
INFOCOM SECURITY 2026
Proactive Cyber Insurance: Ο Καταλύτης της Κυβερνοανθεκτικότητας
Η στρατηγική μετάβαση από τη μεταφορά κινδύνου στην ενεργή διακυβέρνηση.
Νίκος Γεωργόπουλος- Digital Risk Insurance Broker - Cromar Insurance Brokers
NotebookLM

25 YEARS

CROMAR

Lloyd's Market Innovation Awards 2016 Best Coverholder innovation

Insurance Awards Insurance Insight Best Segmentation Award 2017

FM Awards Disruptive Innovation Gold Award 2022

Digital Finance Awards 2023 Bronze Best Monitoring & Optimization Tools Solutions

FM Awards Disruptive Innovation Gold Award 2023

Cyber Security Awards 2024 Gold

FM Awards Customer Centricity Gold Award 2024

Digital Finance Awards 2026 Silver

Cyber Security Awards 2026 Bronze

Η Πραγματικότητα του 2026: Ασύμμετρος Οικονομικός Κίνδυνος

Το κυβερνοέγκλημα δεν αποτελεί πλέον μεμονωμένο τεχνικό συμβάν, αλλά υπαρξιακή απειλή για τον ισολογισμό.

> $28 Εκατομμύρια
Ο μέσος όρος ζημιάς στο ανώτερο 10% των καταστροφικών επιθέσεων το 2024.

$3 Εκατομμύρια
Το μέσο ετήσιο κόστος ανά περιστατικό (Median Loss).

15πλάσια Αύξηση
Αύξηση των μέσων ετήσιων ζημιών τα τελευταία 15 χρόνια.

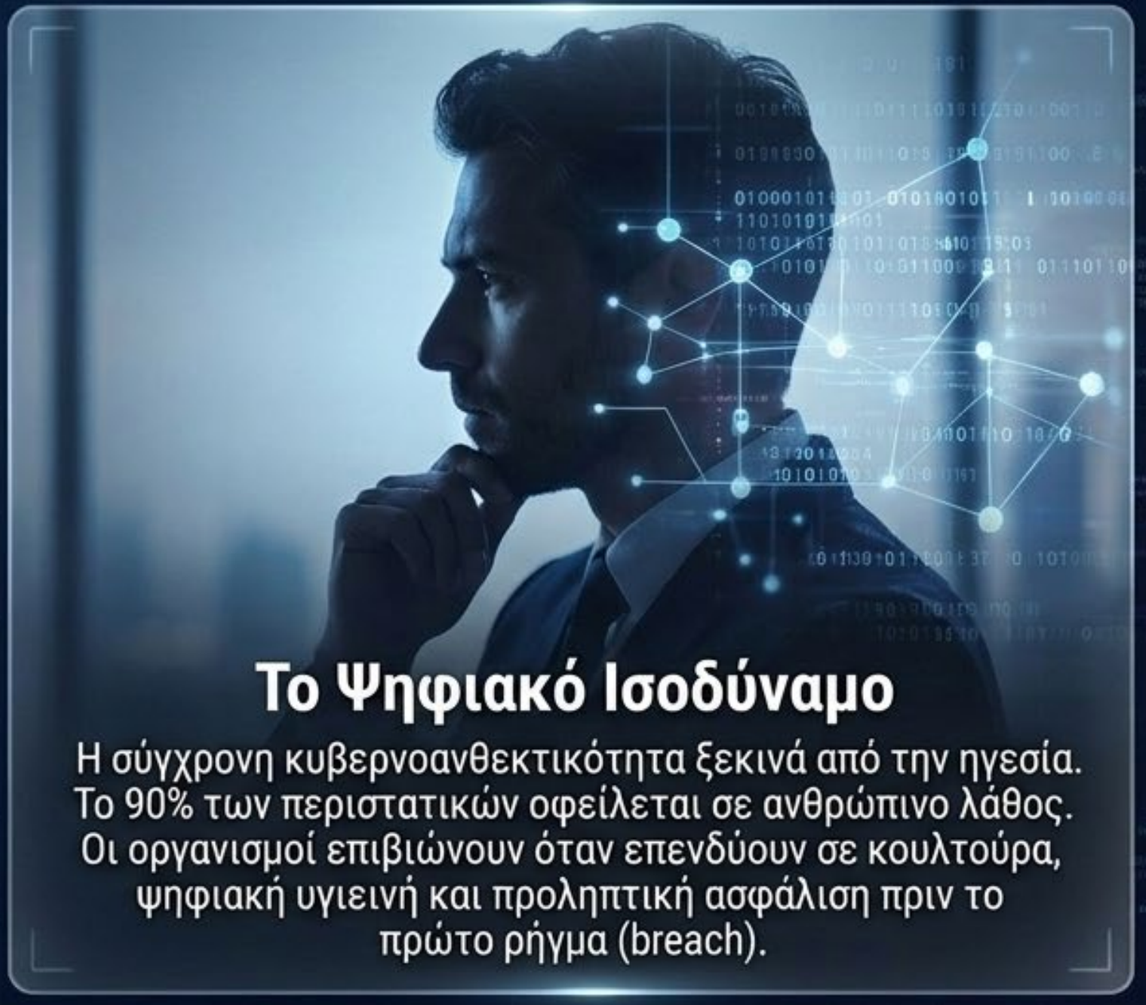
Το Ελληνικό Παράδοξο
Ενώ το διεθνές κενό προστασίας αγγίζει το 95%, στην Ελλάδα το 99% των ΜμΕ παραμένουν ανασφάλιστες. Λιγότερο από το 1% έχει μηχανισμό μεταφοράς κινδύνου.

Ο Κυβερνοκίνδυνος είναι Οικονομικός Κίνδυνος.
Δεν είναι "IT θέμα" – είναι άμεση απειλή ρευστότητας και λειτουργικής συνέχειας.

Το Δίδαγμα του Θεμιστοκλή: Η Προνοητικότητα ως Ασπίδα

Η Πρόβλεψη

Όπως ο Θεμιστοκλής προέβλεψε την περσική απειλή και επέμεινε στην κατασκευή του αθηναϊκού στόλου πριν εμφανιστεί ο κίνδυνος, η ανθεκτικότητα δεν χτίζεται μέσα στην κρίση — χτίζεται πριν από αυτήν.



Το Ψηφιακό Ισοδύναμο

Η σύγχρονη κυβερνοανθεκτικότητα ξεκινά από την ηγεσία. Το 90% των περιστατικών οφείλεται σε ανθρώπινο λάθος. Οι οργανισμοί επιβιώνουν όταν επενδύουν σε κουλτούρα, ψηφιακή υγιεινή και προληπτική ασφάλιση πριν το πρώτο ρήγμα (breach).

Η «Σαλαμίνα» του Κυβερνοχώρου: Επιλέγοντας το Πεδίο Μάχης

Η μεγαλοφυΐα δεν ήταν μόνο ο στόλος, αλλά η επιλογή του πεδίου μάχης. Στον ψηφιακό κόσμο, το πεδίο μάχης το διαμορφώνεις εσύ.

Zero Trust Αρχιτεκτονική

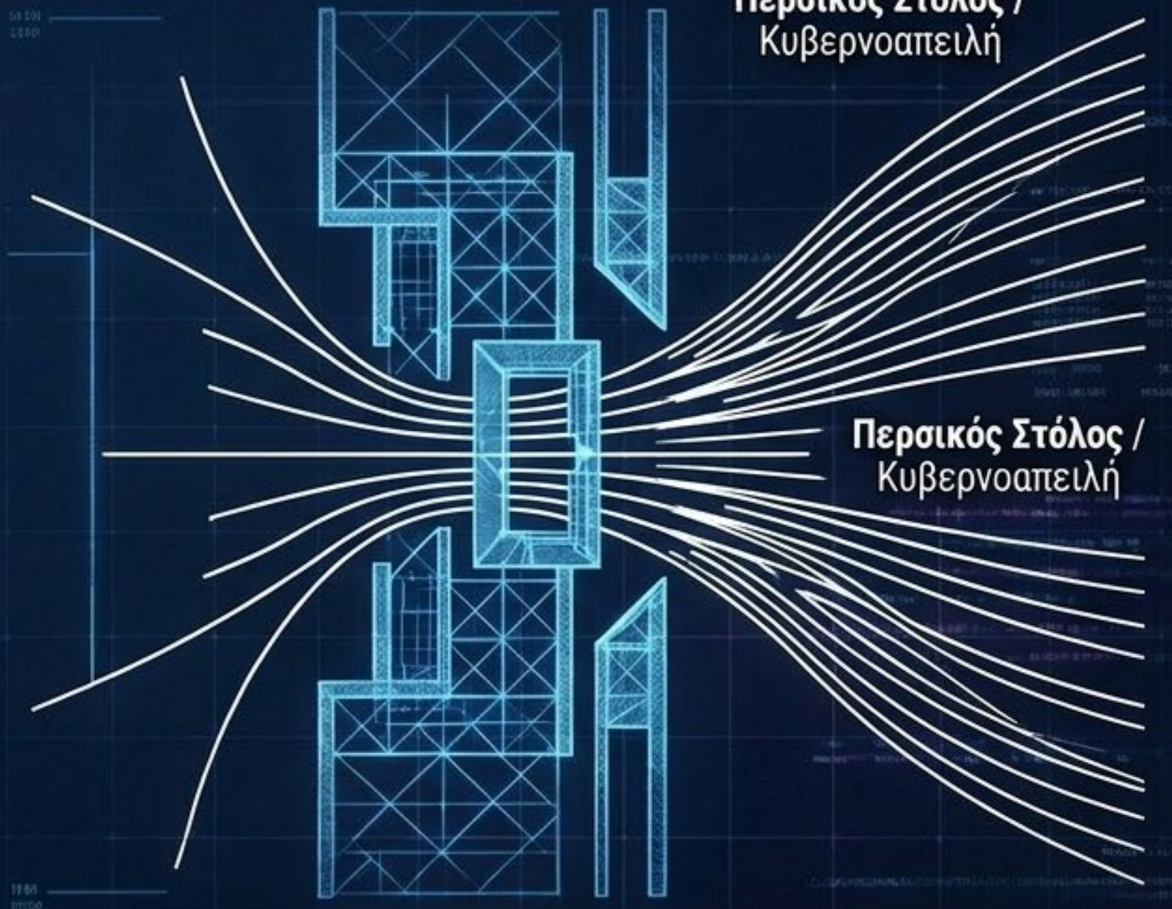
Δεν αφήνεις τον αντίπαλο να κινηθεί ελεύθερα. Κάθε ταυτότητα ελέγχεται συνεχώς.

Network Segmentation

Στενεύεις τα «ψηφιακά στενά» (όπως η Σαλαμίνα), απομονώνοντας τα κρίσιμα συστήματα για να εμποδίσεις την πλευρική κίνηση (lateral movement).

Least Privilege

Μειώνεις την επιφάνεια επίθεσης, εξουδετερώνοντας το αριθμητικό πλεονέκτημα του αντιπάλου.



LOGO

Η Οδηγία NIS2 (Ν. 5160/2024): Η Μετάβαση της Ευθύνης

Η κυβερνοασφάλεια δεν μπορεί πλέον να μεταβιβαστεί (outsourced) αποκλειστικά στο τμήμα IT. Οι ρυθμιστικές αρχές αναζητούν την ενεργό εμπλοκή της διοίκησης.

1. Τεχνικό Κενό

Έλλειψη βασικής κυβερνοϋγιεινής (π.χ. unpatched software).

2. Ρυθμιστικός Έλεγχος

Ενεργοποίηση Ν. 5160/2024 και εθνικών αρχών (ΕΑΚ).

3. Προσωπική Ευθύνη (C-Suite)

Το ανώτατο όργανο διοίκησης λογοδοτεί άμεσα. Απειλή προσωρινής παύσης άσκησης διευθυντικών καθηκόντων και βαριά διοικητικά πρόστιμα.

LOGO

Management Liability: Το Δίχτυ Ασφαλείας της Ψηφιακής Ηγεσίας

Σε ένα περιβάλλον αυστηρής εποπτείας, η ρήτρα Management Liability εντός ενός προληπτικού συμβολαίου μετατρέπει την κυβερνοασφάλεια σε διαχειρίσιμο κίνδυνο.

1. Προσωπική Οικονομική Προστασία

Αποτρέπει την καταστροφή της προσωπικής περιουσίας των μελών του Δ.Σ. και των στελεχών επιπέδου C.

2. Κάλυψη Δικαστικών Εξόδων

Χρηματοδότηση των δαπανών υπεράσπισης κατά τη διάρκεια νομικών ή ρυθμιστικών διενέξεων (π.χ. έρευνες από αρχές).

3. Απόδειξη Προνοητικότητας

Η χρήση Real-Time Threat Intelligence αποδεικνύει την ‘ενεργή εποπτεία’ της διοίκησης, αποκρούοντας κατηγορίες περί αμέλειας.

LOGO

Το Εισιτήριο της Ασφαλισιμότητας: Βασική Ψηφιακή Υγιεινή

Η Proactive Cyber Insurance δεν αναλαμβάνει χαοτικούς κινδύνους. Προϋποθέτει μια βάση ψηφιακής πειθαρχίας. Αυτά δεν είναι «κουτάκια για τσεκάρισμα», αλλά ο θεμέλιος λίθος της προστασίας.

MFA (Πολυπαραγοντική Ταυτοποίηση)

Το απόλυτο φίλτρο. Αποτρέπει πάνω από το 94% των παραβιάσεων ταυτότητας.

Στρατηγική Backups (3-2-1)

Τρία αντίγραφα, σε δύο διαφορετικά μέσα, ένα εκτός τοποθεσίας. Το κλειδί για την ακύρωση του εκβιασμού ransomware.

Patch Management

Συστηματική ενημέρωση συστημάτων. Κλείσιμο των ευπαθειών πριν τις ανακαλύψει ο επιτιθέμενος.

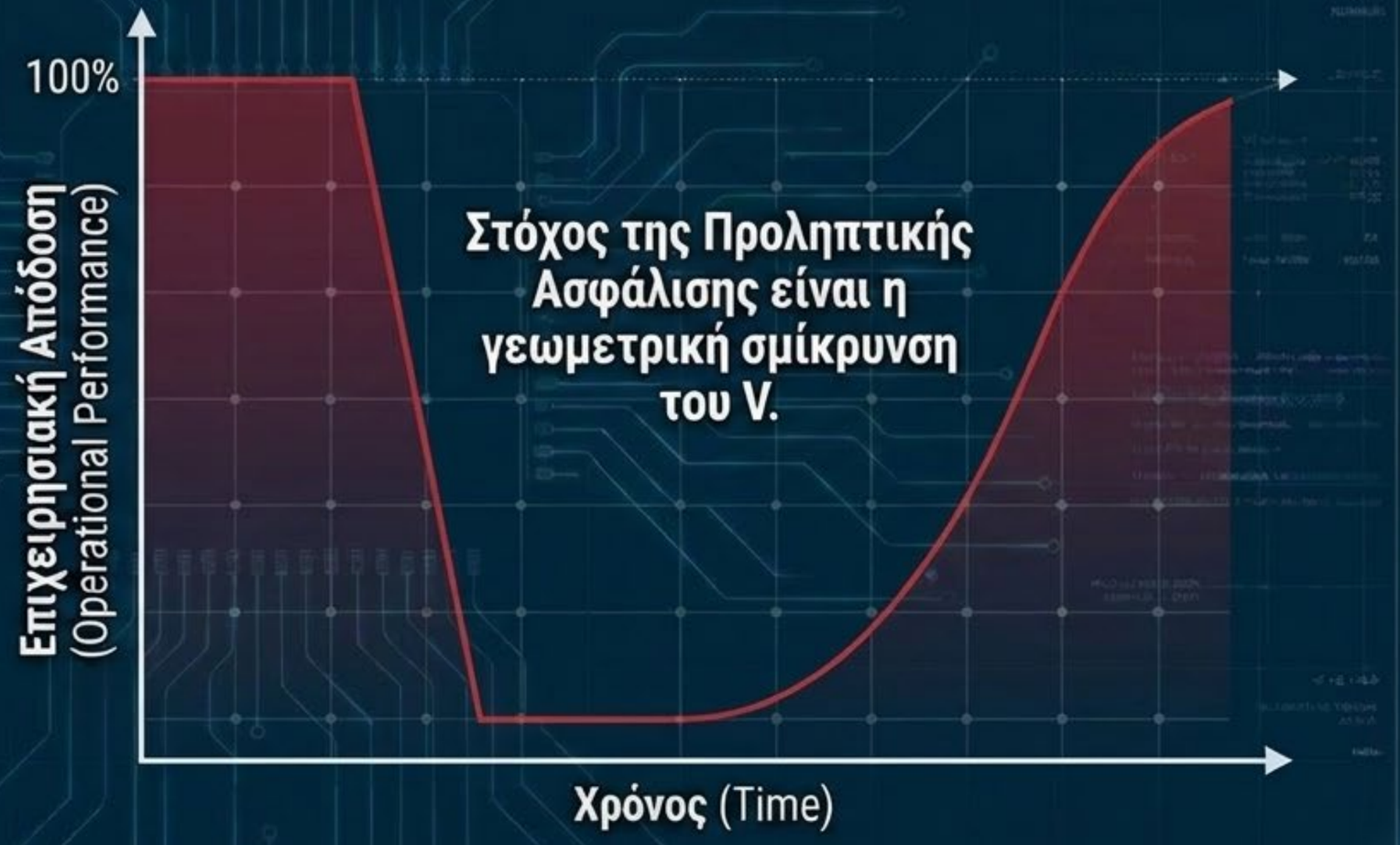
LOGO

Η Αλλαγή Παραδείγματος: Παθητική vs. Προληπτική Ασφάλιση

	Παθητική	Προληπτική
Μηχανισμός Αξιολόγησης	Στατικά ερωτηματολόγια 30 σελίδων άπαξ ετησίως.	Συνεχής τηλεμετρία (Continuous Underwriting) και εργαλεία AI.
Ρόλος Ασφαλιστή	Απλός πληρωτής αποζημιώσεων μετά την καταστροφή.	Ενεργός στρατηγικός σύμβουλος (Insurance-as-a-Service).
Χρόνος Παρέμβασης	Μετά την παραβίαση (Post-breach).	Πριν την παραβίαση (Real-time alerts & Threat Intelligence).

Το «Τρίγωνο της Ανθεκτικότητας»

Η ανθεκτικότητα αποτυπώνεται οπτικά ως ένα "V". Η ζημιά ορίζεται από δύο διαστάσεις: το βάθος της λειτουργικής πτώσης (μέγεθος ζημιάς) και τη χρόνου ανάκαμψης.



Σμίκρυνση του "V" - Μέρος 1: Πρόληψη & Περιορισμός Βάθους

Η προστασία ενεργοποιείται πολύ πριν την επίθεση (Insurance-as-a-Service).

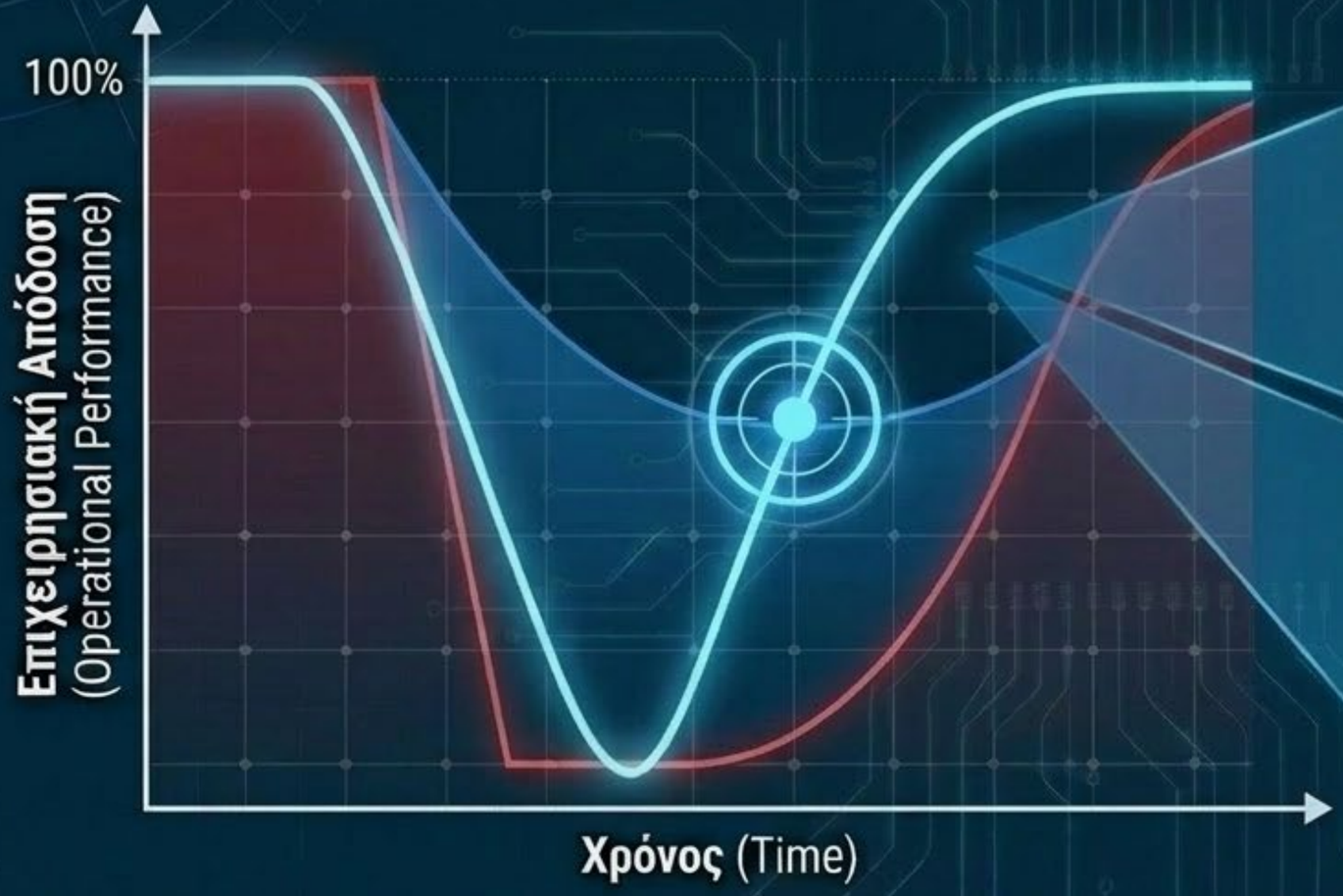
Phase 1: Πριν το Συμβάν

- **Συνεχής Τηλεμετρία & AI:** Αυτόματη ανάλυση δεδομένων από cloud και δίκτυα για τον εντοπισμό ευπαθειών σε πραγματικό χρόνο. Ειδοποίηση για κλείσιμο των "οπών" πριν την εκμετάλλευση.
- **Προειδοποιήσεις Απειλών:** Η ομάδα ασφαλείας ειδοποιείται πριν ο επιτιθέμενος εκμεταλλευτεί το κενό.
- **Αποτέλεσμα:** Το αρχικό "σοκ" απορροφάται. Η πτώση (το βάθος του V) είναι δραματικά μικρότερη, αποτρέποντας την ολική κατάρρευση συστημάτων.

LOGO

Σμίκρυνση του "V" - Μέρος 2: Άμεση Ανταπόκριση & Ταχεία Ανάκαμψη

Όταν το περιστατικό είναι αναπόφευκτο, η ταχύτητη καθορίζει την επιβίωση.



Phase 2: Κατά τη Διάρκεια (Containment)

- **Ενεργός Παρέμβαση** (Incident Response). Πρόσβαση 24/7 σε ειδικούς forensics και νομικούς. Άμεση απομόνωση μολυσμένων συστημάτων για να «σπάσει» η αλυσίδα της επίθεσης (Kill Chain) πριν εξαπλωθεί στο δίκτυο.

Phase 3: Μετά το Συμβάν (Recovery)

- **Οικονομική Ενέσιμη Ρευστότητα.** Κάλυψη απωλειών από Διακοπή Εργασιών (Business Interruption), ταχεία ανασυγκρότηση συστημάτων και αποκατάσταση φήμης. Η επιχείρηση αναδύεται ταχύτερα και πιο ισχυρή.

LOGO

EXECUTIVE STRATEGIC DOSSIER

Τα «Ξύλινα Τείχη» του 2026: Απόλυτη Κυβερνοανθεκτικότητα

Η αληθινή ψηφιακή ανθεκτικότητα δεν αγοράζεται. Συντίθεται.
(Να συνεχίζεις να λειτουργείς, ακόμη κι όταν όλα γύρω σου καταρρέουν).

Ηγεσία
(Η Στρατηγική του Θεμιστοκλή):
Ενεργός εμπλοκή της διοίκησης, Management Liability, κουλτούρα προετοιμασίας (NIS2).

Αρχιτεκτονική
(Τα "Στενά" / Ψηφιακή Υγιεινή):
MFA, Backups, Patching, Zero Trust. Το εισιτήριο εισόδου.

Συμμαχίες
(Ενεργή Ασφάλιση):
Risk Transfer, Continuous Telemetry, AI alerts, και Incident Response.

Η ασφάλιση κυβερνοχώρου παύει να είναι απλή δαπάνη αποζημίωσης. Είναι ο απόλυτος μηχανισμός εταιρικής διακυβέρνησης και επιβίωσης.

LOGO

Το Στρατηγικό Πλεονέκτημα

> “Η διαχείριση του κινδύνου δεν είναι η αποφυγή της μάχης, αλλά η διασφάλιση ότι θα την κερδίσεις.

Η **Proactive Cyber Insurance** είναι ο “Θεμιστοκλής” δίπλα σου.
Σου δίνει τα εργαλεία να προβλέψεις, να εκπαιδεύσεις και, τελικά,
να αποζημιωθείς αν τα “ξύλινα τείχη” υποστούν ζημιές.

Είναι καιρός να περάσουμε από την άγνοια στην ενεργό προστασία.

Νίκος Γεωργόπουλος | Digital Risk Insurance Broker – CCRS – DPO – AI Officer | nikos.georgopoulos@cromar.gr

Nikos Georgopoulos

Add verification badge

🛡️ Digital Risk Insurance Broker| Co-Founder DPO Academy |Cyber Resilience Strategist | Helping Companies Prevent & Recover from Cyber Attacks | DPO | AI Officer | CCRS| Innovator |🏆 Favikon"Cyber Sage"|

Athens Metropolitan Area · Contact info

26,214 followers · 500+ connections

Cromar - Lloyd's Best Coverholder Innovation

ALBA Graduate Business School

youtube.com/@nikosgeorgopoulos6758

YouTube GR

Search

Cyber Snacks by Nikos Georgopoulos

@nikosgeorgopoulos6758 · 33 subscribers · 103 videos

Cyber Snacks by Nikos Georgopoulos! ...more

linkedin.com/in/nikos-georgopoulos

Customize channel Manage videos

Digital Risk Insurance


INFOCOM SECURITY 2026
Proactive Cyber Insurance: Ο Καταλύτης της Κυβερνοανθεκτικότητας
Η στρατηγική μετάβαση από τη μεταφορά κινδύνου στην ενεργή διακυβέρνηση.
Νίκος Γεωργόπουλος- Digital Risk Insurance Broker - Cromar Insurance Brokers
NotebookLM