Ο Ορίζοντας Κυβερνοασφάλειας 2026

Επαναπροσδιορίζοντας την Ανθεκτικότητα στην Εποχή της Τεχνητής Νοημοσύνης.

Στρατηγική ενημέρωση για στελέχη διοίκησης σχετικά με τον συστημικό κίνδυνο, τα όρια της Τεχνητής Νοημοσύνης και τη συνεχή θωράκιση.

Nikos Georgopoulos-Digital Risk Insurance Broker -CCRS -CDPO-AI Officer

Η Ψευδαίσθηση της Ετοιμότητας

82% των στελεχών παγκοσμίως δηλώνουν «έτοιμοι» για τους κυβερνοκινδύνους.

78% αναμένουν πλήρη οικονομική ανάκαμψη μετά από μια επίθεση.

Η Σκληρή Πραγματικότητα

Το 54% των επιθέσεων αξιοποιούν παραβιασμένα διαπιστευτήρια VPN (Q4 2025).

Οι επιθέσεις δεν είναι πλέον μεμονωμένα προβλήματα IT. Έχουν μετατραπεί σε παρατεταμένες λειτουργικές κρίσεις που παραλύουν ολόκληρες αλυσίδες εφοδιασμού.

Η υπερβολική αυτοπεποίθηση των στελεχών αποτελεί στρατηγικό τυφλό σημείο.

Η Εξέλιξη της Κυβερνοαπειλής

Το Παρελθόν
(Μεμονωμένη Απειλή)

Εστίαση: Απώλεια δεδομένων.

Αντίκτυπος: Πρόστιμα IT και μεμονωμένες διαρροές.

Το Παρόν
(Λειτουργική Παράλυση)

Εστίαση: Ransomware & Επιθέσεις σε υποδομές.

Αντίκτυπος: Πλήρης διακοπή λειτουργίας (Outages), απώλεια εσόδων.

2026 & Μετά
(Συστημική Κρίση)

Εστίαση: Τεχνητή Νοημοσύνη, Εφοδιαστική Αλυσίδα, Γεωπολιτική.

Αντίκτυπος: Φυσικές ζημιές (π.χ. παρεμβολές GPS στη ναυτιλία), ευθύνη στελεχών (D&O), ρυθμιστικές ρυθμιστικές συγκρούσεις πολλαπλών δικαιοδοσιών.

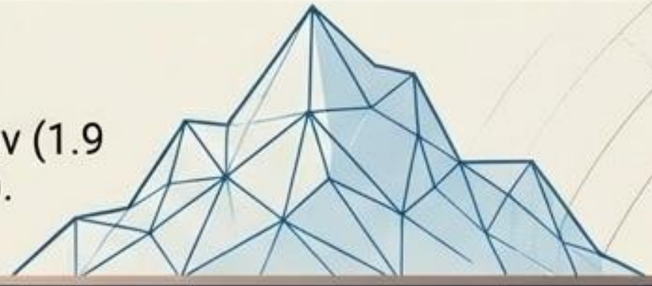
Η νέα πραγματικότητα απαιτεί νέα στρατηγική προστασίας.

Άμεση Λειτουργική Διακοπή

Διάρκεια: 11.6 Ημέρες (Μέσος όρος αδράνειας στη μεταποίηση).

Ενέργειες: Απομόνωση συστημάτων, Forensics, προσωρινές λύσεις.

Κόστος: Άμεση απώλεια εσόδων (1.9 εκατ. $ / ημέρα).



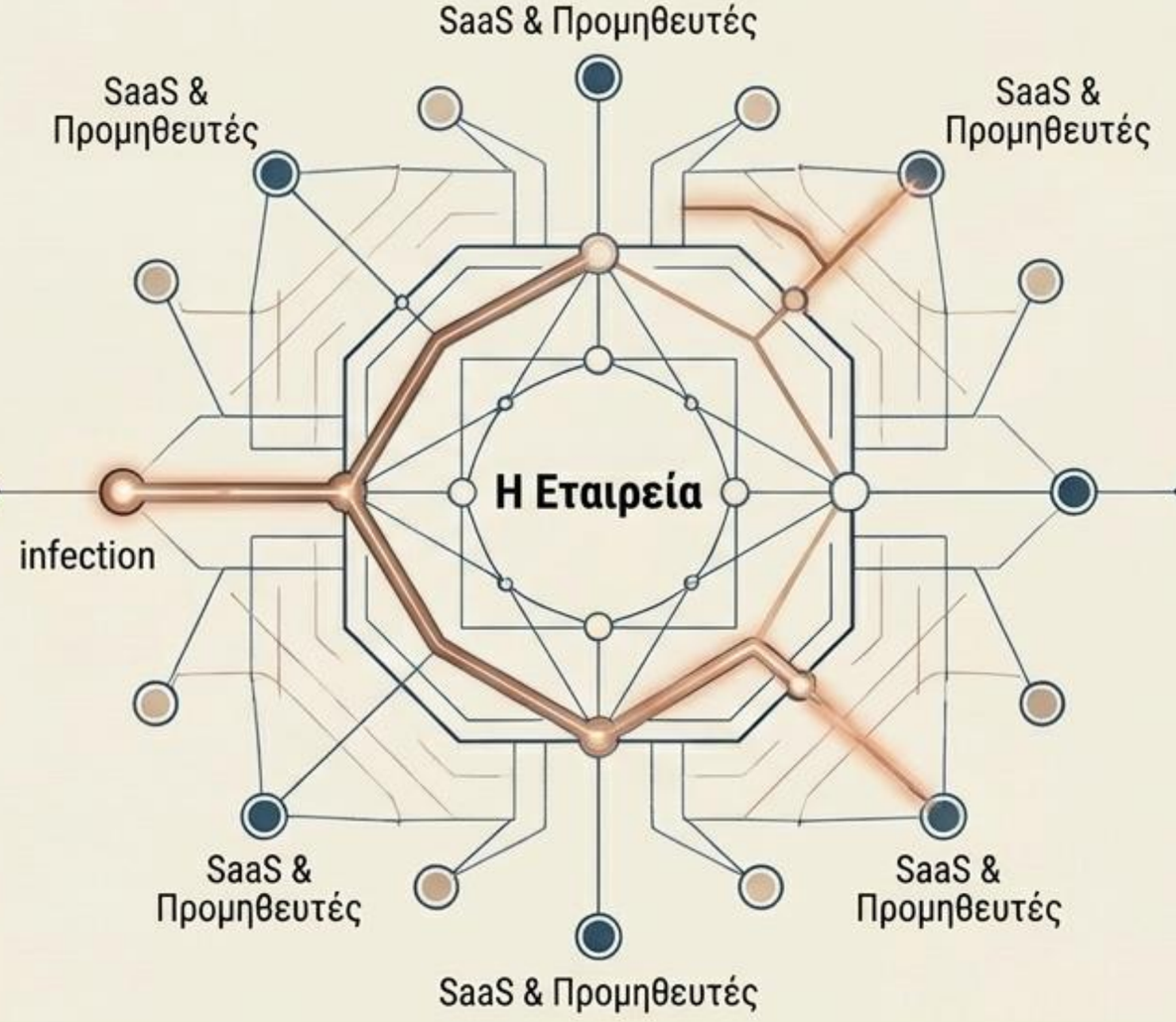
Η Μακρά Ουρά της Κρίσης

Διάρκεια: 6 έως 18+ Μήνες

25%	**της ζημιάς:** Κόστος ανταπόκρισης.
45%	**της ζημιάς:** Πρωτογενείς απώλειες / Διακοπή εργασιών.
30%	**της ζημιάς:** Απαιτήσεις τρίτων (Αγωγές προμηθευτών, ρυθμιστικά πρόστιμα).

Το Φαινόμενο Ντόμινο στην Εφοδιαστική Αλυσίδα

30%
των παραβιάσεων εμπλέκουν τρίτους προμηθευτές (Διπλασιασμός σε ένα έτος).



Ευπάθειες Προμηθευτών: Οι επιτιθέμενοι στοχεύουν παρόχους SaaS ως πύλες εισόδου.

Συστημικές Αστοχίες: Αστοχίες λογισμικού προκαλούν παγκόσμια παράλυση (π.χ. περιστατικό 8.5 εκατ. συσκευών).

Τα βασικά μέτρα προστασίας δεν επαρκούν, εάν το ευρύτερο οικοσύστημά σας καταρρεύσει.

Το Παράδοξο της Τεχνητής Νοημοσύνης: Οφέλη και Κίνδυνοι

Το Καλό (The Good)	Το Κακό (The Bad)	Το Άσχημο (The Ugly)
• **Επιτάχυνση:** Αυτοματοποιημένες αποφάσεις και Vibe Coding (δημιουργία κώδικα από ασαφείς ιδέες σε δευτερόλεπτα). • **Άμυνα:** Ανακάλυψη κινδύνων και απόκριση σε ταχύτητα μηχανής.	• **Σκιώδης Χρήση (Shadow AI):** Αύξηση έως και 250% της μη εγκεκριμένης χρήσης χρήσης AI. • **Υπερβολική Εξουσιοδότηση:** Λανθασμένες αποφάσεις συστημάτων με πλήρη πρόσβαση στα δεδομένα.	• **Παραπλάνηση:** Επιθέσεις Phishing βασισμένες σε AI (82% ποσοστό επιτυχίας). • **Deepfakes:** Συνθετικές εικόνες και κλωνοποίηση φωνής.

Ασύμμετρος Πόλεμος: Η Κλίμακα του Επιτιθέμενου

Παραδοσιακές Επιθέσεις

Αναγνώριση Στόχων → **Χειροκίνητη Προετοιμασία** → **Εκτέλεση Επίθεσης**

Χειροκίνητη διαδικασία, βραδεία αναγνώριση στόχων, υψηλό κόστος εκτέλεσης.

Επιθέσεις Υποβοηθούμενες από AI

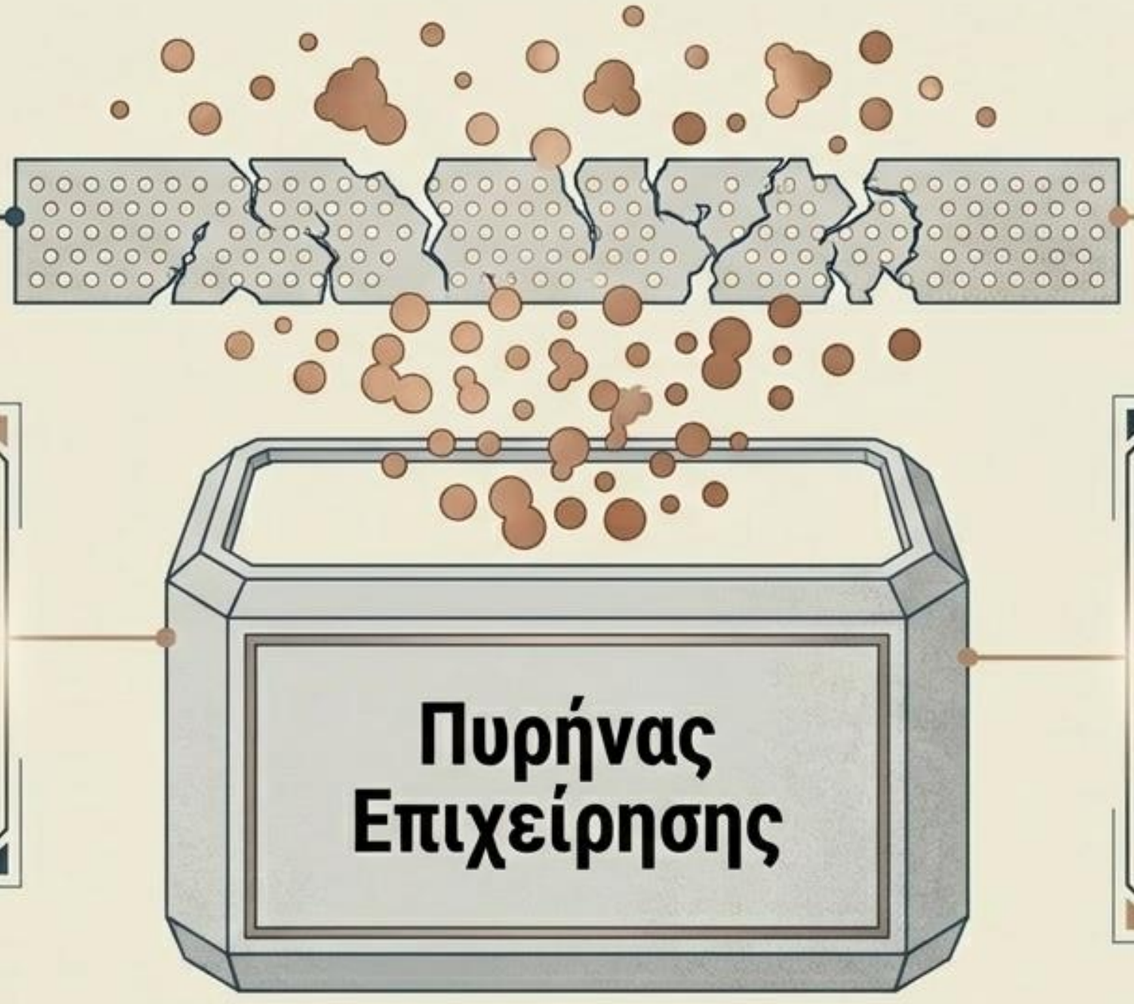
Μαζικές αυτοματοποιημένες εκστρατείες. Οι εγκληματίες ανοιχτά μοντέλα για να βρουν ευπάθειες σε κλάσματα δευτερολέπτου.

Η Ανθρώπινη Ευπάθεια

- **3 δευτερόλεπτα:** Αρκούν για την κλωνοποίηση της φωνής ενός στελέχους με 85% ακρίβεια.
- Το **77%** των θυμάτων απατών με τεχνητή φωνή κατέληξαν σε οικονομική απώλεια.

Το Κενό Διακυβέρνησης: Η Απειλή Εκ των Έσω

Φίλτρο Διακυβέρνησης (Ανεπαρκές)



Σκιώδες AI (Shadow AI)

Το **35%** επενδύουν στο AI για ανθεκτικότητα, αλλά το **72%** αναμένει **απώλειες θέσεων εργασίας σε 18 μήνες** (κίνδυνος εσωτερικών απειλών).

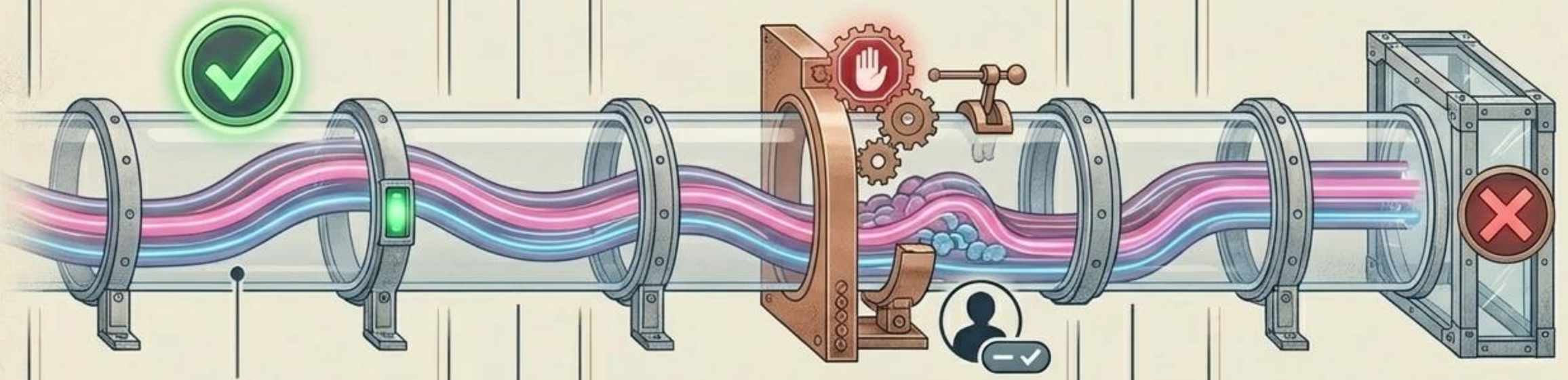
Πυρήνας Επιχείρησης

Ο **Κίνδυνος της Εξουσιοδότησης:** Όταν οι πράκτορες AI συνδέονται με τον πυρήνα χωρίς όρια, ένα απλό σφάλμα (prompt injection) προκαλεί μαζική απώλεια δεδομένων.

Η καινοτομία χωρίς εποπτεία πολλαπλασιάζει την επιφάνεια επίθεσης.

Οριοθετημένη Αυτονομία: Μοντέλο Ασφάλειας από Σχεδιασμού

Ρητά Δικαιώματα



Το σύστημα AI έχει δικαίωμα "**ανάγνωσης**" αλλά **όχι** "**διαγραφής**".

Κλιμακούμενη Έγκριση

Για ενέργειες υψηλού κινδύνου, το AI σταματά και απαιτεί **ανθρώπινη επιβεβαίωση**.

Ασφαλής Προεπιλογή

Αν το σύστημα δεν είναι βέβαιο, **ακυρώνει** την ενέργεια.

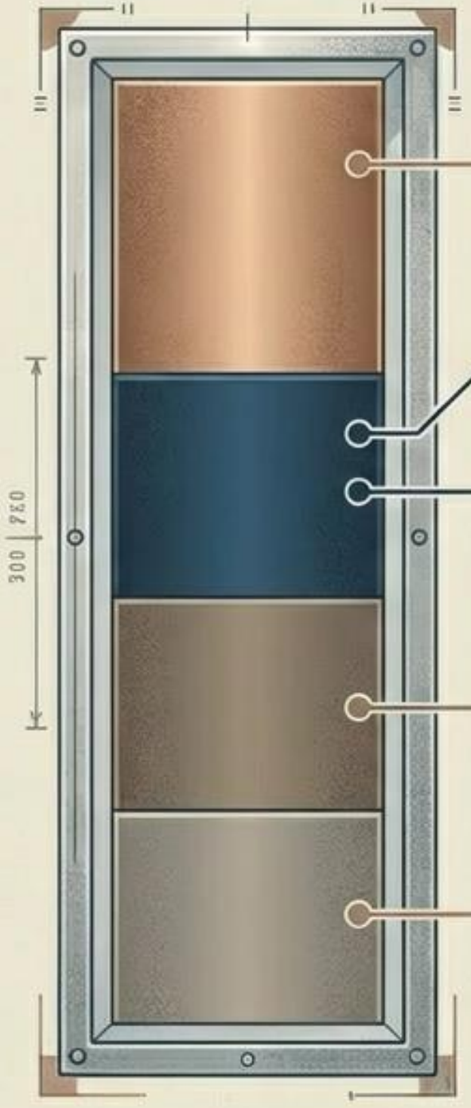
Η αυτοματοποίηση αυξάνει την ταχύτητα. Τα όρια (guardrails) διασφαλίζουν την επιβίωση.

Η Ευπάθεια των ΜμΕ: Ο Αδύναμος Κρίκος στο Οικοσύστημα

73%

των ΜμΕ πιστεύουν ότι μπορούν να ανακάμψουν πλήρως.

Η πραγματικότητα είναι εντελώς διαφορετική.



23%: Απώλεια δεδομένων / Ρυθμιστικά πρόστιμα.

18%: Μακροχρόνια διακοπή επιχειρηματικών λειτουργιών.

17%: Απαιτήσεις από τον χρόνο της διοίκησης.

17%: Απαιτήσεις αστικής ευθύνης τρίτων.

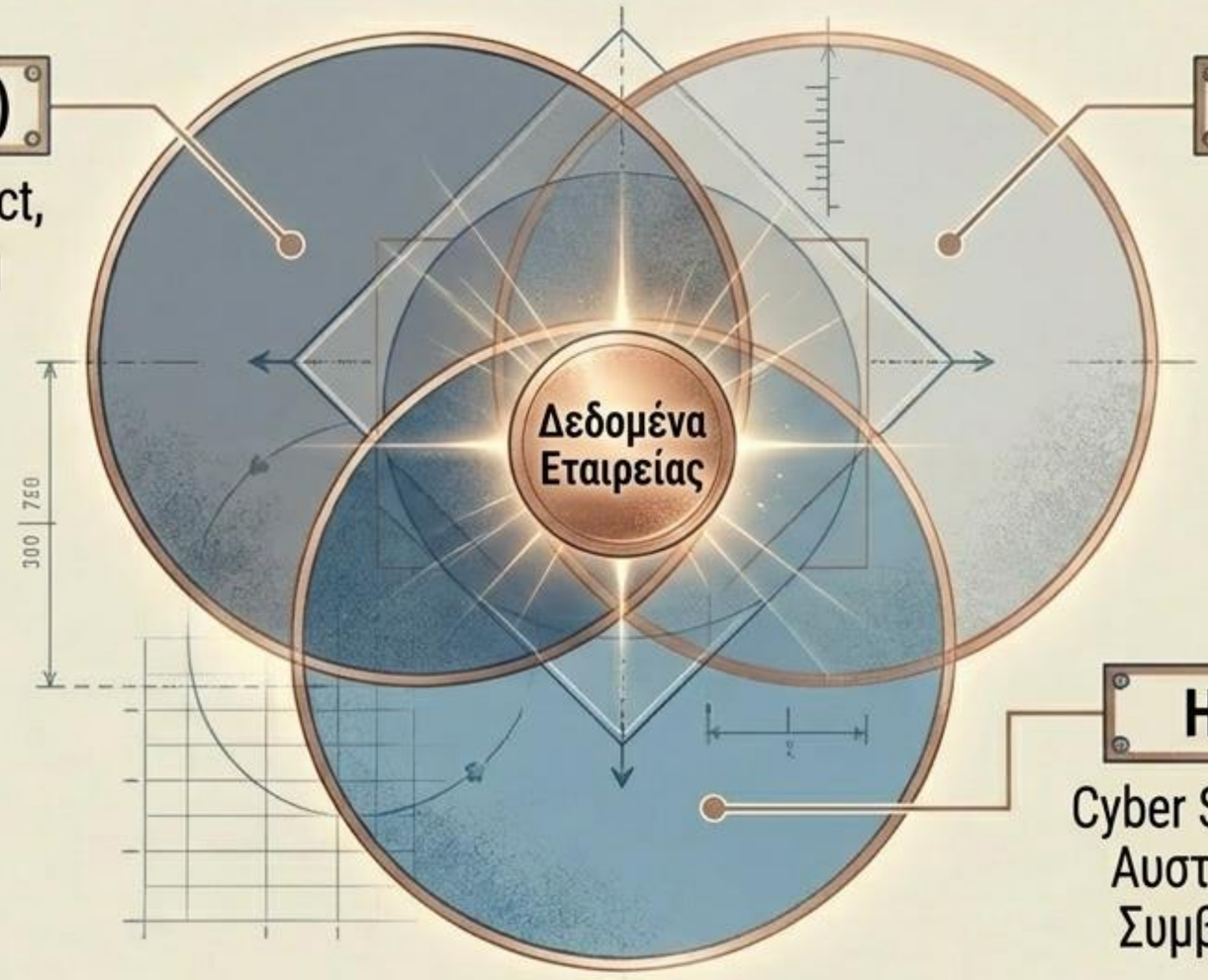
Αόρατο Κόστος

Καταστροφή φήμης, ψηφιακές απάτες, στοχευμένο sextortion και επιπτώσεις στην ψυχική υγεία.

Ο Ρυθμιστικός Λαβύρινθος: Η Γεωπολιτική των Δεδομένων

Ευρώπη (Κυριαρχία)

NIS2, Cyber Resilience Act, DORA, GDPR. Αυστηρή διατήρηση εντός ΕΕ.



ΗΠΑ (Διαφάνεια)

SEC Rules, CIRCIA (Αναφορά σε 72 ώρες), CLOUD Act.

Ηνωμένο Βασίλειο

Cyber Security and Resilience Bill. Αυστηρή ευθύνη Διοικητικών Συμβουλίων.

Μια παραβίαση δεν είναι απλώς τεχνικό σφάλμα. Αποτελεί ταυτόχρονη νομική κρίση σε πολλαπλές δικαιοδοσίες.

Ανασχεδιάζοντας την Ανθεκτικότητα

ΑΠΟ - Το Παλαιό Μοντέλο

- Στατική άμυνα (Firewalls)
- Ετήσιοι έλεγχοι (Audits)
- Η κυβερνοασφάλεια ως “πρόβλημα του IT”
- Πεποίθηση ότι η πρόληψη αρκεί

ΠΡΟΣ - Το Νέο Μοντέλο

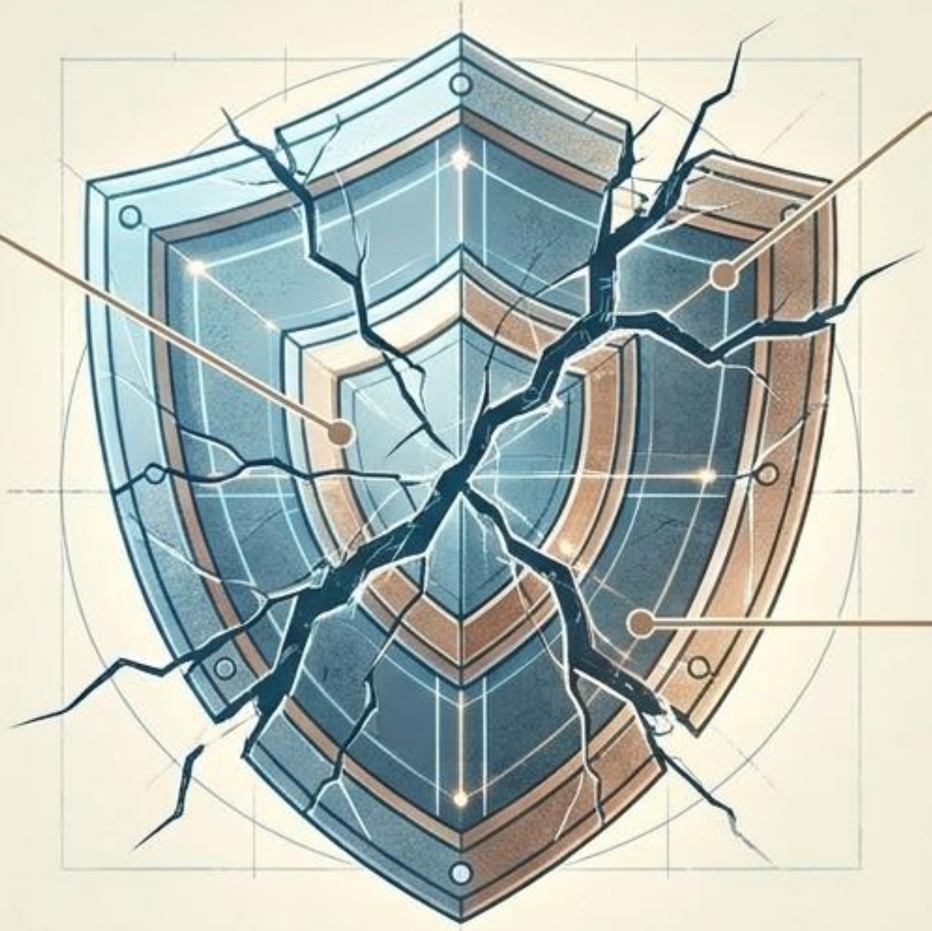
- Διαρκής ανθεκτικότητα
- Συνεχής ορατότητα (MXDR)
- Η κυβερνοασφάλεια ως ευθύνη του Δ.Σ.
- Παραδοχή ότι η παραβίαση είναι αναπόφευκτη

Η ανθεκτικότητα σήμερα δεν σημαίνει αποτροπή κάθε περιστατικού.
Σημαίνει διατήρηση του αντίκτυπου σε μικρή κλίμακα και γρήγορη ανάκαμψη.

Τα Όρια του Ελέγχου: Όταν η Πρόληψη Αποτυγχάνει

Η Υγιεινή δεν αρκεί:

Το MFA παρακάμπτεται από προηγμένη κοινωνική μηχανική.



Zero-Day Ευπάθειες:

Οι επιτιθέμενοι εκμεταλλεύονται κενά πριν υπάρξει λύση προστασίας (patch).

Φυσικές Συνέπειες:

Ψηφιακές επιθέσεις προκαλούν υλικές ζημιές (π.χ. παρεμβολές GPS που οδηγούν σε απώλεια φορτίου).

Πρέπει να προετοιμαστείτε για τη διαχείριση ζημιών που ούτε οι εσωτερικοί έλεγχοι ούτε οι συνεργάτες μπορούν να καλύψουν.

Η Γέφυρα της Ασφάλισης: Χαρτογράφηση των Κενών

Ευθύνη Στελεχών (D&O)

Κίνδυνος αγωγών κατά μελών του Δ.Σ. για παραβίαση καθηκόντων λόγω ελλιπούς προετοιμασίας.

Διακοπή Εργασιών (Business Interruption)

Τα συμβόλαια περιουσίας δεν καλύπτουν ψηφιακή διακοπή. Απαιτείται κάλυψη για τον χαμένο χρόνο και έσοδα.

Φυσικές Ζημιές (Physical Damage)

Η ψηφιακή δολιοφθορά (π.χ. βλάβη εξοπλισμού) εξαιρείται από τα τυπικά ασφαλιστήρια χωρίς ειδική ρήτρα.

Η αποτελεσματική ασφάλιση απαιτεί αναγνώριση και κάλυψη των κενών μεταξύ φυσικής και ψηφιακής ευθύνης.

Αρχιτεκτονική Συνεχούς Ανθεκτικότητας: Το Σχέδιο Δράσης

Μεταφορά Κινδύνου (Risk Transfer)
Ολιστική Κυβερνοασφάλιση. Κάλυψη για D&O, Διακοπή Εργασιών, Υλικές Ζημιές και 24/7 απόκριση.

Αντάφαση Κινδύνου
Safety-by-design, έλεγχος αποφάσεων AI από ανθρώπους, διαχείριση προμηθευτών.

Οριοθετημένη Αυτονομία (Governance)
Safety-by-design, έλεγχος αποφάσεων AI από ανθρώπους, διαχείριση προμηθευτών.

Οριοθετημένη Αυτονομία
Safety-by-design, έλεγχος αποφάσεων AI από ανθρώπους, διαχείριση προμηθευτών.

Η ανθεκτικότητα είναι πλέον μια καθημερινή πειθαρχία σε επίπεδο Διοικητικού Συμβουλίου.