



Cyber Resilience & Proactive Cyber Insurance

Στρατηγική Διακυβέρνηση, Κανονιστική Συμμόρφωση και Προστασία Στελεχών.

Ο Ψηφιακός Λαβύρινθος: Από Τεχνικό Πρόβλημα σε Προσωπική Ευθύνη

75%

Το ποσοστό των συνολικών
απωλειών που αντιπροσωπεύει
πλέον το ransomware.



- **Νομική Μετάβαση:** Με την ενσωμάτωση της Οδηγίας NIS2 (N. 5160/2024), ο κυβερνοκίνδυνος μετεξελίσσεται σε θεμελιώδη επιχειρησιακό και υπαρξιακό κίνδυνο.
- **Η Νέα Πραγματικότητα:** Η ασφάλιση δεν αποτελεί πλέον απλή δαπάνη προμήθειας, αλλά τον πυρήνα του μηχανισμού επιβίωσης του CEO και του Διοικητικού Συμβουλίου.

Αλλαγή Παραδείγματος: Προστασία Πριν την Κρίση

Παραδοσιακή Ασφάλιση (Αντιδραστική)

Ρόλος: Αποκλειστικά πληρωμή ζημιών (Payout-only).

Ενεργοποίηση: Μόνο μετά την καταστροφή.

Αξία: Οικονομική αποζημίωση, συχνά με πολύπλοκες διαδικασίες.

Proactive Cyber Insurance (Προληπτική)



Συνεχής Έλεγχος (24/7): Threat hunting, σάρωση ευπαθειών (vulnerability scanning) και παρακολούθηση του dark web.



Άμεσες Ειδοποιήσεις: Προειδοποίηση της διοίκησης στο κινητό (μέσω app) για στοχευμένες απειλές πριν γίνουν περιστατικά.



Αξία: Αποτροπή επιθέσεων και λειτουργία ως ενεργή ασπίδα του ισολογισμού.



Πυλώνας 1: Η Ασπίδα των Στελεχών (Management Liability)

Η NIS2 (Άρθρα 14 & 20) καθιερώνει άμεση, προσωπική λογοδοσία. Αν δεν υπάρχει σωστή διαχείριση κινδύνου, τα στελέχη κινδυνεύουν με απαγόρευση άσκησης διευθυντικού δικαιώματος.



Πυλώνας 2: Ρυθμιστική Συμβίωση (NIS2 & DORA)

Άρθρο 15 (Διαχείριση Κινδύνων):
Ολιστικά τεχνικά μέτρα και
επιχειρησιακή συνέχεια.



Άρθρο 16 (Αναφορά): Έγκαιρη
προειδοποίηση σε 24 ώρες /
κοινοποίηση σε 72 ώρες (αποφυγή
προστίμων έως €10M ή 2%).



Η Ομάδα Ταχείας Επέμβασης: Απόκριση σε <15 Λεπτά

Λεπτό 0

Εντοπισμός ύποπτης δραστηριότητας (π.χ. ransomware).

Λεπτό 15

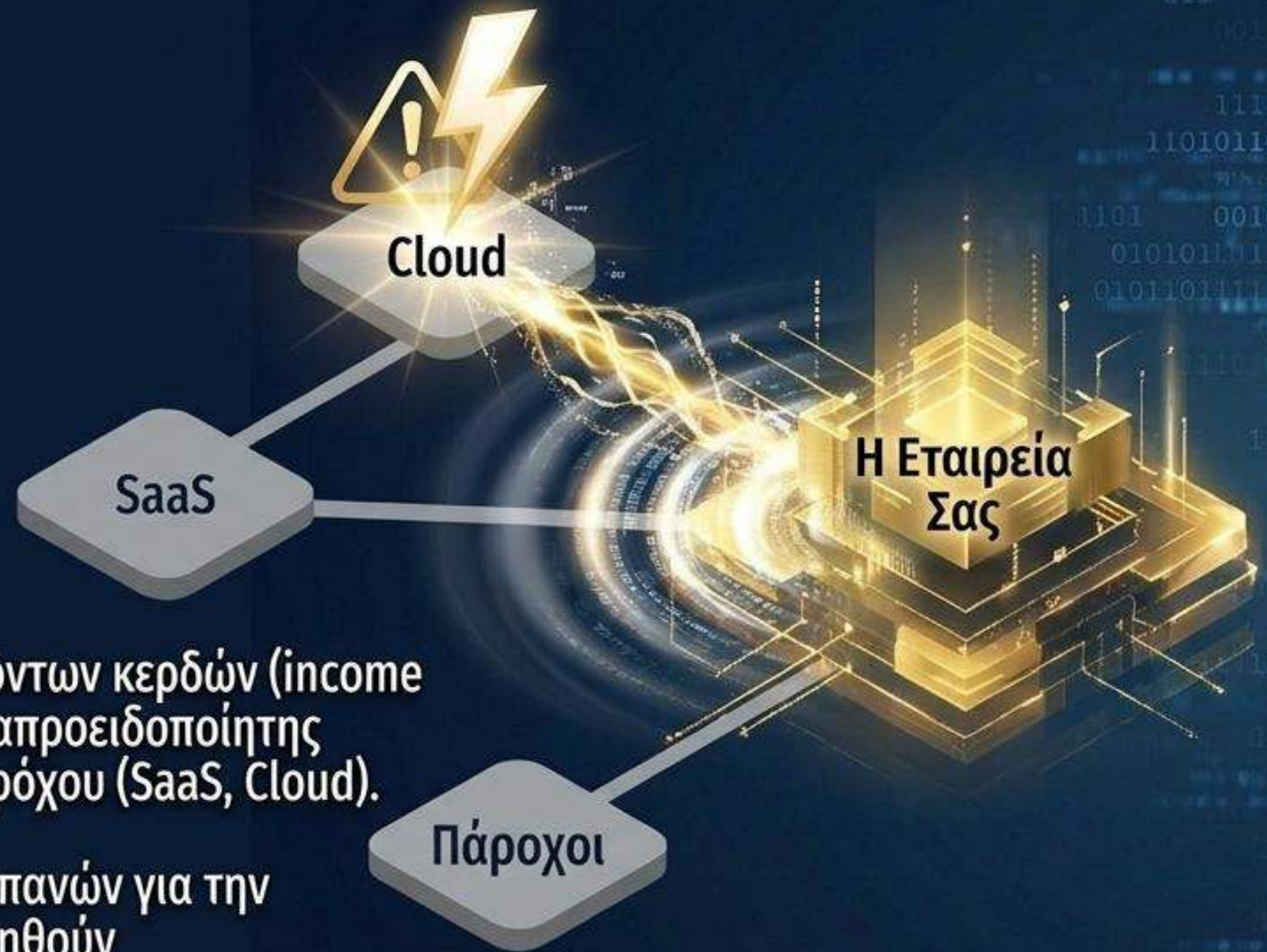
24/7 άμεση πρόσβαση στη μεγαλύτερη in-house ομάδα ειδικών ψηφιακής διερεύνησης (forensics) και νομικών.

Μηδενική Απαλλαγή (Nil Deductible) στην Αρχική Απόκριση

Δεν εφαρμόζεται καμία απαλλαγή στα αρχικά έξοδα διαχείρισης περιστατικού. Η διοίκηση μπορεί (και πρέπει) να ενεργοποιήσει την ομάδα άμεσα, σε κάθε υποψία, χωρίς καμία δεύτερη σκέψη για το βραχυπρόθεσμο κόστος.

Πυλώνας 3: Επιχειρησιακή Συνέχεια & Εφοδιαστική Αλυσίδα

Εξαρτώμενη Διακοπή Εργασιών
(Dependent Business Interruption - DBI).
Τι συμβαίνει όταν καταρρέει ο κρίσιμος
προμηθευτής σας;



Αλυσιδωτές Αστοχίες: Πλήρης κάλυψη διαφυγόντων κερδών (income loss) όταν διακόπτονται οι εργασίες σας λόγω απροειδοποίητης κατάρρευσης συστημάτων ενός εξωτερικού παρόχου (SaaS, Cloud).

Αδιάλειπτη Παραγωγή: Κάλυψη πρόσθετων δαπανών για την εξασφάλιση εναλλακτικών πόρων, ώστε να τηρηθούν οι συμβατικές υποχρεώσεις προς τους πελάτες σας.

Ο Ανθρώπινος Παράγοντας: Λάθη, Απάτες & Social Engineering



Ανθρώπινο Λάθος (Operator Error)

Δεν είναι όλα τα περιστατικά κακόβουλα.
Καλύπτονται καταστροφές από τυχαία
διαγραφή κρίσιμων βάσεων δεδομένων,
λανθασμένες αναβαθμίσεις συστημάτων ή
σφάλματα παραμετροποίησης.



Εξαπάτηση (Fraud & Cybercrime)

- **Invoice Manipulation:** Αποζημίωση αν εγκληματίες παρεισφρήσουν στα email σας, παραποιήσουν τιμολόγια και στείλουν πληρωμές πελατών σε δικούς τους λογαριασμούς.
- **New Vendor Fraud:** Προστασία όταν η εταιρεία εξαπατάται ώστε να πληρώσει έναν απατεώνα που υποδύεται έναν νέο, νόμιμο προμηθευτή.

Πυλώνας 4: Αντιμετώπιση Απειλών Επόμενης Γενιάς



Affirmative AI Coverage: Ρητή και ξεκάθαρη κάλυψη για επιθέσεις που εργαλειοποιούν την Τεχνητή Νοημοσύνη (π.χ. AI-driven κωδικοί πρόσβασης, deepfakes, εξελιγμένο hacking).

Αντικατάσταση Υλικού (Hardware / OT): Κάλυψη για αντικατάσταση φυσικού εξοπλισμού και Βιομηχανικών Συστημάτων Ελέγχου (SCADA/OT) που καταστράφηκαν από malware, εάν η αγορά νέων είναι πιο συμφέρουσα από την επιδιόρθωση λογισμικού.

Εθελοντική Διακοπή (Voluntary Shutdown): Αποζημίωση διαφυγόντων κερδών ακόμα και όταν η διοίκηση αποφασίζει προληπτικά (ή αναγκάζεται από ρυθμιστή) να κλείσει τα συστήματα για να περιορίσει μια εξάπλωση κακόβουλου κώδικα.

Οικονομική Μηχανική: Το Πλεονέκτημα του 'Time Franchise'

Hour 0

Hour 8

Hour 16

Το Πρόβλημα
(Χρονική Απαλλαγή -
Time Retention):



Σε παραδοσιακά συμβόλαια, αν η ζημιά ξεκινάει μετά από 8 ώρες διακοπής, οι πρώτες 8 ώρες δεν αποζημιώνονται ποτέ.

Η Λύση
(Time Franchise):



Με την Proactive Cyber Insurance, εφόσον το σύστημα παραμείνει εκτός λειτουργίας πέραν του χρονικού ορίου (π.χ. 8 ώρες), η κάλυψη ενεργοποιείται αναδρομικά. Καλύπτονται οι απώλειες εσόδων από το πρώτο λεπτό (Hour 1).

Αποτέλεσμα: Δίκαιη και ταχύτερη ανάκαμψη των οικονομικών της εταιρείας.

Θωράκιση Ισολογισμού: Απεριόριστες Επαναφορές Ορίου

Οι κυβερνοεπιθέσεις δεν έχουν 'ετήσιο όριο'. Παραδοσιακά συμβόλαια εξαντλούνται μετά το πρώτο χτύπημα. Η Proactive Cyber Insurance παρέχει Unlimited Reinstatements.



Μάρτιος:

Επίθεση Ransomware εξαντλεί ολόκληρο το όριο του συμβολαίου (π.χ. €1.000.000). Το όριο αποκαθίσταται πλήρως.

Νοέμβριος:

Ανεξάρτητο περιστατικό απάτης (Social Engineering) πλήττει την εταιρεία.

Αποτέλεσμα: Το πλήρες όριο (εκ νέου €1.000.000) είναι άμεσα διαθέσιμο, προστατεύοντας τον ισολογισμό και εξασφαλίζοντας την επιβίωση της επιχείρησης.

Πραγματικά Σενάρια Ολιστικής Κάλυψης (Synthesis)



Απώλεια Διαγωνισμών (Lost Bids)

Αποζημίωση εσόδων που χάθηκαν όταν ένας πελάτης ακυρώνει την ανάθεση συμβολαίου (RFP) λόγω απώλειας εμπιστοσύνης από ένα περιστατικό διαρροής δεδομένων σας.



Ενδιάμεσες Πληρωμές (Interim Payments)

Άμεση παροχή ρευστότητας (πριν την τελική εκτίμηση της ζημιάς) κατά τη διάρκεια παρατεταμένης διακοπής εργασιών, για την επιβίωση της εταιρείας.



Έμμεση Σωματική Βλάβη (Contingent Bodily Injury)

Κάλυψη αγωγών εάν η παραβίαση του βιομηχανικού σας λογισμικού (OT) προκαλέσει δυσλειτουργία μηχανήματος με αποτέλεσμα τον τραυματισμό εργαζομένου.



Κλοπή Κεφαλαίων Πελατών (Client / Escrow Funds)

Προστασία της φήμης σας: Αποζημίωση του πελάτη εάν εξαπατηθείτε (Social Engineering) και μεταφέρετε δικά του κεφάλαια που διαχειρίζεστε, σε απατεώνες.

Ενσωμάτωση: Ο Μηχανισμός Επιβίωσης του CEO

Corporate Incident Response Plan



Τεχνικός Επιταχυντής:

Προσθέτει ένα ενεργό ραντάρ (αισθητήρες) και την ισχυρότερη ιδιωτική «πυροσβεστική» δύναμη δίπλα στην IT ομάδα σας, διαθέσιμη σε κάτω από 15 λεπτά.

Οικονομικό Δίκτυ Ασφαλείας:

Προστατεύει τη ρευστότητα, τα διαφυγόντα κέρδη και αναπληρώνει φυσικό εξοπλισμό.

Προσωπική Ασπίδα:

Θωρακίζει τη διοίκηση από νομικές και κανονιστικές ευθύνες υπό το πρίσμα της NIS2.

Η κανονιστική συμμόρφωση απαιτεί ανθεκτικότητα. Ενσωματώστε την Proactive Cyber Insurance στο Σχέδιο Αντιμετώπισης Περιστατικών (Incident Response Plan) σας σήμερα.