Εκπαιδευτικό Σεμινάριο Ασφαλίσεων Ηλεκτρονικών και Διαδικτυακών Κινδύνων, Cyber Risk Insurance

Κώστας Βούλγαρης,

Financial Lines Manager, AIG

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

Πώς φτάσαμε στο Cyber Insurance;

EIAS

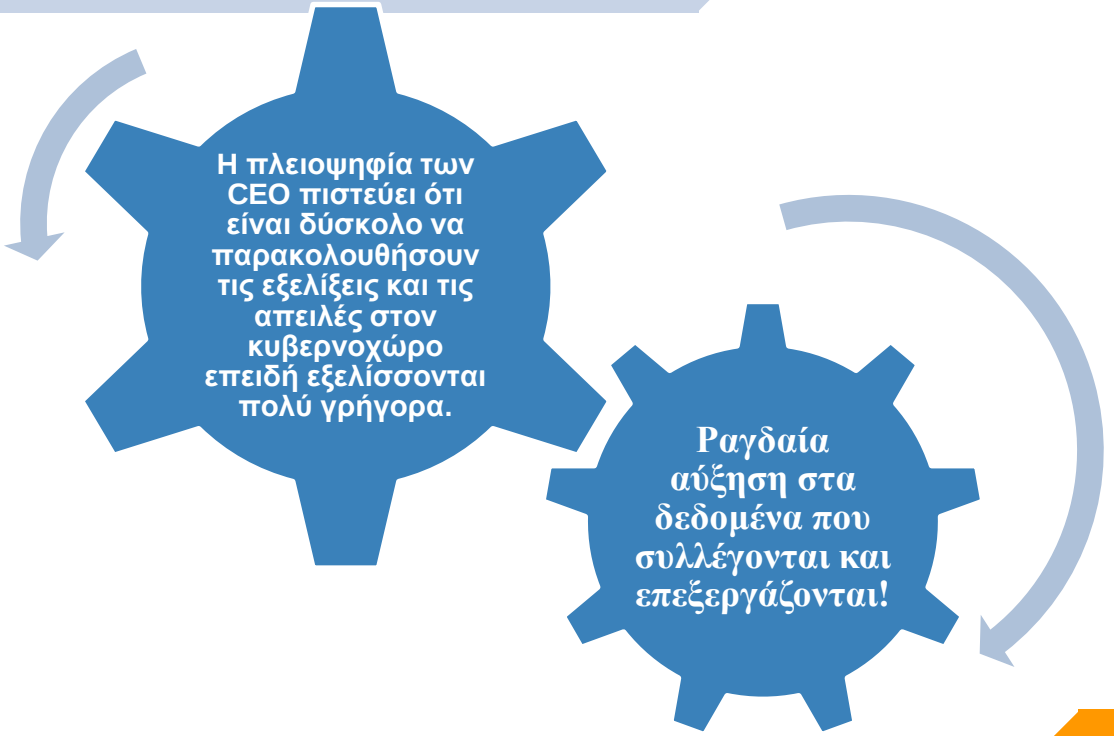
Cyber Risks

Η μεγαλύτερη ανησυχία των πελατών είναι οι κίνδυνοι του κυβερνοχώρου*

1. Κίνδυνοι κυβερνοχώρου	**86%**
2. Απώλεια εισοδημάτων	82%
3. Περιουσιακή ζημία	80%
4. Αποζημίωση εργαζόμενων	78%
5. Διακοπή υπηρεσιών κοινής ωφέλειας	76%
6. Αξιόγραφα / Κίνδυνος επενδύσεων	76%
7. Αστική Ευθύνη οχημάτων και στόλων	65%

** Η έρευνα διεξήχθη για λογαριασμό της AIG το διάστημα Οκτώβριος-Νοέμβριος 2012 σε 256 άτομα από τις παρακάτω κατηγορίες: μεσίτες ασφαλίσεων , υπεύθυνοι διαχείρισης κινδύνου, ανώτατα διευθυντικά στελέχη, υπεύθυνοι διαχείρισης τεχνολογίας πληροφοριών.*

Cyber Risks


Η πλειοψηφία των CEO πιστεύει ότι είναι δύσκολο να παρακολουθήσουν τις εξελίξεις και τις απειλές στον κυβερνοχώρο επειδή εξελίσσονται πολύ γρήγορα.
Ραγδαία αύξηση στα δεδομένα που συλλέγονται και επεξεργάζονται!

❑ Το νομικό πλαίσιο με μια ματιά

- Αποφάσεις Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 (General Data Protection Regulation ‘GDPR’)
- Νόμος 4624/2019 - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680

GDPR

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

Τι είναι ο GDPR

- Πρόκειται για έναν νέο κανονισμό, ο οποίος επιδιώκει την εναρμόνιση της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων όσον αφορά τις δραστηριότητες επεξεργασίας και τη διασφάλιση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών-μελών ΕΕ
- Κάθε επιχείρηση που είναι εγκατεστημένη στην ΕΕ, ή που είναι εγκατεστημένη εκτός ΕΕ και χειρίζεται προσωπικά δεδομένα τα οποία αφορούν σε άτομα που βρίσκονται εντός της ΕΕ, είναι υποχρεωμένη να συμμορφωθεί πλήρως στις επιταγές του νέου Κανονισμού (GDPR), ο οποίος τέθηκε σε εφαρμογή την 25η Μαΐου 2018.

EIAS

GDPR

Τι άλλαξε στην πράξη σε σχέση με τα δικαιώματα του υποκειμένου

- Ο Κανονισμός επιφέρει σημαντικές αλλαγές στο ρυθμιστικό περιβάλλον για τους υπεύθυνους επεξεργασίας δεδομένων, δηλαδή για τις επιχειρήσεις και τους δημόσιους φορείς, κυρίως σε τρία επίπεδα:
- α) έχει ως κεντρική λογική την ελαχιστοποίηση της συλλογής, διατήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα,
- β) επιδιώκει την ενίσχυση της προστασίας των προσωπικών δεδομένων, αναθεωρώντας τις υποχρεώσεις όλων όσων επεξεργάζονται δεδομένα, καθώς πλέον, οι επονομαζόμενοι «Υπεύθυνοι Επεξεργασίας» αλλά και οι «Εκτελούντες την Επεξεργασία» για λογαριασμό των «Υπευθύνων» φέρουν το βάρος της απόδειξης της συμμόρφωσης στις διατάξεις του Κανονισμού, (Λογοδοσία) και

GDPR

Τι άλλαξε στην πράξη σε σχέση με τα δικαιώματα του υποκειμένου

- γ) ανανεώνει και ενισχύει τα δικαιώματα των υποκειμένων, των ιδιοκτητών δηλαδή προσωπικών δεδομένων, γεγονός στο οποίο οφείλουν να προσαρμοστούν οι υπεύθυνοι επεξεργασίας και συνεπώς να μεταβάλλουν ανάλογα τη λειτουργία και τις αποφάσεις τους

GDPR

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

Οι «καινοτομίες» του Κανονισμού

- Ενίσχυση δικαιωμάτων υποκειμένων (Δικαίωμα ενημέρωσης, Δικαίωμα πρόσβασης, Δικαίωμα στη διόρθωση δεδομένων, Δικαίωμα διαγραφής δεδομένων, Δικαίωμα στον περιορισμό της επεξεργασίας, Δικαίωμα στη φορητότητα των δεδομένων, Δικαίωμα αντίρρησης/εναντίωσης)
- Ενίσχυση δικαιώματος στη λήθη - το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί τη διαγραφή και την παύση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν

EIAS

GDPR

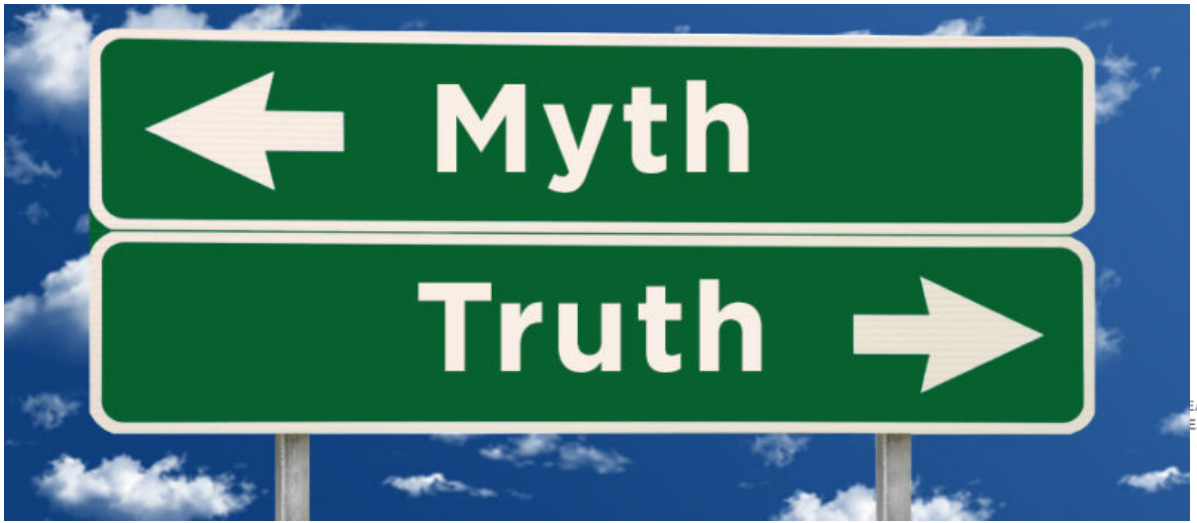
ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

Οι «καινοτομίες» του Κανονισμού

- Ενίσχυση δικαιωμάτων υποκειμένων (Δικαίωμα ενημέρωσης, Δικαίωμα Ενίσχυση δικαιώματος εναντίωσης - το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, όταν η επεξεργασία αυτή βασίζεται είτε σε εκπλήρωση σκοπού δημοσίου συμφέροντος, είτε στην ικανοποίηση εννόμου συμφέροντος. Επιπλέον, το δικαίωμα εναντίωσης μπορεί να ασκηθεί ανά πάσα στιγμή στην επεξεργασία δεδομένων για σκοπούς απευθείας εμπορικής προώθησης.
- Αυστηριοποίηση κυρώσεων - υψηλά πρόστιμα

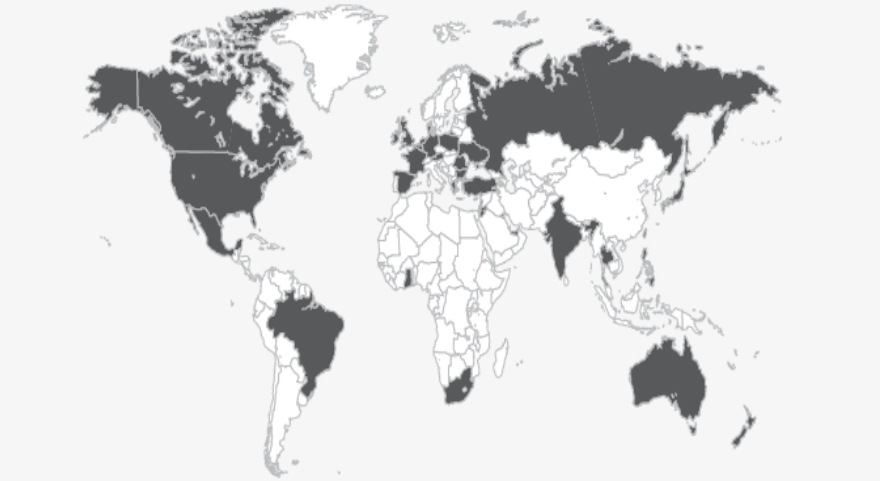
EIAS

Δυο μύθοι…



ΜΑΤΙΚΟ
ΗΤΗΡΙΟ
ΘΗΝΩΝ

Είμαστε στον Χάρτη…



Countries in which a breach was confirmed

Australia	France	Jordan	Poland	United Arab Emirates
Austria	Germany	Kuwait	Romania	Ukraine
Bahamas	Ghana	Lebanon	Russian Federation	United Kingdom
Belgium	Greece	Luxembourg	South Africa	United States
Brazil	India	Mexico	Spain	
Bulgaria	Ireland	Netherlands	Taiwan	
Canada	Israel	New Zealand	Thailand	
Denmark	Japan	Philippines	Turkey	

Verizon 2012 Data breach investigations report

ΚΙΝΔΥΝΟΙ

Οι Διαδικτυακές απειλές δεν είναι πια “προνόμιο” των μεγάλων επιχειρήσεων

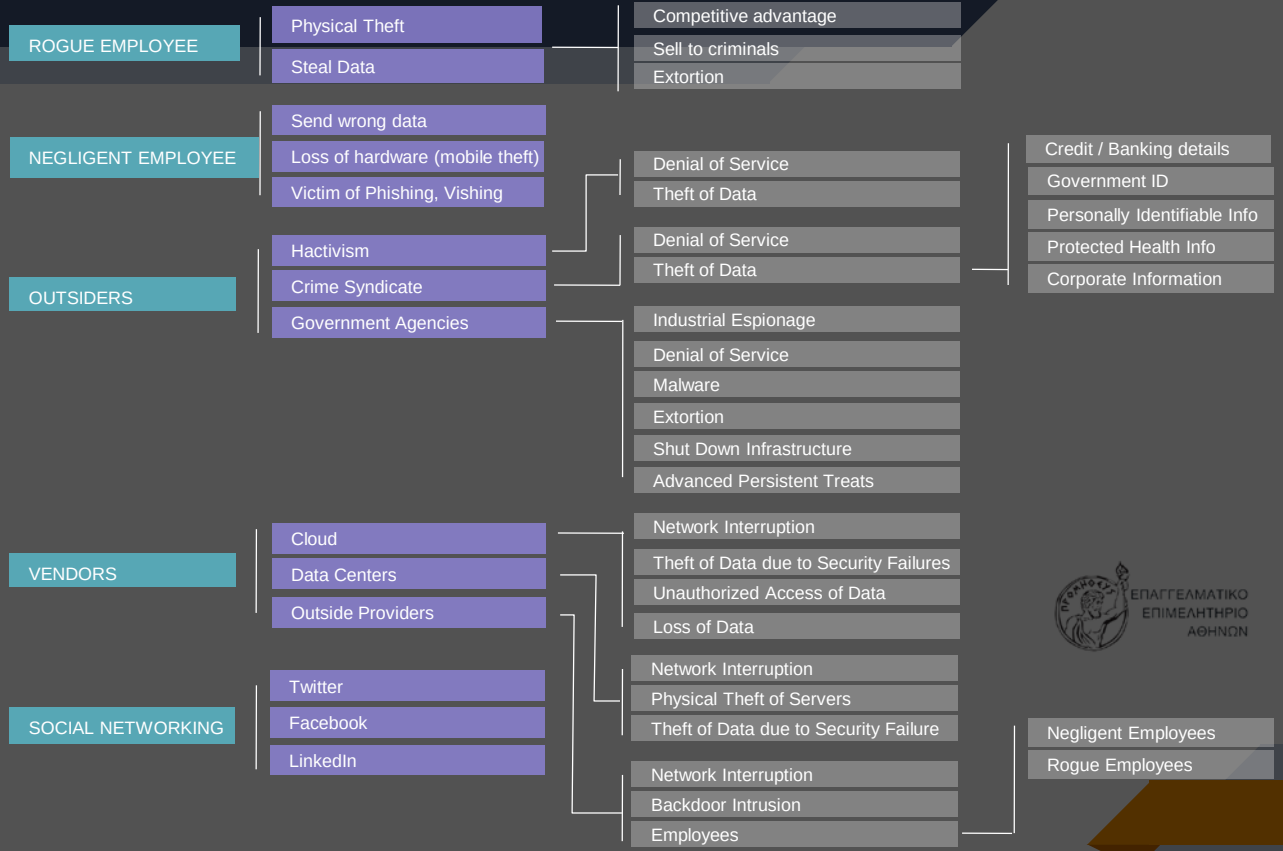
Ολοένα και αυξανόμενο ποσοστό μικρομεσαίων επιχειρήσεων έχει πλέον αντιληφθεί ότι οι διαδικτυακοί κίνδυνοι αποτελούν σοβαρή απειλή για τις ίδιες και ως εκ τούτου η πλειοψηφία αυτών λαμβάνει ορισμένα μέτρα προστασίας, χωρίς ωστόσο να καταφέρνει να αντιμετωπίσει το θέμα συνολικά και να προετοιμαστεί καταλλήλως για μελλοντικά περιστατικά.

Οι επιπτώσεις μιας παραβίασης ασφαλείας σε μια μεσαία επιχείρηση ενδεχομένως να έχουν μεγαλύτερο αντίκτυπο από ότι σε μια μεγαλύτερη επιχείρηση.

ΚΙΝΔΥΝΟΙ

- Οικονομικές επιπτώσεις / Απώλεια εσόδων
- Προσωπική προβολή / Προβολή κοινωνικής ατζέντας
- Οικονομική και Βιομηχανική κατασκοπεία
- Αντίποινα
- Λήψη/αποστολή κακόβουλου λογισμικού ή ιού, που προκαλεί καταστροφή, αλλοίωση, φθορά ή διαγραφή δεδομένων
- Υποκλοπή εμπιστευτικών εταιρικών πληροφοριών / δεδομένων προσωπικού χαρακτήρα
- Εκβιασμός αποκάλυψης δεδομένων
- Διακοπή εργασιών
- Επιθέσεις άρνησης υπηρεσιών/εξυπηρέτησης
- Δυσφήμιση / Κρίση Εταιρικής Φήμης

Οι Συνέπειες

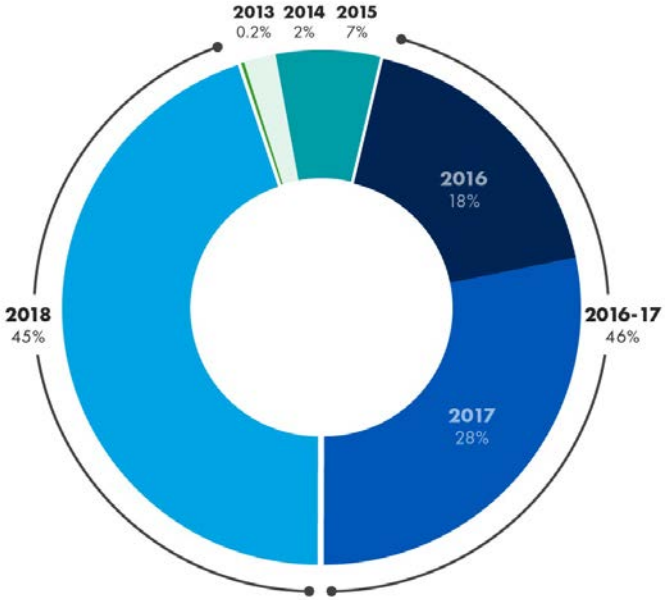


ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

EIAS

Ζημιές Cyber στην Ευρώπη ανά έτος

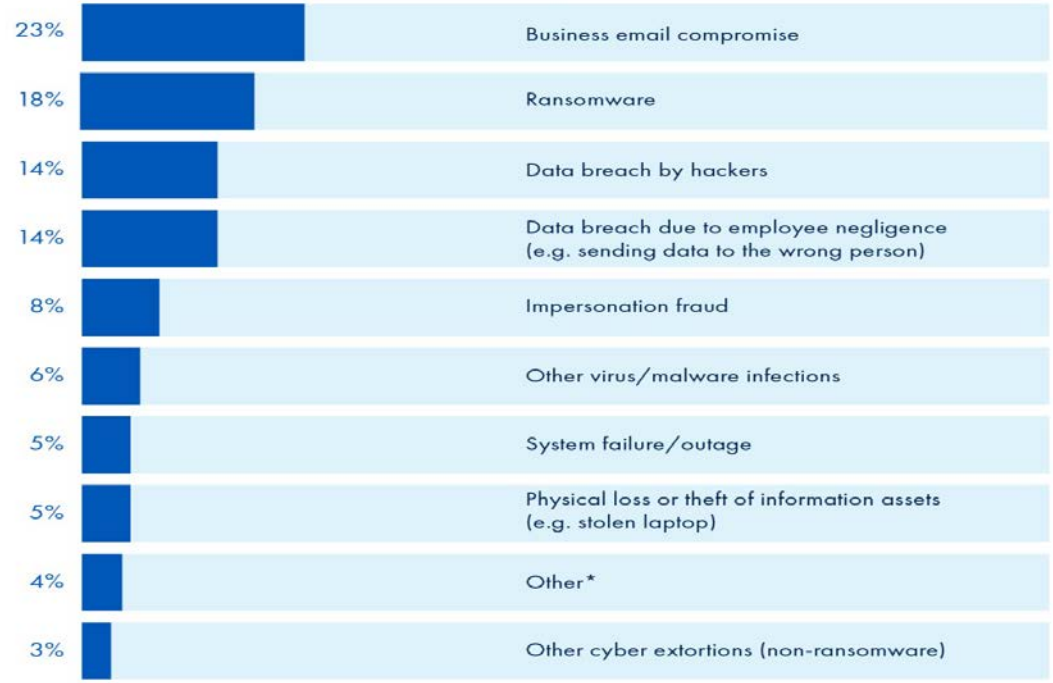
Fig 3 **Cyber Claims Received by AIG EMEA (2013-2018) - Volume**



Πηγή: AIG claims database

2018 – Ζημίες Cyber ανά κατηγορία

Fig 1 **Cyber Claims received by AIG EMEA (2018) – By reported incident**



*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

Πηγή: AIG claims database

2018 – Ζημιές Cyber ανά κατηγορία επιχειρήσεων

Fig 2 **Cyber Claims received by AIG EMEA (2018) – By industry**

*Food & Beverage, Construction, Education
Note: Figures may not add up to 100% due to rounding

Πηγή: AIG claims database

Η ασφάλιση των Διαδικτυακών & Ηλεκτρονικών κινδύνων δεν είναι απλά ένα ασφαλιστικό προϊόν, είναι ένα εργαλείο Risk Management, παρέχοντας όχι μόνο αποζημιώσεις, αλλά κυρίως υπηρεσίες αντιμετώπισης κρίσης!

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

EIAS

Business Enterprise Risk

Αδυναμία πρόσβασης στα συστήματα
- Κόστος χαμένων εργατοωρών κατά την περίοδο του downtime
- Ρίσκο για παρατεταμένο downtime

Αδυναμία πραγματοποίησης πώλησης
- Απώλεια πωλήσεων
- Παραβίαση των service agreements

Συνέπειες στην εφοδιαστική αλυσίδα τρίτων
- Αδυναμία παραγωγής για τους τρίτους
- Παραβίαση συμβατικών υποχρεώσεων

Απρόβλεπτα κόστη
- Δαπάνες για συνέχιση παραγωγής
- Ανάγκη επισκευών ηλεκτρονικών υποδομών
- Έξοδα συμβούλων
- Ανάκτηση ή Αντικατάσταση δεδομένων

Κρίση εταιρικής Φήμης
- Κόστος για την εταιρία
- Ενόχληση καταναλωτών
- Απώλεια υφιστάμενων συμβολαίων αλλά και μελλοντικών εργασιών
- Ενίσχυση των ανταγωνιστών
- Υποχρέωση παροχής εκπτώσεων σε υφιστάμενους πελάτες

Πτώση αξίας μετοχής
- Η μέση πτώση μετοχής συνεπεία ενός cyber event είναι 5%

Έρευνες
- Εσωτερική
- Ελεγκτικών Αρχών
- Μετόχων

Τι είναι η Ασφάλεια των Cyber Risks;

ΕΠΑΓΓΕΛΜΑΤΙΚΟ
ΕΠΙΜΕΛΗΤΗΡΙΟ
ΑΘΗΝΩΝ

EIAS

Cyber Risks

«Σιωπηλός» κίνδυνος

Ένα μεμονωμένο γεγονός που μπορεί να έχει παγκόσμιες συνέπειες

Γίνεται underwriting;

Cyber Risks

- Η Ασφαλιστική αγορά δίνει πλέον βάρος στη πρόληψη σε σχέση με τη προσπάθεια μετριασμού της ζημιάς
- **Στόχος είναι η αποφυγή του περιστατικού**

Παραδείγματα υπηρεσιών που δίνονται μαζί με ασφαλιστήρια Cyber:

- Vulnerability Scans
- Εκπαίδευση προσωπικού

- Εκπτώσεις σε επιπλέον υπηρεσίες ασφάλειας
- Κάλυψή ή Προϊόν;

Ορισμοί

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

Ορισμοί

- Οποιοδήποτε στοιχείο συνδέεται με ένα φυσικό πρόσωπο (το ‘υποκείμενο των δεδομένων’) με βάση το οποίο ταυτοποιείται /αναγνωρίζεται. Ονοματεπώνυμο
- αριθμός ταυτότητας
- ΑΦΜ, ΑΜΚΑ
- Τηλέφωνο, ταχυδρομική και ηλεκτρονική διεύθυνση
- διεύθυνση πρωτοκόλλου διαδικτύου (IP address), γεωχωρικά δεδομένα (GPS), κ.α.
- δηλαδή στοιχεία που μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο.

Ευαίσθητα προσωπικά Δεδομένα

- Ειδικές κατηγορίες’ δεδομένων προσωπικού χαρακτήρα, δηλαδή δεδομένα που αποκαλύπτουν
- τη φυλετική καταγωγή
- τα πολιτικά φρονήματα
- τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή του φυσικού προσώπου σε συνδικαλιστική οργάνωση, καθώς και
- γενετικά δεδομένα, δεδομένα που αφορούν την υγεία

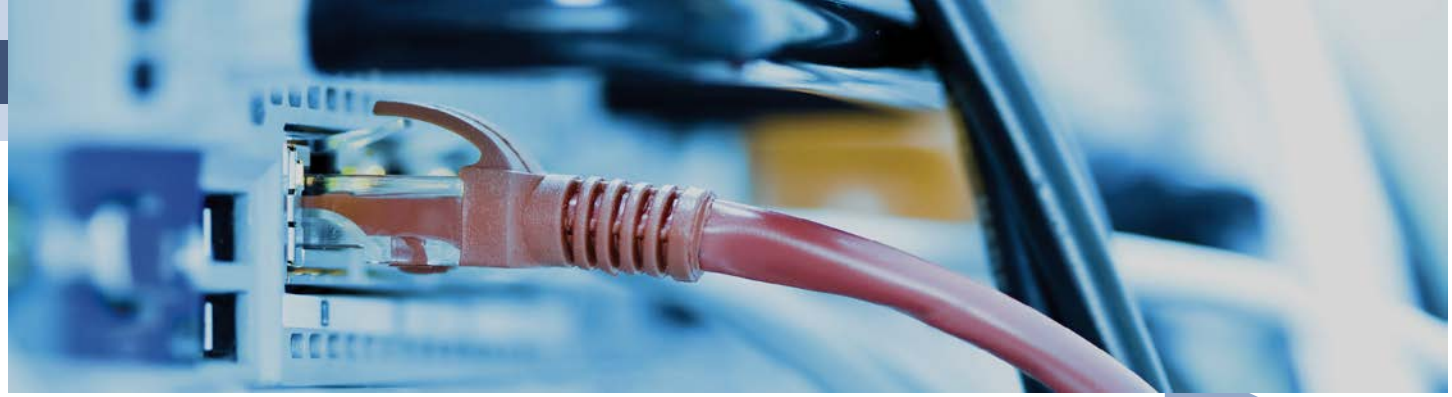
Περιστατικό Παραβίασης Προσωπικών Δεδομένων

Ορισμός παραβίασης δεδομένων προσωπικού χαρακτήρα (άρθρο 4 παρ. 12 GDPR):

παραβίαση της ασφάλειας που οδηγεί σε τυχαία και παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ'άλλο τρόπο σε επεξεργασία.

Συνέπεια μιας παραβίασης είναι ότι ο Υπεύθυνος Επεξεργασίας δεν είναι σε θέση να διασφαλίσει τη συμμόρφωση με τις αρχές που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (οι οποίες περιγράφονται συνοπτικά στο άρθρο 5 GDPR), ιδίως της ακεραιότητας και της εμπιστευτικότητας.

- Τυχαία ή αθέμιτη καταστροφή
- Απώλεια
- Αλλοίωση
- Απαγορευμένη διάδοση / πρόσβαση



Τι καλύπτει

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

EIAS

Συνέπειες για την επιχείρηση

- Ευθύνη για παραβίαση προσωπικών & εταιρικών δεδομένων και ασφάλεια δικτύων
- Έξοδα υπεράσπισης & αποζημιώσεις προς τρίτους
- Έξοδα ερευνών & επαναφοράς δεδομένων
- Κρίση εταιρικής φήμης
- Διακοπή εργασιών λόγω πτώσης συστημάτων
- Επιβολή διοικητικών προστίμων
- Εκβιασμός

Παροχές

Διαχείριση Κρίσεων / Περιστατικών

- Προληπτικές «ερευνητικές» υπηρεσίες
- Τηλεφωνικό κέντρο 24/7
- Κάλυψη εξόδων για τη διερεύνηση και διαπίστωση παραβίασης δεδομένων
- Προστασία φήμης – σχεδιασμός & διαχείριση στρατηγικής επικοινωνίας
- Παρακολούθηση των συνεπειών του περιστατικού
- Διαχείριση περιστατικού εκβιασμού αποκάλυψης δεδομένων

Διακοπή Εργασιών

- Διαχείριση Διακοπής λειτουργίας δικτύου
- Επαναφορά συστημάτων
  - Ανάκτηση δεδομένων
  - Κάλυψη απώλειας καθαρών κερδών μετά από διακοπή λειτουργιάς των συστημάτων της εταιρίας
- Ποσοτική και ποιοτική ανάλυση της ζημιάς

Διοικητικές / Νομικές Υποχρεώσεις

- Νομική υποστήριξη και εκπροσώπηση ενώπιων εποπτικών αρχών αναφορικά με συγκεκριμένο συμβάν
- Κάλυψη εξόδων υπεράσπισης στο πλαίσιο έρευνας της εποπτικής αρχής
- Κάλυψη προστίμων εποπτικών αρχών
- Παροχή συμβουλευτικών υπηρεσιών και εξόδων για τις απαιτούμενες γνωστοποιήσεις προς τα υποκείμενα δεδομένων & τις αρμόδιες αρχές
- Κάλυψη απαιτήσεων τρίτων

Ορισμοί

Ασφαλισμένος

- η **Εταιρεία**
- οποιοδήποτε **Ασφαλισμένο Πρόσωπο**
- οποιοδήποτε φυσικό πρόσωπο που είναι ή έχει διατελέσει υπάλληλος της **Εταιρείας**
- ανεξάρτητος εργολάβος υπό τις οδηγίες και την εποπτεία του **Λήπτη της Ασφάλισης**, μόνο σε σχέση με τις υπηρεσίες που ο ανεξάρτητος εργολάβος παρέχει στον **Λήπτη της Ασφάλισης** και
- κάθε κληρονόμος ή νόμιμος αντιπρόσωπος οιουδήποτε **Ασφαλισμένου** που περιγράφεται στα σημεία (i), (ii) και (iii) αυτού του ορισμού στο μέτρο που εγείρεται κατά αυτών **Απαίτηση** σε σχέση με πράξη, σφάλμα ή παράλειψη αυτού του **Ασφαλισμένου**.

Ορισμοί

Παραβίαση Προσωπικών Πληροφοριών

- η μη εξουσιοδοτημένη αποκάλυψη ή διαβίβαση από **Ασφαλισμένο Προσωπικών Πληροφοριών** για τις οποίες είναι υπεύθυνη η **Εταιρεία** είτε ως Φορέας Επεξεργασίας Δεδομένων είτε ως Φορέας Ελέγχου Δεδομένων, όπως ορίζεται στο πλαίσιο οιασδήποτε εφαρμοστέας **Νομοθεσίας περί Προστασίας Πληροφοριών**.

Απαίτηση

η λήψη από τον **Ασφαλισμένο** ή η επίδοση σε αυτόν ενός από τα ακόλουθα:

- γραπτού αιτήματος που ζητά νόμιμη αποκατάσταση ή
- αστικής ή διοικητικής ή ποινικής δίωξης που ζητά νόμιμη αποκατάσταση, συμμόρφωση ή άλλο μέτρο.

Εξαιρέσεις

- Ρύπανση
- Σωματικές Βλάβες και Υλικές Ζημίες

Απευθύνεται σε επιχειρήσεις που:

- βασίζονται σε τεχνολογικά συστήματα για τη λειτουργία τους
- διατηρούν εταιρική ιστοσελίδα
- διατηρούν ευαίσθητες πληροφορίες σε ηλεκτρονικό αρχεία
- χρησιμοποιούν ‘cloud computing’ για αποθήκευση δεδομένων
- διατηρούν ηλεκτρονικό πελατολόγιο
- παρέχουν τη δυνατότητα ηλεκτρονικής πώλησης

δηλαδή….

σε όλες!!!

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

EIAS

Ενδεικτικές Παροχές Cyber Insurance σε σχέση με τα Παραδοσιακά Ασφαλιστήρια

	Περιουσία	Γενική Αστική Ευθύνη	Απώλειας Χρημάτων	K&R	E&O	Cyber
Ιδίες Ζημίες / Ζημιές Δικτύου						
Φυσική Καταστροφή Δεδομένων						
Καταστροφή δεδομένων λόγω Virus/Hacking						
Επίθεση Αρνησης Παροχής Υπηρεσίας (DDOS)						
BI – Διακοπη Εργασιών λόγω συμβάντων παραβίασης συστημάτων						
Εκβιασμός						
Σαμποτάζ Εργαζομένων με απώλεια δεδομένων						
Αστική Ευθύνη έναντι τρίτων						
Κλοπή / Απώλεια Δεδομένων						
Απώλεια Εταιρικών Πληροφοριών						
E&0 Παροχής Τεχνολογικών Υπηρεσιών						
Media Liability Ευθύνη Δημοσίευσης Περιεχομένου Πολυμέσων						
Παραβίαση Ιδιωτικότητας / Ενημέρωση						
Καταστροφή δεδομένων τρίτου						
Νομική Αντιμετώπιση Συμβάντος/ Διοικητικές Κυρώσεις - Πρόστιμα						
Μετάδοση Virus/Κακόβουλο Λογισμικό						

Καλύπτεται
Ισως Καλύπτεται
Δεν Καλύπτεται

Πηγή: https://www.cyberinsurancegreece.com

Σε ποιους απευθύνεται

Heat Map…

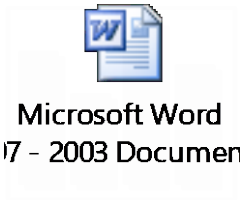
- Βιομηχανία,
- Χονδρεμπόριο
- Logistics
- Κατασκευές

- Λιανεμπόριο
- Μεταφορές
- Εκπαίδευση
- Ψυχαγωγία
- Real Estate

- Τηλεπικοινωνίες
- Υγεία
- E-shops
- Επεξεργασία Δεδομένων
- Υπηρεσίες Outsourcing Telemarketing ΜΜΕ

- Χρηματοοικονομικοί Οργανισμοί

Underwriting



Ερωτηματολόγια

Προασφαλιστικοί Έλεγχοι

Ανατομία ενός Cyber Claim

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

EIAS

Το πριν & το μετά!

- **Πριν**
- Αναγνωρίστε ότι τα δεδομένα σας είναι σε κίνδυνο και φτιάξτε ένα σχέδιο δράστης!
- **Μετά**
- Αναγνώριση παραβίασης
- Άμεση ενημέρωση για απώλειες συσκευών όπως laptops (γιατί το ανθρώπινο λάθος είναι η αιτία για το 75% των παραβιάσεων)
- Έλεγχος log files που θα έχουν καταγράψει μια μη εξουσιοδοτημένη πρόσβαση σε συστήματα – Αλλιώς
- Θα το μάθετε από έναν τρίτο όπως γίνεται στο 86% των περιπτώσεων
- **Το «Πραγματικό» μετά**
- *Οι εταιρίες ανήκουν σε 3 κατηγορίες:*
- Αυτές που αντιδρούν υπερβολικά χωρίς να ξέρουν τι έγινε
- Αυτές που δεν αντιδρούν καθόλου και περιμένουν για μέρες
- Αυτές που έχουν ένα σχέδιο

Ανατομία ενός Cyber Claim

Φάση 1 | Φάση 2 | Φάση 3 | Φάση 4

Φάση 1: 0 - 24 ώρες

- Ενεργοποίηση «Πρώτης Αντίδρασης»
- Νομικοί Σύμβουλοι & Ειδικοί IT αντιδρούν εντός 1 ώρας από τη γνωστοποίηση του περιστατικού
- Εκτίμηση γεγονότος και πρώτες συμβουλές
- Διατήρηση εμπιστευτικότητας
- Διαχείριση κρίσης
- Ανάλυση της διαρροής και προσπάθεια κατανόησης του σκοπού της
- Εντοπισμός των στοιχείων που έχουν διαρρεύσει

Ανατομία ενός Cyber Claim

Φάση 2: 24 – 48 ώρες

- Εκτίμηση του προβλήματος και δημιουργία σχεδίου αντίδρασης
- Παροχή συμβουλευτικών υπηρεσιών σχετικά με την ενημέρωση των υποκειμένων των δεδομένων
- Παροχή συμβουλευτικών υπηρεσιών σχετικά με την επικοινωνία με ρυθμιστικές αρχές
- Συνέχιση της ανάλυσης του περιστατικού
- Επιλογή συμβούλου επικοινωνίας και διαχείρισης του γεγονότος
- Διαχείριση περιστατικών εκβιασμού

Ανατομία ενός Cyber Claim

Φάση 3: 48 to 72 ώρες

- Αναλυτικό σχέδιο για την ενημέρωση των υποκειμένων των δεδομένων
- Ενημέρωση Αρχών και «διαπραγμάτευση» μαζί τους
- Συνέχιση των ενεργειών από της ομάδες των Συμβούλων (PR /IT forensic/ διαχείρισης εκβιασμού) σύμφωνα με τις ανάγκες
- Παροχή συμβουλευτικών υπηρεσιών για την παρακολούθηση των συστημάτων και την ενίσχυση της ασφάλειας τους

Ανατομία ενός Cyber Claim

Φάση 1 | Φάση 2 | Φάση 3 | Φάση 4

Φάση 4: 72+ ώρες

- Εκτίμηση του κόστους και των ζημιών
- Συνέχιση των ενημερώσεων των υποκειμένων των δεδομένων και των επαφών με τις Αρχές
- Διαχείριση σχέσεων με τρίτους που επηρεάστηκαν
- Συνεργασία με αστυνομικές αρχές
- Αναγνώριση μακροπρόθεσμων ζητημάτων που πρέπει να αντιμετωπιστούν
- Ενέργειες για αποζημιώσεις και περιορισμού της ζημιάς
- Ποσοτικοποίηση της απαίτησης για διακοπή εργασιών

Παραδείγματα Απαιτήσεων

ΕΠΑΓΓΕΛΜΑΤΙΚΟ
ΕΠΙΜΕΛΗΤΗΡΙΟ
ΑΘΗΝΩΝ

EIAS

Παραδείγματα Απαιτήσεων

Hacker

- Ο ασφαλισμένος προσφέρει ιατρική και ταξιδιωτική βοήθεια σε 70 χώρες
- Συνεργάζεται με κυβερνήσεις, εταιρίες και ΜΚΟ
- Ο ασφαλισμένος ενημερώθηκε από εταιρία συμβούλων που το είδε σε site hackers

Παραδείγματα Απαιτήσεων

«Κακός» Εργαζόμενος

- Ο ασφαλισμένος είναι τράπεζα με δραστηριότητα και στο εξωτερικό
- Ένας Οικονομικός Αναλυτής στο τμήμα δανείων του ασφαλισμένου κατέβασε 2 εκ φακέλους πελατών
- Πουλούσε 20.000 προφίλ πελατών κάθε εβδομάδα για €500 το καθένα

Ενημέρωση μεγάλου αριθμού πελατών

42 ομαδικές αγωγές

Κόστος: **€40 εκατ.**

Κάλυψη από συμβόλαιο: €20 εκατ.

Παραδείγματα Απαιτήσεων

Hacker	Μεγάλη εμπορική αλυσίδα καταναλωτικών ειδών	Η διαρροή έγινε τον Δεκέμβριο του 2013
Ο ασφαλισμένος το έμαθε από κρατικές αρχές ασφαλείας	Εντοπίστηκε malware σε 43.745 τερματικά πιστωτικών καρτών	Για 20 μέρες το malware υπέκλεπτε τα στοιχεία 40 εκατ. πιστωτικών και χρεωστικών καρτών

Οι «ελληνικές» Ζημίες

Ψυχολογικός εκβιασμός

Διακοπή εργασιών

Malware

Ransomware

Ανθρώπινο λάθος

Σύνοψη της ανατομία μιας ζημιάς και της αντίδρασης ενός Cyber Risk συμβολαίου

1. **Παραβίαση** → Άμεση ανταπόκριση συμβουλών
2. **IT Forensics** → Ειδικοί εντοπίζουν τι έχει επηρεαστεί, πώς μπορούν να περιοριστούν οι επιπτώσεις του περιστατικού και να αποκατασταθεί η ζημιά
3. **Νομική Υποστήριξη & PR** → Ειδικοί αναλαμβάνουν να περιορίσουν την νομική έκθεση σε κίνδυνο και να προστατέψουν τη φήμη της εταιρίας
4. **Ενημερώσεις** → Κόστος ενημέρωσης αρχών και υποκειμένων δεδομένων
5. **Πρόστιμα & Έρευνες** → προετοιμασία για έρευνες από αρχές και κάλυψη ασφαλίσιμων προστίμων
6. **Ευθύνες** → Έξοδα υπεράσπισης και αποζημιώσεις για παραβίαση δεδομένων
7. **Εκβιασμός** → Διαπραγμάτευση και κάλυψη «λύτρων» εκβιασμού
8. **Διακοπή Εργασιών** → Αποζημίωση απώλειας κερδών

Ευχαριστώ για την προσοχή σας

Ερωτήσεις;

ΕΠΑΓΓΕΛΜΑΤΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΘΗΝΩΝ

EIAS