pylones*

THE STATE OF CYBER SECURITY 2025

Insights & Trends shaping Cybersecurity in Greece

About “The State of Cybersecurity”

Για **έκτη συνεχή χρονιά**, η **Pylones Hellas** υλοποιεί την ετήσια έρευνα **“The State of Cybersecurity”**, έναν θεσμό που καταγράφει τις τάσεις, τις προκλήσεις και τις στρατηγικές προστασίας των οργανισμών στην Ελλάδα.

Από το 2020, η έρευνα στοχεύει στην αποτύπωση της πραγματικής κατάστασης της κυβερνοασφάλειας, παρέχοντας αξιόπιστα δεδομένα για τον βαθμό ετοιμότητας, τις τεχνολογικές προτεραιότητες και τη στρατηγική των επιχειρήσεων απέναντι σε κυβερνοαπειλές.

Με τη συμμετοχή επαγγελματιών από τον δημόσιο και ιδιωτικό τομέα, καθώς και την υποστήριξη κορυφαίων τεχνολογικών και ακαδημαϊκών φορέων, το “The State of Cybersecurity” αποτελεί **πολύτιμο εργαλείο κατανόησης και ανάλυσης** της κυβερνοασφάλειας στην ελληνική αγορά.

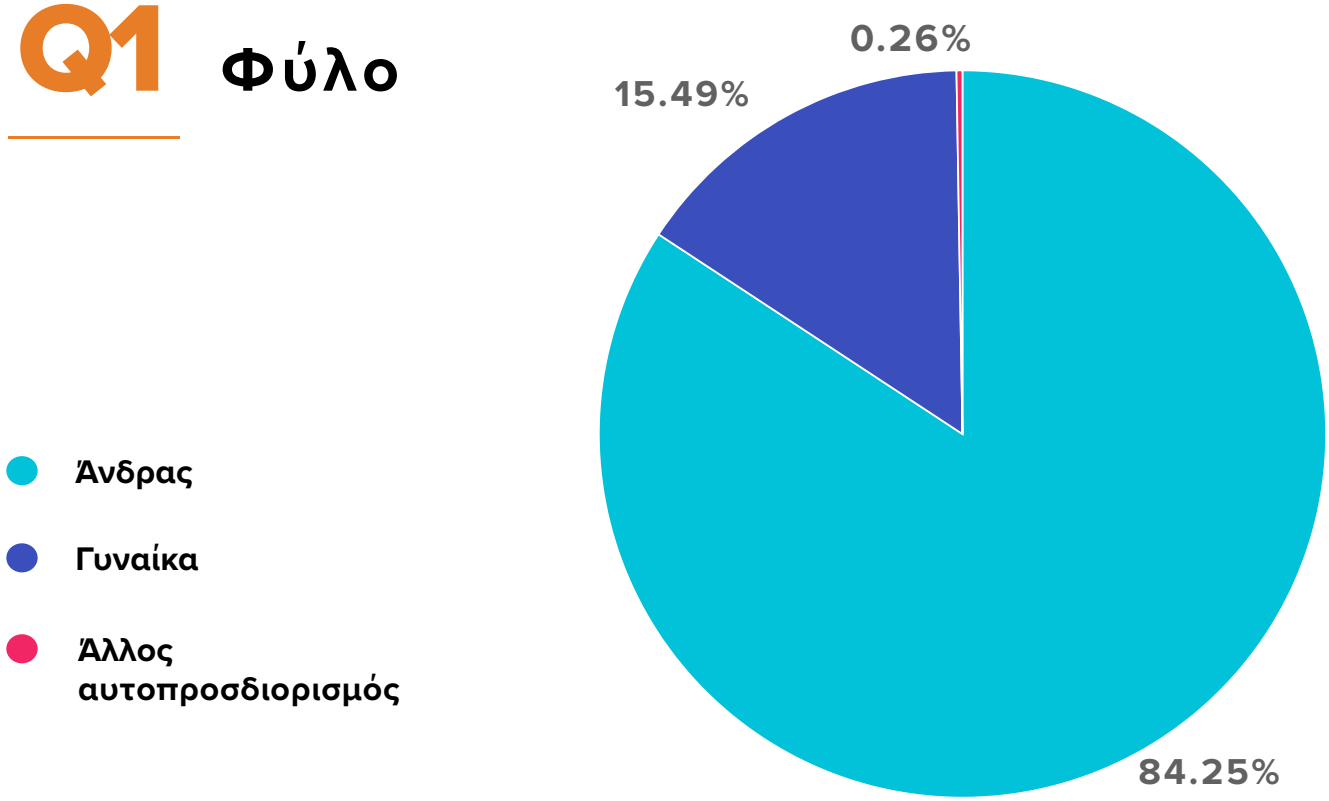
Γενικά στοιχεία

Response Statistics

The State of Cybersecurity 2025

2950	Survey Visits
381	Total Responses
247	Completed Responses
134	Partial Responses
0	Disqualified Responses
0	Over Quota Responses

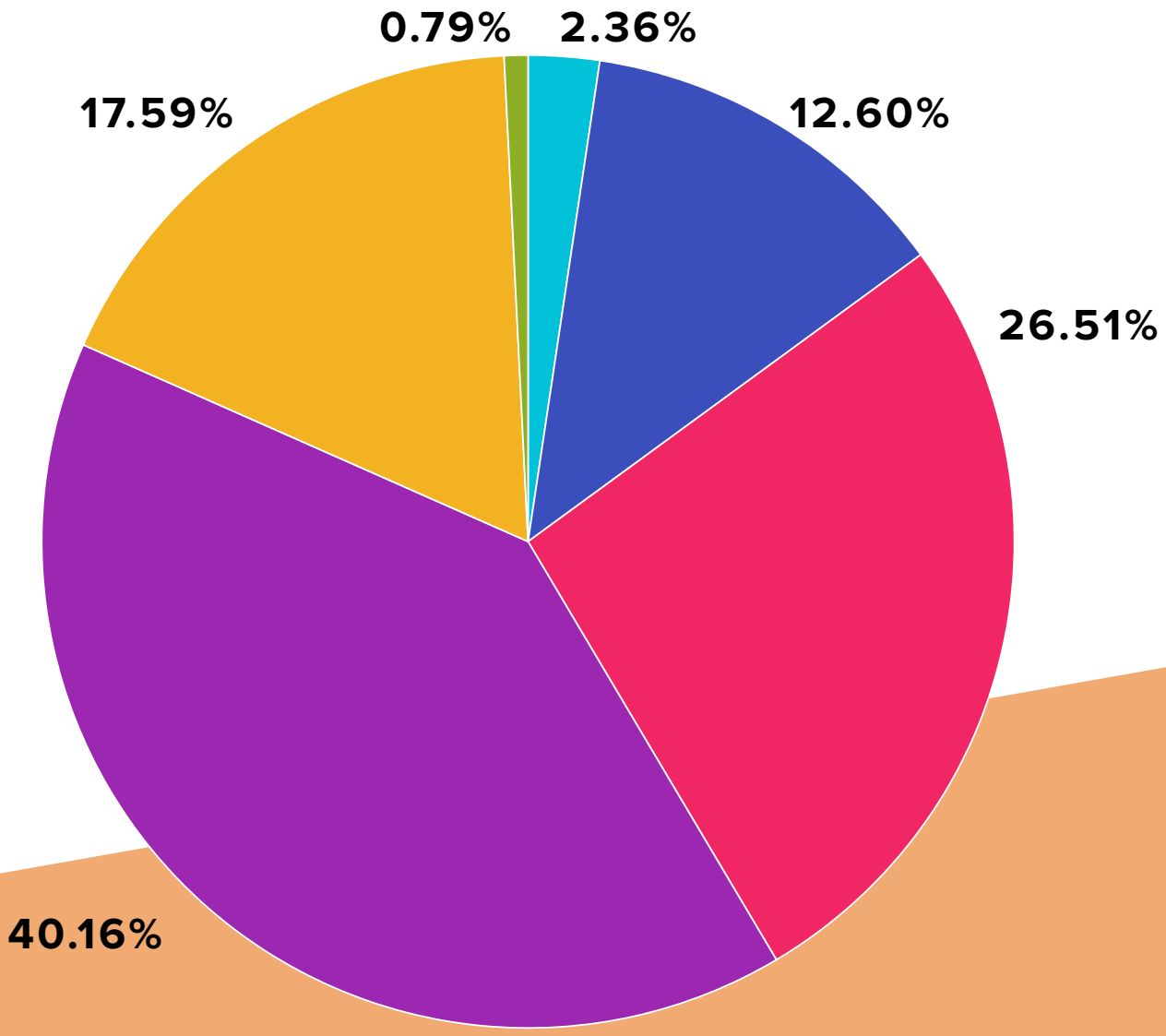
Q1 Φύλο



Choices	Response percent	Response count
Άνδρας	84.25%	321
Γυναίκα	15.49%	59
Άλλος αυτοπροσδιορισμός	0.26%	1

Η συντριπτική πλειοψηφία των συμμετεχόντων είναι άνδρες (84%). Παρότι ο χώρος της κυβερνοασφάλειας παραμένει ανδροκρατούμενος, η παρουσία γυναικών δείχνει σταδιακή διεύρυνση του επαγγελματικού πεδίου

Q2 Ηλικία



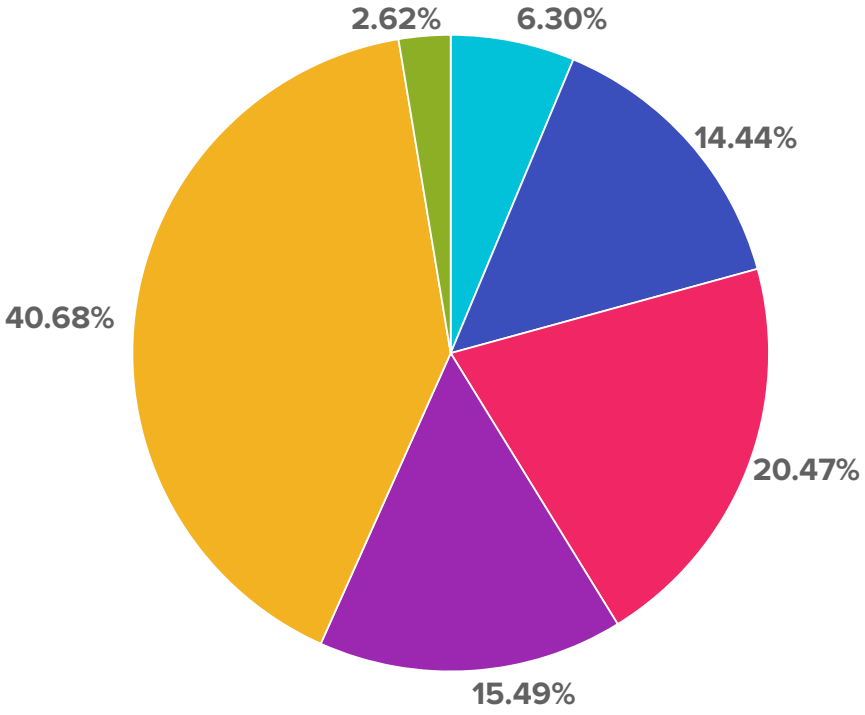
Η μεγαλύτερη μερίδα είναι μεταξύ 45–54 ετών (40%), με ισχυρή παρουσία και στις ηλικίες 35–44. Αυτό δείχνει ότι η ευθύνη της κυβερνοασφάλειας συγκεντρώνεται σε έμπειρα στελέχη μέσης ηλικίας

Ηλικία Q2

- 18 - 24 ετών
- 25 - 34 ετών
- 35 - 44 ετών
- 45 - 54 ετών
- 55 - 64 ετών
- 65 ετών και άνω

Choices	Response percent	Response count
18 - 24 ετών	2.36%	9
25 - 34 ετών	12.60%	48
35 - 44 ετών	26.51%	101
45 - 54 ετών	40.16%	153
55 - 64 ετών	17.59%	67
65 ετών και άνω	0.79%	3

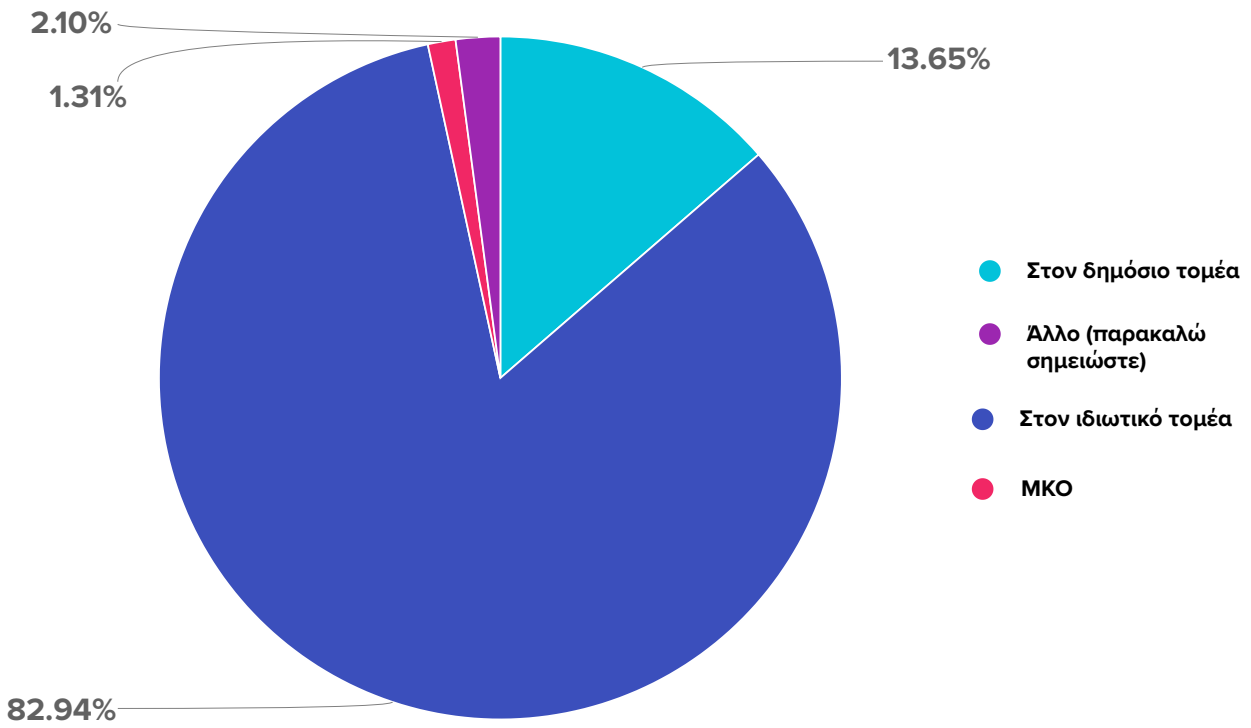
Q3 Πόσα άτομα απασχολεί η εταιρεία / ο οργανισμός όπου εργάζεστε;



Choices	Response percent	Response count
Από 1 έως 10 εργαζόμενους	6.30%	24
Από 11 έως 50 εργαζόμενους	14.44%	55
Από 51 έως 250 εργαζόμενους	20.47%	78
Από 251 έως 500 εργαζόμενους	15.49%	59
Περισσότερους από 500 εργαζόμενους	40.68%	155
Άλλο (παρακαλώ σημειώστε)	2.62%	10

Η μεγαλύτερη μερίδα είναι μεταξύ 45–54 ετών (40%), με ισχυρή παρουσία και στις ηλικίες 35–44. Αυτό δείχνει ότι η ευθύνη της κυβερνοασφάλειας συγκεντρώνεται σε έμπειρα στελέχη μέσης ηλικίας

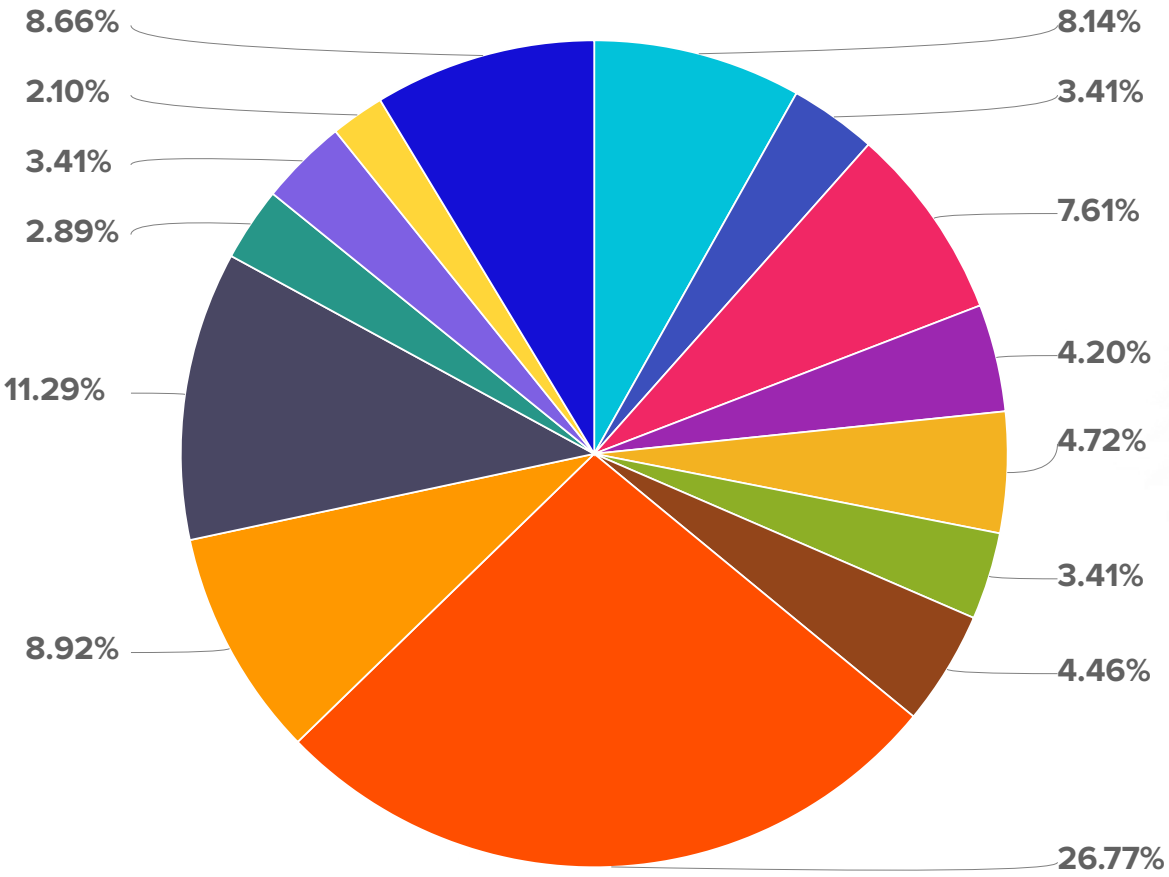
Σε ποιον τομέα ανήκει η εταιρεία / οργανισμός όπου εργάζεστε; Q4



Choices	Response percent	Response count
Στον δημόσιο τομέα	13.65%	52
Στον ιδιωτικό τομέα	82.94%	316
ΜΚΟ	1.31%	5
Άλλο (παρακαλώ σημειώστε)	2.10%	8

Το 83% ανήκει στον ιδιωτικό τομέα. Εκεί φαίνεται πως «παίζεται το παιχνίδι» της ασφάλειας, αφού η επιχειρησιακή συνέχεια εξαρτάται άμεσα από την ψηφιακή προστασία.

Q5 Σε ποιον επαγγελματικό κλάδο ανήκει η εταιρεία σας / ο οργανισμός όπου εργάζεστε;



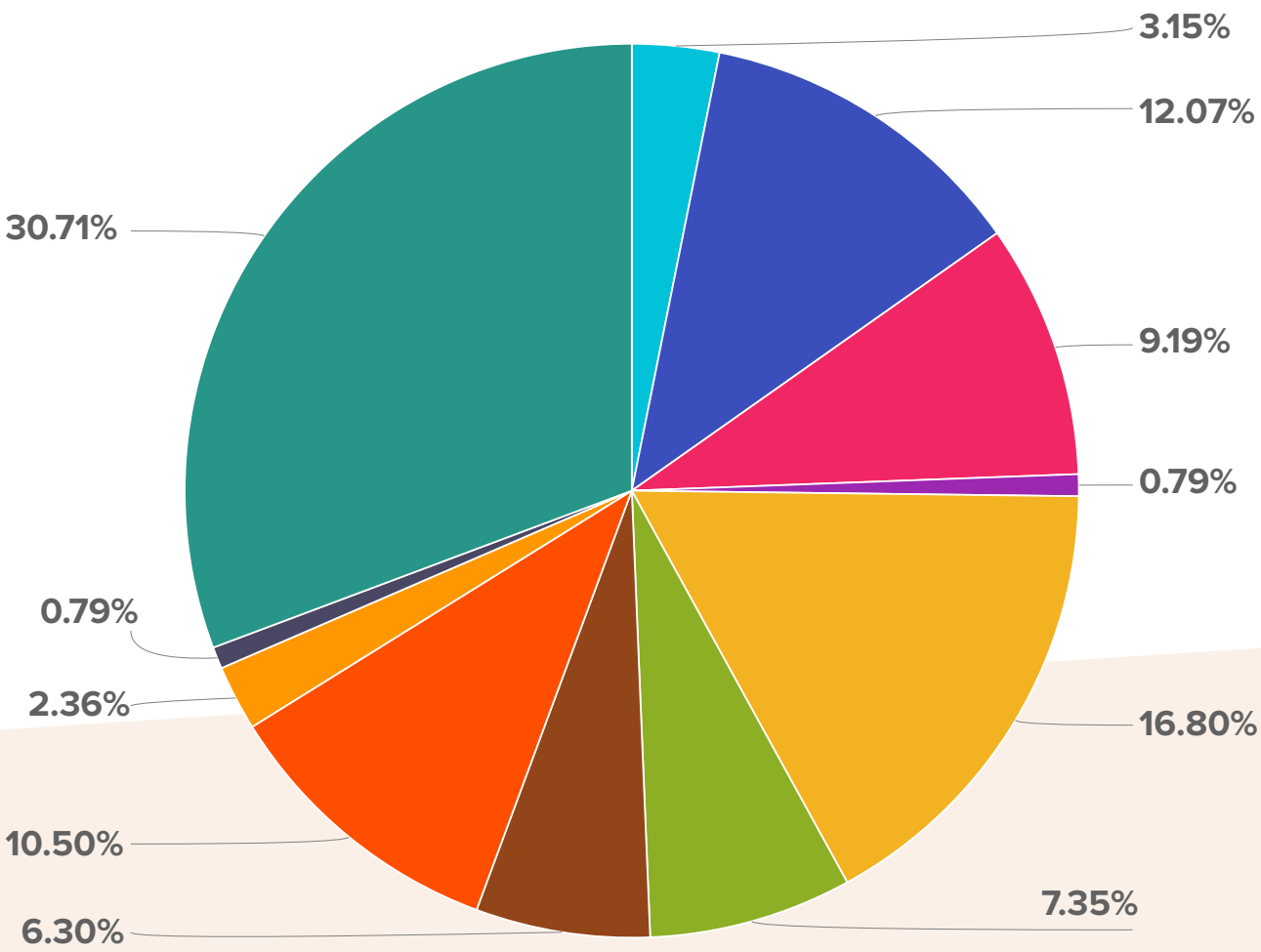
- Δημόσιος Τομέας / Οργανισμός
- Εκπαίδευση
- Εμπόριο / Λιανική / E-commerce
- Ενέργεια
- Κατασκευαστικός
- Μεταφορές / Logistics
- Ναυτιλία
- Τεχνολογία Πληροφορικής
- Τηλεπικοινωνίες
- Τραπεζικός / Χρηματοοικονομικός
- Τουρισμός / Φιλοξενία / Εστίαση / Διασκέδαση
- Υγεία / Φροντίδα υγείας
- Software House / Development
- Άλλο (παρακαλώ σημειώστε)

Πρώτοι σε συμμετοχή: IT (27%), τράπεζες/ χρηματοοικονομικά (11%) και τηλεπικοινωνίες (9%).

Σε ποιον επαγγελματικό κλάδο ανήκει η εταιρεία σας / ο οργανισμός όπου εργάζεστε; Q5

Choices	Response percent	Response count
Δημόσιος Τομέας / Οργανισμός	8.14%	31
Εκπαίδευση	3.41%	13
Εμπόριο / Λιανική / E-commerce	7.61%	29
Ενέργεια	4.20%	16
Κατασκευαστικός	4.72%	18
Μεταφορές / Logistics	3.41%	13
Ναυτιλία	4.46%	17
Τεχνολογία Πληροφορικής	26.77%	102
Τηλεπικοινωνίες	8.92%	34
Τραπεζικός / Χρηματοοικονομικός	11.29%	43
Τουρισμός / Φιλοξενία / Εστίαση / Διασκέδαση	2.89%	11
Υγεία / Φροντίδα υγείας	3.41%	13
Software House / Development	2.10%	8
Άλλο (παρακαλώ σημειώστε)	8.66%	33

Q6 Ποια είναι η επαγγελματική σας ιδιότητα;



- CEO
- CIO
- CISO
- DPO
- Cybersecurity ή IT Consultant
- IT Security
- IT Network
- IT Administrator
- Developer
- Data Analyst
- Άλλο (παρακαλώ σημειώστε)

Σε ποιον επαγγελματικό κλάδο ανήκει η εταιρεία σας / ο οργανισμός όπου εργάζεστε; Q6

Choices	Response percent	Response count
CEO	3.15%	12
CIO	12.07%	46
CISO	9.19%	35
DPO	0.79%	3
Cybersecurity ή IT Consultant	16.80%	64
IT Security	7.35%	28
IT Network	6.30%	24
IT Administrator	10.50%	40
Developer	2.36%	9
Data Analyst	0.79%	3
Άλλο (παρακαλώ σημειώστε)	30.71%	117

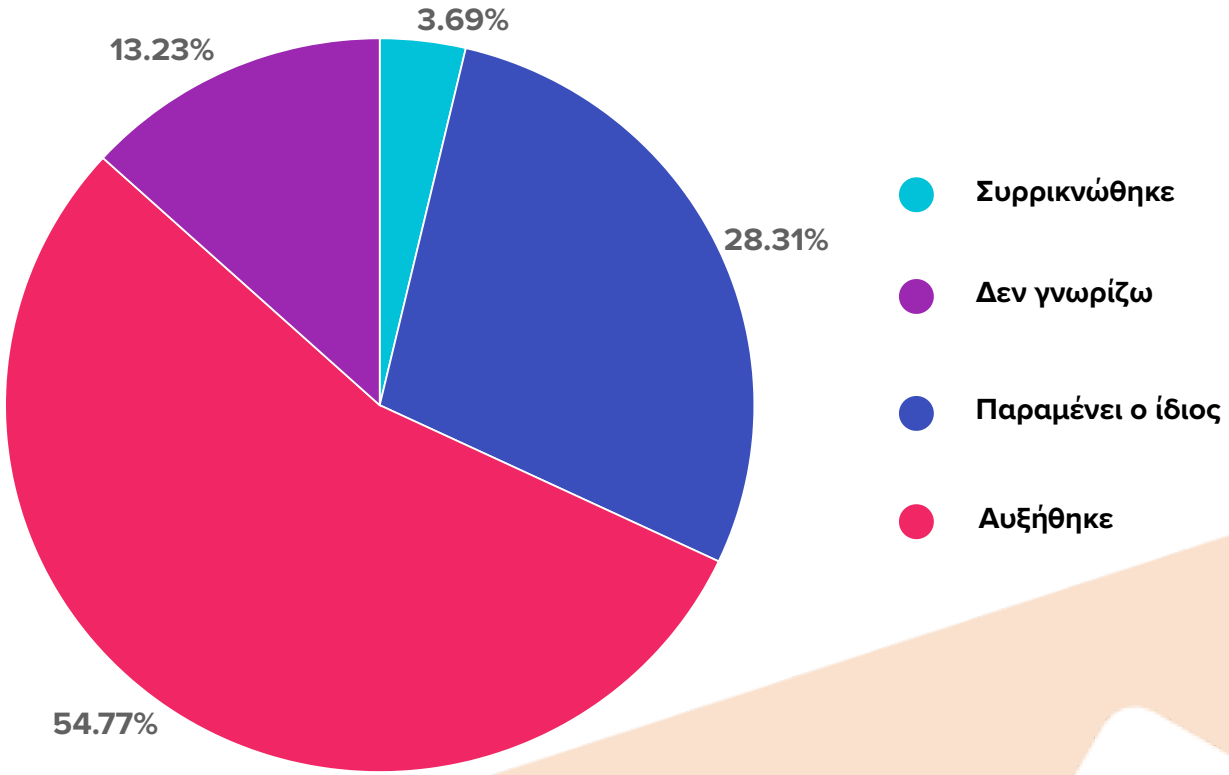
Ένα εντυπωσιακό 31% δηλώνει «άλλη ιδιότητα», γεγονός που δείχνει ότι η κυβερνοασφάλεια απασχολεί όχι μόνο IT στελέχη αλλά όλα τα στελέχη. Παρουσία CIOs, CISOs αλλά και CEOs καταδεικνύει στρατηγική διάσταση.

The State of Cybersecurity 2025

Επενδύσεις και προϋπολογισμός κυβερνοασφάλειας

Πώς μεταβλήθηκε ο προϋπολογισμός ασφάλειας IT (cybersecurity-budget) τηςεταιρείας σας σε σχέση με τους προηγούμενους 12 μήνες;

Q7

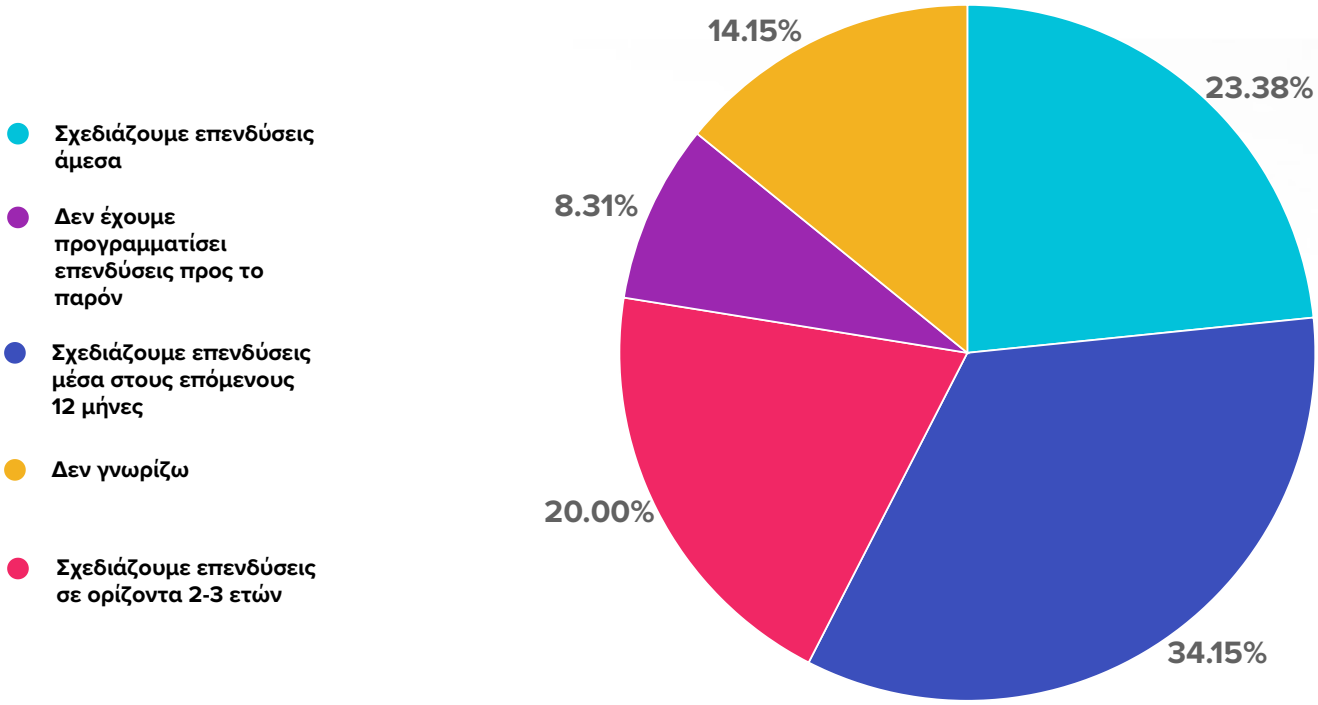


Choices	Response percent	Response count
Συρρικνώθηκε	3.69%	12
Παραμένει ο ίδιος	28.31%	92
Αυξήθηκε	54.77%	178
Δεν γνωρίζω	13.23%	43

Πάνω από τους μισούς (55%) δηλώνουν ότι αυξήθηκε ο προϋπολογισμός ασφάλειας. Η κυβερνοασφάλεια παύει να θεωρείται κόστος και αντιμετωπίζεται ως αναγκαιότητα και επένδυση.

Q8

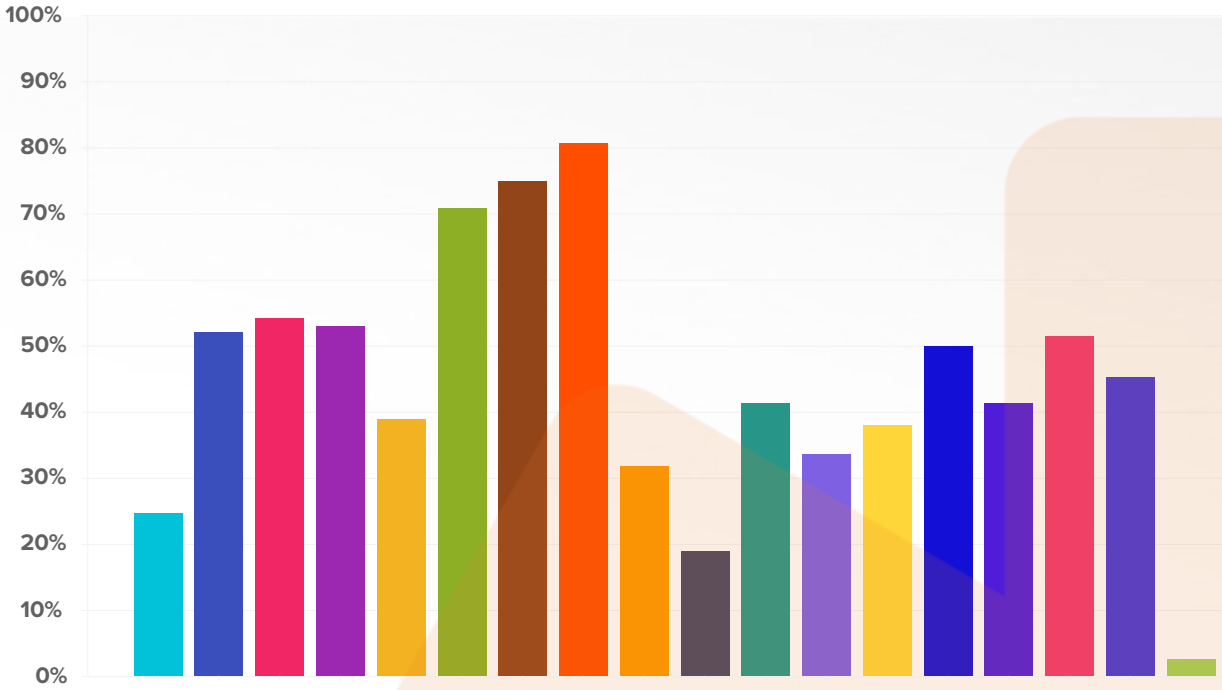
Ποιο είναι το χρονικό πλαίσιο επενδύσεων της εταιρείας σας στον τομέα της κυβερνοασφάλειας;



Choices	Response percent	Response count
Σχεδιάζουμε επενδύσεις άμεσα	23.38%	76
Σχεδιάζουμε επενδύσεις μέσα στους επόμενους 12 μήνες	34.15%	111
Σχεδιάζουμε επενδύσεις σε ορίζοντα 2-3 ετών	20.00%	65
Δεν έχουμε προγραμματίσει επενδύσεις προς το παρόν	8.31%	27
Δεν γνωρίζω	14.15%	46

Το 23% επενδύει άμεσα και το 34% μέσα στο έτος. Η πρόληψη γίνεται προτεραιότητα και οι κινήσεις επισπεύδονται.

Ποιες από τις ακόλουθες τεχνολογίες έχετε υιοθετήσει; Q9



- API Security & Management
- Cloud Security
- Cyber security awareness training
- DDoS Protection
- DLP (Data Loss Prevention) Security Solution
- Email Security and Protection
- Endpoint Security
- Firewall & Network Protection
- Identity & Access Management (IDaaS)
- Identity Governance
- Incident Response
- Managed Security Services
- Privileged Access Management (PAM)
- Security Operations Center (SOC)
- Threat intelligence
- Vulnerability management
- Web - Application Security
- Άλλο (παρακαλώ σημειώστε)

Τα βασικά μέτρα άμυνας (firewalls, endpoint, email protection) εφαρμόζονται από την πλειοψηφία. Σημαντική επένδυση γίνεται και στην εκπαίδευση προσωπικού (54%), που αναγνωρίζεται ως άμυνα πρώτης γραμμής.

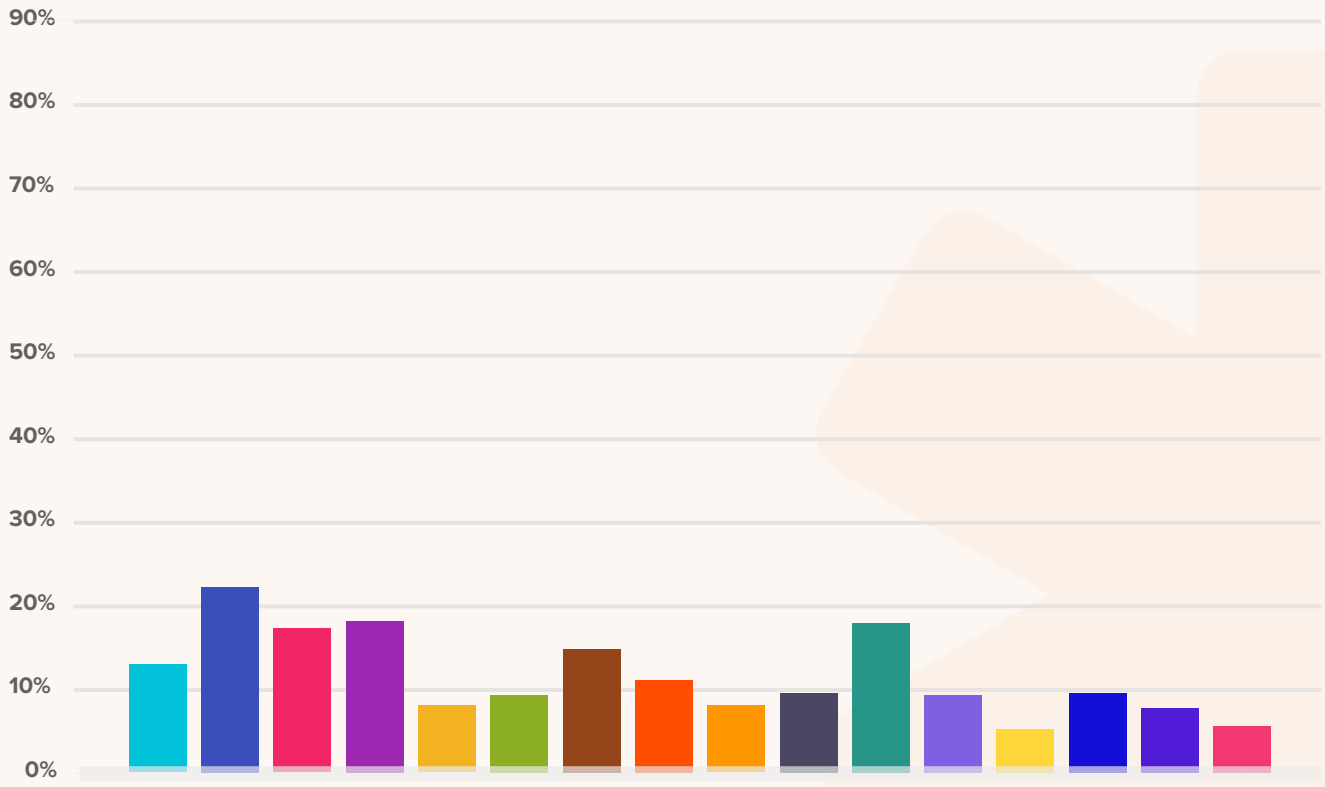
Q9

Ποιες από τις ακόλουθες τεχνολογίες έχετε υιοθετήσει;

Choices	Response percent	Response count
API Security & Management	24.62%	80
Cloud Security	52.00%	169
Cyber security awareness training	54.15%	176
DDoS Protection	52.92%	172
DLP (Data Loss Prevention) Security Solution	38.77%	126
Email Security and Protection	70.77%	230
Endpoint Security	74.77%	243
Firewall & Network Protection	80.62%	262
Identity & Access Management (IDaaS)	31.69%	103
Identity Governance	18.77%	61
Incident Response	41.23%	134
Managed Security Services	33.54%	109
Privileged Access Management (PAM)	37.85%	123
Security Operations Center (SOC)	49.85%	162
Threat intelligence	41.23%	134
Vulnerability management	51.38%	167
Web - Application Security	45.23%	147
Άλλο (παρακαλώ σημειώστε)	2.46%	8

Σε ποιο είδος ασφάλειας ή λύσης θα επενδύατε για καλύτερη κάλυψη στον τομέα της Cybersecurity; (έως 2 επιλογές)

Q10



- API Security & Management
- Cloud Security
- Cyber security awareness training
- DLP (Data Loss Prevention) Security Solution
- Email Security and Protection
- Endpoint Security
- Firewall & Network Protection
- Identity & Access management (IDaaS)
- Identity Governance
- Incident response
- Security Operations Center (SOC)
- Threat intelligence
- Managed Security Services
- Privileged Access Management (PAM)
- Vulnerability management
- Web - Application Security

Q10

Σε ποιο είδος ασφάλειας ή λύσης θα επενδύατε για καλύτερη κάλυψη στον τομέα της Cybersecurity; (έως 2 επιλογές)

Choices	Response percent	Response count
API Security & Management	12.92%	42
Cloud Security	22.15%	72
Cyber security awareness training	17.23%	56
DLP (Data Loss Prevention) Security Solution	18.15%	59
Email Security and Protection	8.00%	26
Endpoint Security	9.23%	30
Firewall & Network Protection	14.77%	48
Identity & Access management (IDaaS)	11.08%	36
Identity Governance	8.00%	26
Incident response	9.54%	31
Security Operations Center (SOC)	17.85%	58
Threat intelligence	9.23%	30
Managed Security Services	5.23%	17
Privileged Access Management (PAM)	9.54%	31
Vulnerability management	7.69%	25
Web - Application Security	5.54%	18

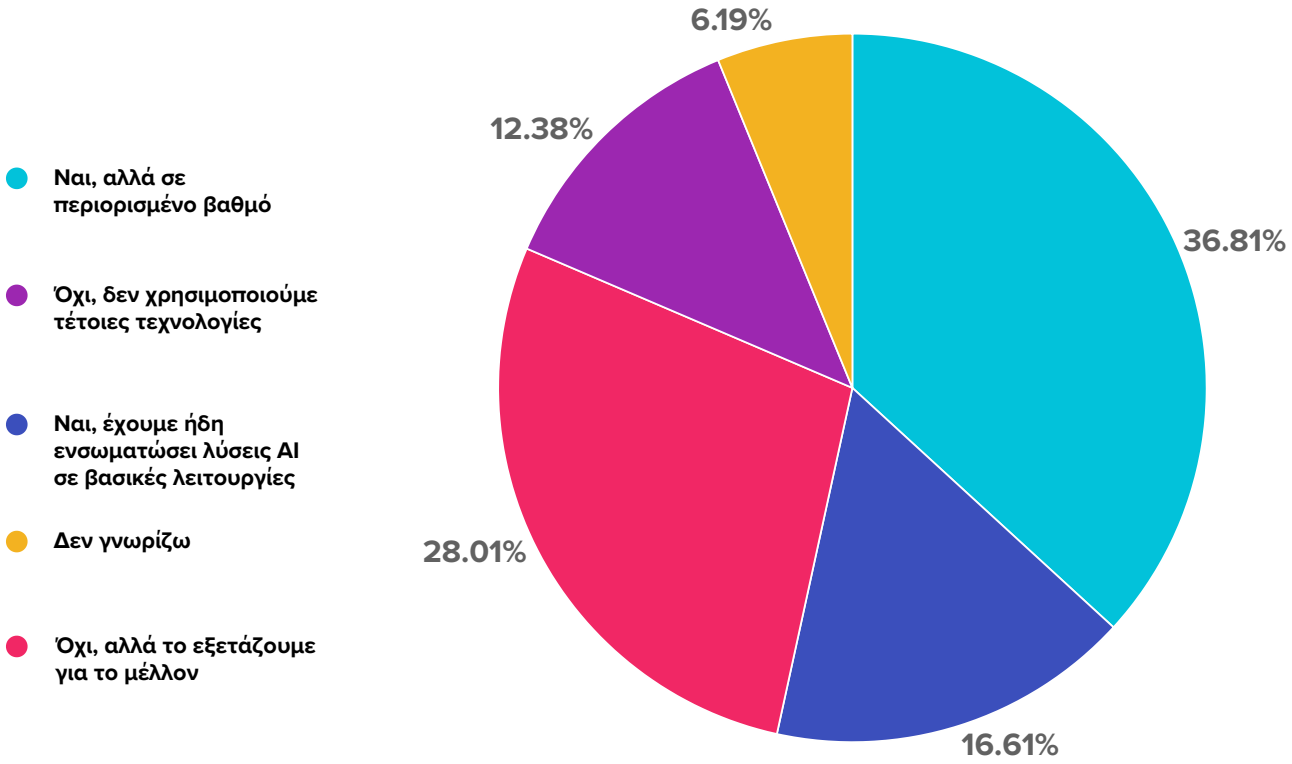
Μοιρασμένες τάσεις με επικρατέστερες τις επενδύσεις σε cloud security (22%), SOC (18%) και DLP (18%). Η διασπορά δείχνει την έντονη ανησυχία για διάφορα θέματα που υπάρχουν στις υποδομές και στην αντιμετώπιση των επιθέσεων.

The State of Cybersecurity 2025

Τεχνητή Νοημοσύνη (AI) και κυβερνοασφάλεια

Χρησιμοποιεί η εταιρεία σας λύσεις Τεχνητής Νοημοσύνης (AI), ή όχι;

Q11

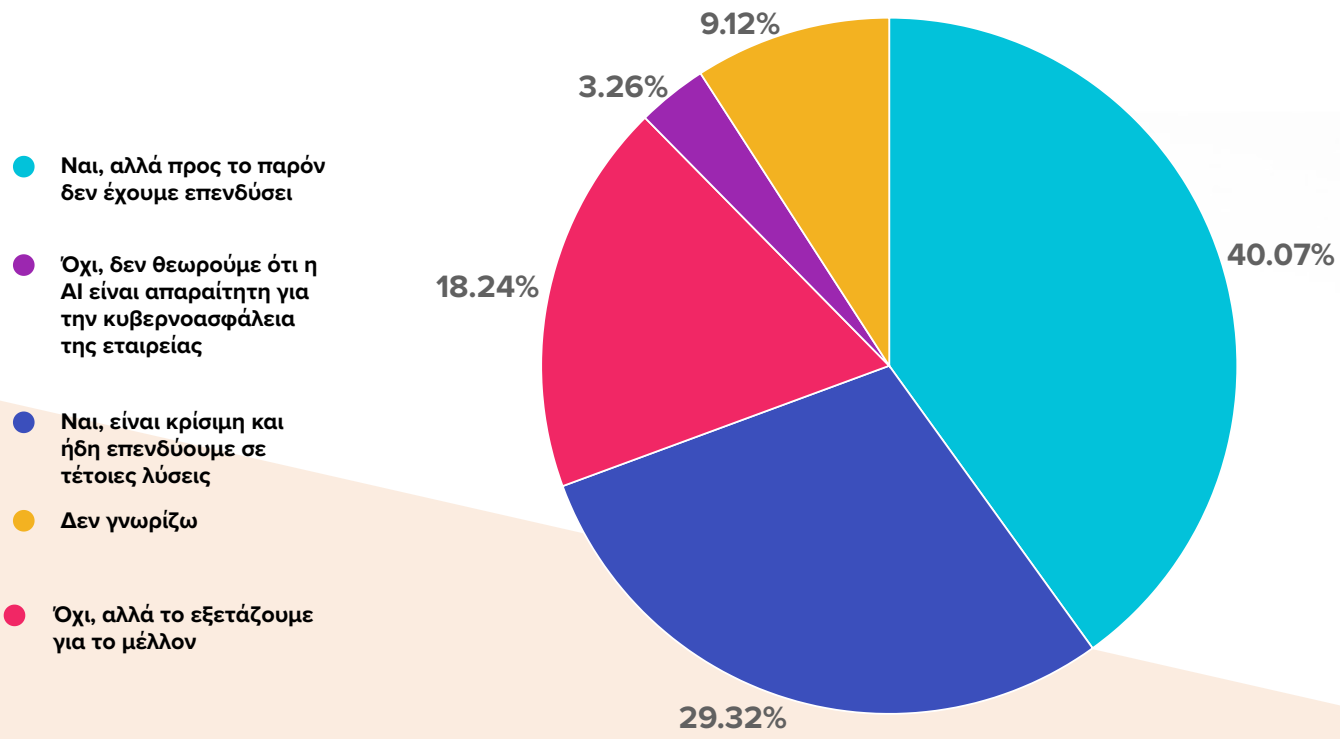


Choices	Response percent	Response count
Ναι, αλλά σε περιορισμένο βαθμό	36.81%	113
Ναι, έχουμε ήδη ενσωματώσει λύσεις AI σε βασικές λειτουργίες	16.61%	51
Όχι, αλλά το εξετάζουμε για το μέλλον	28.01%	86
Όχι, δεν χρησιμοποιούμε τέτοιες τεχνολογίες	12.38%	38
Δεν γνωρίζω	6.19%	19

Πέντε στις δέκα εταιρείες χρησιμοποιούν ήδη AI, έστω και περιορισμένα. Η AI τεχνολογία μπαίνει με γρήγορα βήματα στη φαρέτρα της άμυνας.

Q12

Πιστεύετε ότι η επένδυση σε AI-driven λύσεις είναι απαραίτητη για την κυβερνοασφάλεια της εταιρείας σας, ή όχι;

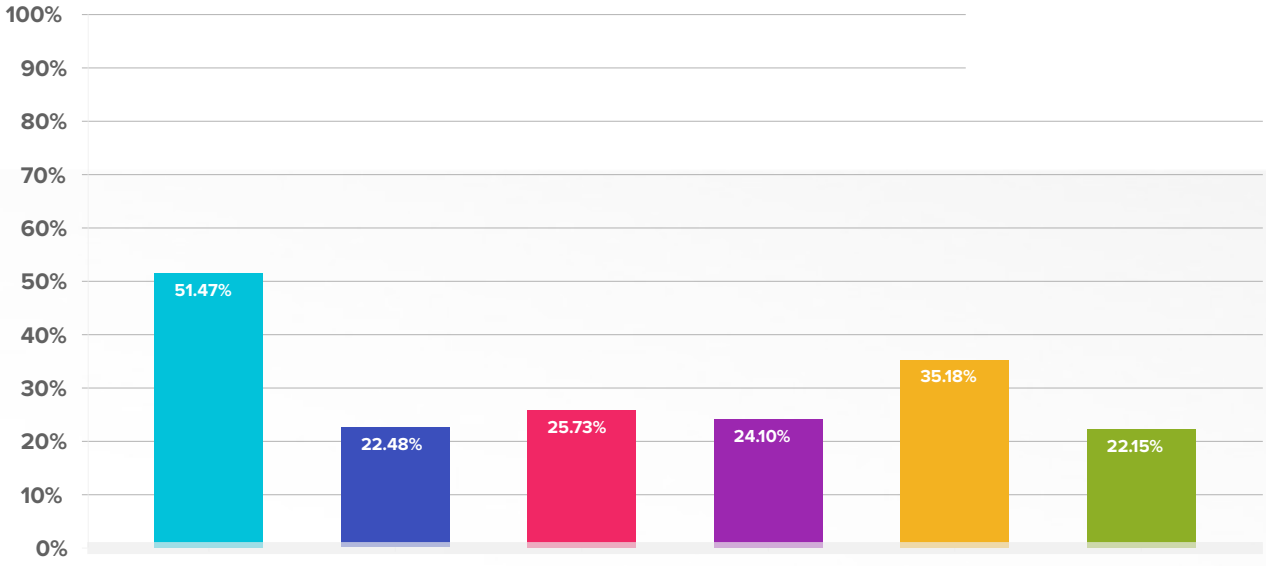


Choices	Response percent	Response count
Ναι, αλλά προς το παρόν δεν έχουμε επενδύσει	40.07%	123
Ναι, είναι κρίσιμη και ήδη επενδύουμε σε τέτοιες λύσεις	29.32%	90
Όχι, αλλά το εξετάζουμε για το μέλλον	18.24%	56
Όχι, δεν θεωρούμε ότι η AI είναι απαραίτητη για την κυβερνοασφάλεια της εταιρείας	3.26%	10
Δεν γνωρίζω	9.12%	28

Το 40% θεωρεί την AI κρίσιμη αλλά δεν έχει επενδύσει ακόμη, ενώ το 29% επενδύει ήδη. Υπάρχει ώριμη πρόθεση αλλά και επιφυλακτικότητα.

Ποια θεωρείτε ότι είναι η μεγαλύτερη πρόκληση στην υιοθέτηση λύσεων AI για την κυβερνοασφάλεια; (έως 2 επιλογές)

Q13



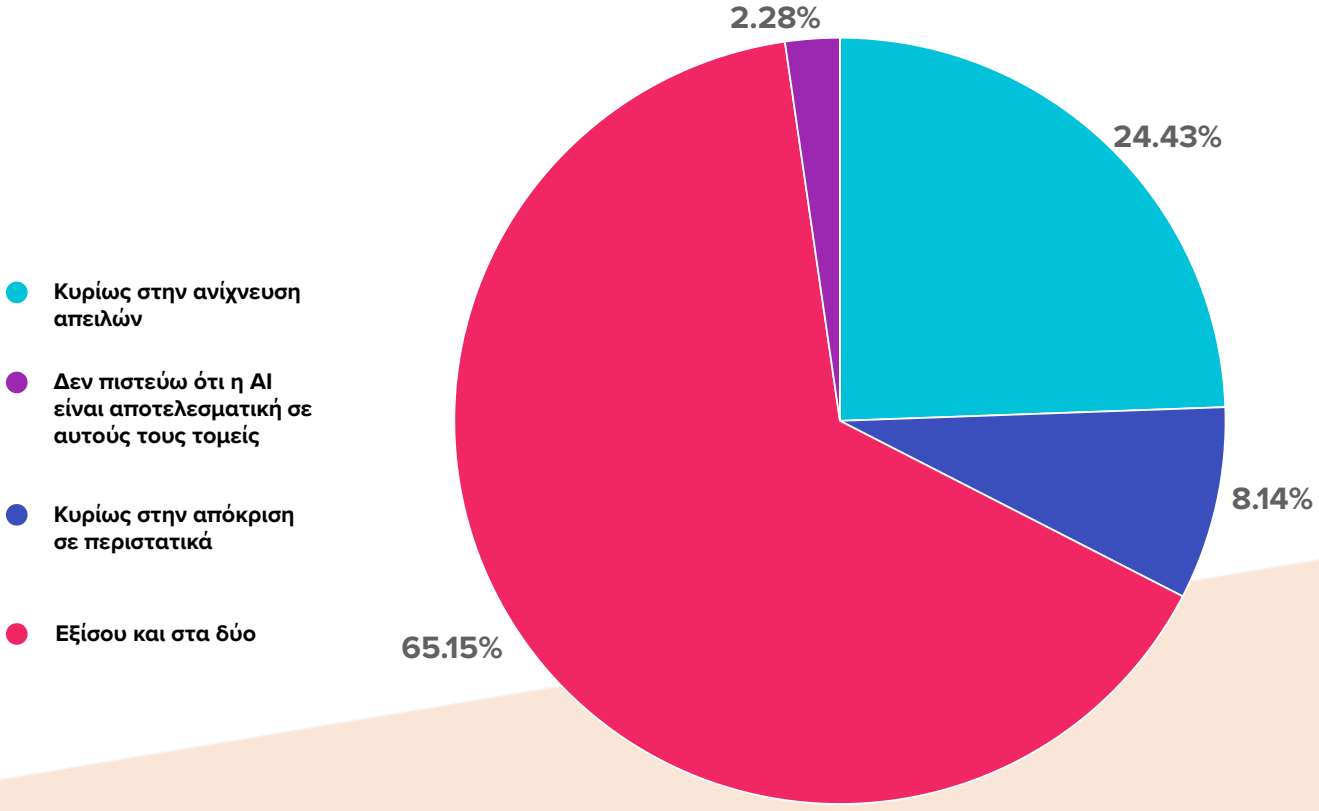
- Έλλειψη κατάλληλης τεχνογνωσίας και εξειδικευμένου προσωπικού
- Υψηλό κόστος υλοποίησης και συντήρησης
- Δυσκολία ενσωμάτωσης της AI στις υπάρχουσες διαδικασίες ασφάλειας
- Ανάγκη για διαφάνεια και επεξήγηση αποφάσεων AI (explainability)
- Κίνδυνος σφαλμάτων και ψευδώς θετικών/ αρνητικών ενδείξεων
- Προβληματισμοί σχετικά με τη συμμόρφωση και την προστασία προσωπικών δεδομένων

Choices	Response percent	Response count
Έλλειψη κατάλληλης τεχνογνωσίας και εξειδικευμένου προσωπικού	51.47%	158
Υψηλό κόστος υλοποίησης και συντήρησης	22.48%	69
Δυσκολία ενσωμάτωσης της AI στις υπάρχουσες διαδικασίες ασφάλειας	25.73%	79
Ανάγκη για διαφάνεια και επεξήγηση αποφάσεων AI (explainability)	24.10%	74
Κίνδυνος σφαλμάτων και ψευδώς θετικών/ αρνητικών ενδείξεων	35.18%	108
Προβληματισμοί σχετικά με τη συμμόρφωση και την προστασία, προσωπικών δεδομένων	22.15%	68

Έλλειψη εξειδικευμένου προσωπικού (51%) και ψευδείς συναγερμοί (35%) είναι τα βασικά εμπόδια. Η ενσωμάτωση σε υφιστάμενες διαδικασίες δυσκολεύει επίσης.

Q14

Πιστεύετε ότι η AI μπορεί να συμβάλει πιο αποτελεσματικά στην ανίχνευση ή στην απόκριση σε κυβερνοεπιθέσεις;

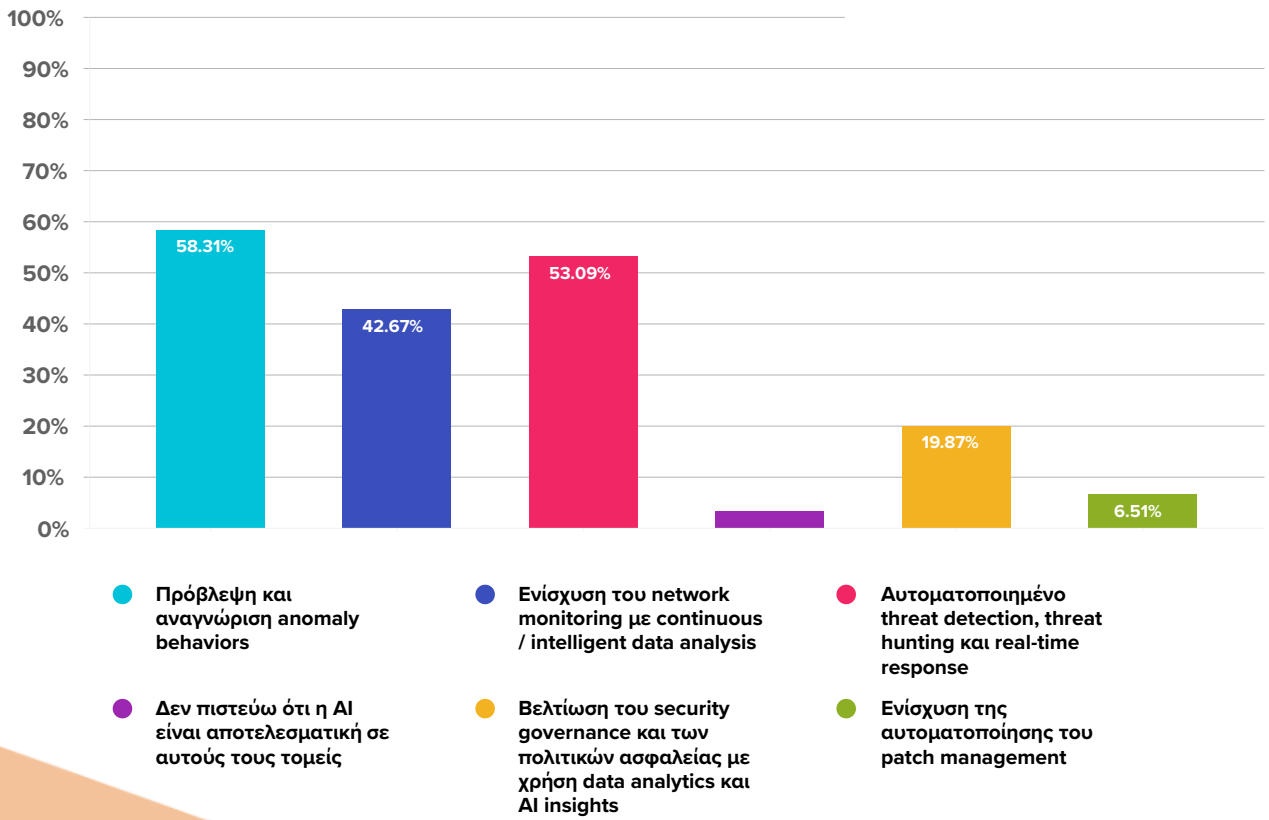


Choices	Response percent	Response count
Κυρίως στην ανίχνευση απειλών	24.43%	75
Κυρίως στην απόκριση σε περιστατικά	8.14%	25
Εξίσου και στα δύο	65.15%	200
Δεν πιστεύω ότι η AI είναι αποτελεσματική σε αυτούς τους τομείς	2.28%	7

Η πλειοψηφία (65%) πιστεύει ότι είναι εξίσου χρήσιμη σε ανίχνευση και απόκριση. Δείχνει κατανόηση της δυναμικής της τεχνολογίας.

Πώς θα μπορούσε η εταιρεία σας να αξιοποιήσει την τεχνητή νοημοσύνη (AI) για την ενίσχυση των μέτρων ασφαλείας και την ανίχνευση πιθανών κυβερνοεπιθέσεων; (έως 2 επιλογές)

Q15



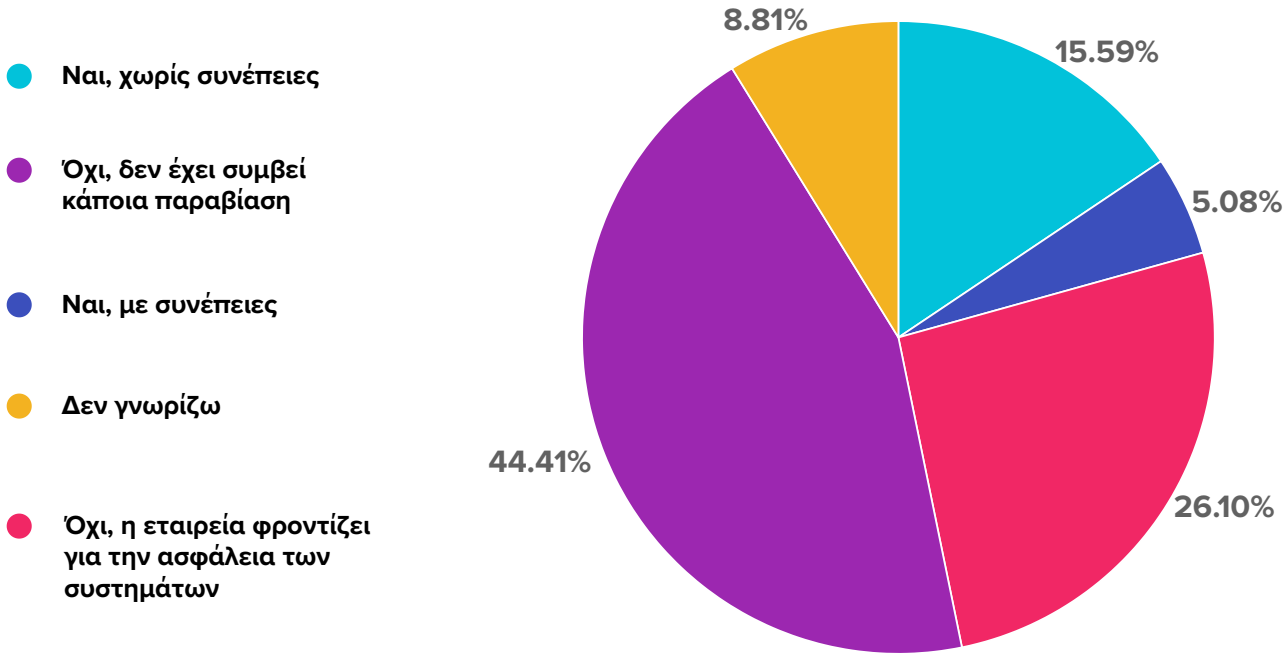
Choices	Response percent	Response count
Πρόβλεψη και αναγνώριση anomaly behaviors	58.31%	179
Ενίσχυση του network monitoring με continuous / intelligent data analysis	42.67%	131
Αυτοματοποιημένο threat detection, threat hunting και real-time response	53.09%	163
Δεν πιστεύω ότι η AI είναι αποτελεσματική σε αυτούς τους τομείς	3.26%	10
Βελτίωση του security governance και των πολιτικών ασφαλείας με χρήση data analytics και AI insights	19.87%	61
Ενίσχυση της αυτοματοποίησης του patch management	6.51%	20

Πρώτη χρήση: πρόβλεψη ανώμαλων συμπεριφορών (58%) και αυτοματοποίηση threat detection/response (53%). Η AI προορίζεται για κρίσιμες γραμμές άμυνας.

The State of Cybersecurity 2025

Απειλές / Επιθέσεις

Αντιμετώπισε η εταιρεία σας κάποια παραβίαση ασφάλειας στα συστήματά της, ή όχι; Q16

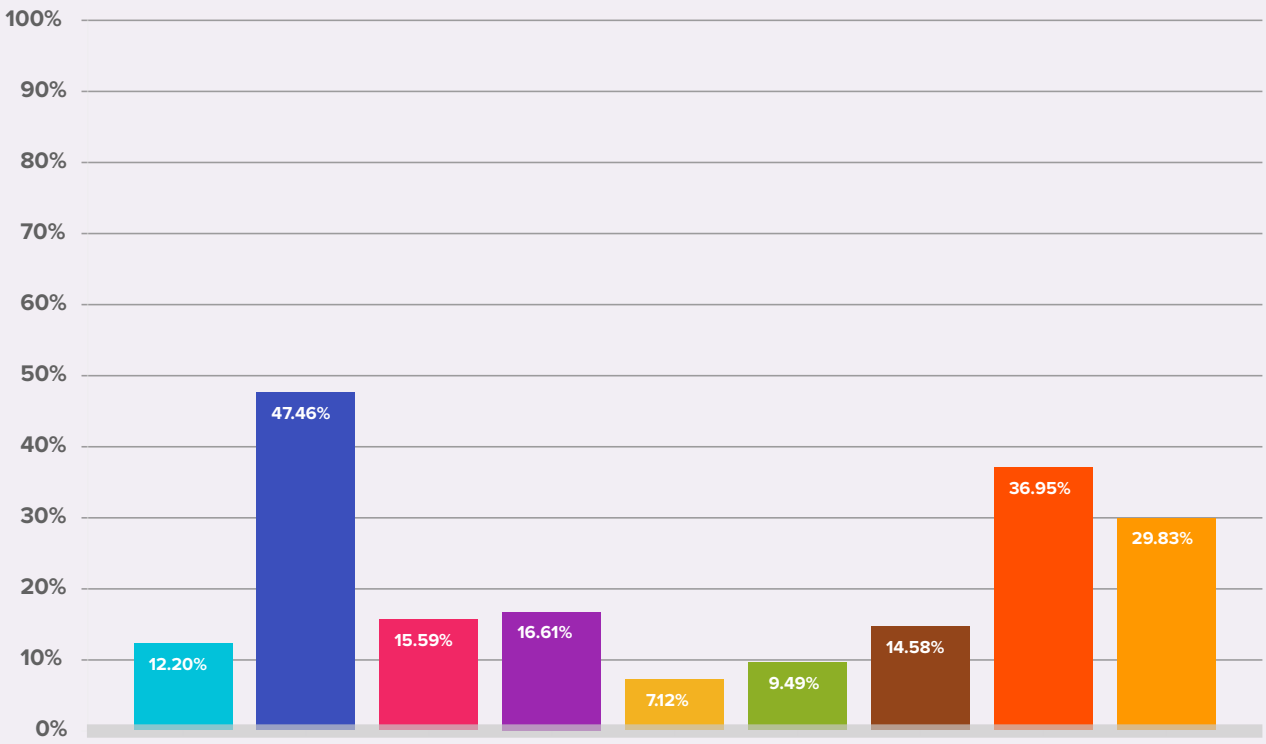


Choices	Response percent	Response count
Ναι, χωρίς συνέπειες	15.59%	46
Ναι, με συνέπειες	5.08%	15
Όχι, η εταιρεία φροντίζει για την ασφάλεια των συστημάτων	26.10%	77
Όχι, δεν έχει συμβεί κάποια παραβίαση	44.41%	131
Δεν γνωρίζω	8.81%	26

Ένας στους πέντε οργανισμούς έχει υποστεί παραβίαση, με ή χωρίς συνέπειες. Το 44% δηλώνει ότι δεν έχει αντιμετωπίσει περιστατικό.

Q17

Ποιοι τύποι κινδύνων απασχολούν περισσότερο την ασφάλεια της επιχείρησής σας; (έως 2 επιλογές)



- APT (Advanced Persistent Threats) & στοχευμένες επιθέσεις με χρήση τεχνικών όπως Lateral Movement & Privilege Escalation
- Εκμετάλλευση ευπαθειών (CVE Exploits) σε εφαρμογές, λειτουργικά συστήματα και APIs
- Network Cyber-attacks
- Διαρροή δεδομένων (Data Exfiltration & Data Breaches)
- Identity Based Attacks
- Phishing & Credential Theft
- DDoS & Botnet-driven Attacks
- IoT Security Risks
- Ransomware & Business Email Compromise (BEC)

Ποιοι τύποι κινδύνων απασχολούν περισσότερο την ασφάλεια της επιχείρησής σας; (έως 2 επιλογές)

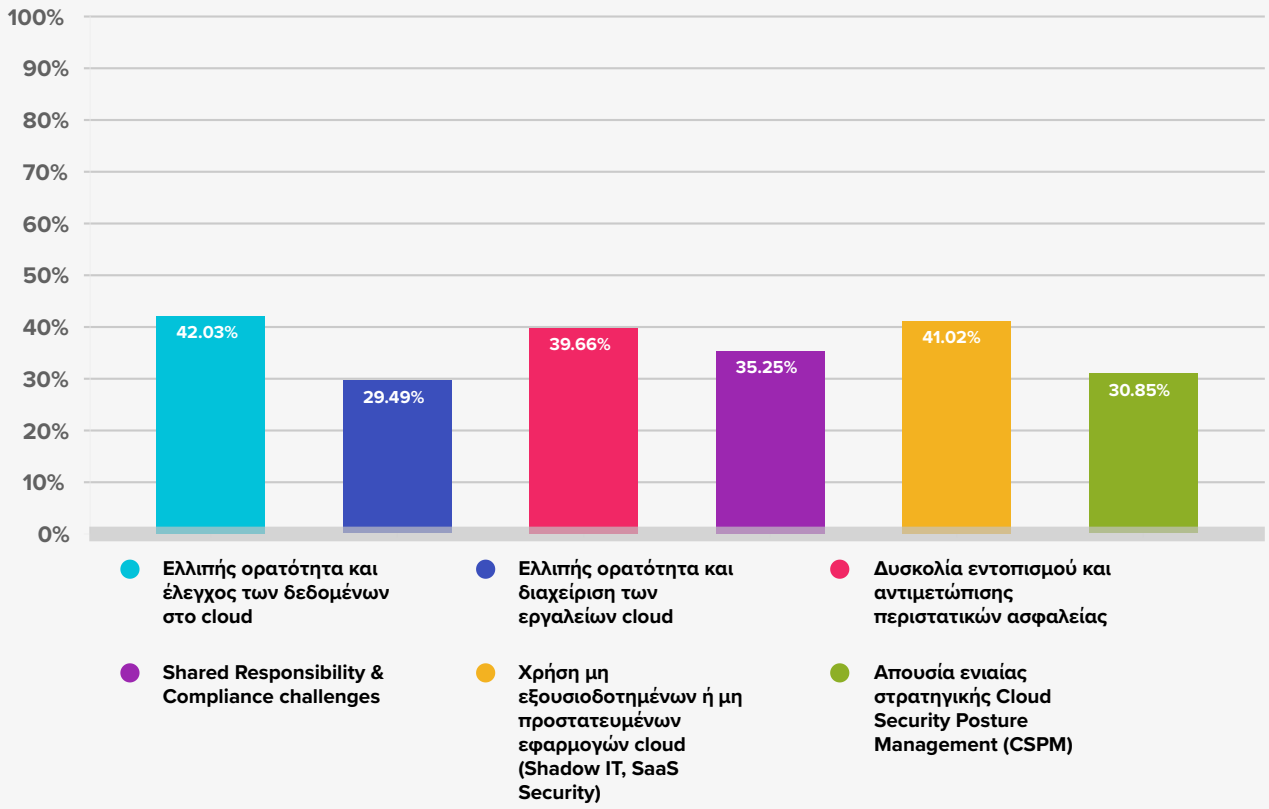
Q17

Choices	Response percent	Response count
APT (Advanced Persistent Threats) & στοχευμένες επιθέσεις με χρήση τεχνικών όπως Lateral Movement & Privilege Escalation	12.20%	36
Διαρροή δεδομένων (Data Exfiltration & Data Breaches)	47.46%	140
DDoS & Botnet-driven Attacks	15.59%	46
Εκμετάλλευση ευπαθειών (CVE Exploits) σε εφαρμογές, λειτουργικά συστήματα και APIs	16.61%	49
Identity Based Attacks	7.12%	21
IoT Security Risks	9.49%	28
Network Cyber-attacks	14.58%	43
Phishing & Credential Theft	36.95%	109
Ransomware & Business Email Compromise (BEC)	29.83%	88

Μεγαλύτερη ανησυχία οι διαρροές δεδομένων (47%), phishing (37%) και ransomware (30%). Τα δεδομένα θεωρούνται «ο μεγαλύτερος στόχος».

Q18

Ποιες είναι οι μεγαλύτερες προκλήσεις ασφάλειας στο cloud που αντιμετωπίζετε; (Επιλέξτε όλα όσα ισχύουν)

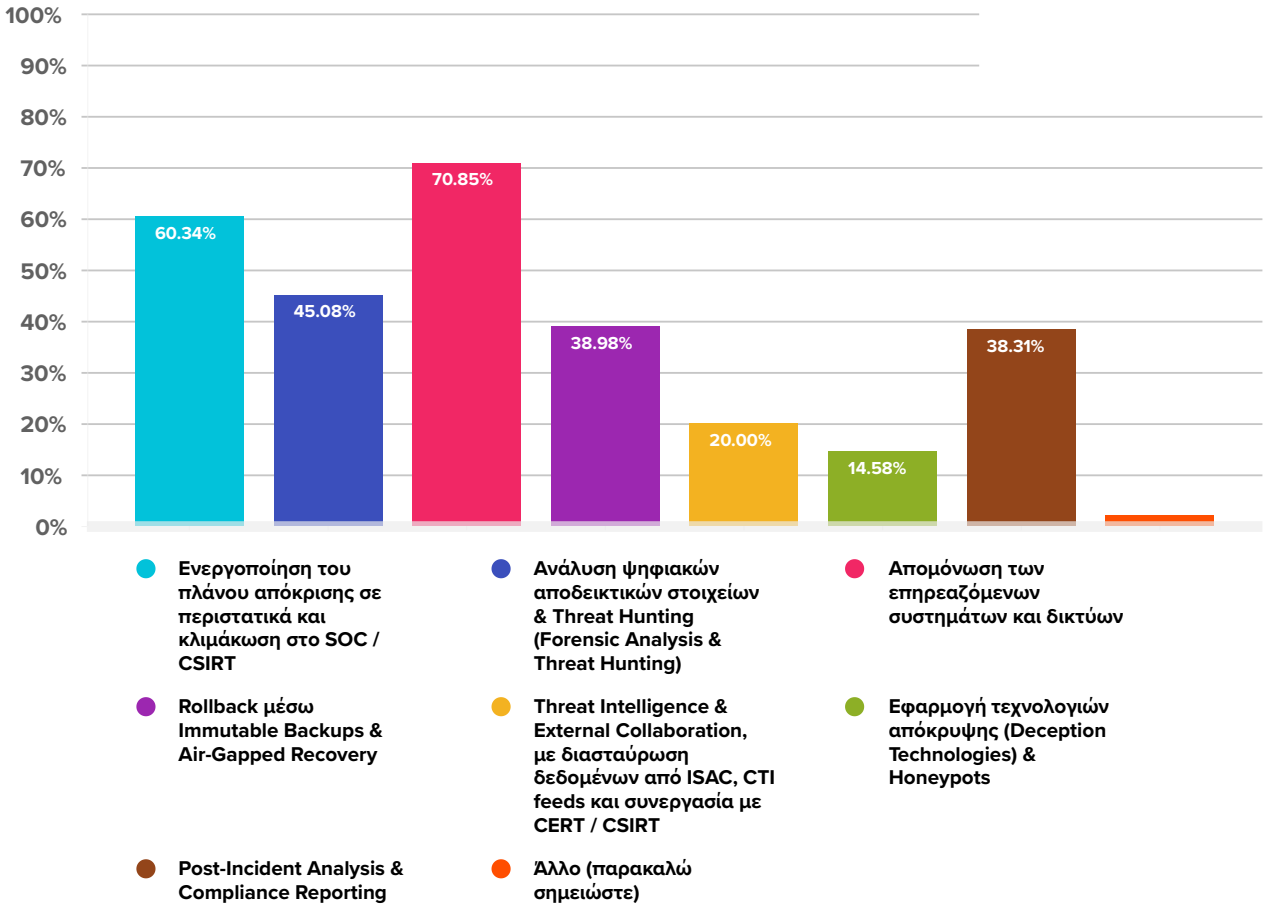


Choices	Response percent	Response count
Ελλιπής ορατότητα και έλεγχος των δεδομένων στο cloud	42.03%	124
Ελλιπής ορατότητα και διαχείριση των εργαλείων cloud	29.49%	87
Δυσκολία εντοπισμού και αντιμετώπισης περιστατικών ασφαλείας	39.66%	117
Shared Responsibility & Compliance challenges	35.25%	104
Χρήση μη εξουσιοδοτημένων ή μη προστατευμένων εφαρμογών cloud (Shadow IT, SaaS Security)	41.02%	121
Απουσία ενιαίας στρατηγικής Cloud Security Posture Management (CSPM)	30.85%	91

Κυριότερα θέματα: ορατότητα/έλεγχος δεδομένων (42%), shadow IT (41%) και δυσκολία εντοπισμού περιστατικών (40%). Το cloud συνεχίζει να εισάγει νέα τρωτά σημεία.

Σε περίπτωση όπου μία κυβερνο-επίθεση είναι σε εξέλιξη, με ποιους τρόπους αντιμετωπίζεται από την εταιρεία σας; (παραπάνω από μια επιλογή)

Q19



Choices	Response percent	Response count
Ενεργοποίηση του πλάνου απόκρισης σε περιστατικά και κλιμάκωση στο SOC / CSIRT	60.34%	178
Ανάλυση ψηφιακών αποδεικτικών στοιχείων & Threat Hunting (Forensic Analysis & Threat Hunting)	45.08%	133
Απομόνωση των επηρεαζόμενων συστημάτων και δικτύων	70.85%	209
Rollback μέσω Immutable Backups & Air-Gapped Recovery	38.98%	115
Threat Intelligence & External Collaboration, με διασταύρωση δεδομένων από ISAC, CTI feeds και συνεργασία με CERT / CSIRT	20.00%	59
Εφαρμογή τεχνολογιών απόκρυψης (Deception Technologies) & Honeypots	14.58%	43
Post-Incident Analysis & Compliance Reporting	38.31%	113
Άλλο (παρακαλώ σημειώστε)	2.03%	6

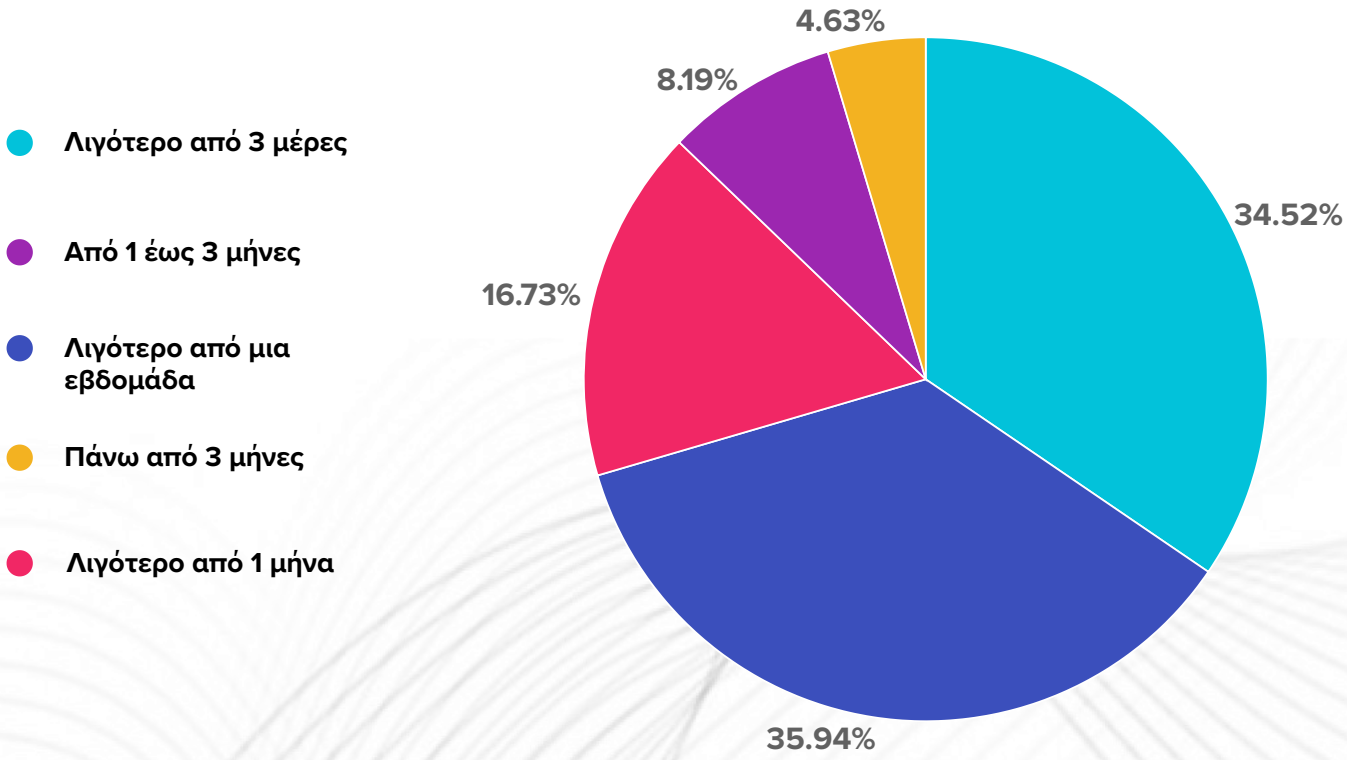
Συνηθέστερες πρακτικές: απομόνωση συστημάτων (71%) και πλάνο απόκρισης (60%). Ωστόσο, πιο προχωρημένα εργαλεία (deception, collaboration) εφαρμόζονται περιορισμένα.

The State of Cybersecurity 2025

Ανθεκτικότητα και Αποκατάσταση

Αντιμετώπισε η εταιρεία σας κάποια παραβίαση ασφάλειας στα συστήματά της, ή όχι;

Q20

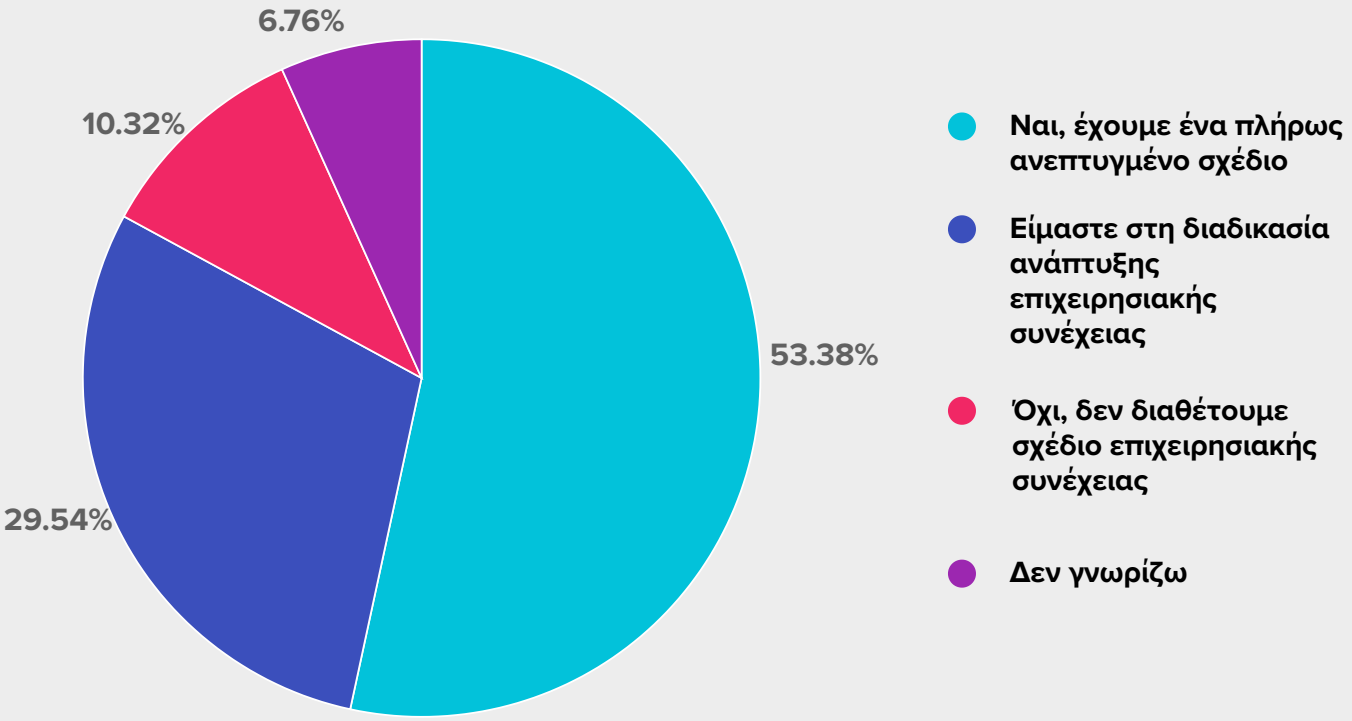


Choices	Response percent	Response count
Λιγότερο από 3 μέρες	34.52%	97
Λιγότερο από μια εβδομάδα	35.94%	101
Λιγότερο από 1 μήνα	16.73%	47
Από 1 έως 3 μήνες	8.19%	23
Πάνω από 3 μήνες	4.63%	13

7 στις 10 επιχειρήσεις εκτιμούν ότι μπορούν να επανέλθουν σε λιγότερο από μία εβδομάδα. Υπάρχει εμπιστοσύνη στις υποδομές τους και στις δυνατότητες αποκατάστασης.

Q21

Διαθέτετε σχέδιο επιχειρησιακής συνέχειας σε περίπτωση κυβερνοεπίθεσης, ή όχι;

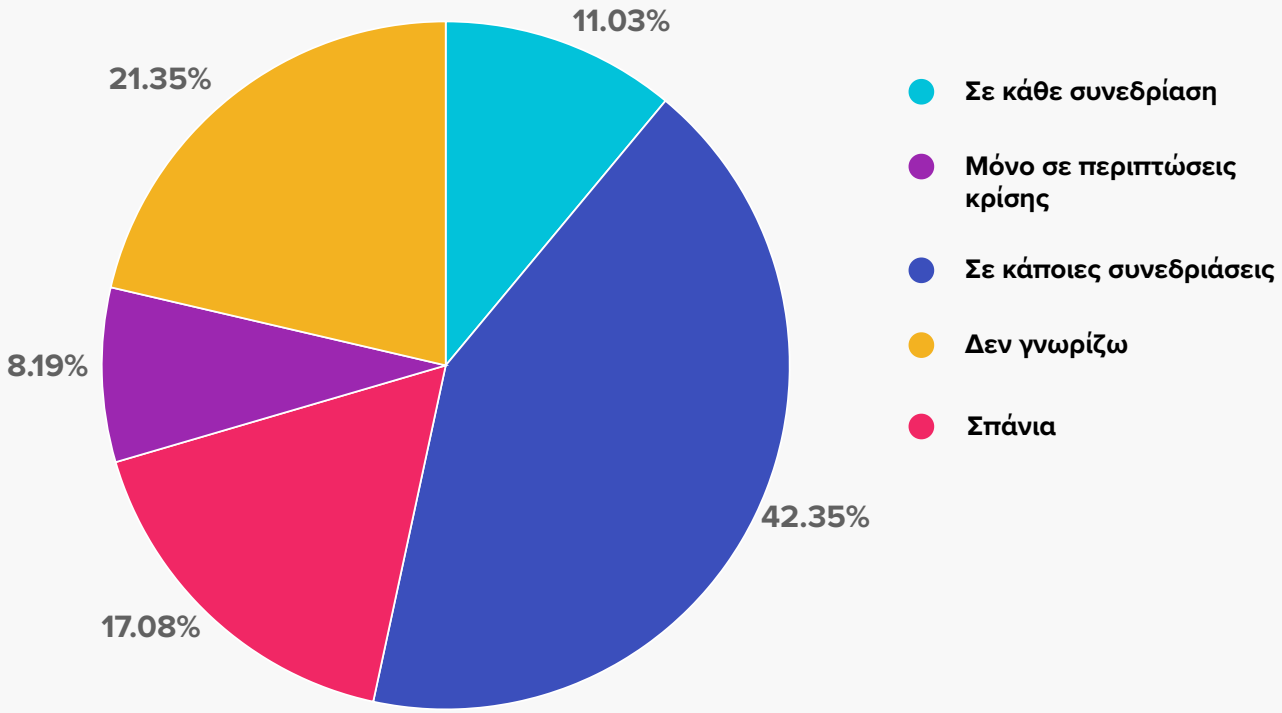


Choices	Response percent	Response count
Ναι, έχουμε ένα πλήρως ανεπτυγμένο σχέδιο	53.38%	150
Είμαστε στη διαδικασία ανάπτυξης επιχειρησιακής συνέχειας	29.54%	83
Όχι, δεν διαθέτουμε σχέδιο επιχειρησιακής συνέχειας	10.32%	29
Δεν γνωρίζω	6.76%	19

Το 53% έχει ήδη σχέδιο, ενώ 30% βρίσκεται σε φάση ανάπτυξης. Αποδεικνύει αυξανόμενη ωριμότητα.

Πόσο συχνά αποτελεί η κυβερνοασφάλεια θέμα ημερήσιας διάταξης στις συνεδριάσεις του διοικητικού συμβουλίου της επιχείρησής σας;

Q22

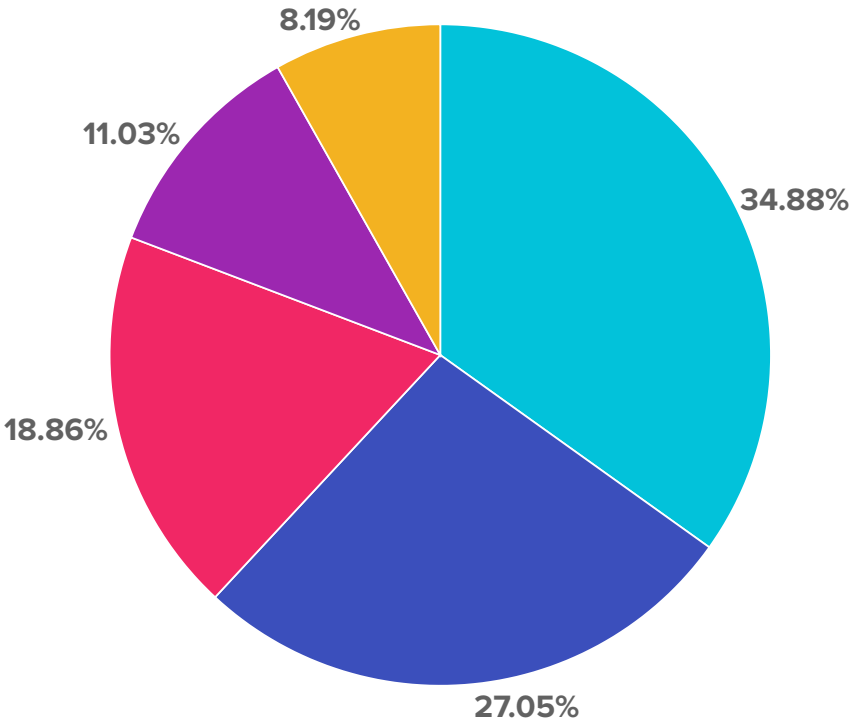


Choices	Response percent	Response count
Σε κάθε συνεδρίαση	11.03%	31
Σε κάποιες συνεδριάσεις	42.35%	119
Σπάνια	17.08%	48
Μόνο σε περιπτώσεις κρίσης	8.19%	23
Δεν γνωρίζω	21.35%	60

Τα θέματα της κυβερνοασφάλειας φαίνεται ότι απασχολούν σε μόνιμη ή τακτική βάση πάνω από τις μισές εταιρείες. Η παρουσία της στην ατζέντα δείχνει στρατηγική σημασία.

Q23

Έχετε πραγματοποιήσει προσομοιώσεις επιθέσεων για να δοκιμάσετε την ετοιμότητά σας, ή όχι;

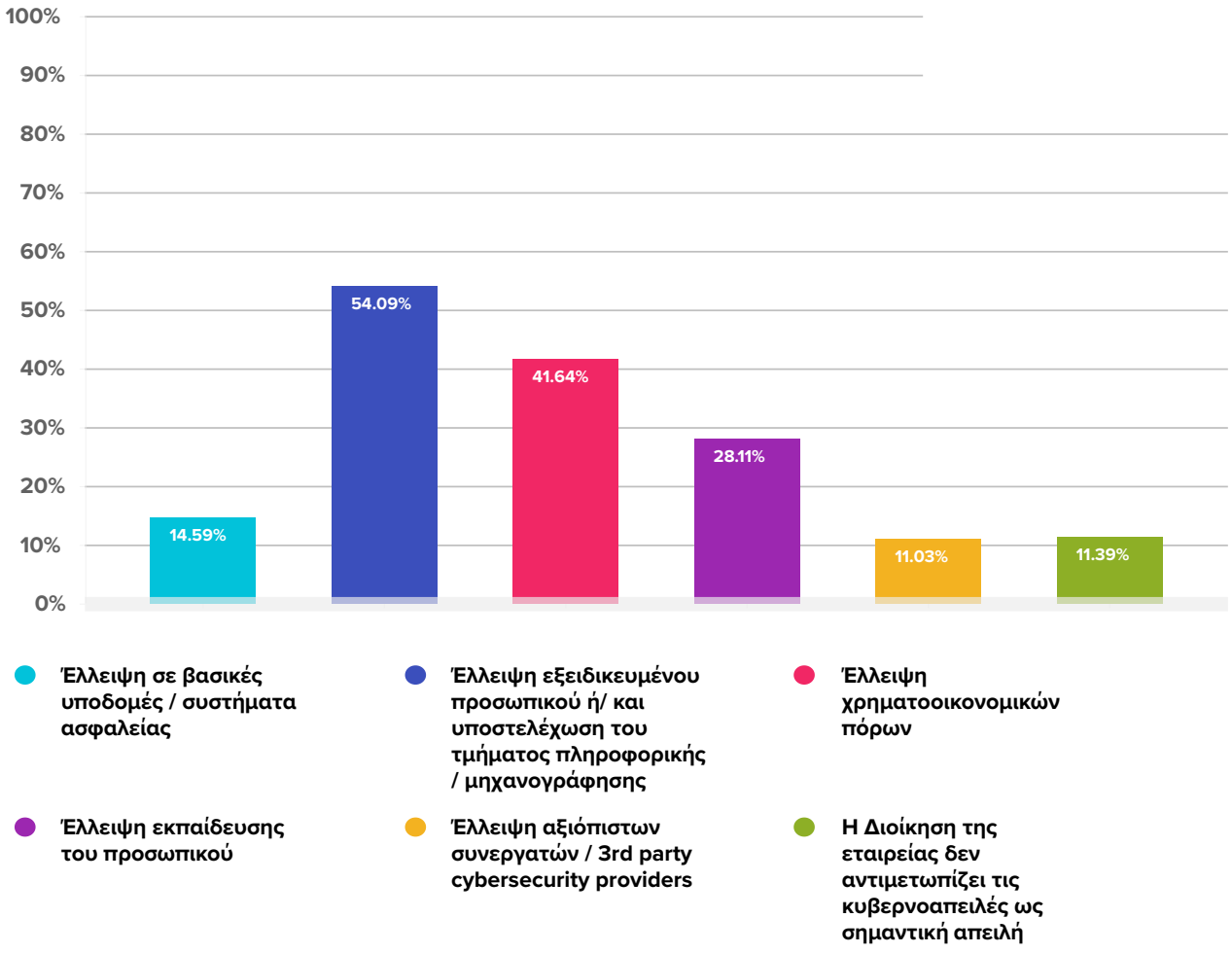


Choices	Response percent	Response count
Ναι, πραγματοποιούμε προσομοιώσεις επιθέσεων τακτικά (π.χ. Ανά εξάμηνο / χρόνο)	34.88%	98
Ναι, έχουμε πραγματοποιήσει προσομοιώσεις, αλλά όχι σε τακτική βάση	27.05%	76
Όχι, αλλά σχεδιάζουμε να το κάνουμε στο μέλλον	18.86%	53
Όχι, δεν έχουμε πραγματοποιήσει ποτέ προσομοίωση	11.03%	31
Δεν γνωρίζω	8.19%	23

Μόνο το 35% κάνει τακτικές ασκήσεις. Παρά την πρόοδο, η πρακτική ετοιμότητα δεν είναι πάντα επαρκής.

Ποιοι παράγοντες εμποδίζουν την επιχείρηση σας να οικοδομήσει ένα ολοκληρωμένο πλάνο κυβερνοασφάλειας; (έως 2 επιλογές)

Q24



Choices	Response percent	Response count
Έλλειψη σε βασικές υποδομές / συστήματα ασφαλείας	14.59%	41
Έλλειψη εξειδικευμένου προσωπικού ή/ και υποστελέχωση του τμήματος πληροφορικής / μηχανογράφησης	54.09%	152
Έλλειψη χρηματοοικονομικών πόρων	41.64%	117
Έλλειψη εκπαίδευσης του προσωπικού	28.11%	79
Έλλειψη αξιόπιστων συνεργατών / 3rd party cybersecurity providers	11.03%	31
Η Διοίκηση της εταιρείας δεν αντιμετωπίζει τις κυβερνοαπειλές ως σημαντική απειλή	11.39%	32

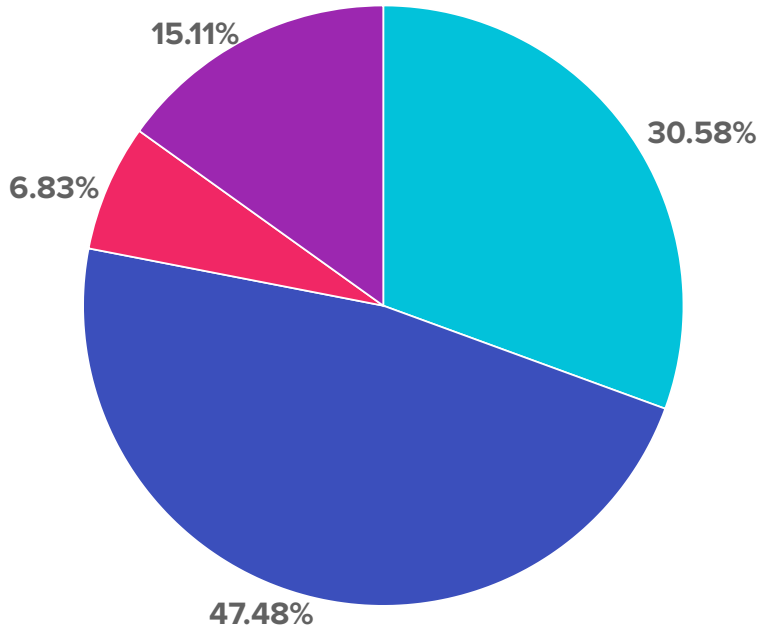
Βασικά εμπόδια: έλλειψη προσωπικού (54%) και οικονομικοί πόροι (42%). Η εκπαίδευση προσωπικού παραμένει επίσης πρόκληση (28%).

The State of Cybersecurity 2025

ESG και στρατηγική κυβερνοασφάλειας

Q25

Θεωρείτε ότι η κυβερνοασφάλεια συνδέεται με τους στόχους βιώσιμης ανάπτυξης (ESG) του οργανισμού σας, ή όχι;

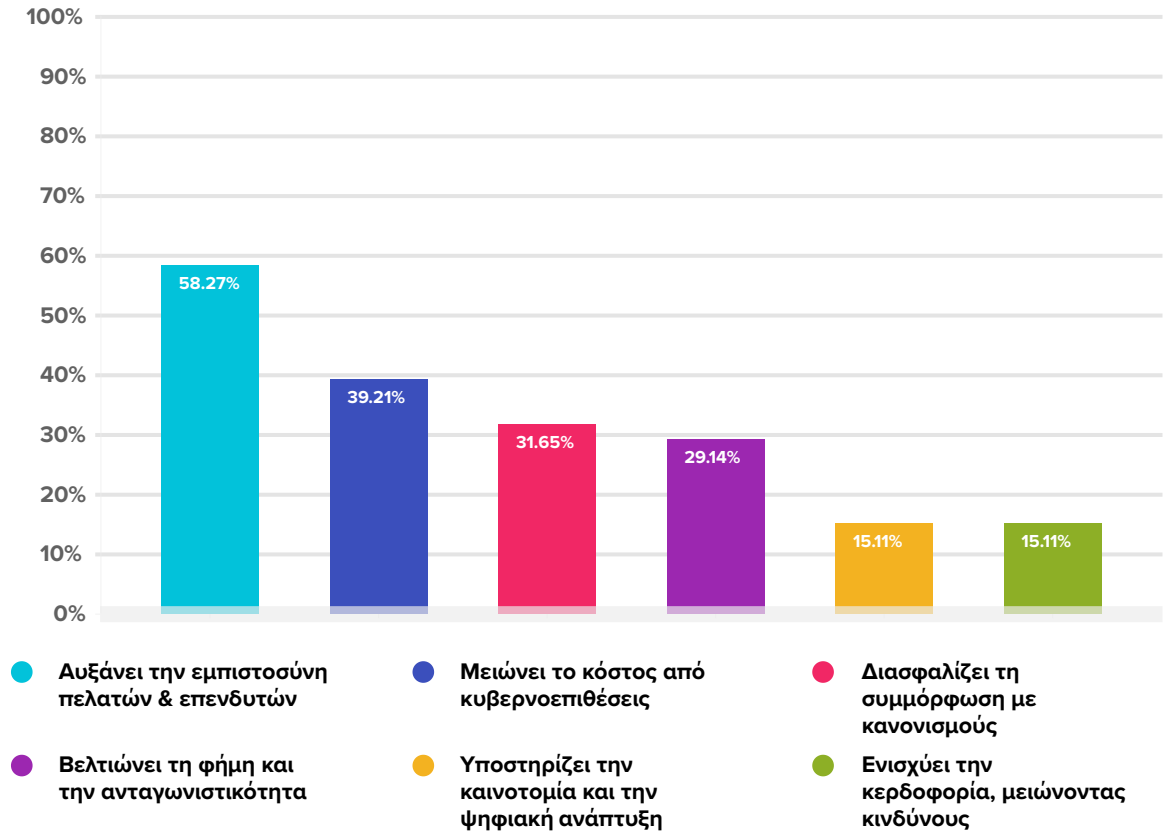


Choices	Response percent	Response count
Ναι, σε μεγάλο βαθμό. Η κυβερνοασφάλεια αποτελεί βασικό στοιχείο της ESG στρατηγικής μας	30.58%	85
Ναι, σε κάποιο βαθμό. Υπάρχει σύνδεση, αλλά δεν αποτελεί πρωταρχική προτεραιότητα.	47.48%	132
Όχι, δεν τη θεωρούμε σχετική με τους ESG στόχους μας.	6.83%	19
Δεν γνωρίζω	15.11%	42

Σχεδόν 80% αναγνωρίζει σχέση μεταξύ ESG και κυβερνοασφάλειας. Το 31% τη θεωρεί βασικό στοιχείο στρατηγικής.

Q26

Πώς συμβάλλει η χρήση υπηρεσιών κυβερνοασφάλειας στην αειφορία μιας εταιρείας; (έως 2 επιλογές)



Choices	Response percent	Response count
Αυξάνει την εμπιστοσύνη πελατών & επενδυτών	58.27%	162
Μειώνει το κόστος από κυβερνοεπιθέσεις	39.21%	109
Διασφαλίζει τη συμμόρφωση με κανονισμούς	31.65%	88
Βελτιώνει τη φήμη και την ανταγωνιστικότητα	29.14%	81
Υποστηρίζει την καινοτομία και την ψηφιακή ανάπτυξη	15.11%	42
Ενισχύει την κερδοφορία, μειώνοντας κινδύνους	15.11%	42

Κυρίως ενισχύει την εμπιστοσύνη πελατών/επενδυτών (58%) και μειώνει το κόστος από επιθέσεις (39%). Παράλληλα διασφαλίζει συμμόρφωση και φήμη.

About Pylones Hellas

Η Pylones Hellas είναι διεθνής εταιρεία τεχνολογίας με πάνω από 25 χρόνια εμπειρίας στην Ελλάδα και την Κύπρο. Ειδικεύεται στον σχεδιασμό και την υλοποίηση λύσεων πληροφορικής υποδομής, δικτύωσης και ασφάλειας, εστιάζοντας στην αξιοπιστία, την ανθεκτικότητα, την ταχύτητα και την ασφάλεια των δεδομένων. Με ισχυρές συνεργασίες με κορυφαίους τεχνολογικούς παρόχους, η Pylones Hellas υποστηρίζει επιχειρήσεις στη ψηφιακή τους μεταμόρφωση.

Special thank to:

1. RED.comm

Η RED.comm είναι ανεξάρτητη εταιρεία επικοινωνίας με έδρα την Αθήνα και μέλος του GlobalCom PR Network, ενός διεθνούς δικτύου με παρουσία σε πάνω από 100 χώρες. Ειδικεύεται στον στρατηγικό σχεδιασμό, τις δημόσιες σχέσεις, τα ψηφιακά μέσα και την οργάνωση εκδηλώσεων, με βαθιά γνώση σε τομείς όπως η κυβερνοασφάλεια και οι τεχνολογίες πληροφορικής.

2. IT Security Pro

Η IT Security Pro είναι η μοναδική ελληνική B2B έκδοση περιοδικού που εστιάζει στις υποδομές πληροφορικής και την ψηφιακή ασφάλεια. Απευθύνεται σε επαγγελματίες IT και οργανισμούς του ιδιωτικού και δημόσιου τομέα, παρέχοντας ενημέρωση για σύγχρονες τεχνολογίες, στρατηγικές και τάσεις στον τομέα της κυβερνοασφάλειας. Διοργανώνει επίσης το συνέδριο Infocom Security, το μεγαλύτερο event στην Ελλάδα για την ασφάλεια πληροφοριών.

pylones*

www.pylones.gr
LinkedIn: Pylones Hellas SA
info@pylones.gr
96 Marinou Antipa, 142 35, Nea Ionia,
Athens, Greece
+30 210 7483700