AIG

CyberEdge

Κώστας Βούλγαρης
Financial Lines & Casualty Manager

Δήλωση αποποίησης ευθύνης & πνευματικής ιδιοκτησίας

- Η Παρουσίαση αυτή ετοιμάστηκε από την AIG και προορίζεται αποκλειστικά για σκοπούς ενημέρωσης των Συνεργατών της Εταιρίας. Σε καμία περίπτωση δεν μπορεί να εκληφθεί ως προσφορά ή συμβουλή για σύναψη οποιασδήποτε ασφαλιστικής ή άλλης σύμβασης.
- Η εν λόγω παρουσίαση περιλαμβάνει πληροφορίες γενικού μόνο χαρακτήρα. Η Παρουσίαση αυτή δεν πρέπει να θεωρηθεί ότι εξαντλεί πλήρως τα θέματα στα οποία αναφέρεται και ότι περιέχει όλες τις πληροφορίες που ο αποδέκτης δύναται να ζητήσει.
- Καμία απόφαση σύναψης σύμβασης δεν μπορεί να στηριχθεί αποκλειστικά στις πληροφορίες που περιέχονται στην Παρουσίαση αυτή.
- Η παρουσίαση αυτή αποτελεί πνευματική ιδιοκτησία της AIG. Απαγορεύεται η αναπαραγωγή ή αντιγραφή του συνόλου ή μέρους αυτής της Παρουσίασης και της πληροφόρησης που περιέχει, για οποιοδήποτε σκοπό, χωρίς την προηγούμενη έγγραφη άδεια της AIG.

Πώς φτάσαμε στο CyberEdge;

CyberEdge

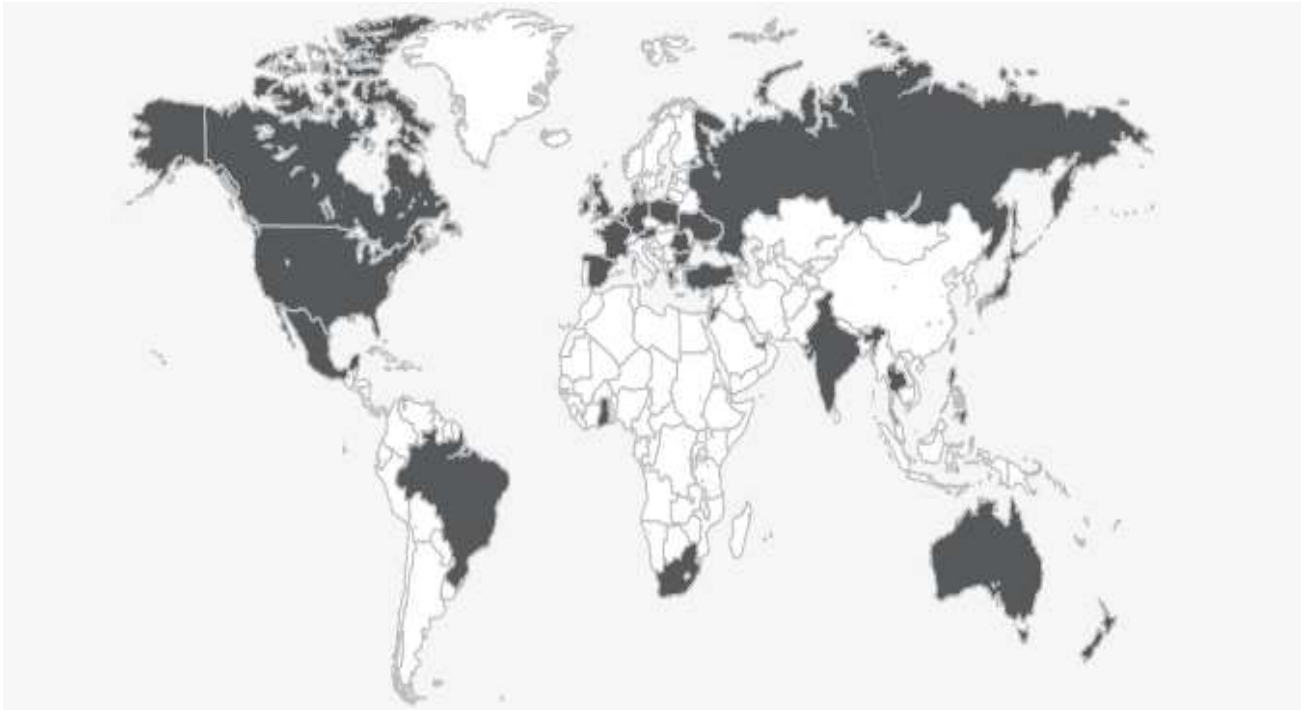
Η μεγαλύτερη ανησυχία των πελατών είναι οι κίνδυνοι του κυβερνοχώρου*

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.*

AIG

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

Κίνδυνος των «μεγάλων»;

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.

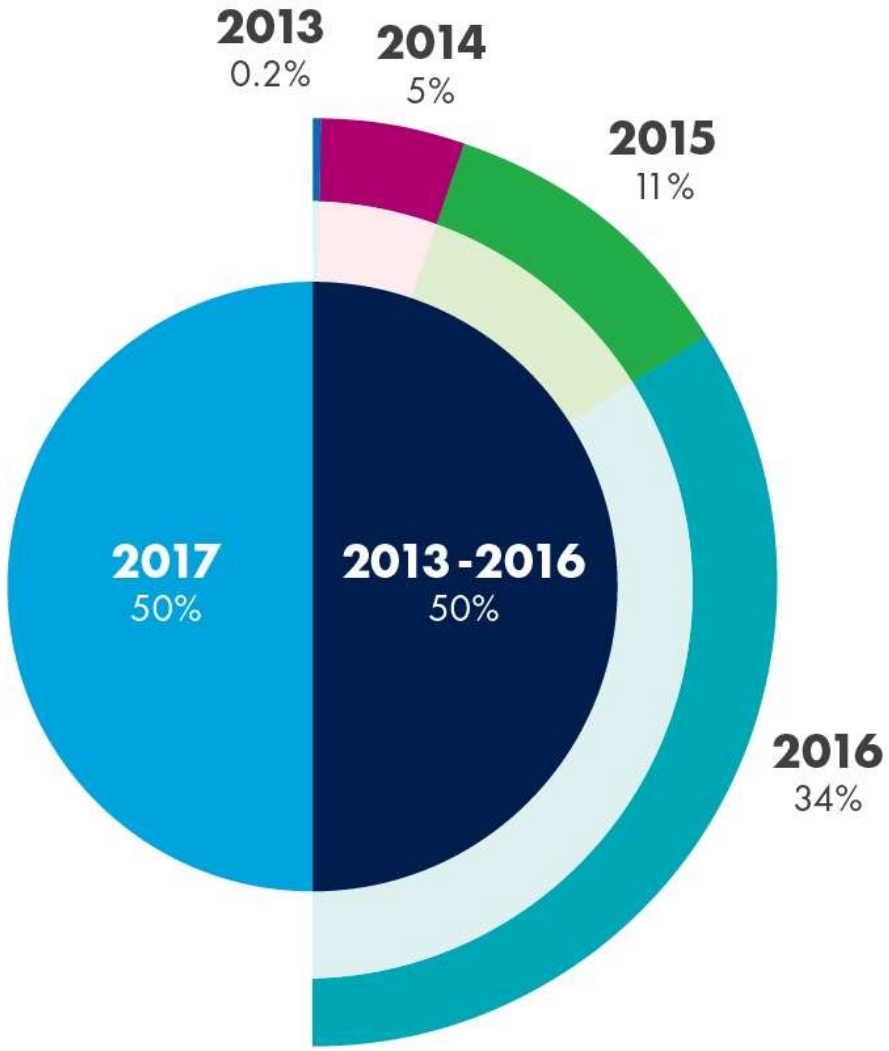
AIG

Κίνητρα Διαδικτυακών Επιθέσεων

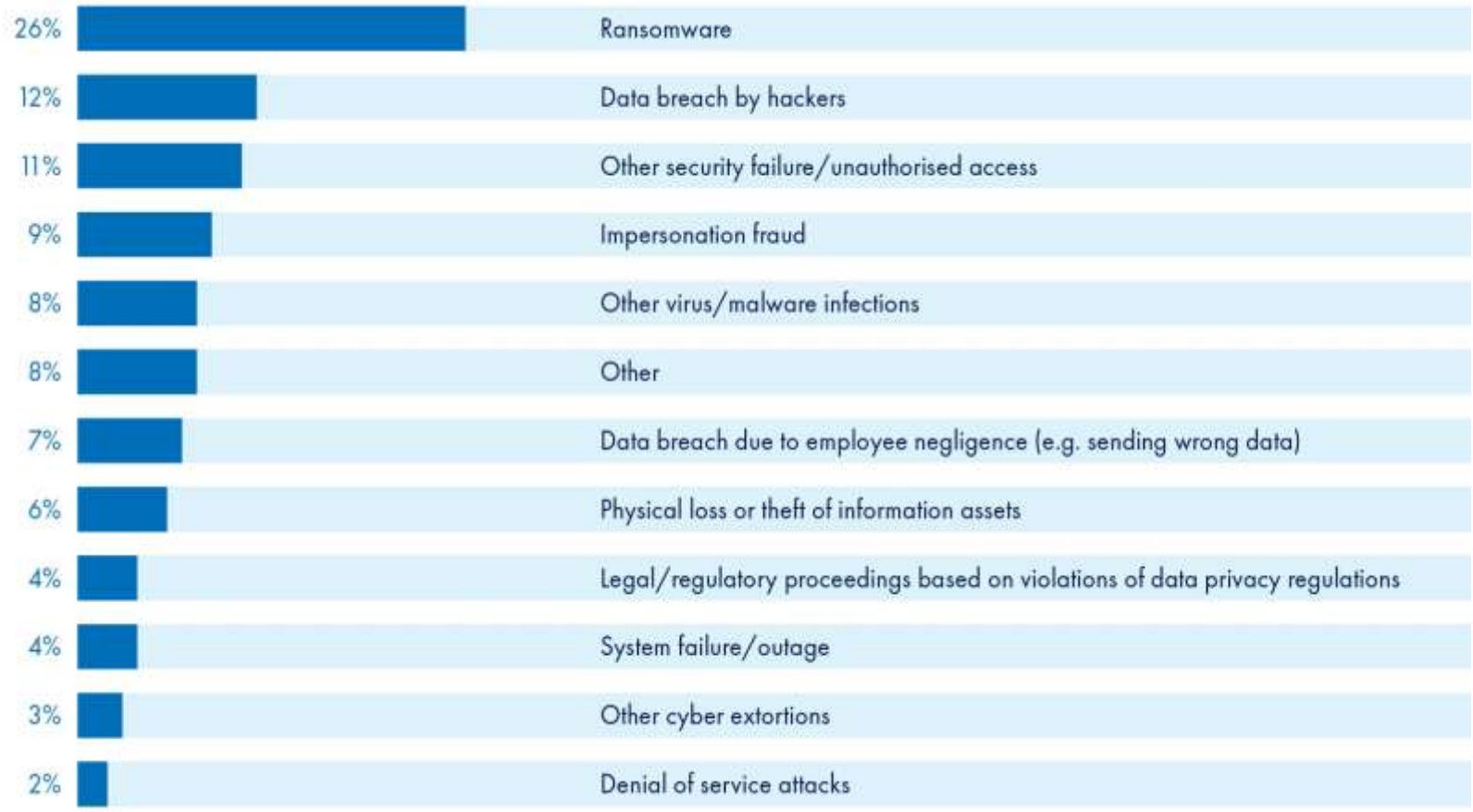
- Άμεσο / έμμεσο οικονομικό όφελος
- Προσωπική προβολή / Προβολή κοινωνικής ατζέντας
- Βιομηχανική κατασκοπεία
- Αντίποινα
- Υποκλοπή δεδομένων προσωπικού χαρακτήρα
- Πρόκληση Άρνησης υπηρεσιών
- Δυσφήμιση

AIG

Ζημιές Cyber στην Ευρώπη ανά έτος

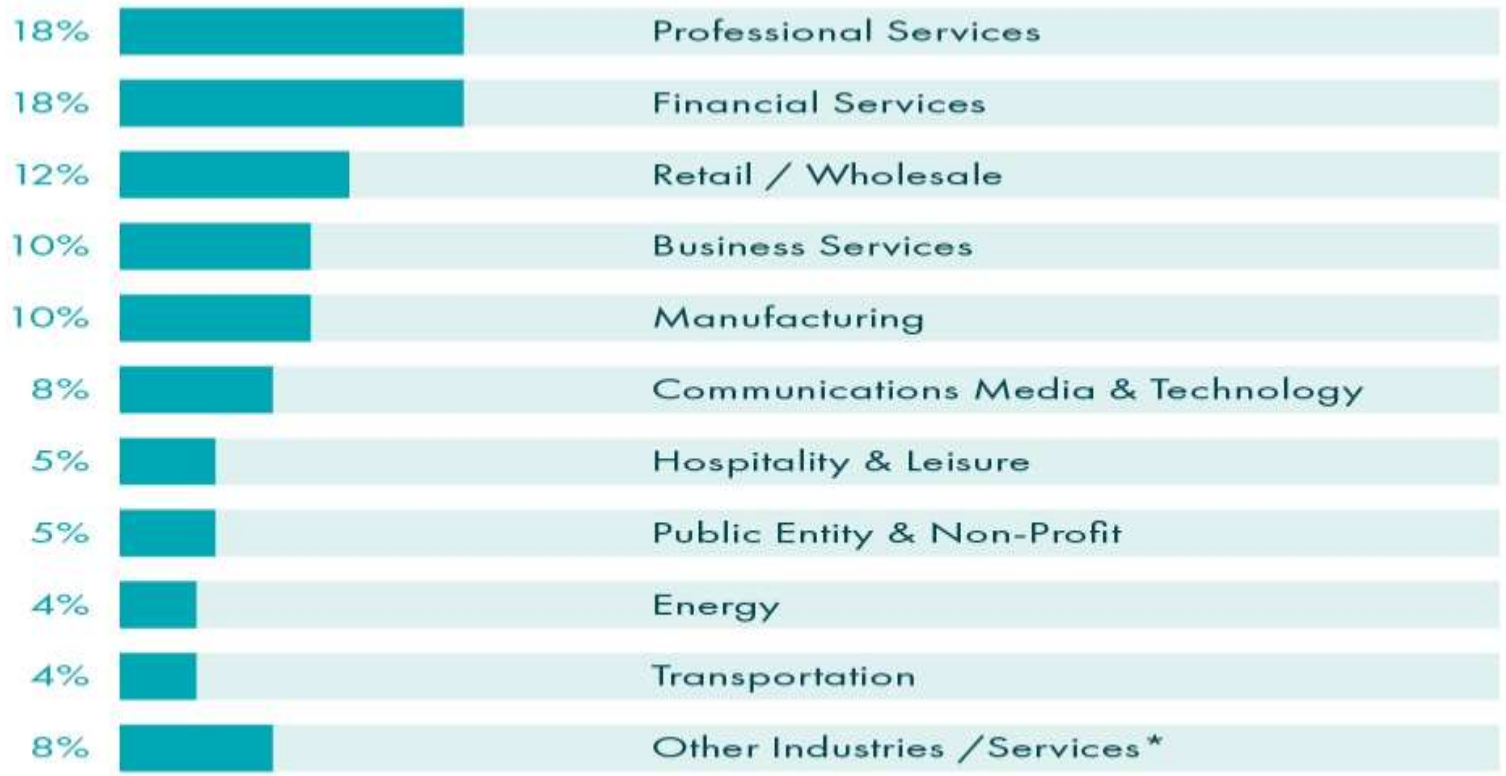


2017 – Ζημίες Cyber ανά κατηγορία περιστατικών



AIG

2017 – Ζημιές Cyber ανά κατηγορία επιχειρήσεων



*Food & Beverage, Construction, Real Estate, Agriculture, Information Services

Note: Figures may not add up to 100% due to rounding

AIG

Τι είναι το CyberEdge ;

AIG

CyberEdge

- Ασφαλιστικό προϊόν
- Καλύπτει Αποζημιώσεις προς τρίτους
- Παρέχει Υπηρεσίες αντιμετώπισης κρίσης / περιστατικών
- **Αποτελεί πλήρης ασφαλιστική λύση Διαχείρισης Ρίσκου**

AIG

Τι καλύπτει το CyberEdge

AIG

Παροχές CyberEdge

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

AIG

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

AIG

Ανατομία ενός Cyber Claim

Τι συμβαίνει και πότε;

Ανατομία ενός Cyber Claim

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

AIG

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

AIG

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

AIG

Ανατομία ενός Cyber Claim

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

AIG

Σύνοψη της ανατομία μιας ζημιάς και της αντίδρασης του CyberEdge

1. **Παραβίαση** → Άμεση αντίδραση μέσα σε 1 ώρα
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

AIG

Γιατί AIG;

- Εκτεταμένη εμπειρία ανάληψης κινδύνων
- Χρήση εξειδικευμένων παρόχων υπηρεσιών
- Εύκολη τιμολόγηση
- Ελληνικοί όροι συμβολαίου
- Συνεχής αναβάθμιση και εξέλιξη των όρων και των υπηρεσιών
- Εξειδικευμένη διαχείριση αξιώσεων με ευαισθησία και διακριτικότητα
- Επιθυμία να κτίσουμε μακροχρόνιες σχέσεις με τους συνεργάτες / πελάτες μας

AIG

www.aig.com.gr/CyberEdge


AIG