The State of cybersecurity 2023

437
Total Responses

437 Completed Responses

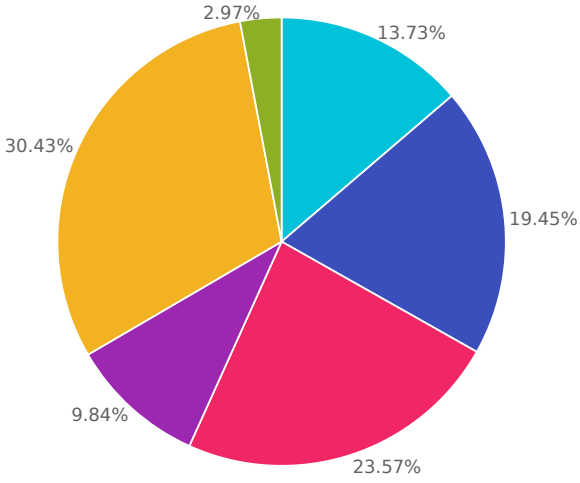
0 Partial Responses

4248
Survey Visits

Q1

Πόσα άτομα απασχολεί η εταιρεία / οργανισμός που εργάζεστε;

Answered: 437 Skipped: 0

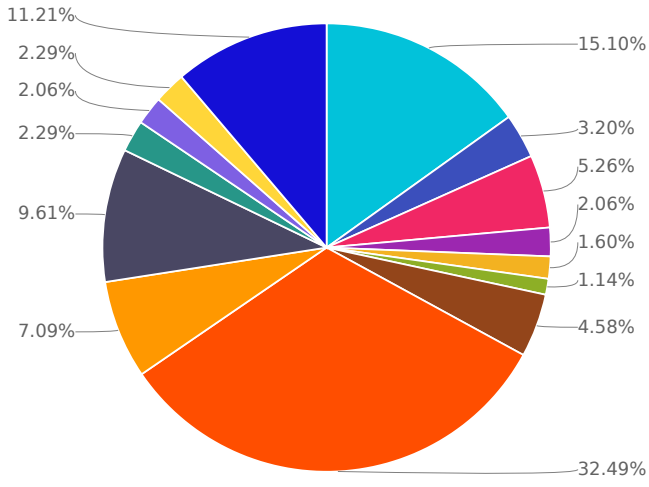


Choices	Response percent	Response count
Από 1 έως 10 εργαζόμενους	13.73%	60
Από 11 έως 50 εργαζόμενους	19.45%	85
Από 51 έως 250 εργαζόμενους	23.57%	103
Από 251 έως 500 εργαζόμενους	9.84%	43
Περισσότερους από 500 εργαζόμενους	30.43%	133
Άλλο (Παρακαλώ σημειώστε)	2.97%	13

Q2

Σε ποιον επαγγελματικό κλάδο ανήκει η εταιρεία σας / που εργάζεστε.

Answered: 437 Skipped: 0



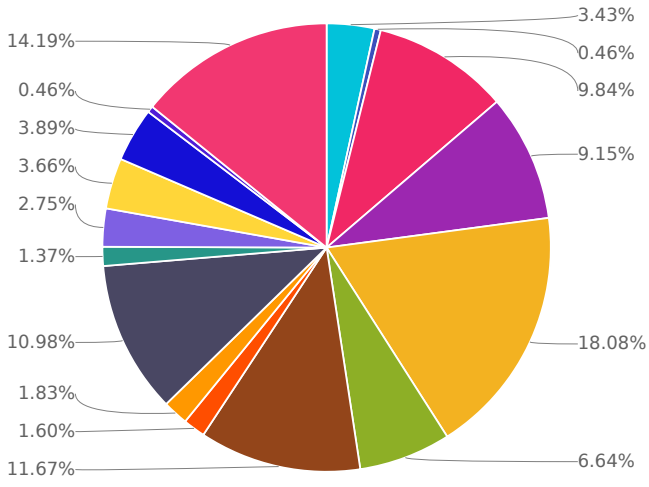
- Δημόσιος Τομέας / Οργανισμός
- Εκπαίδευση
- Εμπόριο / Λιανική / E-commerce
- Ενέργειας
- Κατασκευαστικός
- Μεταφορές / Logistics
- Ναυτιλία
- Τεχνολογία Πληροφορικής
- Τηλεπικοινωνίες
- Τραπεζικός / Χρηματοοικονομικός
- Υγεία/Φροντίδα υγείας
- Φιλοξενίας / Εστίασης / Διασκέδασης
- Software House / Development
- Άλλο (Παρακαλώ σημειώστε)

Choices	Response percent	Response count
Δημόσιος Τομέας / Οργανισμός	15.10%	66
Εκπαίδευση	3.20%	14
Εμπόριο / Λιανική / E-commerce	5.26%	23
Ενέργειας	2.06%	9
Κατασκευαστικός	1.60%	7
Μεταφορές / Logistics	1.14%	5
Ναυτιλία	4.58%	20
Τεχνολογία Πληροφορικής	32.49%	142
Τηλεπικοινωνίες	7.09%	31
Τραπεζικός / Χρηματοοικονομικός	9.61%	42
Υγεία/Φροντίδα υγείας	2.29%	10
Φιλοξενίας / Εστίασης / Διασκέδασης	2.06%	9
Software House / Development	2.29%	10
Άλλο (Παρακαλώ σημειώστε)	11.21%	49

Q3

Ποια είναι η επαγγελματική σας ιδιότητα;

Answered: 437 Skipped: 0



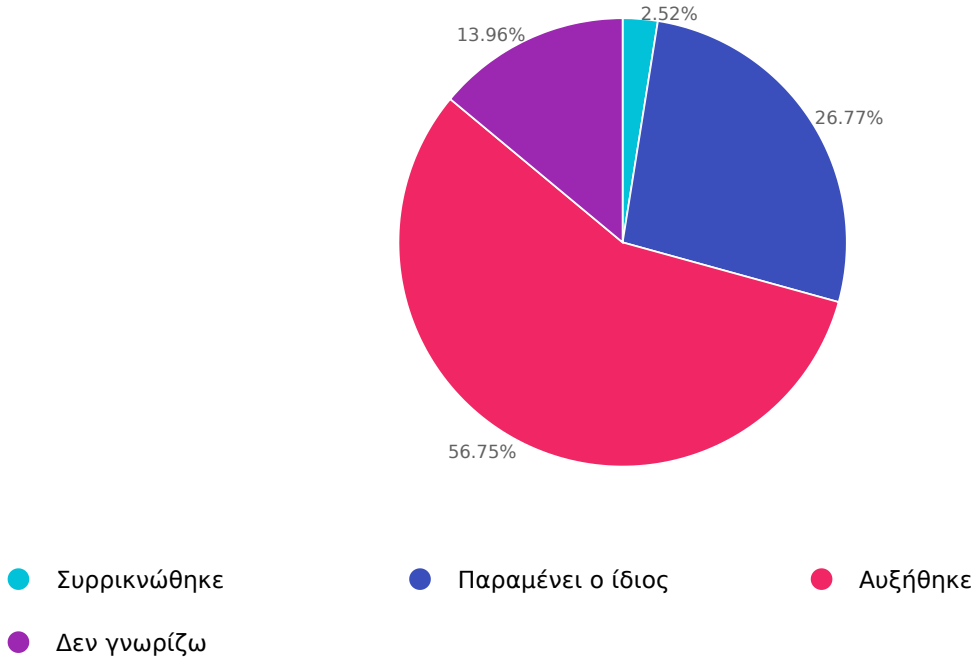
- CEO
- CCO
- CISO / CIO
- IT Consultant / Partner / Reseller
- IT Security
- IT Network
- IT Administrator
- Developer
- Analyst
- Sales / Business Development
- Finance / Procurement
- HR
- Business Operations
- Student / Researcher
- Άνεργη / ος
- Άλλο (Παρακαλώ σημειώστε)

Choices	Response percent	Response count
CEO	3.43%	15
CCO	0.46%	2
CISO / CIO	9.84%	43
IT Consultant / Partner / Reseller	9.15%	40
IT Security	18.08%	79
IT Network	6.64%	29
IT Administrator	11.67%	51
Developer	1.60%	7
Analyst	1.83%	8
Sales / Business Development	10.98%	48
Finance / Procurement	1.37%	6
HR	2.75%	12
Business Operations	3.66%	16
Student / Researcher	3.89%	17
Άνεργη / ος	0.46%	2
Άλλο (Παρακαλώ σημειώστε)	14.19%	62

Q4

Πως μεταβλήθηκε ο προϋπολογισμός ασφάλειας IT (cyber-budget) της εταιρείας σας για τους προηγούμενους 12 μήνες;

Answered: 437 Skipped: 0

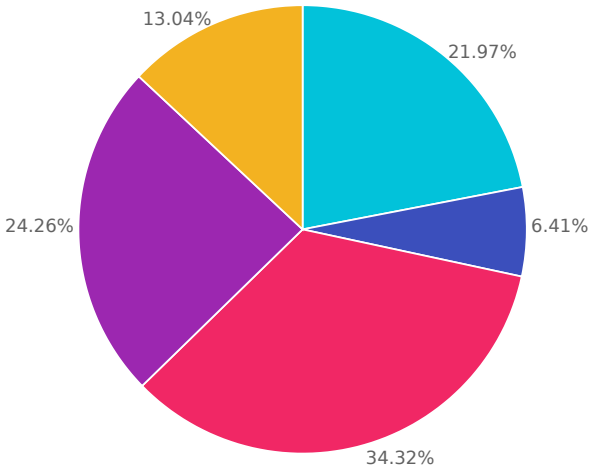


Choices	Response percent	Response count
Συρρικνώθηκε	2.52%	11
Παραμένει ο ίδιος	26.77%	117
Αυξήθηκε	56.75%	248
Δεν γνωρίζω	13.96%	61

Q5

Αντιμετώπισε η εταιρεία σας κάποια κυβερνο-απειλή ή παραβίαση ασφάλειας στον κυβερνοχώρο ή στο μηχανογραφικό της σύστημα;

Answered: 437 Skipped: 0

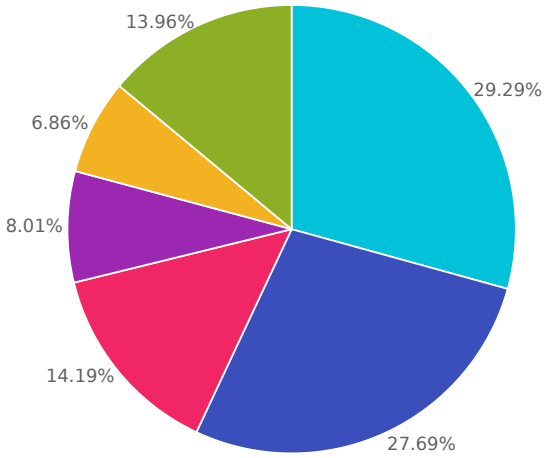


Choices	Response percent	Response count
ΝΑΙ, χωρίς συνέπειες	21.97%	96
ΝΑΙ, με συνέπειες	6.41%	28
ΟΧΙ, φροντίζει η εταιρεία την ασφάλεια των συστημάτων	34.32%	150
ΟΧΙ, δεν έτυχε	24.26%	106
Δεν γνωρίζω	13.04%	57

Q6

Σε πόσο διάστημα θεωρείτε ότι η εταιρεία μπορεί να είναι full operational μετά από μια μεγάλης κλίμακας κυβερνο-επίθεση;

Answered: 437 Skipped: 0



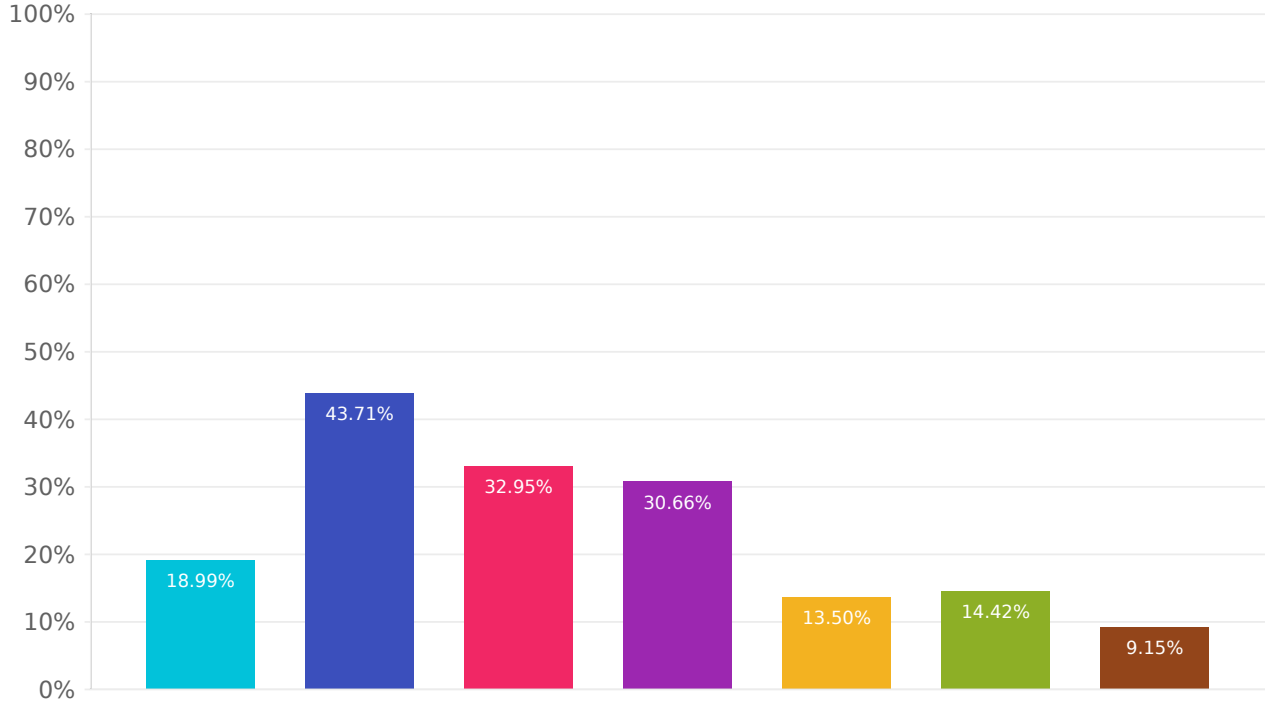
Λιγότερο από 3 μέρες
Λιγότερο από μια εβδομάδα
Λιγότερο από 1 μήνα
1 με 3 μήνες
Περισσότερο από 3 μήνες
Δεν γνωρίζω

Choices	Response percent	Response count
Λιγότερο από 3 μέρες	29.29%	128
Λιγότερο από μια εβδομάδα	27.69%	121
Λιγότερο από 1 μήνα	14.19%	62
1 με 3 μήνες	8.01%	35
Περισσότερο από 3 μήνες	6.86%	30
Δεν γνωρίζω	13.96%	61

Q7

Ποιοι παράγοντες εμποδίζουν την επιχείρηση σας να οικοδομήσει ένα ολοκληρωμένο πλάνο κυβερνο-ασφάλειας; (2 επιλογές)

Answered: 437 Skipped: 0



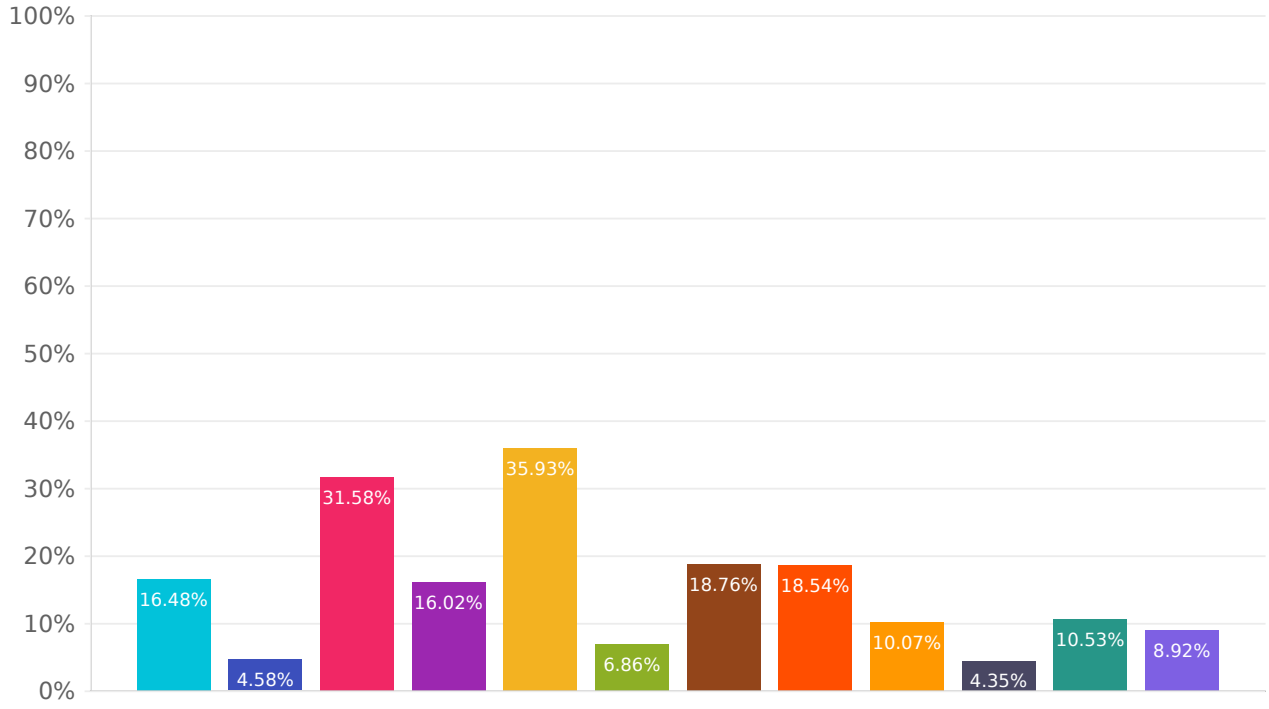
- Έλλειψη σε βασικές υποδομές - συστήματα ασφαλείας
- Έλλειψη εξειδικευμένου προσωπικού ή και υποστελέχωση του τμήματος πληροφορικής/ μηχανογράφησης
- Έλλειψη χρηματοοικονομικών πόρων
- Έλλειψη εκπαίδευσης του προσωπικού
- Έλλειψη αξιόπιστων συνεργατών/3rd party cybersecurity providers
- Η Διοίκηση της εταιρείας δεν αντιμετωπίζει τις κυβερνο-απειλές ως σημαντική απειλή
- Άλλο (Παρακαλώ διευκρινίστε)

Choices	Response percent	Response count
Έλλειψη σε βασικές υποδομές - συστήματα ασφαλείας	18.99%	83
Έλλειψη εξειδικευμένου προσωπικού ή και υποστελέχωση του τμήματος πληροφορικής/μηχανογράφησης	43.71%	191
Έλλειψη χρηματοοικονομικών πόρων	32.95%	144
Έλλειψη εκπαίδευσης του προσωπικού	30.66%	134
Έλλειψη αξιόπιστων συνεργατών/3rd party cybersecurity providers	13.50%	59
Η Διοίκηση της εταιρείας δεν αντιμετωπίζει τις κυβερνο-απειλές ως σημαντική απειλή	14.42%	63
Άλλο (Παρακαλώ διευκρινίστε)	9.15%	40

Q8

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

Answered: 437 Skipped: 0



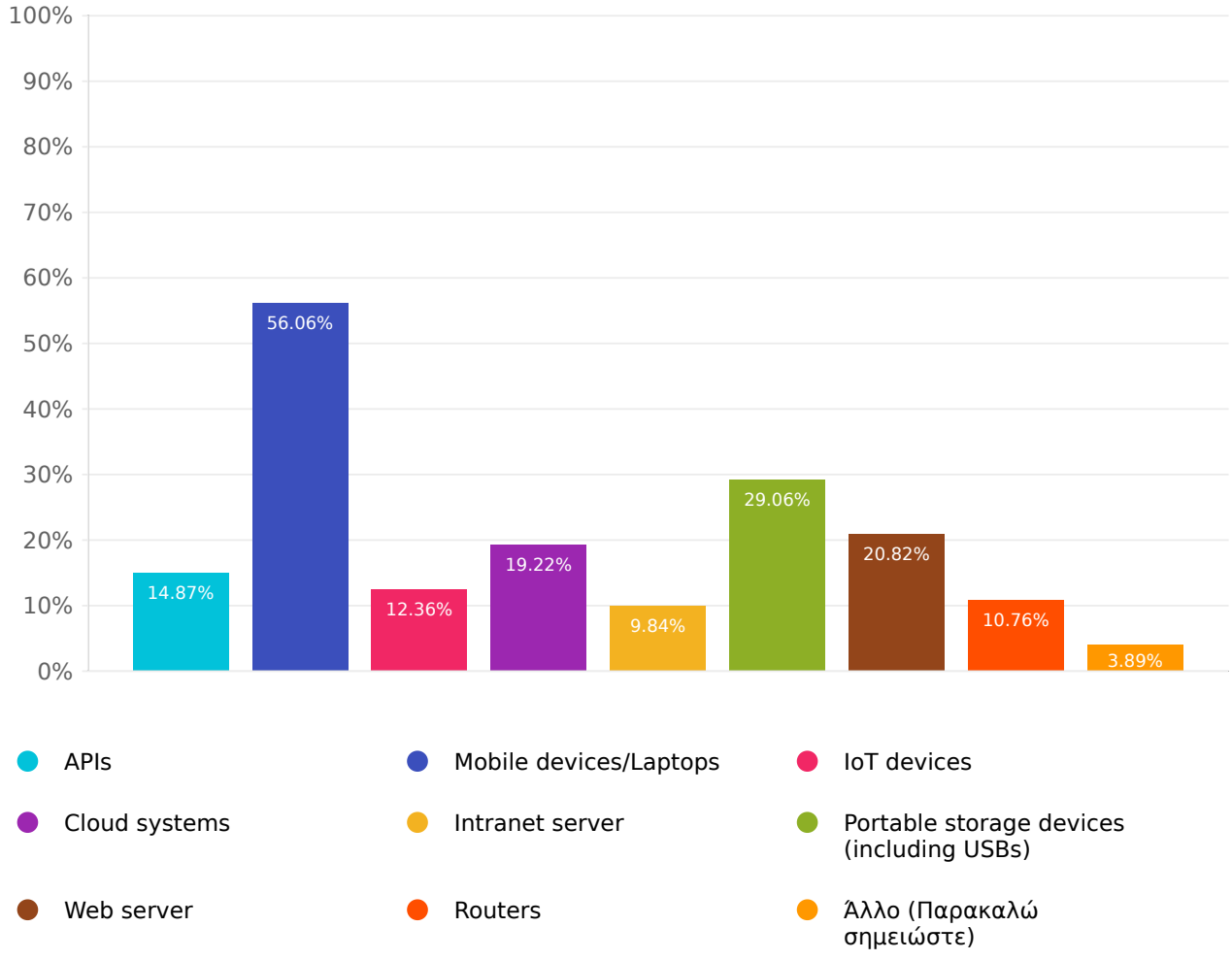
- Web – API attacks
- Identity Governance
- Business email compromise (BEC) /social engineering-related threats (Phishing)
- Compromised employee credentials
- Κακόβουλο λογισμικό (Malware)
- IOT Security
- Compromised Endpoints (Ransomware / Data exfiltration)
- Network Cyber-attacks
- Denial of services / Distributed Denial of services
- Supply-chain attacks
- Bring your own device (BYOD) system attacks
- Δεν γνωρίζω

Choices	Response percent	Response count
Web – API attacks	16.48%	72
Identity Governance	4.58%	20
Business email compromise (BEC) /social engineering-related threats (Phishing)	31.58%	138
Compromised employee credentials	16.02%	70
Κακόβουλο λογισμικό (Malware)	35.93%	157
IOT Security	6.86%	30
Compromised Endpoints (Ransomware / Data exfiltration)	18.76%	82
Network Cyber-attacks	18.54%	81
Denial of services / Distributed Denial of services	10.07%	44
Supply-chain attacks	4.35%	19
Bring your own device (BYOD) system attacks	10.53%	46
Δεν γνωρίζω	8.92%	39

Q9

Ποια σημεία εισόδου στο δίκτυο / συστήματα της επιχείρησής σας θεωρείτε πιο ευάλωτα; (2 επιλογές)

Answered: 437 Skipped: 0

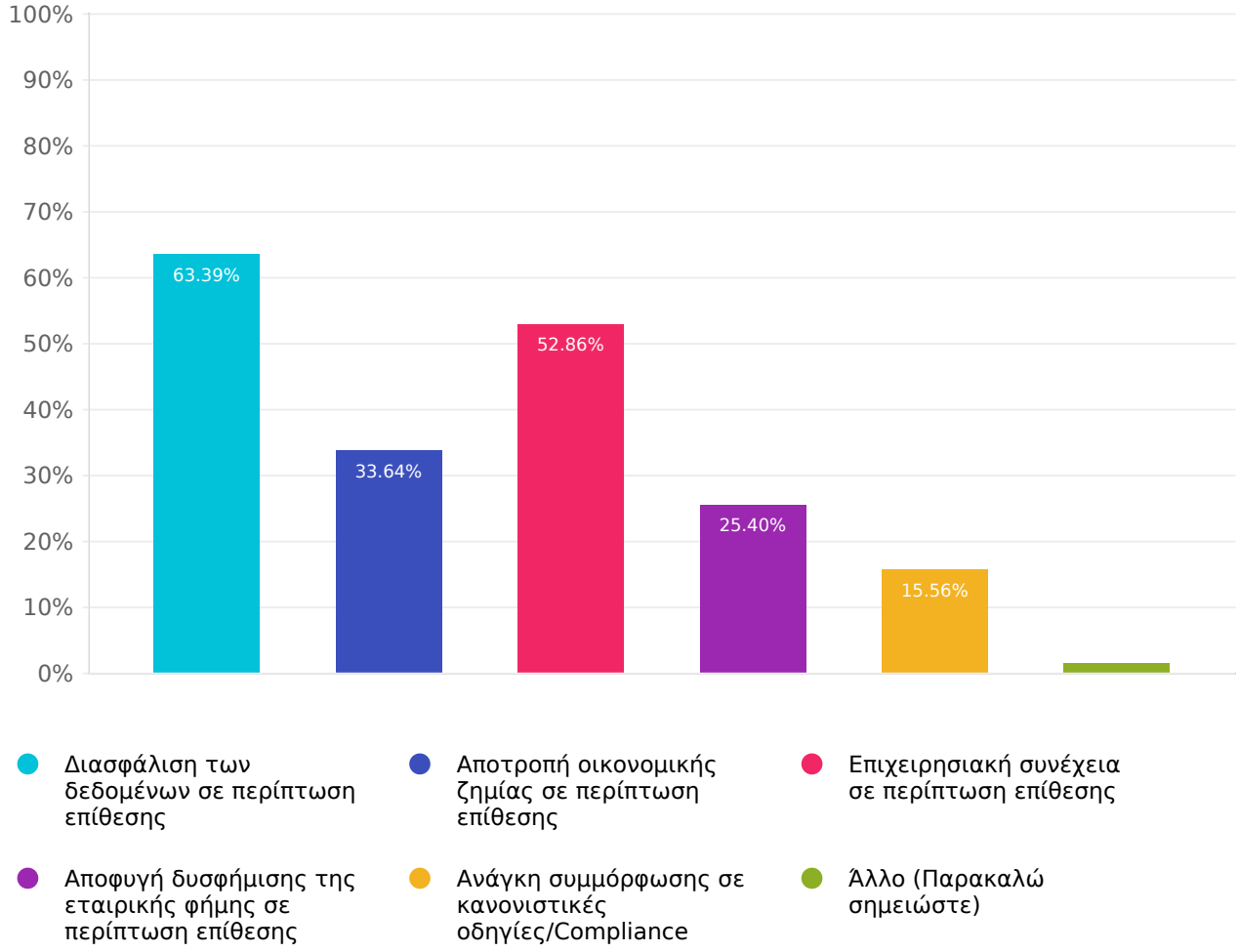


Choices	Response percent	Response count
APIs	14.87%	65
Mobile devices/Laptops	56.06%	245
IoT devices	12.36%	54
Cloud systems	19.22%	84
Intranet server	9.84%	43
Portable storage devices (including USBs)	29.06%	127
Web server	20.82%	91
Routers	10.76%	47
Άλλο (Παρακαλώ σημειώστε)	3.89%	17

Q10

Για ποιους λόγους οφείλει η επιχείρηση σας να επενδύσει στο Cybersecurity; (2 επιλογές)

Answered: 437 Skipped: 0

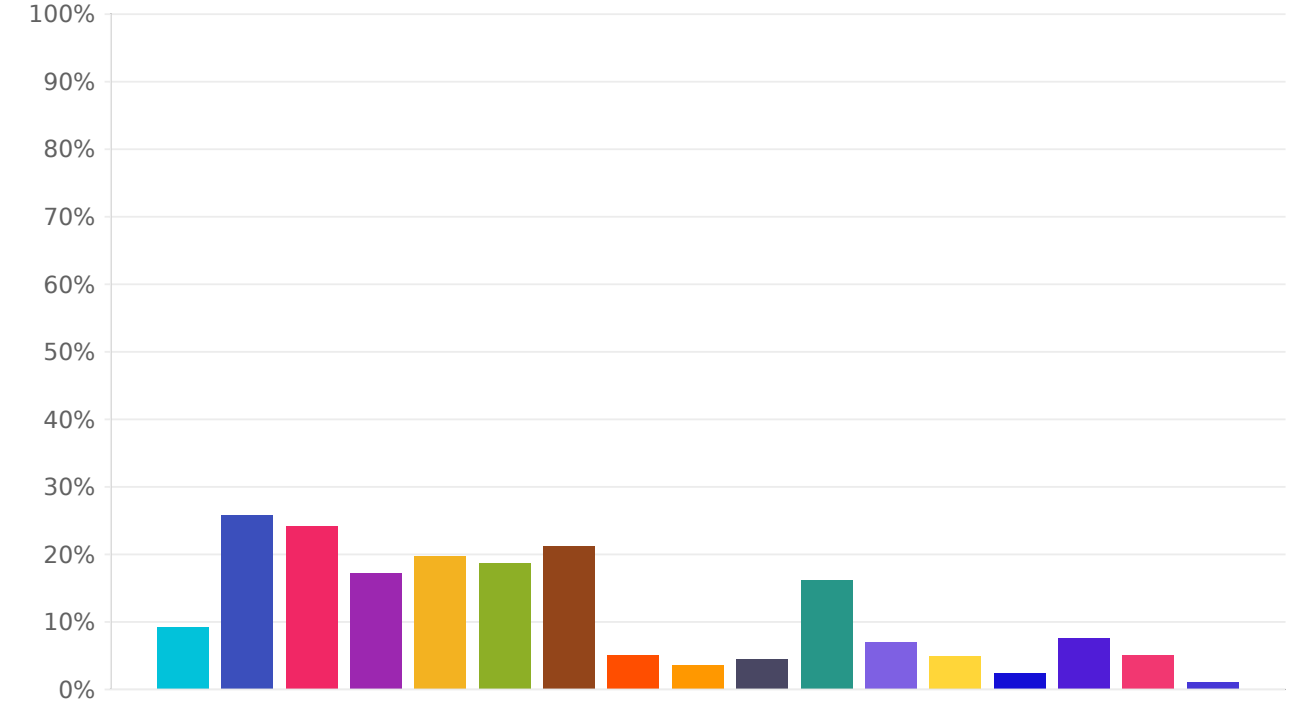


Choices	Response percent	Response count
Διασφάλιση των δεδομένων σε περίπτωση επίθεσης	63.39%	277
Αποτροπή οικονομικής ζημίας σε περίπτωση επίθεσης	33.64%	147
Επιχειρησιακή συνέχεια σε περίπτωση επίθεσης	52.86%	231
Αποφυγή δυσφήμισης της εταιρικής φήμης σε περίπτωση επίθεσης	25.40%	111
Ανάγκη συμμόρφωσης σε κανονιστικές οδηγίες/Compliance	15.56%	68
Άλλο (Παρακαλώ σημειώστε)	1.37%	6

Q11

Σε ποιο είδος/τομέα θα επενδύατε για καλύτερη κάλυψη στον τομέα του Cybersecurity; (2 επιλογές)

Answered: 437 Skipped: 0



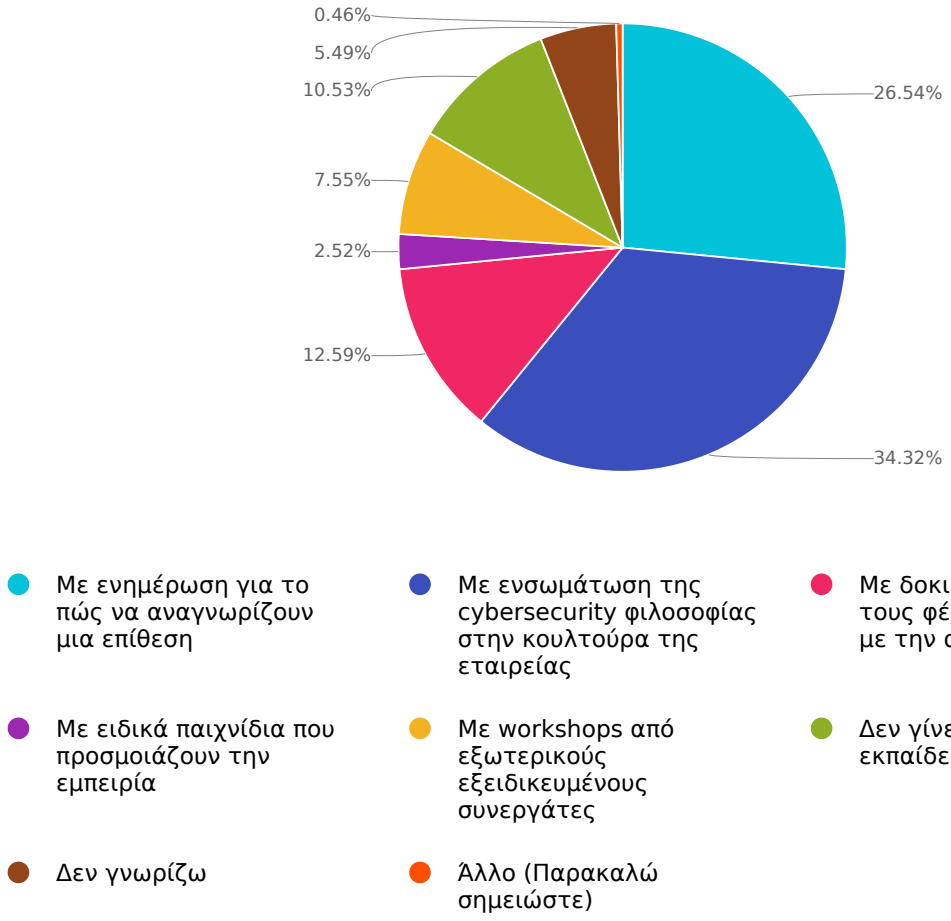
- API Security & Management
- Cloud Security
- Cyber security awareness training
- DLP (Data Loss Prevention) Security Solution
- Email Security and Protection
- Endpoint Security
- Firewall & Network Protection
- Identity & Access management (IDaaS)
- Identity Governance
- Incident response
- Security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

Choices	Response percent	Response count
API Security & Management	9.15%	40
Cloud Security	25.63%	112
Cyber security awareness training	24.03%	105
DLP (Data Loss Prevention) Security Solution	17.16%	75
Email Security and Protection	19.68%	86
Endpoint Security	18.54%	81
Firewall & Network Protection	21.05%	92
Identity & Access management (IDaaS)	5.03%	22
Identity Governance	3.43%	15
Incident response	4.35%	19
Security Operation Center (SOC)	16.02%	70
Threat intelligence	6.86%	30
Managed Security Services	4.81%	21
Privileged Access Management (PAM)	2.29%	10
Vulnerability management	7.55%	33
Web - Application Security	5.03%	22
Άλλο (Παρακαλώ σημειώστε)	0.92%	4

Q12

Με ποιον τρόπο εκπαιδεύει η εταιρεία το προσωπικό σε θέματα Cybersecurity;

Answered: 437 Skipped: 0

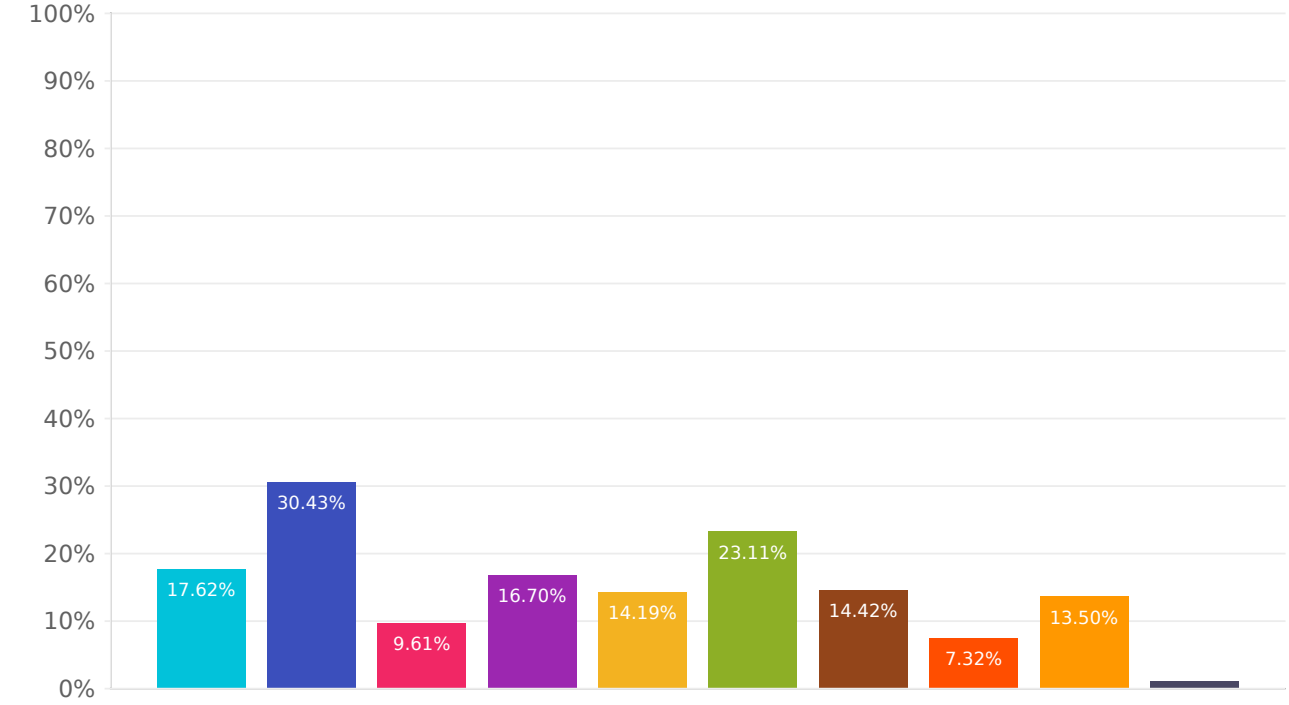


Choices	Response percent	Response count
Με ενημέρωση για το πώς να αναγνωρίζουν μια επίθεση	26.54%	116
Με ενσωμάτωση της cybersecurity φιλοσοφίας στην κουλτούρα της εταιρείας	34.32%	150
Με δοκιμαστικά test που τους φέρνουν σε επαφή με την απειλή	12.59%	55
Με ειδικά παιχνίδια που προσμοιάζουν την εμπειρία	2.52%	11
Με workshops από εξωτερικούς εξειδικευμένους συνεργάτες	7.55%	33
Δεν γίνεται κάποια εκπαίδευση	10.53%	46
Δεν γνωρίζω	5.49%	24
Άλλο (Παρακαλώ σημειώστε)	0.46%	2

Q13

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

Answered: 437 Skipped: 0



- Η ορατότητα και διαχείριση των περιουσιακών στοιχείων μου
- Ο εντοπισμός και η αντιμετώπιση περιστατικών ασφαλείας στο cloud
- Δεν γνωρίζω αν πληροί τους κανονισμούς συμμόρφωσης
- Η επένδυση σε εκπαίδευση του προσωπικού και σε εργαλεία ασφάλειας
- Η μη εξουσιοδοτημένης χρήσης του cloud
- Η ανάκτηση δεδομένων και η επιχειρησιακή συνέχεια
- Ο ελλιπής έλεγχος από πλευράς μου των διαδικασιών ασφάλειας που εφαρμόζονται
- Η δυσκολία όσον αφορά στο configuration
- Δεν γνωρίζω
- Άλλο (Παρακαλώ σημειώστε)

Choices	Response percent	Response count
Η ορατότητα και διαχείριση των περιουσιακών στοιχείων μου	17.62%	77
Ο εντοπισμός και η αντιμετώπιση περιστατικών ασφαλείας στο cloud	30.43%	133
Δεν γνωρίζω αν πληροί τους κανονισμούς συμμόρφωσης	9.61%	42
Η επένδυση σε εκπαίδευση του προσωπικού και σε εργαλεία ασφάλειας	16.70%	73
Η μη εξουσιοδοτημένης χρήσης του cloud	14.19%	62
Η ανάκτηση δεδομένων και η επιχειρησιακή συνέχεια	23.11%	101
Ο ελλιπής έλεγχος από πλευράς μου των διαδικασιών ασφάλειας που εφαρμόζονται	14.42%	63
Η δυσκολία όσον αφορά στο configuration	7.32%	32
Δεν γνωρίζω	13.50%	59
Άλλο (Παρακαλώ σημειώστε)	0.92%	4

Q14

Συμπληρώστε τα στοιχεία σας για να μπείτε στην κλήρωση για ένα δώρο (Προαιρετικά)

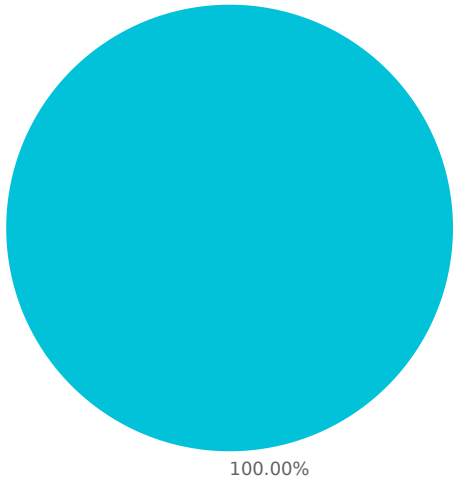
Answered: 395 Skipped: 42

Field label	Response percent	Response count
Ονοματεπώνυμο	98.73%	390 Responses
Τηλέφωνο	91.14%	360 Responses
Εταιρεία	80.51%	318 Responses
E-mail	97.47%	385 Responses

Q15

Αποδέχομαι τους Όρους & Προϋποθέσεις για τη συμμετοχή στο διαγωνισμό.

Answered: 434 Skipped: 3



Choices	Response percent	Response count
Yes	100.00%	434
No	0.00%	0