

NIS2 & Proactive Cyber Insurance: Ο Στρατηγικός Οδικός Χάρτης για τον CEO

Πλοήγηση στον «Ψηφιακό Λαβύρινθο» και η
Θωράκιση της Ηγεσίας (N. 5160/2024)



Η Νέα Πραγματικότητα σε Μία Σελίδα



Ο Κίνδυνος

Ο «Ψηφιακός Λαβύρινθος» αλλάζει κάθε βράδυ. Το ransomware ευθύνεται για >75% των συνολικών απωλειών. Ο κίνδυνος είναι πλέον υπαρξιακός, όχι τεχνικός.



Ο Νόμος

Η Οδηγία NIS2 (N. 5160/2024) καθιερώνει άμεση, προσωπική ευθύνη για τα όργανα διοίκησης (C-Level).



Η Λύση

Η Proactive Cyber Insurance δεν είναι απλή δαπάνη. Είναι μηχανισμός επιβίωσης που καλύπτει νομική ευθύνη, επιχειρησιακή συνέχεια και τεχνική απόκριση.

Από Τεχνικό Πρόβλημα σε Υπαρξιακό Κίνδυνο

Στη σύγχρονη επιχειρηματική πραγματικότητα, οι κυβερνοαπειλές δεν αφορούν μόνο το τμήμα πληροφορικής. Για τον CEO, ο κυβερνοκίνδυνος έχει μετεξελιχθεί σε θεμελιώδη επιχειρησιακό κίνδυνο.



«Ο 'Ψηφιακός Λαβύρινθος' στον οποίο κινούνται οι εταιρείες αλλάζει μορφή κάθε βράδυ.»

Ο Καταλύτης: Νόμος 5160/2024 (NIS2)

Ενσωμάτωση

Η Οδηγία NIS2 ενσωματώθηκε στην ελληνική νομοθεσία, καθιστώντας την κυβερνοασφάλεια αναπόσπαστο κομμάτι της Εταιρικής Διακυβέρνησης.

Οι Κυρώσεις

Πρόστιμα που φτάνουν τα €10.000.000 ή το 2% του παγκόσμιου κύκλου εργασιών.

Η Αλλαγή

Η συμμόρφωση δεν είναι προαιρετική, αλλά από μόνη της δεν αρκεί για την προστασία.



Τι είναι η Proactive Cyber Insurance;

Ένας δυναμικός μηχανισμός επιβίωσης, όχι απλώς ένα συμβόλαιο αποζημίωσης.



Παραδοσιακή Ασφάλιση:
Πληρωμή μετά τη ζημιά.



Proactive Cyber Insurance:
Πρόληψη + Απόκριση + Αποζημίωση.

Προσφέρει ενεργή προστασία (vulnerability scanning, threat hunting) καθ' όλη τη διάρκεια του συμβολαίου, λειτουργώντας ως «δίκτυ ασφαλείας» δίπλα στα εσωτερικά μέτρα IT.

Η Προσωπική Ευθύνη της Ηγεσίας (NIS2 Άρθρο 14)

Ο ΚΙΝΔΥΝΟΣ

Η NIS2 καθιερώνει άμεση και προσωπική λογοδοσία για τα όργανα διοίκησης. Το Διοικητικό Συμβούλιο και τα C-level στελέχη είναι υπεύθυνα για την έγκριση και επίβλεψη μέτρων.



Κίνδυνος: Προσωπική ευθύνη για παραβάσεις και πιθανή απαγόρευση άσκησης διευθυντικού δικαιώματος.

Η ΑΣΠΙΔΑ

Management Liability Coverage

Η Proactive Cyber Insurance παρέχει κάλυψη που προστατεύει τα στελέχη έναντι απαιτήσεων από κυβερνοπεριστατικά.



Καλύπτει πλήρως τις αποζημιώσεις και τα έξοδα υπεράσπισης.

Ενισχύοντας την Ανθεκτικότητα: Πρόληψη (NIS2 Άρθρο 15)

Το Άρθρο 15 επιβάλλει μια «ολιστική προσέγγιση» με τεχνικά και οργανωτικά μέτρα.



«Πρόληψη έναντι Αποζημίωσης» – Το συμβόλαιο λειτουργεί πριν συμβεί το περιστατικό.

Διασφάλιση Επιχειρησιακής Συνέχειας & Ρευστότητας

Η ανάγκη διατήρησης της λειτουργίας μετά από επίθεση (Business Continuity) είναι κρίσιμη.



Ανάκτηση

Κάλυψη κόστους ανασύστασης δεδομένων.



Hardware & OT

Αντικατάσταση υλικού (συμπεριλαμβανομένων συστημάτων OT/SCADA) αν είναι πιο οικονομική από την επισκευή.

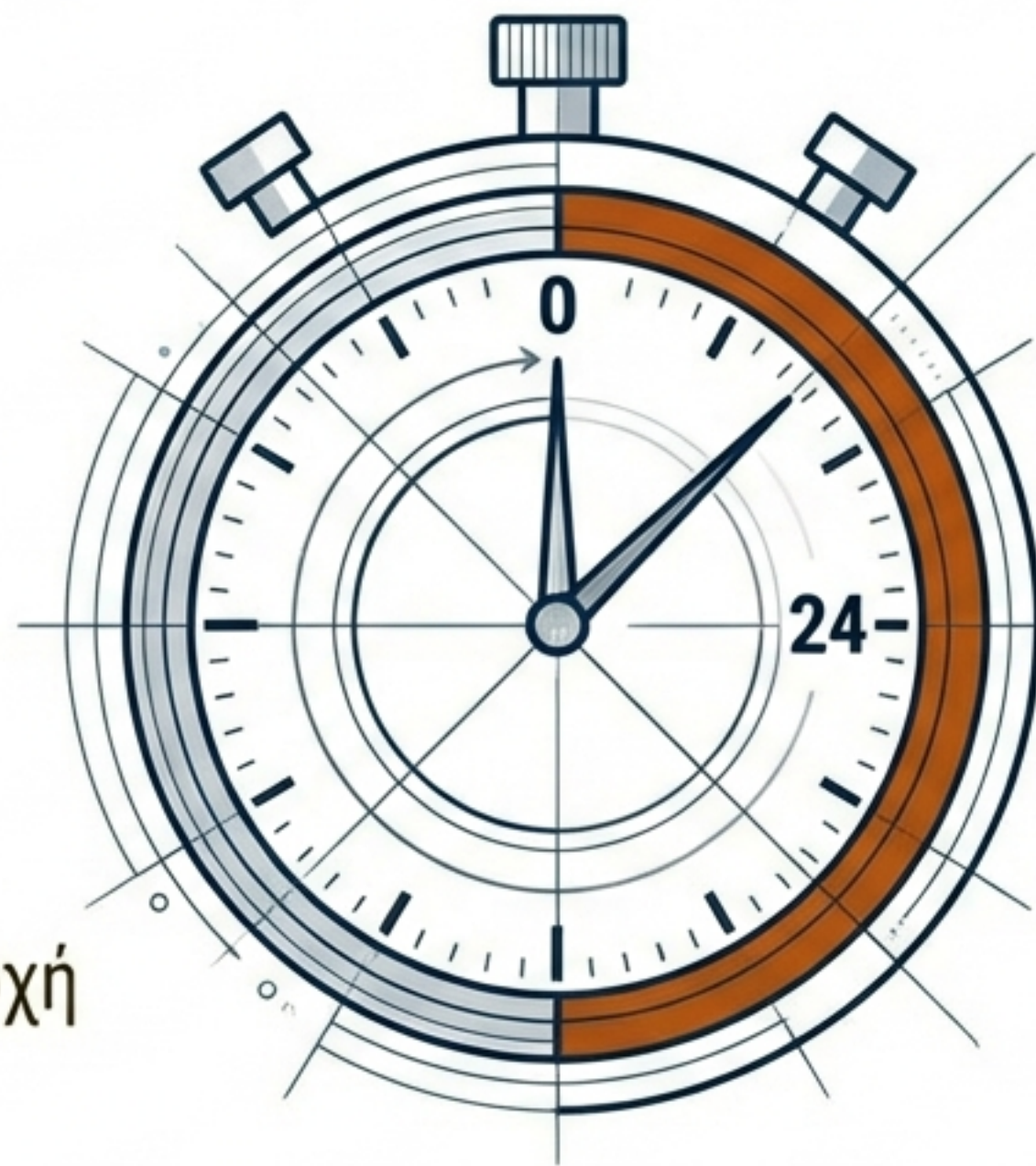


Ο Αγώνας με τον Χρόνο: Αναφορά σε 24 Ώρες (NIS2 Άρθρο 16)

Η ανάγκη διατήρησης της λειτουργίας της γακιαρής Fedtoyecos (Roboto - Editorial) ε ποιτίων.

Η «Rapid Response Team»

- ✓ **<15 Λεπτά:** Χρόνος απόκρισης μέσω της 24/7 γραμμής.
- ✓ **Forensics & Legal:** Άμεση πρόσβαση σε ειδικούς ψηφιακής διερεύνησης και νομικούς.
- ✓ **Compliance:** Κάλυψη εξόδων για τη σύνταξη αναφορών προς την Εθνική Αρχή Κυβερνοασφάλειας, αποφεύγοντας πρόσθετα πρόστιμα.



Έγκαιρη προειδοποίηση εντός **24 ωρών**. Κοινοποίηση εντός **72 ωρών**.

Οικονομική Θωράκιση του Ισολογισμού

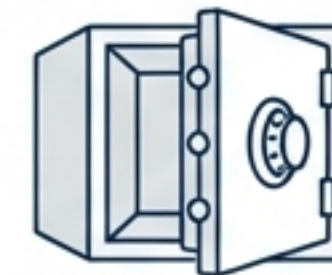
Απεριόριστες Επαναφορές Ορίου (Unlimited Reinstatement)



Το όριο κάλυψης αποκαθίσταται πλήρως μετά από κάθε απαίτηση. Αν συμβούν δύο ανεξάρτητα περιστατικά, το πλήρες ποσό είναι διαθέσιμο και για τα δύο.

Μηδενική Απαλλαγή (Zero Deductible)

Incident Response Cost = €0 Deductible



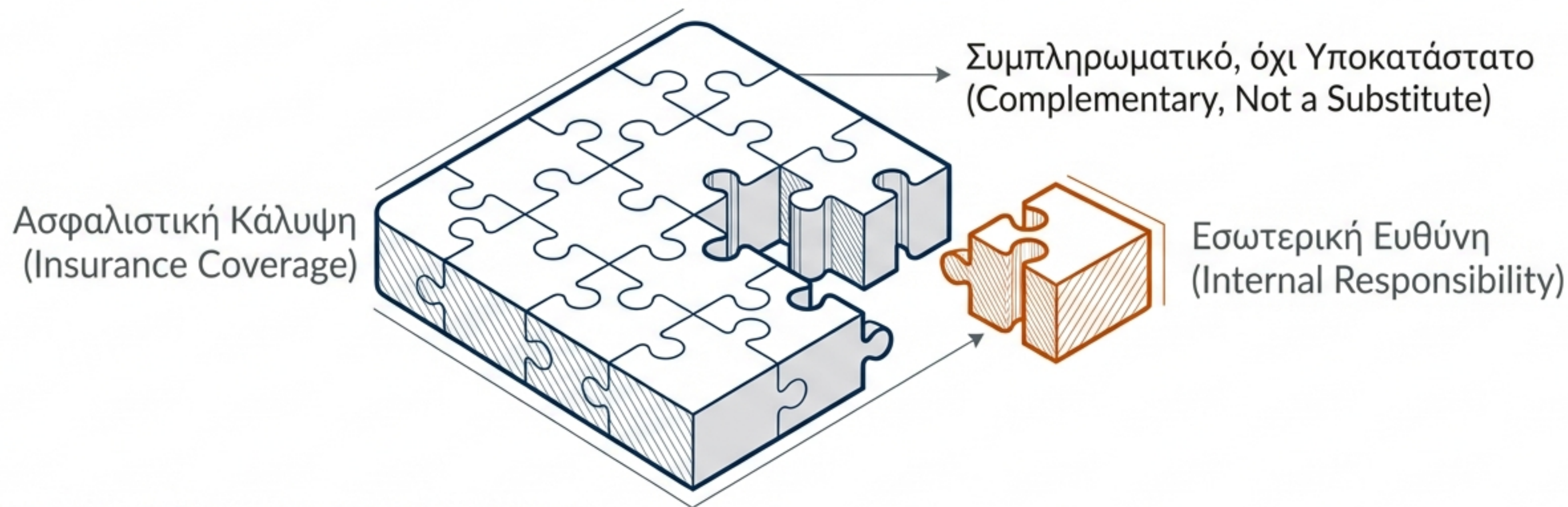
Δεν εφαρμόζεται απαλλαγή για το αρχικό κόστος απόκρισης.
Ενθαρρύνει τη διοίκηση να αναφέρει άμεσα κάθε υποψία.

Συγκριτικός Πίνακας: Συμμόρφωση vs. Θωράκιση

NIS2 Requirement	Traditional Insurance	Proactive Cyber Insurance
Προσωπική Ευθύνη (Art 14)	Μόνο Αποζημίωση Εταιρείας	Management Liability Coverage
Τεχνικά Μέτρα (Art 15)	Καμία Υπηρεσία	Vuln. Scanning & Threat Hunting
Αναφορά 24h (Art 16)	Αργή Απόκριση / Γραφειοκρατία	Απόκριση <15' & Νομική Σύνταξη

Τι Πρέπει να Γνωρίζει ο CEO: Όρια και Ευθύνες

Η ασφάλιση λειτουργεί συμπληρωματικά. Δεν υποκαθιστά την εσωτερική ευθύνη.



Τι ΔΕΝ καλύπτεται (Exclusions)

- **Προληπτικές επενδύσεις** υποδομής (π.χ. αγορά MFA, Firewalls).
- Περιστατικά που οφείλονται σε **δόλια πράξη** της ανώτατης διοίκησης.
- **Γενικευμένη αποτυχία** βασικών υποδομών διαδικτύου (Internet backbone failure).

Υποχρέωση: Η διοίκηση οφείλει να συνεχίσει την εκπαίδευση και την επίβλεψη των μέτρων.

Η Αναλογία της Πυρασφάλειας

NIS2 = Κανονισμός Πυρασφάλειας



Οι κανόνες και οι πυροσβεστήρες που πρέπει να έχετε (Compliance).

Proactive Insurance = Ιδιωτική Πυροσβεστική



Αισθητήρες καπνού συνδεδεμένοι με μια δύναμη που είναι ήδη σε επιφυλακή.

«Η συμμόρφωση χωρίς **Proactive Cyber Insurance** είναι σαν να προσπαθείτε να θωρακίσετε μια **πόλη από πυρκαγιές** έχοντας μόνο έναν **αυστηρό κανονισμό.**»

Επόμενα Βήματα: Το Σχέδιο Δράσης



1. Ενσωμάτωση

Εντάξτε το ασφαλιστήριο (και την τηλεφωνική γραμμή ανάγκης) στο επίσημο Σχέδιο Αντιμετώπισης Περιστατικών.



2. Αξιολόγηση

Ελέγξτε αν η τρέχουσα κάλυψη περιλαμβάνει **Management Liability** (Art 14) και έξοδα αναφοράς αρχών (Art 16).



3. Ενεργοποίηση

Αξιοποιήστε άμεσα τις προληπτικές υπηρεσίες (scanning/training) που προσφέρει το συμβόλαιο.



**Χρησιμοποιήστε το ως «οικονομικό δίκτυ ασφαλείας»
και «τεχνικό επιταχυντή».**

Επενδύστε σε έναν Μηχανισμό Επιβίωσης



Νίκος Γεωργόπουλος

Digital Risk Insurance Broker, Cromar
Co-Founder, DPO Academy

[linkedin.com/in/nikos-georgopoulos/](https://www.linkedin.com/in/nikos-georgopoulos/)