5	8	3	5	12	5
ΔΓ/ΔΑ (αυθ.)	1	*	1	1	*	2	*	*

Τέλος, όσον αφορά το θεσμικό πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας, αυτό είναι οικείο στο ήμισυ των εν λόγω επιχειρήσεων (52% το γνωρίζουν ή το έχουν ακουστά)...

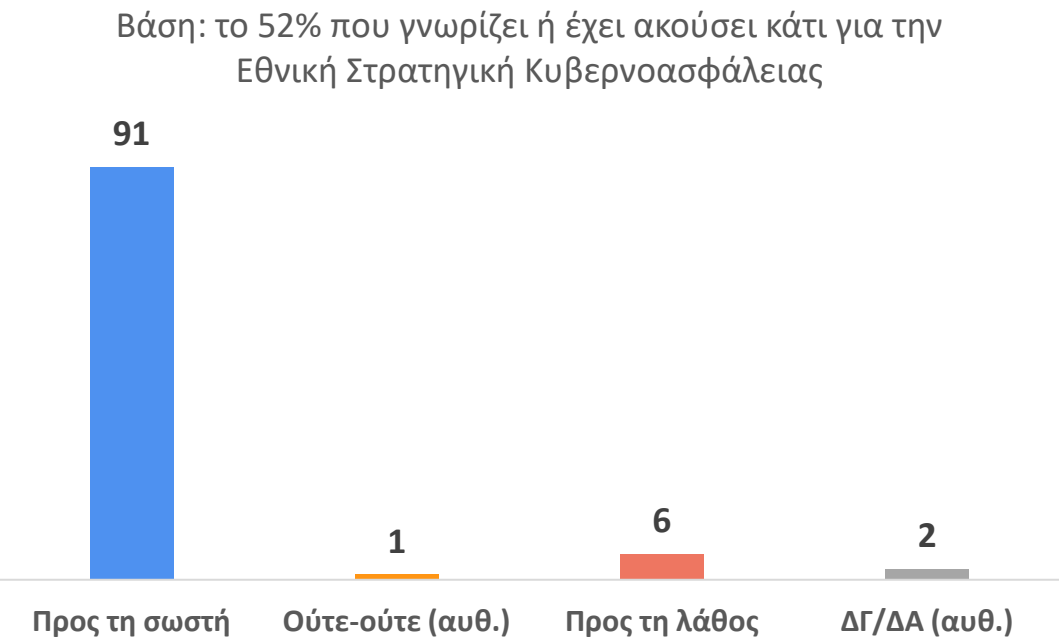
Γνωρίζετε ή έχετε ακούσει κάτι για την Εθνική Στρατηγική Κυβερνοασφάλειας;



		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Ναι την γνωρίζω	16	24	9	12	33	15	14	18
Ναι κάτι έχω ακούσει	36	29	41	35	39	42	28	36
Όχι δε γνωρίζω	48	47	50	54	27	43	58	46

...και εφόσον το γνωρίζουν, θεωρούν ότι κινείται σε σωστή κατεύθυνση

Και τι άποψη έχετε για τους στόχους, τις προτεραιότητες και τα μέτρα πολιτικής που περιλαμβάνει; Είναι προς τη σωστή ή προς τη λάθος κατεύθυνση;



		Περιοχή		Αριθμός εργαζομένων		Κλάδος		
	Σύνολο	Αττική	Λοιπές περιφέρειες	10-50 εργαζόμενοι	Πάνω από 50 εργαζόμενοι	Βιομηχανία	Εμπόριο	Υπηρεσίες
Προς τη σωστή	91	95	87	92	88	92	95	87
Ούτε-ούτε (αυθ.)	1	*	2	2	*	*	*	3
Προς τη λάθος	6	5	7	3	12	5	5	7
ΔΓ/ΔΑ (αυθ.)	2	*	4	3	*	3	*	3



Σύνοψη Αποτελεσμάτων

Σύνοψη Αποτελεσμάτων I

Η συνολική εικόνα που αποτυπώνεται στην παρούσα έρευνα είναι αυτή μιας αίσθησης εντεινόμενων απειλών στον χώρο του διαδικτύου, σε συνδυασμό και με τη διευρυνόμενη χρήση του διαδικτύου από τις επιχειρήσεις. Το **82%** θεωρεί ότι οι κίνδυνοι κυβερνοασφάλειας είναι μεγαλύτεροι σήμερα απ' ό,τι πριν 5 χρόνια, και ένα **83%** θεωρεί ότι η χρήση του διαδικτύου εγκυμονεί κινδύνους για τις επιχειρήσεις (**94%** στις μεγαλύτερες επιχειρήσεις) – ιδίως όσον αφορά το κακόβουλο λογισμικό και την εξαπάτηση σε αγορές/συναλλαγές.

Οι επιχειρήσεις παρέχουν ή/και χρησιμοποιούν κατά κανόνα περισσότερο online υπηρεσίες απ' ό,τι το γενικό κοινό (**98%** email έναντι **82%** στο γενικό κοινό, **96%** ψηφιακή πρόσβαση σε δημόσιες υπηρεσίες έναντι **75%**, **94%** online τραπεζικές συναλλαγές έναντι **71%**). Παράλληλα, η πανδημία είχε ως αποτέλεσμα την περαιτέρω επέκταση της ψηφιοποίησης των επιχειρήσεων, πράγμα που θεωρείται όμως ότι αύξησε και τους κινδύνους κυβερνοασφάλειας, ειδικά για τις μικρότερες επιχειρήσεις.

Από την άλλη, η ασφάλεια των προσωπικών δεδομένων δεν φαίνεται να αξιολογείται ως πρωτεύων κίνδυνος, καθώς για το **41%** είναι περισσότερο ασφαλή απ' ό,τι πριν 5 χρόνια (**58%** στις μεγαλύτερες επιχειρήσεις), ενώ ο κίνδυνος κατάχρησης προσωπικών δεδομένων αξιολογείται ως σημαντικός από το **25%** των ερωτώμενων, έναντι **32%** στο γενικό κοινό.

Σύνοψη Αποτελεσμάτων II

Σχεδόν 1 στις 3 επιχειρήσεις αναφέρει περιστατικά κυβερνοεπίθεσης/κυβερνοεγκλήματος (**30%**, έναντι **11%** στο γενικό κοινό), που αφορούν κατά κύριο λόγο παραπλανητικά emails (**76%**, λιγότερο σύνηθες στο γενικό κοινό: **62%**) αλλά και κακόβουλο λογισμικό (**57%**, περισσότερο σύνηθες στο γενικό κοινό: **65%**).

Η επίπτωση αυτών των περιστατικών στις επιχειρήσεις αξιολογείται ως μετρίως σοβαρή (**39%** τη θεωρούν πολύ/αρκετά σοβαρή αλλά **51%** όχι τόσο σοβαρή έως ασήμαντη). Ωστόσο, η πλειονότητα θεωρεί πολύ/αρκετά πιθανό το ενδεχόμενο να επαναληφθεί κάποιο παρόμοιο περιστατικό στο μέλλον. Σε αυτό το πλαίσιο, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει εμπεδώσει την παρουσία της ως φορέας συνδρομής σε θέματα κυβερνοασφάλειας, με το **21%** των ερωτώμενων να δηλώνουν ότι έχουν απευθυνθεί σε αυτήν για θέματα ασφάλειας στο διαδίκτυο (έναντι **9%** στο γενικό κοινό).

Πάντως, μόλις **2%** αναφέρουν ότι έχουν υπάρξει περιπτώσεις παραβίασης προσωπικών δεδομένων πελατών, και άλλο ένα **2%** ότι πελάτες έχουν διαμαρτυρηθεί για θέμα προστασίας προσωπικών δεδομένων – στοιχείο που συντείνει στην προαναφερθείσα αίσθηση μικρότερου αντιλαμβανόμενου κινδύνου όσον αφορά την προστασία προσωπικών δεδομένων.

Σύνοψη Αποτελεσμάτων III

Όσον αφορά τα μέτρα πρόληψης και αντιμετώπισης κυβερνοεπιθέσεων, διαφαίνεται ένας διαχωρισμός ανάμεσα στις μικρότερες και τις μεγαλύτερες επιχειρήσεις.

Πράγματι, ενώ η μεγάλη πλειονότητα δηλώνει ότι γενικά λαμβάνει μέτρα διαφύλαξης της ασφάλειας σε ηλεκτρονικές αγορές/συναλλαγές (**85%**, αρκετά περισσότερο από το γενικό κοινό: **67%**), αυτό αφορά σε μεγαλύτερο βαθμό τις επιχειρήσεις άνω των 50 εργαζομένων (**94%**). Τα μέτρα διαφύλαξης της ασφάλειας συναλλαγών αφορούν σε κάθε περίπτωση την εγκατάσταση λογισμικού ενάντια στις κυβερνοεπιθέσεις και άλλες απειλές (**99%**, έναντι **79%** στο γενικό κοινό), αλλά και μέτρα ασφαλέστερης πλοήγησης, όπως το μη άνοιγμα emails αγνώστου αποστολέα ή η αποφυγή ιστοσελίδων μη εμπιστοσύνης.

Από εκεί και πέρα όμως, μόνο λίγο περισσότερες από τις μισές επιχειρήσεις διαθέτουν ένα ευρύτερο σχέδιο πρόληψης/αντιμετώπισης κυβερνοεπιθέσεων (**57%**), και μάλιστα πολύ περισσότερο οι επιχειρήσεις άνω των 50 εργαζομένων (**85%**) απ' ό,τι οι επιχειρήσεις 10-50 εργαζομένων (**50%**) – παρ' όλο που υπάρχει ευρεία συναίνεση ότι η θωράκιση σε θέματα κυβερνοασφάλειας ενισχύει την εικόνα και τη φήμη της επιχείρησης.

Σύνοψη Αποτελεσμάτων IV

Το διαθέσιμο σχέδιο αφορά πρωτίστως τη διασφάλιση των προσωπικών δεδομένων (**86%**, αλλά **96%** στις μεγαλύτερες επιχειρήσεις), και κατόπιν τη διασφάλιση των χρησιμοποιούμενων συσκευών (**85%**), την περιορισμένη πρόσβαση στα ηλεκτρονικά συστήματα και δεδομένα (**83%**), καθώς και τη διασφάλιση των υπηρεσιών cloud (**75%**, και πάλι περισσότερο στις μεγαλύτερες επιχειρήσεις: **93%**).

Η ανάθεση της ευθύνης για την πρόληψη/αντιμετώπιση κυβερνοεπιθέσεων ποικίλλει: **38%** των επιχειρήσεων την έχουν αναθέσει σε εξωτερικό συνεργάτη, **30%** σε εργαζόμενο της επιχείρησης (αλλά **64%** σε μεγαλύτερες επιχειρήσεις, που διαθέτουν και περισσότερους εργαζόμενους), ενώ άλλο ένα **31%** δεν την έχει αναθέσει σε συγκεκριμένο πρόσωπο.

Πάντως, όσον αφορά τα προσωπικά δεδομένα και το GDPR, όπου υφίσταται σχετικό θεσμικό πλαίσιο, η μεγάλη πλειονότητα (**81%**, και **94%** στις μεγαλύτερες επιχειρήσεις) δηλώνει ότι διαθέτει πολιτική ορθής εφαρμογής.

Σύνοψη Αποτελεσμάτων V

Αξίζει να σημειωθεί, επίσης, ότι ενώ τα αντιλαμβανόμενα ευάλωτα σημεία των επιχειρήσεων γενικά σε θέματα κυβερνοεπιθέσεων δεν είναι τόσο τα ελλιπή μέτρα ασφαλείας (**19%**) όσο η γνώση των κινδύνων και η συναφής εκπαίδευση/κουλτούρα του προσωπικού (**37%** και **22%/21%** αντίστοιχα), ωστόσο 7 στις 10 εν λόγω επιχειρήσεις δεν έχουν διοργανώσει τον τελευταίο χρόνο κάποια σχετική εκπαίδευση του προσωπικού τους. Και πάλι, πάντως, οι μεγαλύτερες επιχειρήσεις είναι αυτές που σε μεγαλύτερο βαθμό διοργανώνουν σχετικά σεμινάρια εκπαίδευσης, είτε αυτοτελώς είτε σε συνεργασία με κάποιον φορέα.

Τέλος, όσον αφορά τα μέτρα πολιτικής, φαίνεται να προκρίνονται σχετικά τα εξατομικευμένα εργαλεία που βοηθούν τους χρήστες του διαδικτύου να προστατευθούν μόνοι τους (**48%**) παρά τα ρυθμιστικά-θεσμικά μέτρα βάσει νομοθεσίας (**35%** - τα οποία όμως προκρίνονται από τις μεγαλύτερες επιχειρήσεις: **52%**).

Ωστόσο, δεδομένου και ότι μόνο το **19%** δηλώνουν ότι έχουν αξιοποιήσει εθνική/ευρωπαϊκή χρηματοδότηση για τεχνολογική αναβάθμιση στο πεδίο της κυβερνοασφάλειας, ομόφωνα σχεδόν υποστηρίζεται η ανάγκη για περισσότερα κίνητρα και χρηματοδοτήσεις προς τις επιχειρήσεις.

Το δε θεσμικό πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας αξιολογείται θετικά, αλλά μόνο για το ήμισυ των εν λόγω επιχειρήσεων που το έχουν υπόψιν.

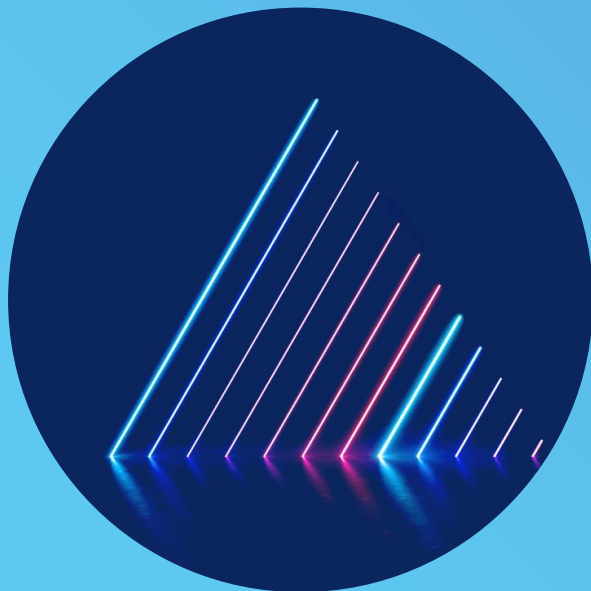
+



○

Πανελλαδική Έρευνα B2B για την Ασφάλεια στο Διαδίκτυο

Δεκέμβριος 2023



•



METRON ANALYSIS

6 Sinopis Str., 115 27 Athens

T: +30 210 745 1800, F: +30 210 745 1888

W: www.metronanalysis.gr