

## The State of cybersecurity 2022

---

**237**

Total Responses

237 Completed Responses

0 Partial Responses

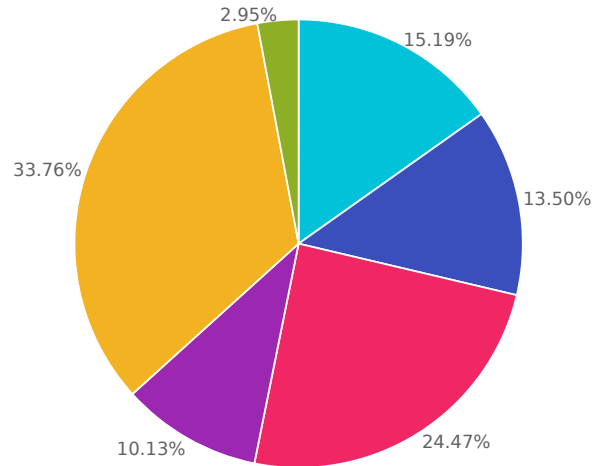
**941**

Survey Visits

Q1

**Πόσα άτομα απασχολεί η εταιρεία / οργανισμός που εργάζεστε;**

Answered: 237 Skipped: 0



● Από 1 έως 10  
εργαζόμενους

● Από 11 έως 50  
εργαζόμενους

● Από 51 έως 250  
εργαζόμενους

● Από 250 έως 500  
εργαζόμενους

● Περισσότερους από 500  
εργαζόμενους

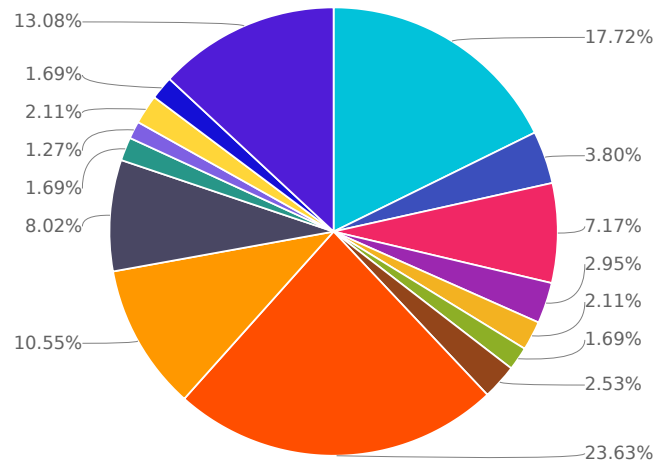
● Άλλο (Παρακαλώ  
σημειώστε)

Choices	Response percent	Response count
Από 1 έως 10 εργαζόμενους	15.19%	36
Από 11 έως 50 εργαζόμενους	13.50%	32
Από 51 έως 250 εργαζόμενους	24.47%	58
Από 250 έως 500 εργαζόμενους	10.13%	24
Περισσότερους από 500 εργαζόμενους	33.76%	80
Άλλο (Παρακαλώ σημειώστε)	2.95%	7

Q2

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

Answered: 237 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

Startup

Άλλο (Παρακαλώ σημειώστε)

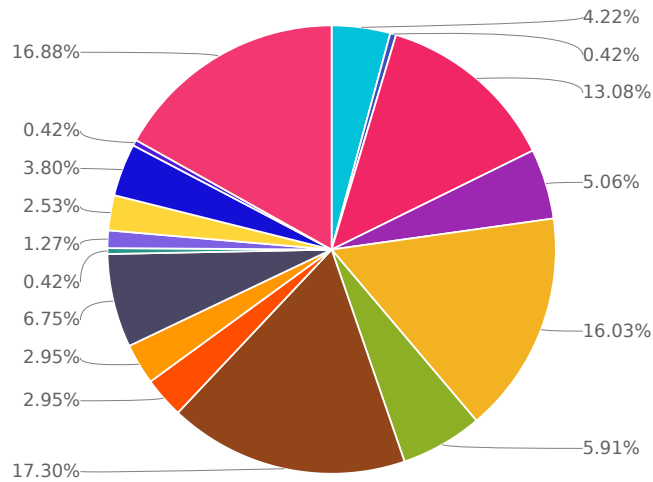
Choices	Response percent	Response count
Δημόσιος Τομέας / Οργανισμός	17.72%	42
Εκπαίδευση	3.80%	9
Εμπόριο / Λιανική / e-commerce	7.17%	17
Ενέργειας	2.95%	7
Κατασκευαστικός	2.11%	5
Μεταφορές / Logistics	1.69%	4
Ναυτιλία	2.53%	6
Τεχνολογία Πληροφορικής	23.63%	56
Τηλεπικοινωνίες	10.55%	25
Τραπεζικός / Χρηματοοικονομικός	8.02%	19
Υγεία/Φροντίδα υγείας	1.69%	4
Φιλοξενίας / Εστίασης / διασκέδασης	1.27%	3
Software House / Development	2.11%	5
Startup	1.69%	4
Άλλο (Παρακαλώ σημειώστε)	13.08%	31

---

Q3

### Ποια είναι η επαγγελματική σας ιδιότητα;

Answered: 237 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)

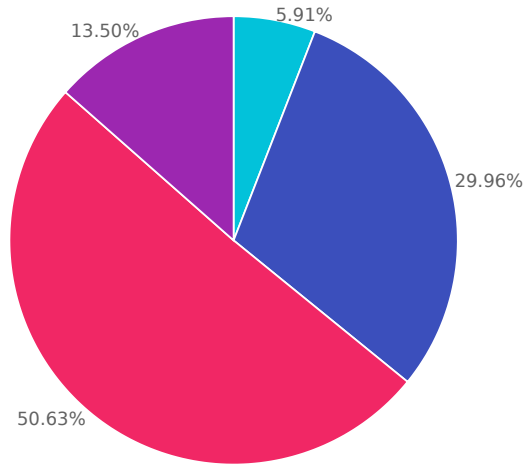
Choices	Response percent	Response count
CEO	4.22%	10
CCO	0.42%	1
CISO / CIO	13.08%	31
IT Consultant / Partner / Reseller	5.06%	12
IT Security	16.03%	38
IT Network	5.91%	14
IT Administrator	17.30%	41
Developer	2.95%	7
Analyst	2.95%	7
Sales / Business Development	6.75%	16
Finance / Procurement	0.42%	1
HR	1.27%	3
Business Operations	2.53%	6
Student / Researcher	3.80%	9
Άνεργη / ος	0.42%	1
Άλλο (Παρακαλώ σημειώστε)	16.88%	40

---

Q4

**Πως μεταβλήθηκε ο προϋπολογισμός ασφάλειας IT (cyber-budget) της εταιρείας σας για τους προηγούμενους 12 μήνες, με βάσει την εικόνα που έχετε;**

Answered: 237 Skipped: 0



● Συρρικνώθηκε  
● Δεν έχω εικόνα

● Παραμένει ο ίδιος

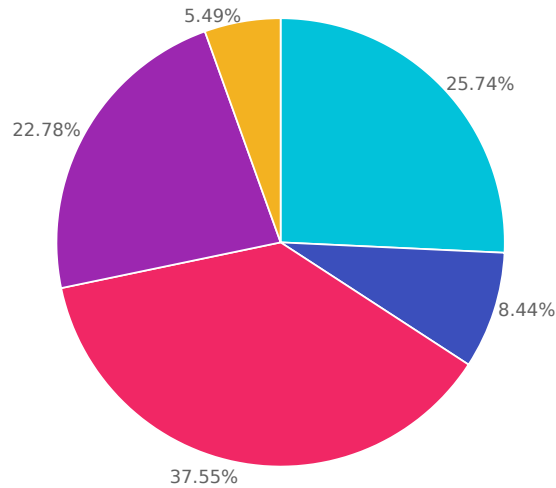
● Αυξήθηκε

Choices	Response percent	Response count
Συρρικνώθηκε	5.91%	14
Παραμένει ο ίδιος	29.96%	71
Αυξήθηκε	50.63%	120
Δεν έχω εικόνα	13.50%	32

Q5

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

Answered: 237 Skipped: 0



● ΝΑΙ, χωρίς συνέπειες

● ΝΑΙ, με συνέπειες

● ΟΧΙ, φροντίζει η εταιρεία την ασφάλεια των συστημάτων

● ΟΧΙ, δεν έτυχε

● Δεν γνωρίζω

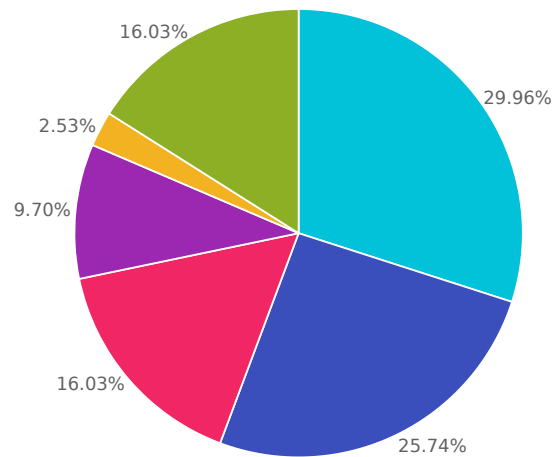
Choices	Response percent	Response count
ΝΑΙ, χωρίς συνέπειες	25.74%	61
ΝΑΙ, με συνέπειες	8.44%	20
ΟΧΙ, φροντίζει η εταιρεία την ασφάλεια των συστημάτων	37.55%	89
ΟΧΙ, δεν έτυχε	22.78%	54
Δεν γνωρίζω	5.49%	13



Q6

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

Answered: 237 Skipped: 0



● Λιγότερο από 3 μέρες

● Λιγότερο από μια εβδομάδα

● Λιγότερο από 1 μήνα

● 1 με 3 μήνες

● Περισσότερο από 3 μήνες

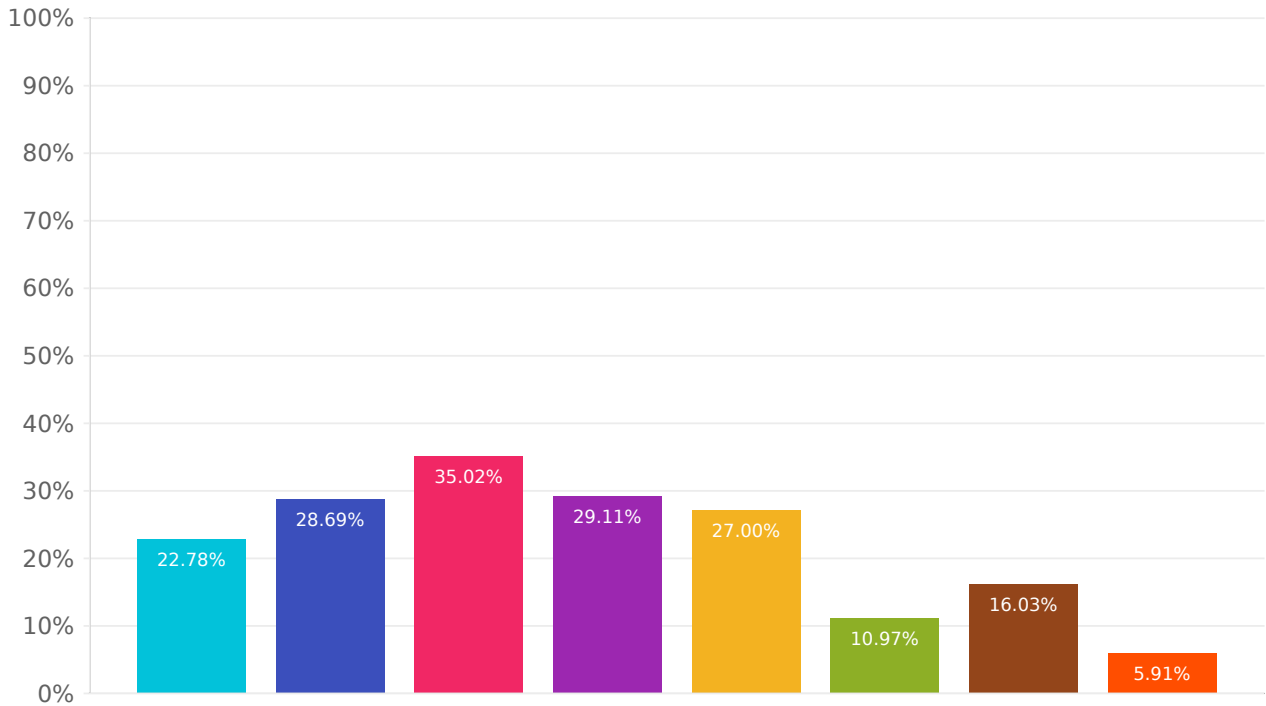
● Δεν γνωρίζω

Choices	Response percent	Response count
Λιγότερο από 3 μέρες	29.96%	71
Λιγότερο από μια εβδομάδα	25.74%	61
Λιγότερο από 1 μήνα	16.03%	38
1 με 3 μήνες	9.70%	23
Περισσότερο από 3 μήνες	2.53%	6
Δεν γνωρίζω	16.03%	38

Q7

### Ποιοι είναι οι κύριοι παράγοντες που εμποδίζουν την επιχείρηση σας να οικοδομήσει ένα ολοκληρωμένο πλάνο κυβερνο-ασφάλειας; (2 επιλογές)

Answered: 237 Skipped: 0



● Έλλειψη σε βασικές υποδομές - συστήματα ασφαλείας

● Έλλειψη εξειδικευμένου προσωπικού

● Υπο-στελέχωση του τμήματος πληροφορικής/μηχανογράφησης

● Έλλειψη χρηματοοικονομικών πόρων

● Έλλειψη εκπαίδευσης του προσωπικού

● Έλλειψη αξιόπιστων συνεργατών/3rd party cybersecurity providers

● Η Διοίκηση της εταιρίας δεν αντιμετωπίζει τις κυβερνο-απειλές ως σημαντική απειλή

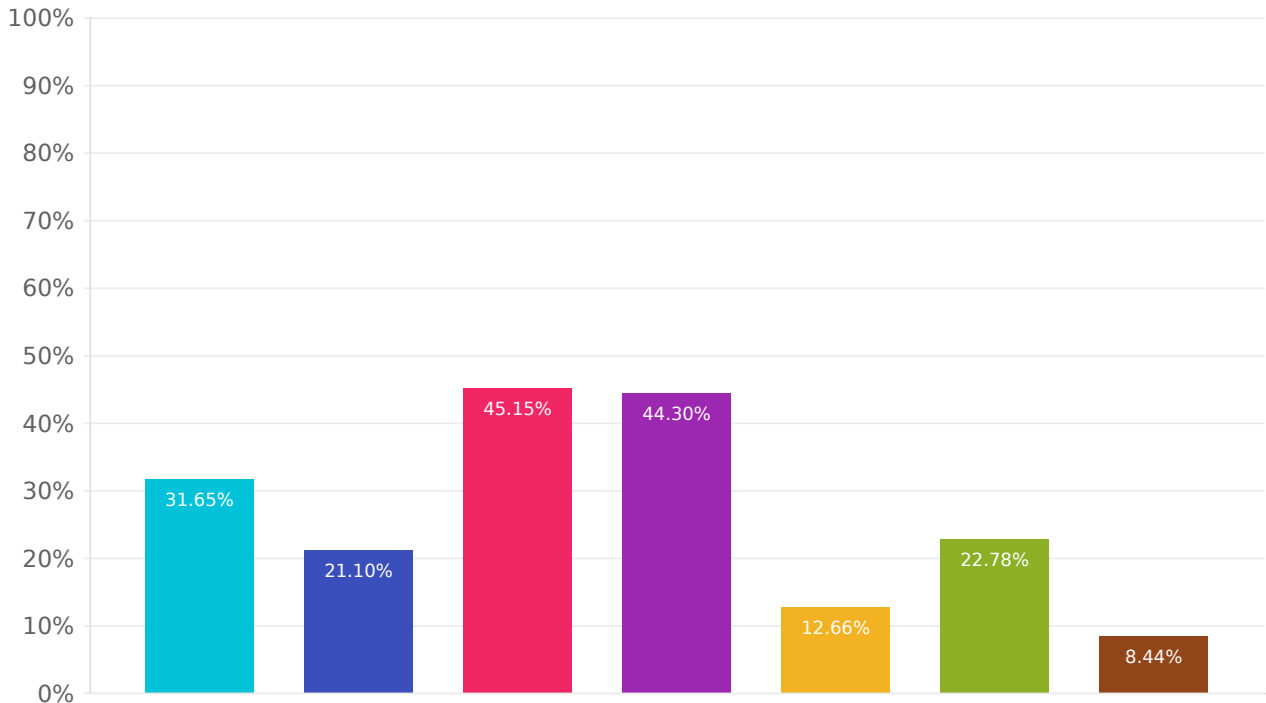
● Άλλο (Παρακαλώ διευκρινίστε)

Choices	Response percent	Response count
Έλλειψη σε βασικές υποδομές - συστήματα ασφαλείας	22.78%	54
Έλλειψη εξειδικευμένου προσωπικού	28.69%	68
Υπο-στελέχωση του τμήματος πληροφορικής/μηχανογράφησης	35.02%	83
Έλλειψη χρηματο-οικονομικών πόρων	29.11%	69
Έλλειψη εκπαίδευσης του προσωπικού	27.00%	64
Έλλειψη αξιόπιστων συνεργατών/3rd party cybersecurity providers	10.97%	26
Η Διοίκηση της εταιρίας δεν αντιμετωπίζει τις κυβερνο-απειλές ως σημαντική απειλή	16.03%	38
Άλλο (Παρακαλώ διευκρινίστε)	5.91%	14

---

## Ποια στάδια του cybersecurity lifecycle καλύπτει αποτελεσματικότερα το πλάνο κυβερνοασφάλειας της επιχείρησής σας; (2 επιλογές)

Answered: 237 Skipped: 0



● Risk management  
(Διαχείριση κινδύνου)

● Identification  
(Αναγνώριση / Διάγνωση κινδύνου)

● Protection (Προστασία  
έναντι κινδύνου)

● Monitoring & Detection  
(Παρακολούθηση &  
Ανίχνευση κινδύνου)

● Respond (Απόκριση σε  
επίθεση)

● Recovery (Ανάκτηση /  
Επαναφορά μετά από  
επίθεση)

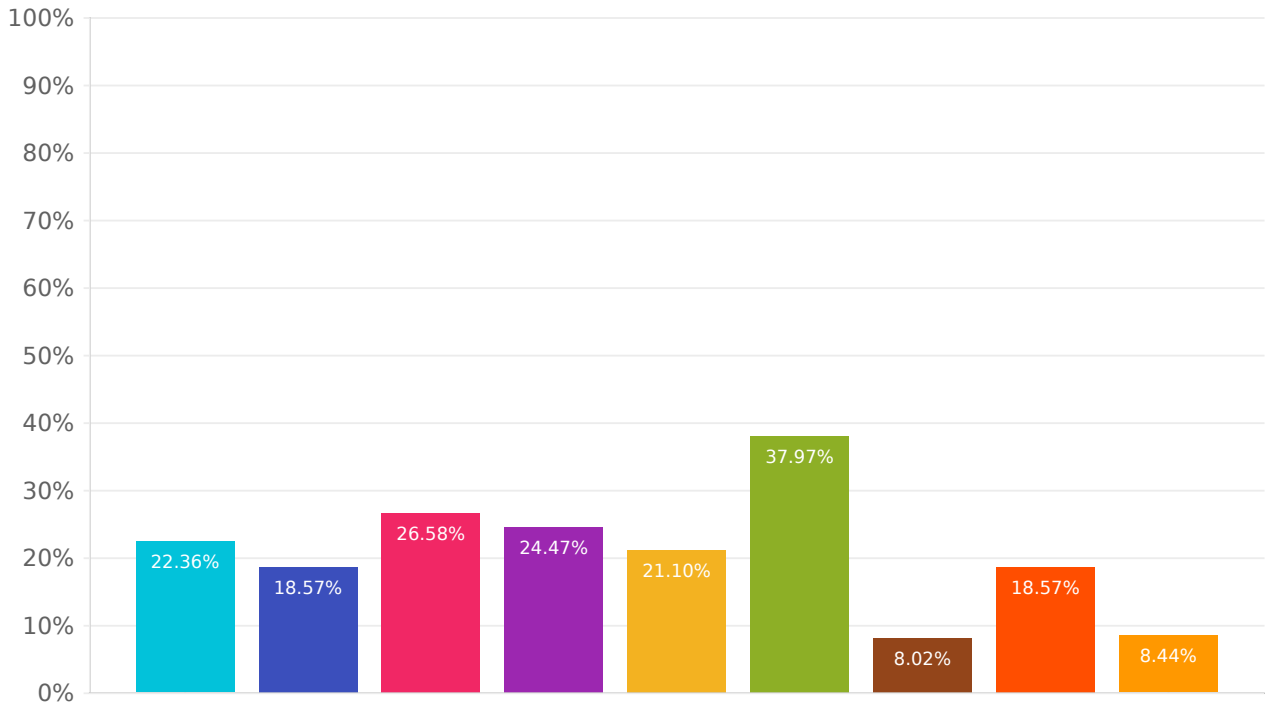
● Δεν γνωρίζω

Choices	Response percent	Response count
Risk management (Διαχείριση κινδύνου)	31.65%	75
Identification (Αναγνώριση / Διάγνωση κινδύνου)	21.10%	50
Protection (Προστασία έναντι κινδύνου)	45.15%	107
Monitoring & Detection (Παρακολούθηση & Ανίχνευση κινδύνου)	44.30%	105
Respond (Απόκριση σε επίθεση)	12.66%	30
Recovery (Ανάκτηση / Επαναφορά μετά από επίθεση)	22.78%	54
Δεν γνωρίζω	8.44%	20



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

Answered: 237 Skipped: 0



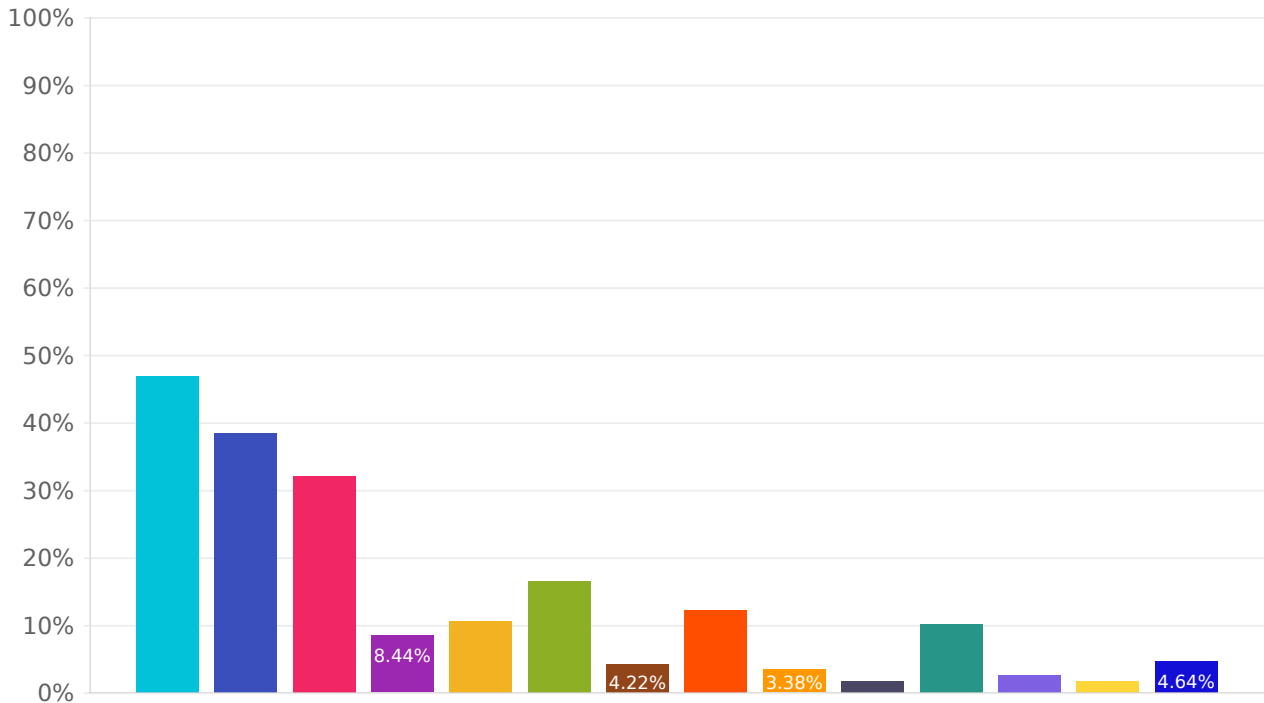
- Bring your own device (BYOD) system attacks
- Cloud-based attacks
- Compromised employee credentials
- Data Linkage
- Identity and access management attacks
- Network Cyber-attacks
- Supply-chain attacks
- Web-applications attacks
- Δεν γνωρίζω

Choices	Response percent	Response count
Bring your own device (BYOD) system attacks	22.36%	53
Cloud-based attacks	18.57%	44
Compromised employee credentials	26.58%	63
Data Linkage	24.47%	58
Identity and access management attacks	21.10%	50
Network Cyber-attacks	37.97%	90
Supply-chain attacks	8.02%	19
Web-applications attacks	18.57%	44
Δεν γνωρίζω	8.44%	20

---

## Ποιες απειλές ασφάλειας σας ανησυχούν περισσότερο σε σχέση με την προστασία των δεδομένων και συστημάτων της επιχείρησής σας; (2 επιλογές)

Answered: 237 Skipped: 0



Κακόβουλο λογισμικό (Malware)

Business email compromise (BEC) / social engineering related threats (Phishing)

Κλοπή προσωπικών δεδομένων

Κακόβουλα web sites

Εσωτερικές επιθέσεις (Insider attacks)

Μη εξουσιοδοτημένος χρήστης / προνομαϊκή πρόσβαση

Εξαγορά λογαριασμού (Account takeover)

Απειλές λόγω BYOD (Bring Your Own Device)

API injection attacks

Compromised / stolen devices

Denial of services

SQL injection

Cross-site scripting

Δεν γνωρίζω

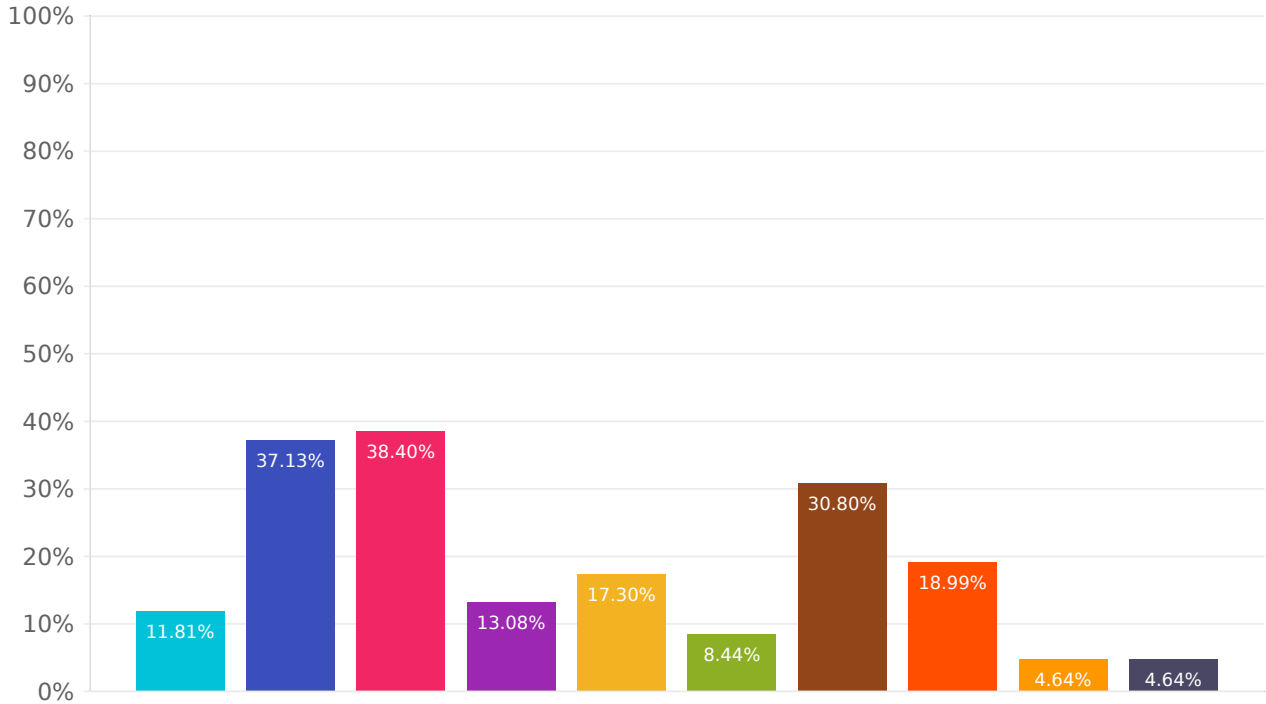


Choices	Response percent	Response count
Κακόβουλο λογισμικό (Malware)	46.84%	111
Business email compromise (BEC) / social engineering related threats (Phishing)	38.40%	91
Κλοπή προσωπικών δεδομένων	32.07%	76
Κακόβουλα web sites	8.44%	20
Εσωτερικές επιθέσεις (Insider attacks)	10.55%	25
Μη εξουσιοδοτημένος χρήστης / προνομαϊκή πρόσβαση	16.46%	39
Εξαγορά λογαριασμού (Account takeover)	4.22%	10
Απειλές λόγω BYOD (Bring Your Own Device)	12.24%	29
API injection attacks	3.38%	8
Compromised / stolen devices	1.69%	4
Denial of services	10.13%	24
SQL injection	2.53%	6
Cross-site scripting	1.69%	4
Δεν γνωρίζω	4.64%	11

Q11

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

Answered: 237 Skipped: 0



- APIs
- Mobile devices
- Laptops
- IoT devices
- Cloud systems
- Intranet server
- Portable storage devices (including USBs)
- Web server
- Routers
- Άλλο (Παρακαλώ σημειώστε)

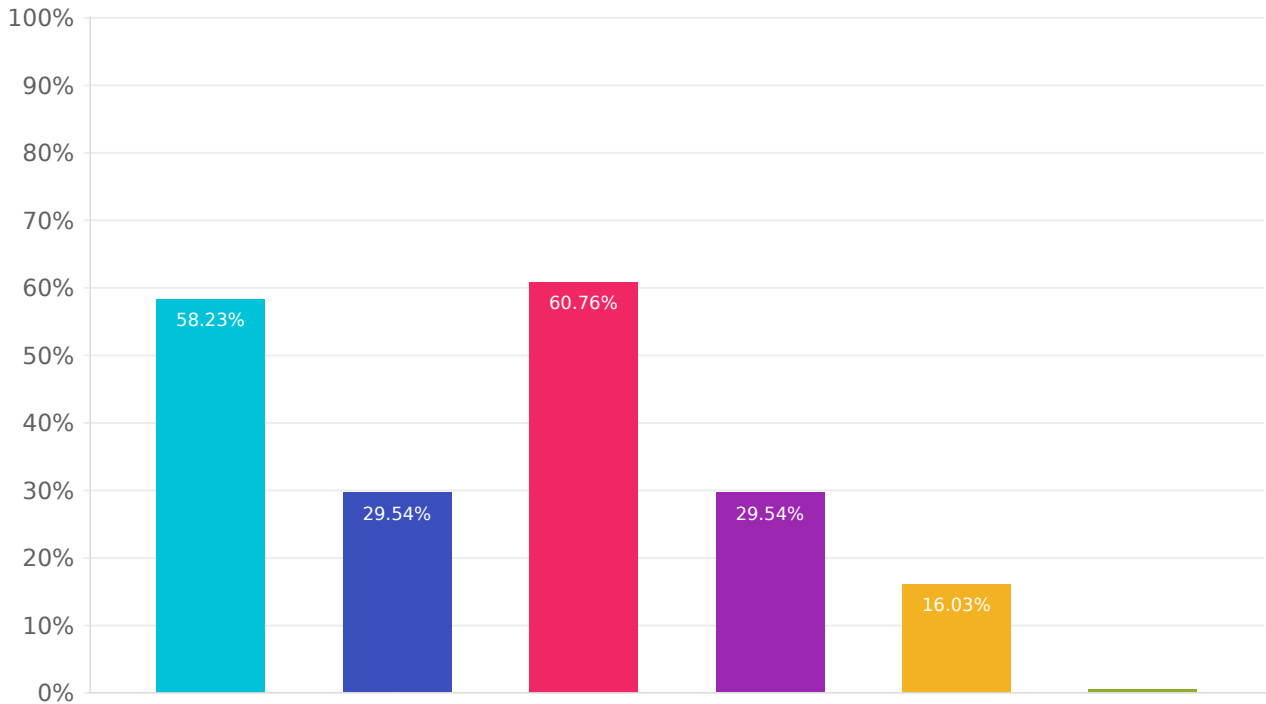
Choices	Response percent	Response count
APIs	11.81%	28
Mobile devices	37.13%	88
Laptops	38.40%	91
IoT devices	13.08%	31
Cloud systems	17.30%	41
Intranet server	8.44%	20
Portable storage devices (including USBs)	30.80%	73
Web server	18.99%	45
Routers	4.64%	11
Άλλο (Παρακαλώ σημειώστε)	4.64%	11

---

Q12

### Ποιο θεωρείτε πιο σημαντικό λόγο για τον οποίο η επιχείρησή σας οφείλει να επενδύσει στη Κυβερνοασφάλεια; (2 επιλογές)

Answered: 237 Skipped: 0



● Διασφάλιση των δεδομένων σε περίπτωση επίθεσης

● Αποτροπή οικονομικής ζημίας σε περίπτωση επίθεσης

● Επιχειρησιακή συνέχεια σε περίπτωση επίθεσης

● Αποφυγή δυσφήμισης της εταιρικής φήμης σε περίπτωση επίθεσης

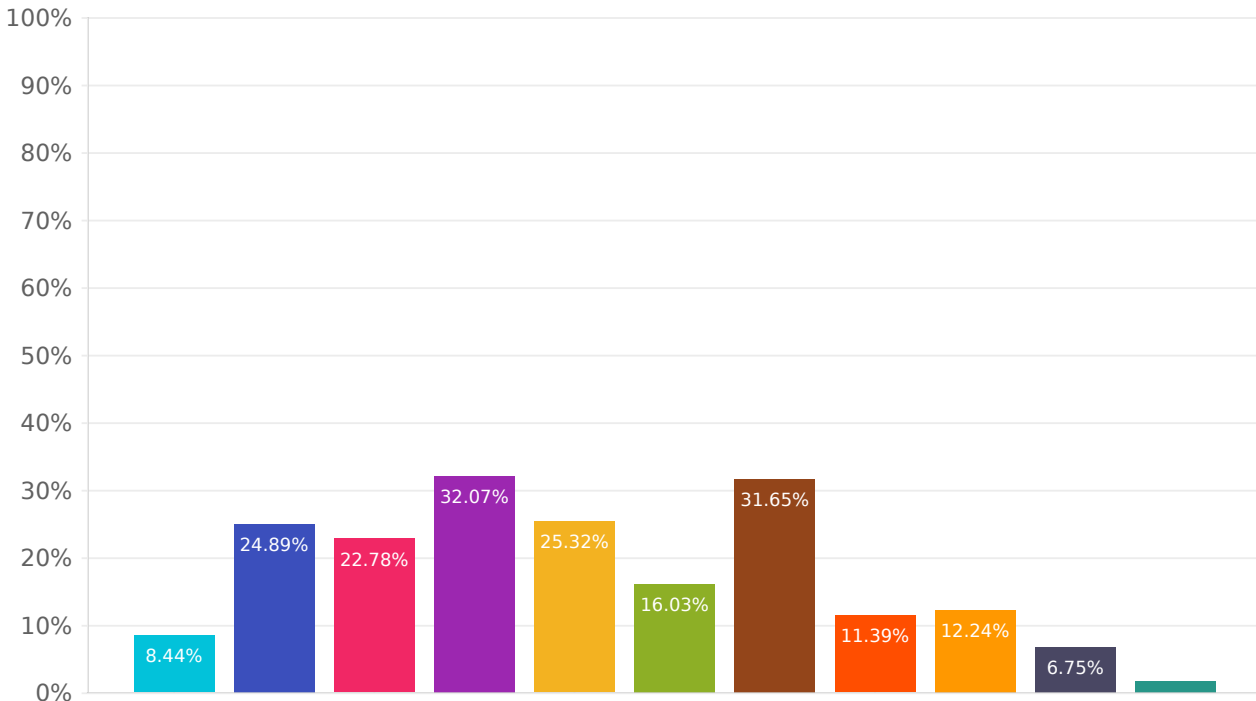
● Ανάγκη συμμόρφωσης σε κανονιστικές οδηγίες/Compliance

● Άλλο (Παρακαλώ σημειώστε)

Choices	Response percent	Response count
Διασφάλιση των δεδομένων σε περίπτωση επίθεσης	58.23%	138
Αποτροπή οικονομικής ζημίας σε περίπτωση επίθεσης	29.54%	70
Επιχειρησιακή συνέχεια σε περίπτωση επίθεσης	60.76%	144
Αποφυγή δυσφήμισης της εταιρικής φήμης σε περίπτωση επίθεσης	29.54%	70
Ανάγκη συμμόρφωσης σε κανονιστικές οδηγίες/Compliance	16.03%	38
Άλλο (Παρακαλώ σημειώστε)	0.42%	1

### Βάσει της εμπειρίας των τελευταίων μηνών, σε ποιο τομέα, θα επενδύατε περισσότερο ώστε να έχετε μεγαλύτερη ασφάλεια ως προς το cyber security; (2 επιλογές)

Answered: 237 Skipped: 0



- API Security & Management
- Cloud Security
- DLP (Data Loss Prevention) Security Solution
- Email Security and Protection
- Firewall & Network Protection
- Identity & Access management (IDaaS)
- IT security awareness training
- Managed Security Services
- Privileged Access Management (PAM)
- Web - Application Security
- • Άλλο (Παρακαλώ σημειώστε)

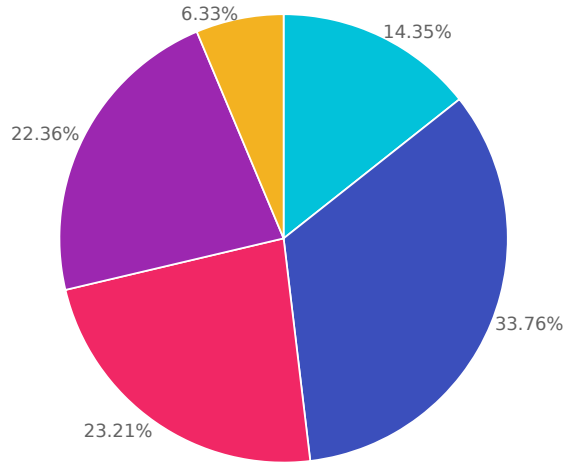
Choices	Response percent	Response count
API Security & Management	8.44%	20
Cloud Security	24.89%	59
DLP (Data Loss Prevention) Security Solution	22.78%	54
Email Security and Protection	32.07%	76
Firewall & Network Protection	25.32%	60
Identity & Access management (IDaaS)	16.03%	38
IT security awareness training	31.65%	75
Managed Security Services	11.39%	27
Privileged Access Management (PAM)	12.24%	29
Web - Application Security	6.75%	16
• Άλλο (Παρακαλώ σημειώστε)	1.69%	4

---

Q14

### Η επιχείρησή σας εφαρμόζει κάποιο πρόγραμμα εκπαίδευσης του προσωπικού σε θέματα cybersecurity awareness;

Answered: 237 Skipped: 0



● Ναι όλοι οι εργαζόμενοι εκπαιδεύονται σε τακτά χρονικά διαστήματα από ανεξάρτητο φορέα

● Ναι όλοι οι εργαζόμενοι εκπαιδεύονται σε τακτά χρονικά διαστήματα εσωτερικά

● Ναι υπάρχει περιστασιακή εκπαίδευση των εργαζομένων

● Όχι, δεν υπάρχει πρόγραμμα εκπαίδευσης

● Δεν γνωρίζω

Choices	Response percent	Response count
Ναι όλοι οι εργαζόμενοι εκπαιδεύονται σε τακτά χρονικά διαστήματα από ανεξάρτητο φορέα	14.35%	34
Ναι όλοι οι εργαζόμενοι εκπαιδεύονται σε τακτά χρονικά διαστήματα εσωτερικά	33.76%	80
Ναι υπάρχει περιστασιακή εκπαίδευση των εργαζομένων	23.21%	55
Όχι, δεν υπάρχει πρόγραμμα εκπαίδευσης	22.36%	53
Δεν γνωρίζω	6.33%	15

Q15

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

Answered: 188 Skipped: 49

Field label	Response percent	Response count
Όνοματεπώνυμο	98.40%	185 Responses
Τηλέφωνο	95.21%	179 Responses
Εταιρεία	84.57%	159 Responses
E-mail	97.87%	184 Responses

---