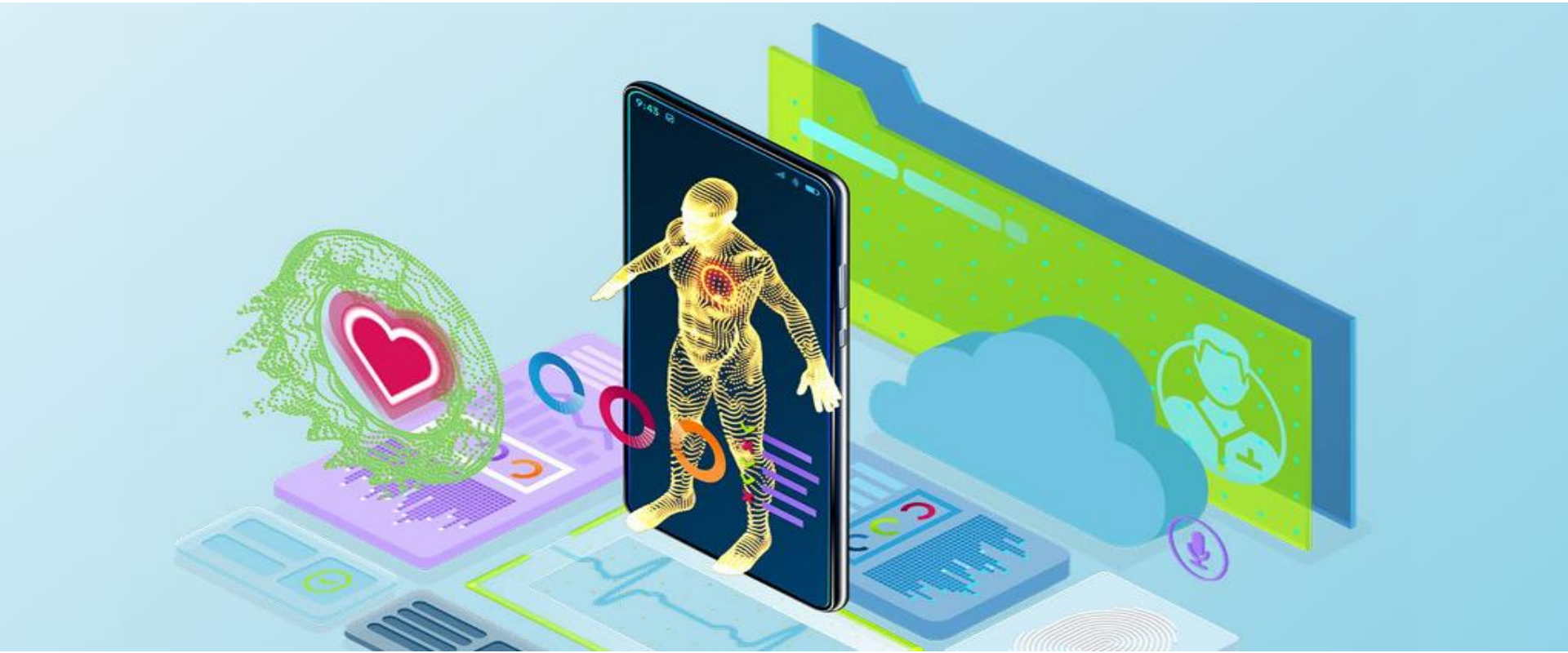


HDHC
Hellenic Digital Health Cluster

HELLENIC CYBER SECURITY TEAM

CROMAR INSURANCE BROKERS SA

Ψηφιακή Υγεία , ΤΝ, Κυβερνοασφάλεια και Ασφάλιση

Νίκος Γεωργόπουλος - Digital Risks Insurance Broker
Co-Founder DPO ACADEMY

Cromar Insurance Brokers

- **25 χρόνια παρουσίας στην ελληνική αγορά**
- Μεσίτες ασφαλίσεων και αντασφαλίσεων με άμεση πρόσβαση στην αγορά των Lloyd's του Λονδίνου και σε άλλες εξειδικευμένες αγορές.
- **Εξειδικευμένοι στην παροχή λύσεων ασφάλισης ψηφιακών κινδύνων και εταιρειών τεχνολογίας**
- **Βραβεία καινοτομίας από τους Lloyd's και άλλους φορείς**
- **Συμμετοχή στο ευρωπαϊκό έργο SECONDO (Σχέση κυβερνοασφάλειας και ασφάλισης στον κυβερνοχώρο)**
- **Υποστηρικτής της Ελληνικής ομάδας Κυβερνοασφάλειας**
- **Μέλος του Hellenic Digital Health Cluster**

Cromar Innovation Lab for Digital Risks

- Το **Cromar Innovation Lab for Digital Risks,** δημιουργήθηκε για να ενισχύσουμε την καινοτομία εντός και εκτός της εταιρίας. Παρακολουθούμε τις διεθνείς εξελίξεις στον τεχνολογικό τομέα, και πως αυτές επηρεάζουν τα επιχειρηματικά μοντέλα δημιουργώντας ασφαλιστικές λύσεις **Digital Risks** και υπηρεσίες που υποστηρίζονται από την αγορά των Lloyd's και άλλες εξειδικευμένες ασφαλιστικές αγορές.

- **Το Cromar Innovation Lab for Digital Risks είναι το πρώτο που δημιουργήθηκε από Μεσιτική εταιρία ασφαλίσεων στην Ελλάδα και έχει βραβευθεί στο διαγωνισμό Digital Finance Awards 2023.**

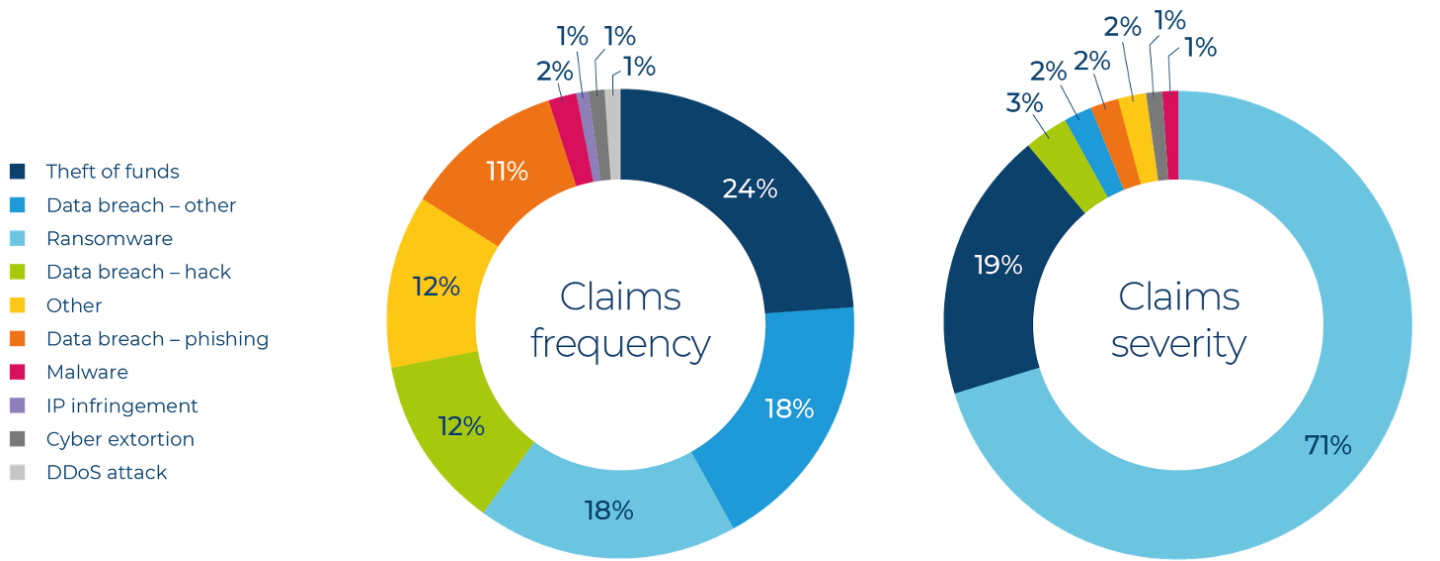
25 YEARS

CROMAR

2024 Cyber Insurance - Ανασκόπηση

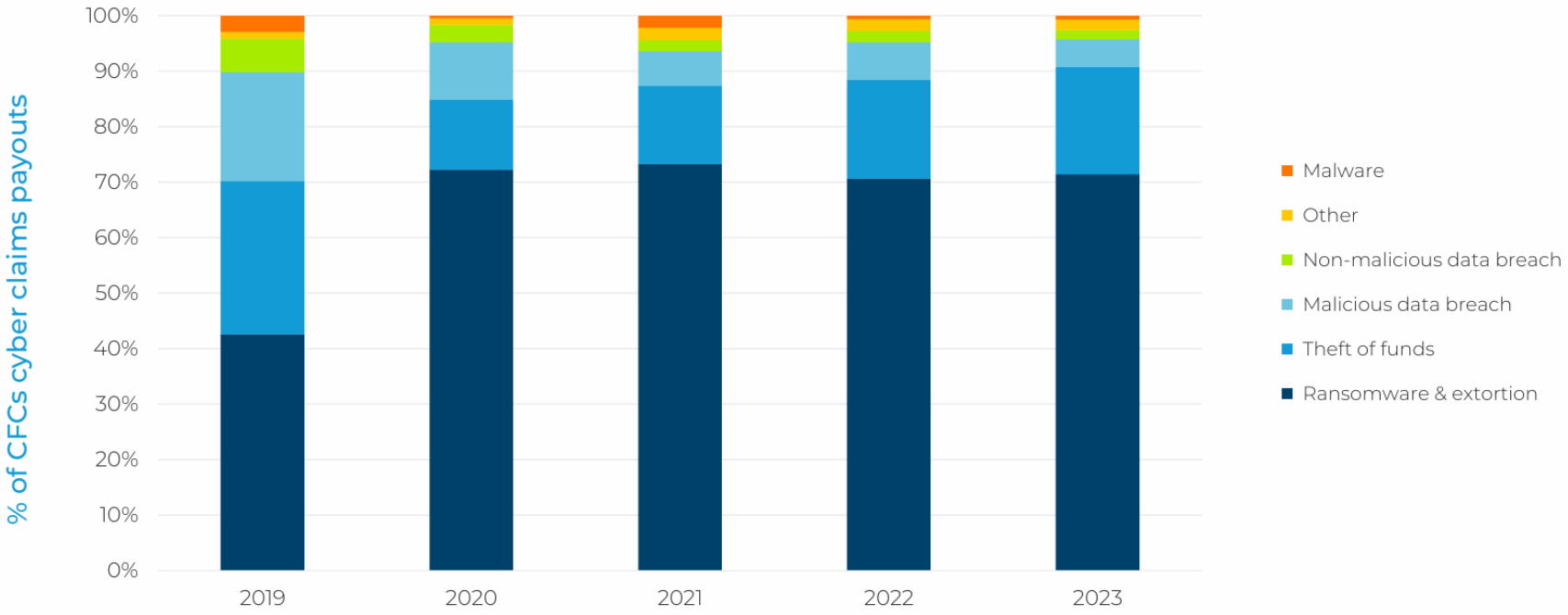
- Η αγορά ασφάλισης στον κυβερνοχώρο αναμένεται να αυξηθεί σε 22,5 δισεκατομμύρια δολάρια παγκοσμίως έως το 2025
- Ransomware: Το 2025 οι παγκόσμιες ζημιές από ransomware αναμένεται να ξεπεράσουν τα 20 δισ. Δολάρια
- Οι κορυφαίοι κίνδυνοι περιλαμβάνουν ransomware, phishing και ευπάθειες στις συσκευές περιμετρικής ασφάλειας
- Το 47% των περιστατικών ransomware προέρχεται από παραβιασμένα διαπιστευτήρια
- Το 90% των παραβιάσεων δεδομένων αρχίζει με επιθέσεις phishing
- Η έλλειψη εκπαίδευσης είναι η βασική αιτία των περισσότερων επιτυχημένων παραβιάσεων στον κυβερνοχώρο

Top Cyber Threats



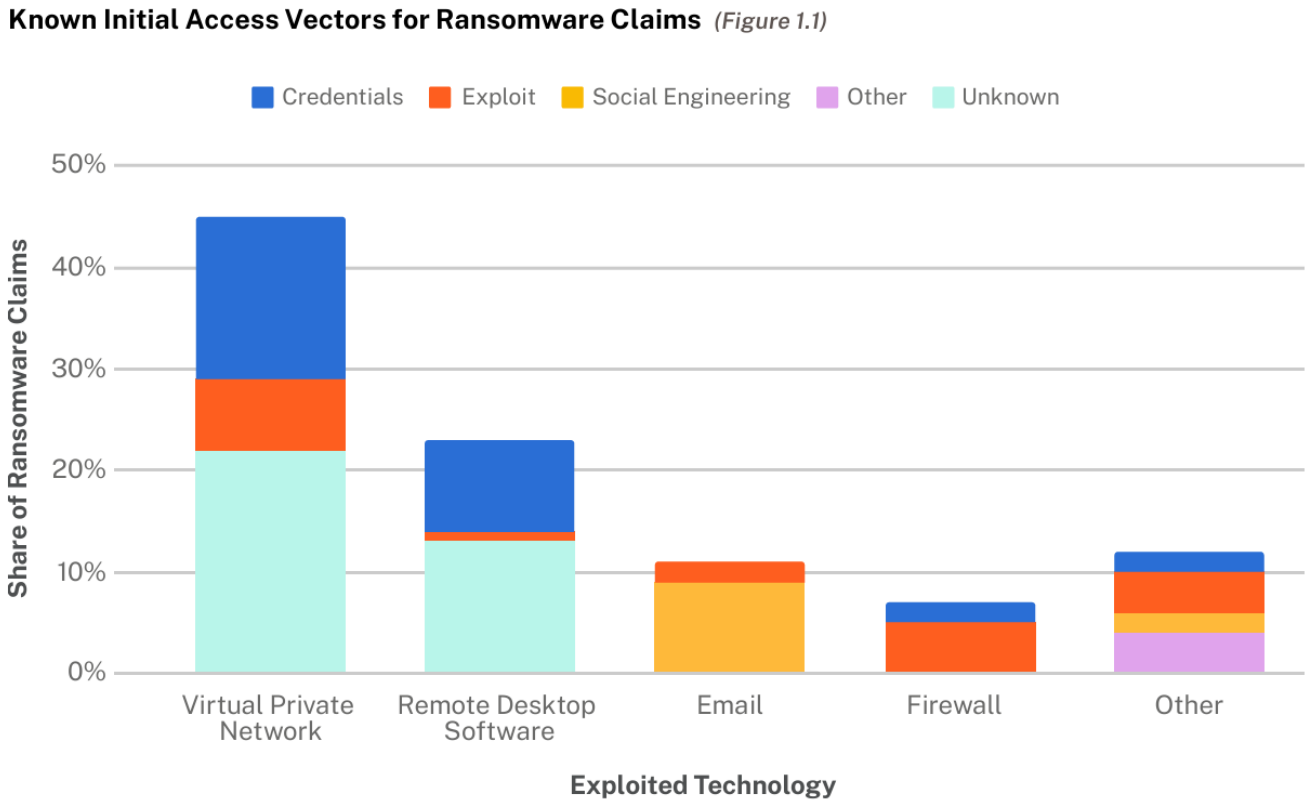
*CFC cyber claims data from January – December 2023

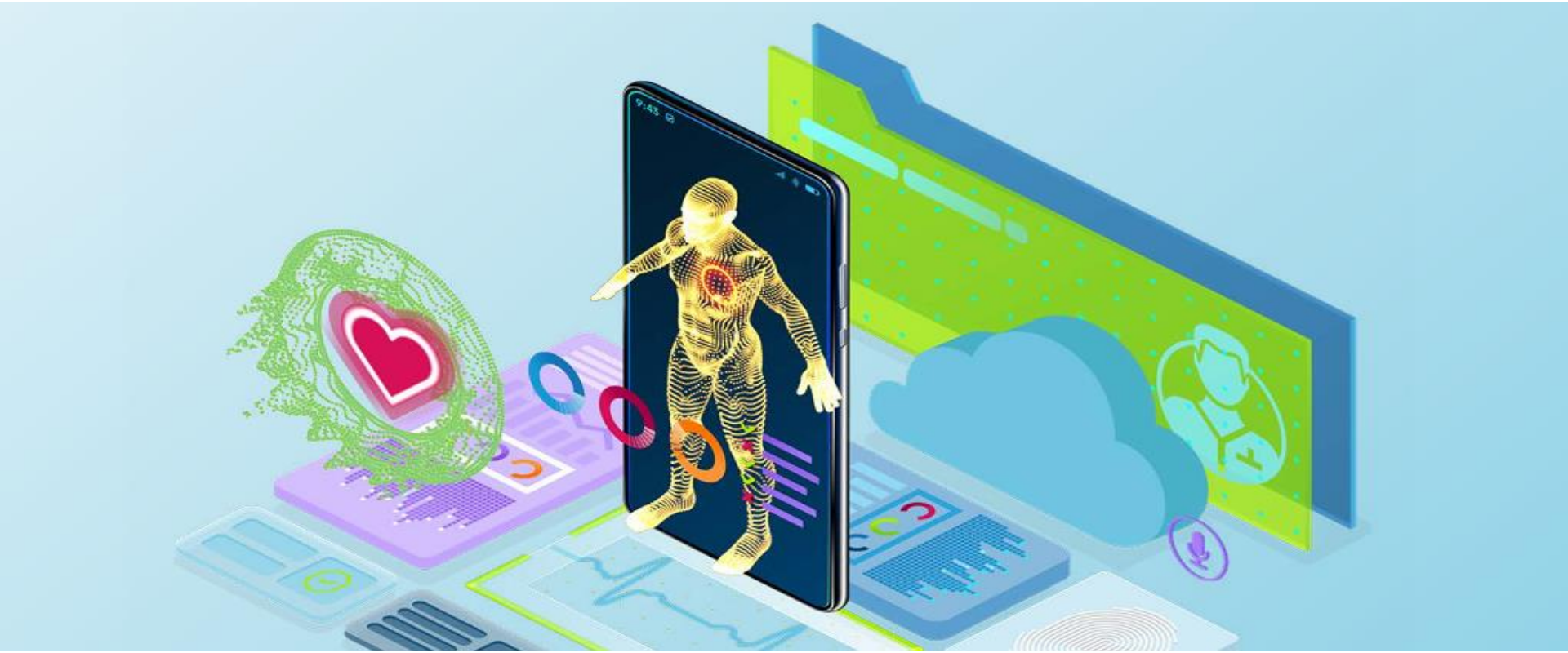
Ransomware αποτελεί το 71% των αποζημιώσεων



CFC cyber claims data from January – December 2023

Αιτίες Ζημιών Ransomware - Coalition





HDHC
Hellenic Digital Health Cluster

HELLENIC CYBER SECURITY TEAM

CROMAR INSURANCE BROKERS SA

Ψηφιακή Υγεία , ΤΝ, Κυβερνοασφάλεια και Ασφάλιση

Νίκος Γεωργόπουλος - Digital Risks Insurance Broker
Co-Founder DPO ACADEMY

Τι είναι η Ψηφιακή Υγεία;

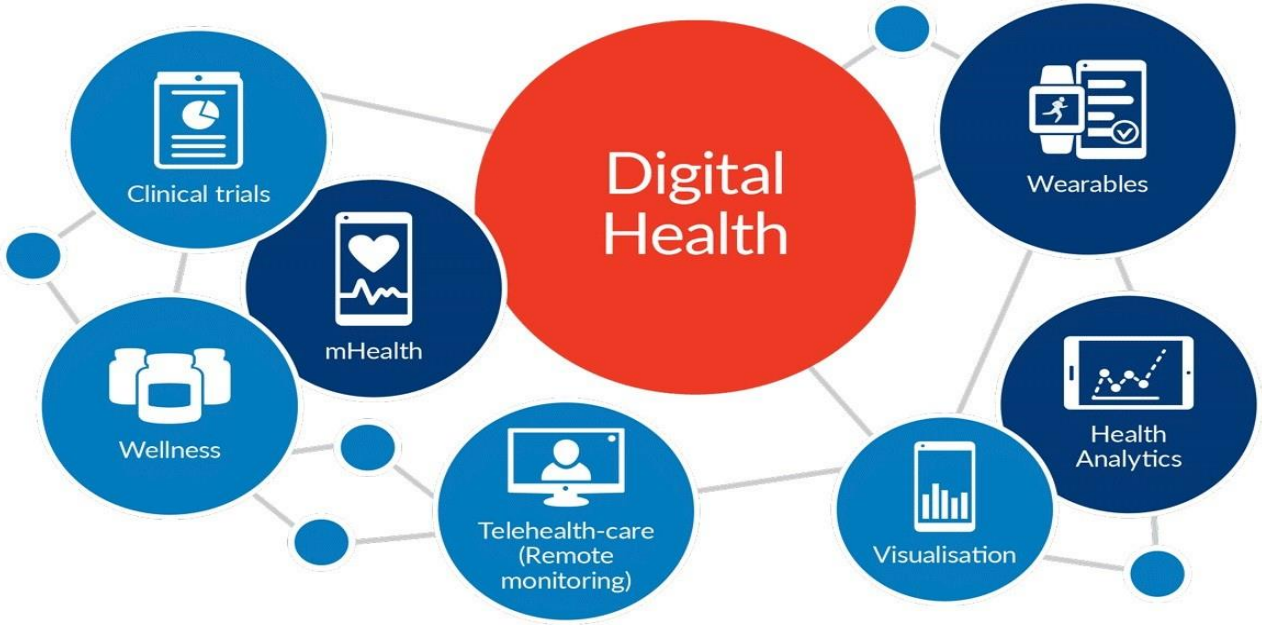
- Η ψηφιακή υγεία αναφέρεται στη χρήση ψηφιακών τεχνολογιών για τη βελτίωση της παροχής υγειονομικής περίθαλψης, τη βελτίωση της υγείας και της ευημερίας των ασθενών και τον εξορθολογισμό των ιατρικών διαδικασιών.

- Περιλαμβάνει ένα ευρύ φάσμα καινοτομιών, συμπεριλαμβανομένων των mobile health apps, της τηλεϊατρικής, των φορητών συσκευών, της τεχνητής νοημοσύνης στη διάγνωση και των ηλεκτρονικών φακέλων υγείας. **Η ενσωμάτωση αυτών των τεχνολογιών μετατρέπει την υγειονομική περίθαλψη σε ένα πιο συνδεδεμένο και ευέλικτο σύστημα.**

- Οι επιχειρήσεις που δραστηριοποιούνται στον τομέα της ψηφιακής υγειονομικής περίθαλψης μπορεί να είναι ιατρεία, νοσοκομεία, κατασκευαστές συσκευών και εταιρείες λογισμικού.

Η αγορά της Ψηφιακής Υγείας

Η αγορά της ψηφιακής υγείας αναμένεται να φτάσει τα 1,1 τρις δολαρίων ΗΠΑ έως το 2032, αυξανόμενη με CAGR 22,2% από το 2022 έως το 2032. (Market Research Report)



Τι προσφέρει η Ψηφιακή Υγεία;

- Ταχύτερες και ακριβέστερες διαγνώσεις
- Απομακρυσμένη παρακολούθηση
- Εξατομικευμένα σχέδια θεραπείας
- Καλύτερη πρόσβαση στην ιατρική φροντίδα
- Βελτιωμένη τήρηση της φαρμακευτικής αγωγής

Τεχνητή Νοημοσύνη στην Ψηφιακή Υγεία

- **Τεχνητή νοημοσύνη στη διάγνωση:** Τα μοντέλα μηχανικής μάθησης εντοπίζουν μοτίβα στις ιατρικές απεικονίσεις, βοηθώντας στην ανίχνευση ασθενειών όπως ο καρκίνος, οι καρδιαγγειακές παθήσεις και οι νευρολογικές διαταραχές με αξιοσημείωτη ακρίβεια.
- **Εξατομικευμένη θεραπεία:** Η ΤΝ βοηθά στην προσαρμογή της φαρμακευτικής αγωγής και της θεραπείας στα ατομικά προφίλ των ασθενών με βάση γενετικούς δείκτες και ιστορικά δεδομένα υγείας.
- **Χειρουργική με τη βοήθεια ρομπότ:** Τα ρομποτικά συστήματα με τεχνητή νοημοσύνη ενισχύουν τη χειρουργική ακρίβεια, μειώνοντας τους χρόνους ανάρρωσης και βελτιώνοντας τα αποτελέσματα.

Τεχνητή Νοημοσύνη στην Ψηφιακή Υγεία

- **Διοικητική αποτελεσματικότητα:** Η τεχνητή νοημοσύνη αυτοματοποιεί εργασίες ρουτίνας, όπως ο προγραμματισμός ραντεβού, η διαχείριση αρχείων ασθενών και η επεξεργασία ασφαλιστικών απαιτήσεων, μειώνοντας το φόρτο εργασίας και βελτιώνοντας την παραγωγικότητα.

Ενώ η ΤΝ προσφέρει πολυάριθμα οφέλη, οι προκλήσεις όπως η μεροληψία του αλγορίθμου, οι ηθικές ανησυχίες και η πολυπλοκότητα των κανονιστικών ρυθμίσεων απαιτούν προσεκτική πλοήγηση για να εξασφαλιστεί η υπεύθυνη εφαρμογή.

Κίνδυνοι που απειλούν την Ψηφιακή Υγεία

- Phishing attacks -Επιθέσεις Ηλεκτρονικού Ψαρέματος
- Ransomware
- Malware & Viruses -Κακόβουλο λογισμικό και ιοί
- Weak Passwords and Authentication -Αδύναμοι κωδικοί πρόσβασης και ταυτοποίηση
- Social Engineering – Κοινωνική Μηχανική
- Outdated Software and Systems - Ξεπερασμένο λογισμικό και συστήματα
- Data Breaches and Information theft -Παραβιάσεις δεδομένων και κλοπή πληροφοριών
- Misconfigured Cloud resources - Εσφαλμένες ρυθμίσεις πόρων Cloud
- Technology E&O - Τεχνολογικά λάθη ή παραλείψεις
- Products Liability - Ευθύνη προϊόντων
- Intellectual Property – Πνευματική Ιδιοκτησία

Ενίσχυση της Κυβερνοασφάλειας στην Ψηφιακή Υγεία

Για τον μετριασμό των κινδύνων, οι πάροχοι υγειονομικής περίθαλψης και οι εταιρείες τεχνολογίας πρέπει να υιοθετήσουν ισχυρές στρατηγικές ασφάλειας.

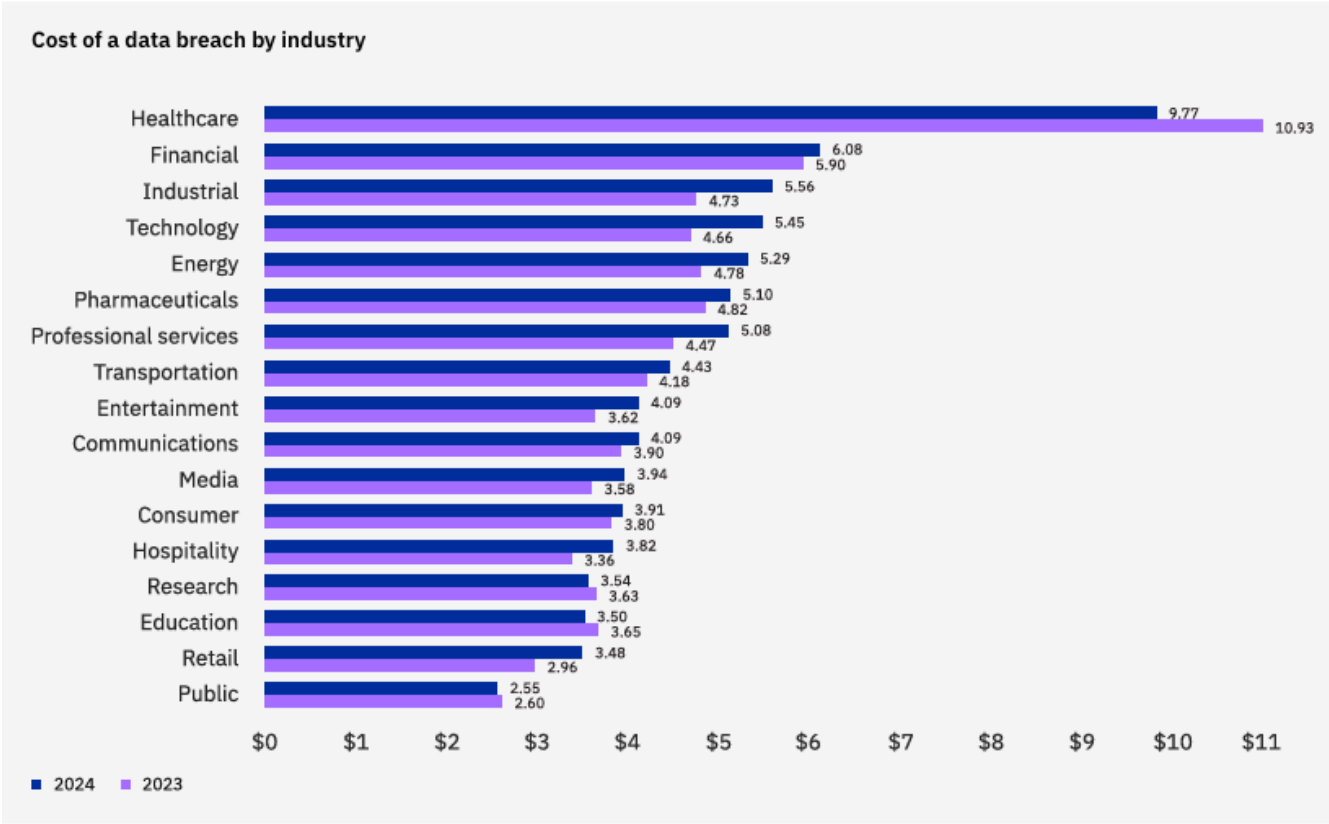
Βέλτιστες πρακτικές για την κυβερνοασφάλεια στην υγειονομική περίθαλψη:

- **Συστηματική Εκπαίδευση του Ανθρώπινου Δυναμικού**
- **Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA):** Η εφαρμογή MFA ενισχύει την ασφάλεια σύνδεσης για τα συστήματα υγειονομικής περίθαλψης.
- **Αντίγραφα Ασφαλείας - Backup**
- **Κρυπτογράφηση δεδομένων:** Η κρυπτογράφηση ευαίσθητων δεδομένων ασθενών εξασφαλίζει προστασία από μη εξουσιοδοτημένη πρόσβαση.

Ενίσχυση της Κυβερνοασφάλειας στην Ψηφιακη Υγεία

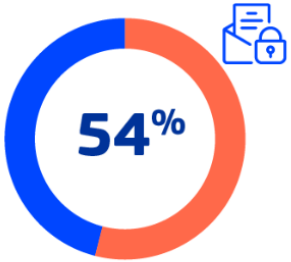
- **Τακτικοί έλεγχοι ασφαλείας:** Η διενέργεια περιοδικών αξιολογήσεων συμβάλλει στον εντοπισμό ευπαθειών και στην ενίσχυση της άμυνας.
- **Συμμόρφωση με τους κανονισμούς:** Η τήρηση νόμων όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων **(GDPR),** η **NIS2**,η **AI Act**, η **Medical Device Regulation (MDR)** διασφαλίζει την προστασία της ιδιωτικής ζωής την προστασία των υποδομών και των ασθενών
- **Η συμμόρφωση με τους κανονισμούς κάνει διαχειρίσιμο τον Κίνδυνο και την ευθύνη τους**
- **Η διασφάλιση της τεχνολογίας της υγειονομικής περίθαλψης απαιτεί συνεχή επαγρύπνηση και προσαρμογή στις αναδυόμενες απειλές.**

Κόστος Περιστατικού Απώλειας Δεδομένων



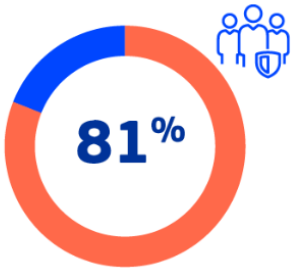
Στατιστικά Στοιχεία Περιστατικών Κυβερνοασφάλειας

309 περιστατικά κυβερνοασφάλειας αναφέρθηκαν από τα κράτη μέλη το 2023.
Πηγή: ENISA.



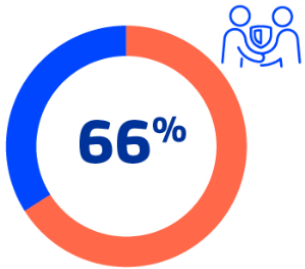
Το

54 % των περιστατικών ransomware* ευθύνονται για περιστατικά κυβερνοασφάλειας στον τομέα της υγείας (2021-2023).
Πηγή: Τοπίο απειλών του ENISA: Τομέας Υγείας (Ιούλιος 2023)



Το

81 % των εταιρειών θεωρεί ότι οι δυσκολίες στην πρόσληψη προσωπικού στον κυβερνοχώρο συνιστούν κίνδυνο για κυβερνοεπιθέσεις.
Πηγή: 2024 Ευρωβαρόμετρο για τις ψηφιακές δεξιότητες.



Το

66 % των ρόλων στον κυβερνοχώρο καλύπτονται από υπαλλήλους που μεταβαίνουν από θέσεις που δεν σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

Πηγή: 2024 Ευρωβαρόμετρο για τις ψηφιακές δεξιότητες.

Ένα περιστατικό ransomware είναι ένα είδος κυβερνοεπίθεσης όπου μη εξουσιοδοτημένα μέρη αποκτούν πρόσβαση και κρυπτογραφούν ευαίσθητα δεδομένα καθιστώντας τα απρόσιτα και απαιτούν πληρωμή σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης.

Οι επιθέσεις ransomware θέτουν τους ασθενείς σε κίνδυνο

- **Μια υπάλληλος ενός νοσοκομείου άνοιξε κατά λάθος ένα phishing email και ένα κρυμμένο σε αυτο αρχείο κατέβηκε στο δίκτυο.**
- Αυτό αρχείο μπλόκαρε το δίκτυο του νοσοκομείου με αποτέλεσμα **την ακύρωση χειρουργείων, αναβολές ραντεβού για μαστογραφία και καθυστερήσεις στις θεραπείες ορισμένων ασθενών με καρκίνο.**
- Η επίθεση ransomware που ακολούθησε ανάγκασε τους αξιωματούχους να κλείσουν όλες τις συνδέσεις στο Διαδίκτυο, συμπεριλαμβανομένης **της πρόσβασης στα ηλεκτρονικά αρχεία υγείας των ασθενών**, για να περιοριστεί η **ζημιά.**

Οι επιθέσεις ransomware θέτουν τους ασθενείς σε κίνδυνο

- **«Όλα ήταν κάτω. Έτσι τα τηλέφωνά μας ήταν κλειστά. Δεν είχαμε πλέον συσκευές φαξ. Δεν μπορούσαμε να χρησιμοποιήσουμε το ηλεκτρονικό ταχυδρομείο για να επικοινωνήσουμε»,** δήλωσε σχετικά με την επίθεση ο CEO,. **«Εκείνο το πρώτο βράδυ, στείλαμε πραγματικά ανθρώπους στο Best Buy για να αγοράσουν γουόκι-τόκι».**

- Τα τελευταία χρόνια, **ένας αυξανόμενος αριθμός νοσοκομείων και οργανισμών υγειονομικής περίθαλψης έχουν αντιμετωπίσει κυβερνοεπιθέσεις, διακόπτοντας τη φροντίδα και θέτοντας τους ασθενείς σε κίνδυνο.**

Ransomware σε Κατασκευαστή Ιατρικών Συσκευών

- **Η Artivion, κορυφαίος κατασκευαστής ιατρικών συσκευών καρδιοχειρουργικής, αποκάλυψε ότι έπεσε θύμα επίθεσης (ransomware), η οποία έλαβε χώρα στις 21 Νοεμβρίου 2024 και διέκοψε τις λειτουργίες της.**
- Μετά την ανακάλυψη της επίθεσης, **η Artivion έθεσε ορισμένα συστήματα εκτός σύνδεσης και ξεκίνησε έρευνα με τη συμμετοχή εξωτερικών συμβούλων, με σκοπό την αξιολόγηση, τον περιορισμό και την αντιμετώπιση του περιστατικού**.
- Η Artivion δεν ανέφερε άμεσα ότι επρόκειτο για επίθεση ransomware, αλλά αποκάλυψε ότι οι εισβολείς κρυπτογράφησαν ορισμένα από τα συστήματά της και έκλεψαν δεδομένα από παραβιασμένα συστήματα.
- “Το περιστατικό αφορούσε την απόκτηση και την κρυπτογράφηση αρχείων. Η Εταιρεία εργάζεται για την ασφαλή αποκατάσταση των συστημάτων της το συντομότερο δυνατό και για την αξιολόγηση τυχόν υποχρεώσεων ειδοποίησης“, ανέφερε.

Responding to a cyber incident

You receive an email from a ransomware group stating they have stolen client and employee data and your IT team suggest there may have been unauthorised access to files. What's your next move?

In this moment, do you have the know-how to respond?

You'll need help to stop the attack, fix the problem, identify the what's lost, stolen, missing or compromised, manage and resolve compromised systems, and then design and implement a plan to prevent follow-up attacks.

Is this level of detail in your Business Continuity Plan and Incident Response Plan? Is your IT team ready to respond or do you have back-up in-place, ready to support you in an instant?

A strong cyber support team can carry you through: a specialist cyber insurance policy not only provides financial protection to cover costs, but also gives you direct access to a range of cyber expertise that helps you respond to a suspected incident at every stage and helps get you back up and running again.

Areas to consider and plan for

Incident response

Incident response services

Hiring IT forensic investigators, response teams or consultants

Investigation and forensics

- Forensic analysis to determine the extent of the breach
- Legal and regulatory investigation expenses

Specialist expertise

Data recovery

- Restoring data from backups
- Rebuilding affected systems and infrastructure

Business interruption

- Downtime and operational disruption
- Loss of productivity and revenue during recovery

Notifications costs

- Informing affected customers and stakeholders
- Setting up call centres to handle inquiries

Legal advice

- Initial legal consultation to determine legal obligations to customers, third parties, regulators
- Communicating with any regulators, responding to inquiries

Public relations

- Costs to respond to media inquiries
- Communications to customers, clients or third parties

Reducing long term impact

Ongoing legal costs

- Continued legal fees from class-action lawsuits or other legal actions
- Costs related to regulatory audits and compliance checks

Legal and regulatory fines

- Fines for non-compliance with data protection regulations (e.g., GDPR, HIPAA)
- Settlements from lawsuits

Long-term security improvements

- Investments in new security infrastructure and technology
- Training programs for employees on cybersecurity awareness

Reputation damage

- Loss of customer trust and confidence
- Brand damage leading to reduced customer base

Ψηφιακή Υγεία: Ρυθμιστικά και Δεοντολογικά Ζητήματα

Καθώς η τεχνητή νοημοσύνη και η κυβερνοασφάλεια διαδραματίζουν ολοένα και σημαντικότερο ρόλο στην υγειονομική περίθαλψη, τα ρυθμιστικά πλαίσια πρέπει να εξελιχθούν ώστε να αντιμετωπίσουν ηθικές ανησυχίες και νομικές επιπτώσεις.

Βασικές ρυθμιστικές πτυχές:

- Η συμμόρφωση με τον **GDPR,** τη **NIS2**, την **AI Act**, τη **Medical Device Regulation (MDR)**
- **Διαφάνεια των αλγορίθμων:** Οι αποφάσεις υγειονομικής περίθαλψης που βασίζονται στην ΤΝ πρέπει να είναι εξηγήσιμες και απαλλαγμένες από προκαταλήψεις.
- **Ιατρική δεοντολογία:** Ο ρόλος της τεχνητής νοημοσύνης στις αποφάσεις θεραπείας εγείρει ηθικές ανησυχίες σχετικά με τη λογοδοσία και τη συγκατάθεση.

Ο Ρόλος της Ασφάλισης στην Ψηφιακή Υγεία

Η ασφάλιση διαδραματίζει κρίσιμο ρόλο στην προστασία των παρόχων υγειονομικής περίθαλψης, των ασθενών και των εταιριών τεχνολογίας που παρέχουν προϊόντα και υπηρεσίες ψηφιακής υγείας από απρόβλεπτους κινδύνους.

Καθώς η ψηφιακή υγεία εξελίσσεται με την ενσωμάτωση εφαρμογών Τεχνητής Νοημοσύνης, οι ασφαλιστές προσαρμόζονται στις νέες προκλήσεις που σχετίζονται με την **ασφάλεια στον κυβερνοχώρο** την **επαγγελματική ευθύνη των εταιριών εταιριών τεχνολογίας** που παρέχουν προϊόντα και υπηρεσίες ψηφιακής υγείας.

Ο Ρόλος της Ασφάλισης στην Ψηφιακή Υγεία

- **Cyber Insurance - Ασφάλιση αστικής ευθύνης στον κυβερνοχώρο:** Καλύπτει οικονομικές απώλειες που προκύπτουν από επιθέσεις στον κυβερνοχώρο και παραβιάσεις δεδομένων του ασφαλισμένου και την ευθύνη του έναντι τρίτων
- **Ασφάλιση Επαγγελματικής Ευθύνης εταιριών που δημιουργούν προϊόντα και υπηρεσίες ψηφιακής υγείας για λάθη ή παραλείψεις**
- **Ασφάλιση Ευθύνης Ιατρικών Συσκευών:** Καλύπτει οικονομικές απώλειες που προκύπτουν από λάθη ή παραλείψεις των κατασκευαστών και σωματικές βλάβες χρηστών.
- **Ασφάλιση Ευθύνης Στελεχών (D&O)**

Digital Health – Ασφαλιστικές Καλύψεις

- Σωματικές βλάβες που προκύπτουν από υπηρεσίες υγειονομικής περίθαλψης, δραστηριότητες τεχνολογίας, συμβάντα στον κυβερνοχώρο και διακοπές λειτουργίας του συστήματος
- Τεχνολογικά σφάλματα και παραλείψεις
- Προϊόντα που δεν αποδίδουν σύμφωνα με τις προδιαγραφές τους
- Κίνδυνος στον Κυβερνοχώρο και προστασία της ιδιωτικής ζωής των εταιρειών υγειονομικής περίθαλψης
- Γενική ευθύνη, ευθύνη εργοδοτών και νομικά έξοδα.
- Παγκόσμια Κάλυψη

Ποιες είναι οι πιο συχνές Αιτίες Ζημιών

- Οι **σωματικές βλάβες** αντιπροσωπεύουν 1 στις 3 απαιτήσεις (αφορούν περιστατικά που οφείλονται σε cyber events & διακοπές λειτουργίας συστημάτων) ενώ τα υπόλοιπα 2 τρίτα αποδίδονται στον κυβερνοχώρο, τεχνολογία και άλλες αιτίες

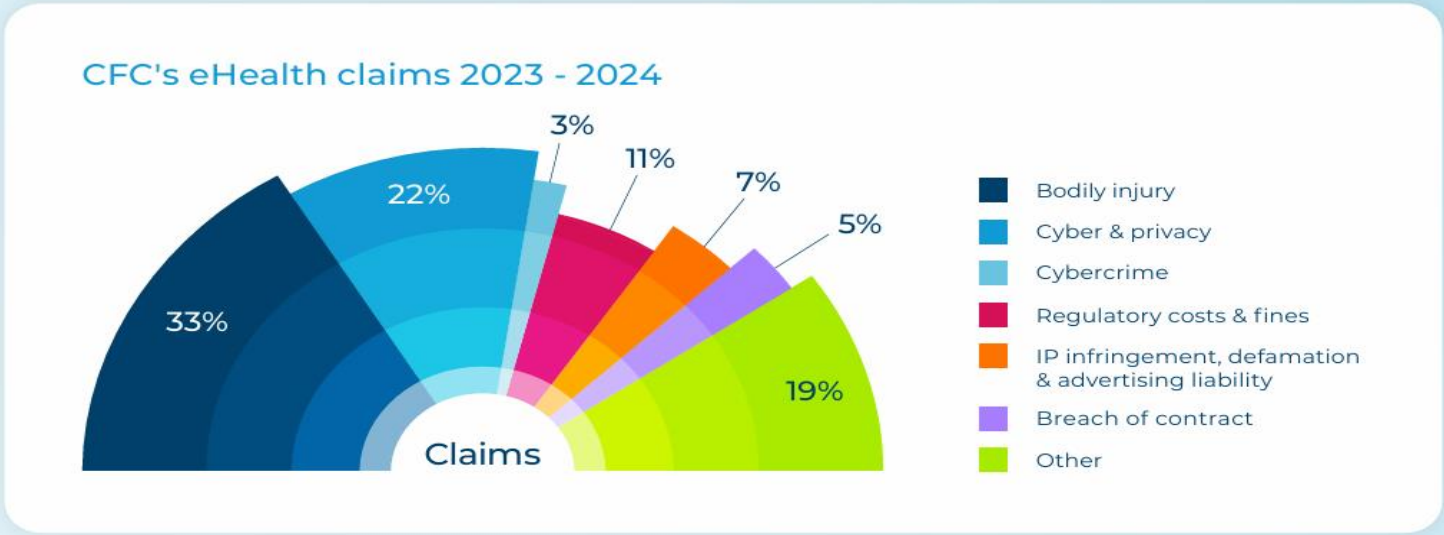
- Ο **κυβερνοχώρος και η προστασία της ιδιωτικής ζωής** αποτελούν βασική ανησυχία, οδηγώντας στο 25% του συνόλου των απαιτήσεων ψηφιακής υγείας

- Το 7% των αξιώσεων οφείλονται σε παραβιάσεις **Πνευματικής Ιδικτησίας**

- Η κατηγορία «Άλλο» αποτελείται από **τεχνολογικά λάθη και παραλείψεις** κατα την παροχή προϊόντων και υπηρεσιών ψηφιακής υγείας , **γενική αστική ευθύνη**, **ευθύνη προϊόντων**, βλάβη φήμης, ευθύνη από εργασιακές πρακτικές.

Digital Health -Ποιες είναι οι πιο συχνές Αιτίες Ζημιών

Two-thirds of our claims now stem from emerging sources such as advertising liability, IP or cybercrime which would not be covered under a traditional medical malpractice policy. While bodily injury, cyber and privacy remain key exposures, the sources of these claims continue to evolve.



Note: "Other" is made up of technology errors & omissions, crime/fraud, general liability, products liability, reputational harm, sexual misconduct & physical abuse, property and employment practices liability. Claims may trigger multiple insuring clauses but are categorised and assessed individually.

Συμπέρασματα

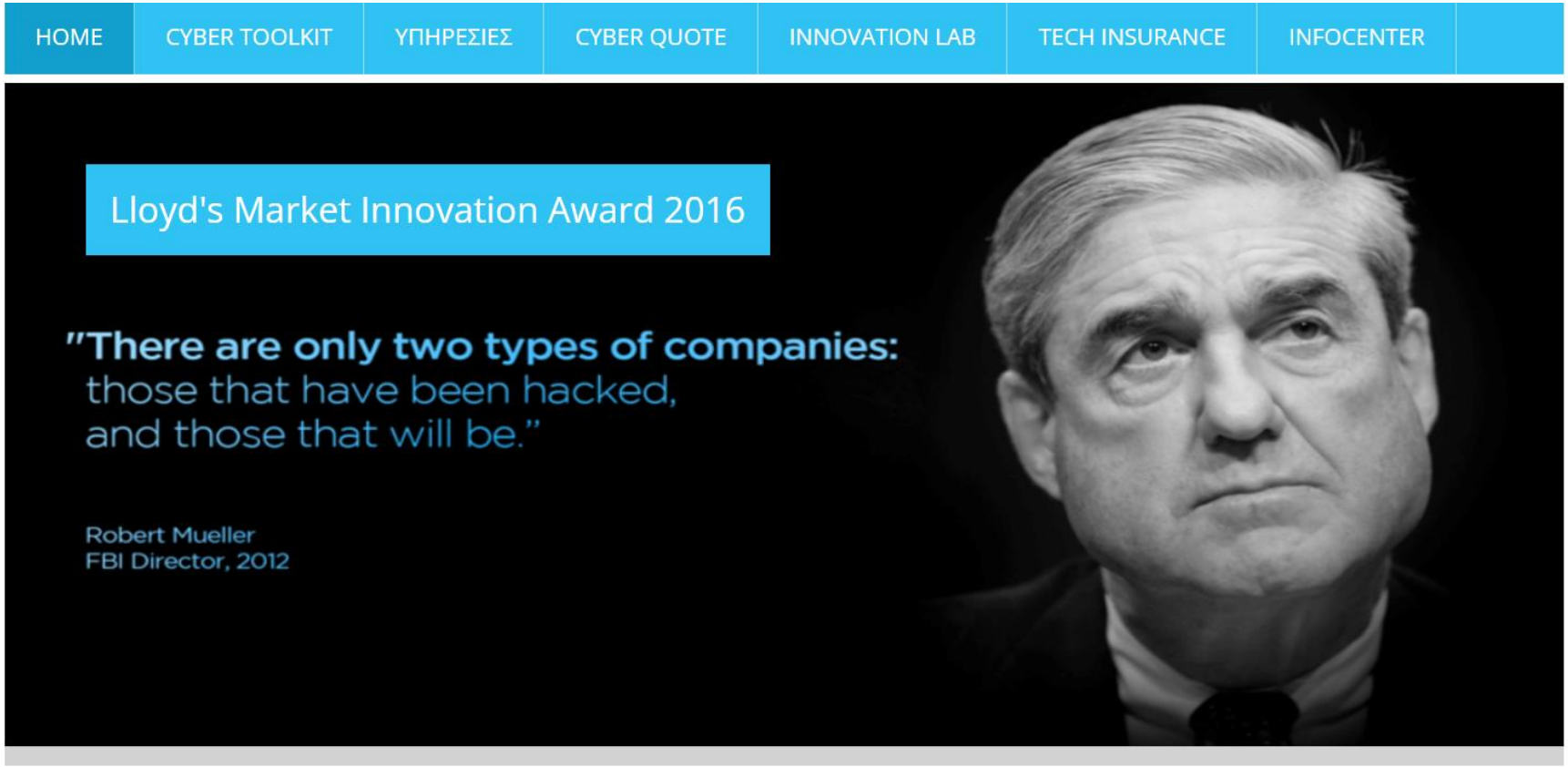
- Η σύγκλιση της ψηφιακής υγείας, της τεχνητής νοημοσύνης, της κυβερνοασφάλειας και της ασφάλισης παρουσιάζει ευκαιρίες και προκλήσεις που απαιτούν συνεργασία μεταξύ παρόχων υγειονομικής περίθαλψης, προγραμματιστών τεχνολογίας, εμπειρογνωμόνων ασφαλείας και φορέων χάραξης πολιτικής.

- Η καινοτομία πρέπει να εξισορροπηθεί με την ασφάλεια και την ηθική, ώστε να διασφαλιστεί ότι η ψηφιακή υγεία θα αξιοποιήσει τις δυνατότητές της.

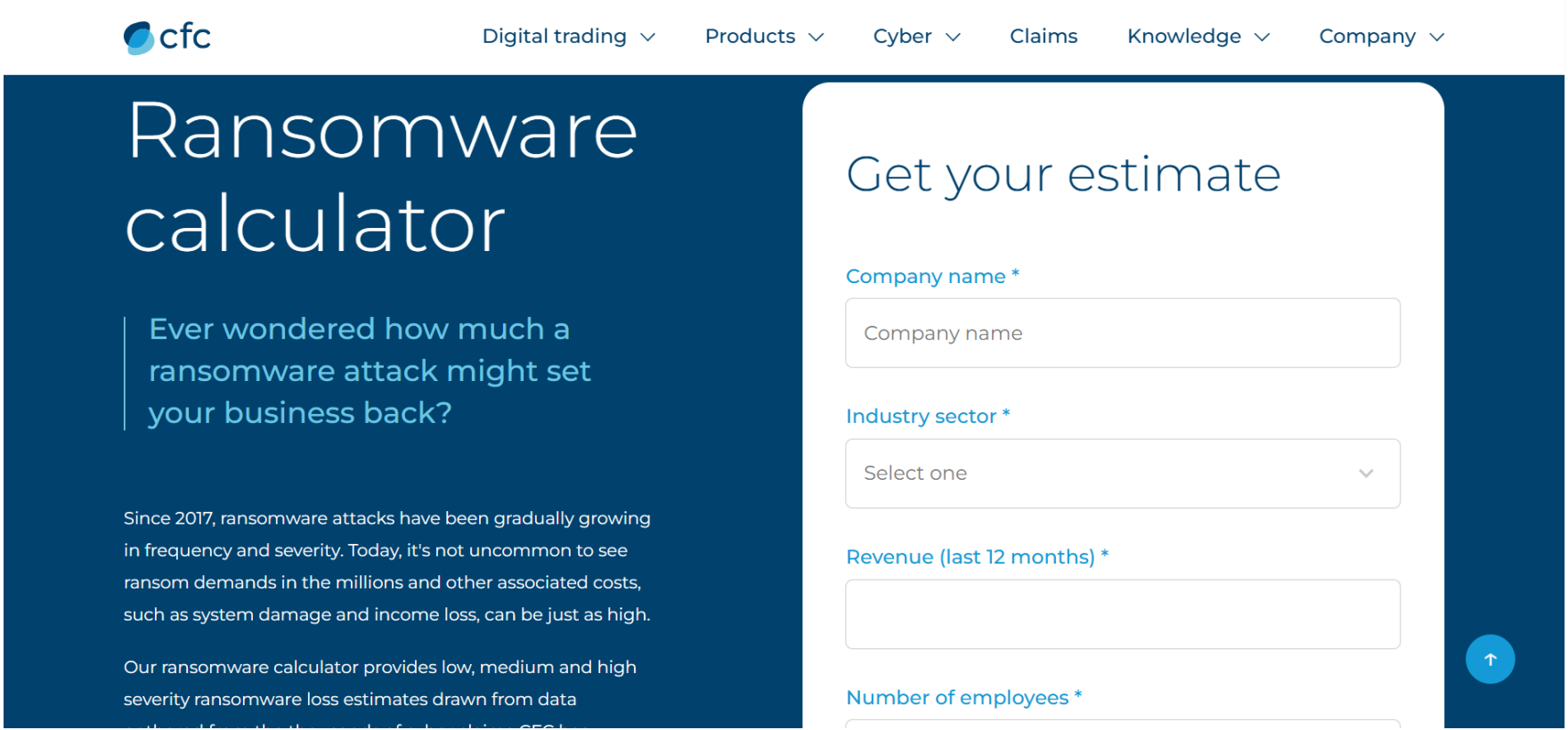
- Καθώς ψηφιακή υγεία θα εξελίσσεται, η υγειονομική περίθαλψη θα βελτιώνεται, η υιοθέτηση της τεχνητής νοημοσύνης με παράλληλη ενίσχυση των μέτρων κυβερνοασφάλειας θα είναι υψίστης σημασίας για τη διασφάλιση της ιδιωτικής ζωής των ασθενών και τη βελτίωση των ιατρικών αποτελεσμάτων.


CROMAR
CYBER SECURITY AWARDS 2024
GOLD
Cyber Secure Solution
Ασφάλιση Κινδύνων Διαδικτύου
CYBER SECURITY AWARDS 2024
GOLD

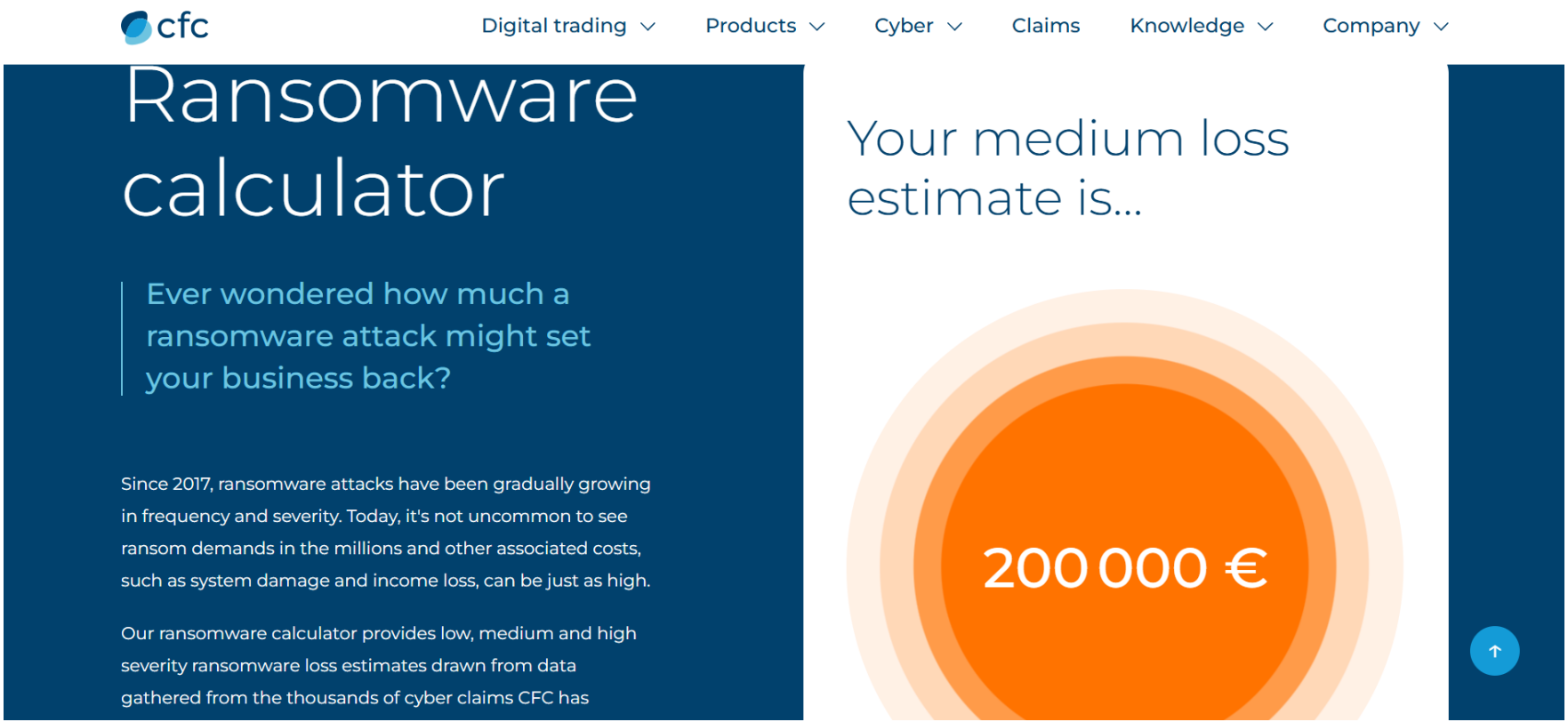
www.cyberinsurancequtote.gr



www.cyberinsurancequote.gr



www.cyberinsurancequote.gr

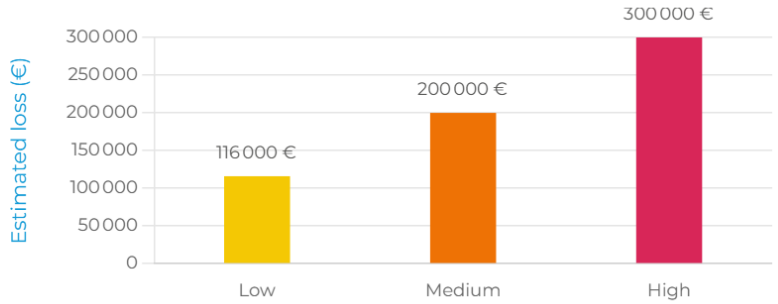


Loss estimate

Based on the information you provided, we've produced three loss estimates of varying degrees of severity.

More details, including information about our cost breakdowns and methodology, can be found in the full report. Click the button below to download your copy.

DOWNLOAD THE FULL REPORT



Ransomware loss scenarios by severity

Proactive Cyber Attack Prevention

Online GP: Our mobile app for cyber

The quickest and most secure line of communication with our cyber security team.

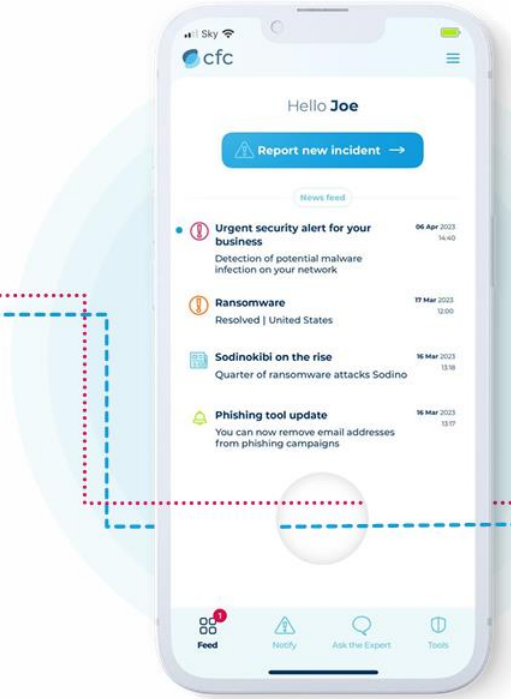
Try it today!

Response, our mobile app

Demo policy number:
DEMOCFC000

CFC

Real-time, actionable threat alerts & cyber security support



Insured

Direct and secure way to notify us of a cyber incident or request help

cfc

CROMAR INSURANCE BROKERS SA

Ready to buy checklist – the essentials for a robust cyber insurance policy

Having a robust cyber insurance policy has become a necessity rather than a luxury. You may be investing in cybersecurity measures already, but no system is ever foolproof. Cyber insurance enables companies to transfer some of the financial risks associated with cyber threats to the insurer.

But how do you know what your business needs?

Here's a checklist to help you evaluate your cyber risks:

Assess your risk profile

- **Data sensitivity:** Consider the type and volume of data your business stores. Personal identifiable information (PII), payment details, and proprietary information are high-value targets for cybercriminals.
- **Regulatory requirements:** Understand the data security compliance requirements specific to your industry, such as GDPR, HIPAA, or PCI-DSS. These regulations often require specific levels of protection and reporting, which should be reflected in your insurance coverage.
- **Contractual obligations:** Some contracts, especially with larger companies or government entities, may require you to carry a specific amount of cyber insurance.

Understand the potential financial impact of a cyber attack

- **Incident response & recovery costs:** Consider the cost of a potential data breach, including computer forensics, data recovery, notification costs, legal fees, regulatory fines, and public relations efforts.
- **Business interruption:** Factor in the potential loss of income if your operations are disrupted by a cyber event.
- **Ransom payments:** If your business could be a target for ransomware, consider the potential ransom demands.
- **Reputational damage:** Consider the potential long-term impact on your reputation and customer trust, which might require additional marketing or communication efforts to repair.

Additional expert cyber support

- Do you need access to cyber experts when an issue happens? Consider what help you need, forensic experts, legal advisors, and public relations firms, all which can be crucial during a crisis.

Identify the scope of coverage

Coverage varies and so does the type and level of protection.

- A good insurance broker can assess your specific needs, exposures and potential financial impacts to recommend appropriate coverage and tailor the policy to cover:

  First-party coverage: This includes financial costs directly associated with a cyber incident, breach or system failure, such as data recovery costs, business interruption losses, and cyber extortion negotiations and payments associated with a ransomware attack.
- **Third-party coverage:** Protects against claims made by customers, partners, or other third parties affected by a cyber incident at your business. This includes lawsuits, regulatory defence and penalties, legal fees, settlements, and regulatory fines.
- **Incident response costs:** Ensure your policy covers the cost of hiring experts for forensic investigations, public relations, and legal consultation following a breach.
- eCrime provides first party protections against loss of funds due to fraudulent instruction or funds transfer fraud.

Περισσότερες Πληροφορίες

CYBER SECURITY AWARDS 2024

GOLD

Nikos Georgopoulos

Digital Risks Insurance Broker

Email: nikos.georgopoulos@cromar.gr