Σας ευχαριστούμε για την συμμετοχή σας στα σεμινάρια της AIG

Τα μικρόφωνά σας παρακαλούμε να είναι απενεργοποιημένα
για την αποφυγή θορύβου.
Εάν θέλετε να κάνετε μια ερώτηση σε έναν από εμάς, μπορείτε να το κάνετε μέσω της λειτουργίας συνομιλίας (chat).
Για να το κάνετε αυτό, κάντε κλικ στο εικονίδιο chat στο κάτω μέρος της οθόνης σας.
Θα συγκεντρώσουμε τις ερωτήσεις και στην ενότητα Q&A στο τέλος αυτού του διαδικτυακού σεμιναρίου θα σας απαντήσουμε.

AIG

CYBEREDGE

AIG

Ρήτρα Αποποίησης Ευθύνης

- 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 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.
- 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.

Πως φτάσαμε στο Cyber Insurance;

Η μεγαλύτερη ανησυχία των πελατών είναι οι κίνδυνοι του κυβερνοχώρου*

Κίνδυνοι Κυβερνοχώρου 86%

Απώλεια εισοδημάτων 82%

Περιουσιακή ζημία 80%

Αποζημίωση εργαζόμενων 78%

Διακοπή υπηρεσιών κοινής ωφέλειας 76%

Αξιόγραφα/κίνδυνος επενδύσεων 76%

Αστική Ευθύνη οχημάτων και στόλων 65%

AIG

** 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.*

Ραγδαία αύξηση του όγκου της πληροφορίας, των πληροφοριακών ροών και των επικοινωνιών· η κλίμακα της συλλογής και της ανταλλαγής δεδομένων προσωπικού χαρακτήρα αυξήθηκε σημαντικά. Η τεχνολογική εξέλιξη διευκόλυνε την παραβίαση των δεδομένων, καθιστώντας αναγκαία τη λήψη μέτρων

Η πλειοψηφία των CEO πιστεύει ότι είναι δύσκολο να παρακολουθήσει τις εξελίξεις και τις απειλές στον κυβερνοχώρο επειδή αυξάνονται πολύ γρήγορα.

CyberEdge

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

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.

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:

A. έχει ως κεντρική λογική την ελαχιστοποίηση της συλλογής, διατήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα,

B. 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

C. 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

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
- 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

Verizon 2012

Figure 7. Countries represented in combined caseload

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	

Είμαστε στο χάρτη

AIG

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

Κίνδυνοι

- 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

Συνέπειες

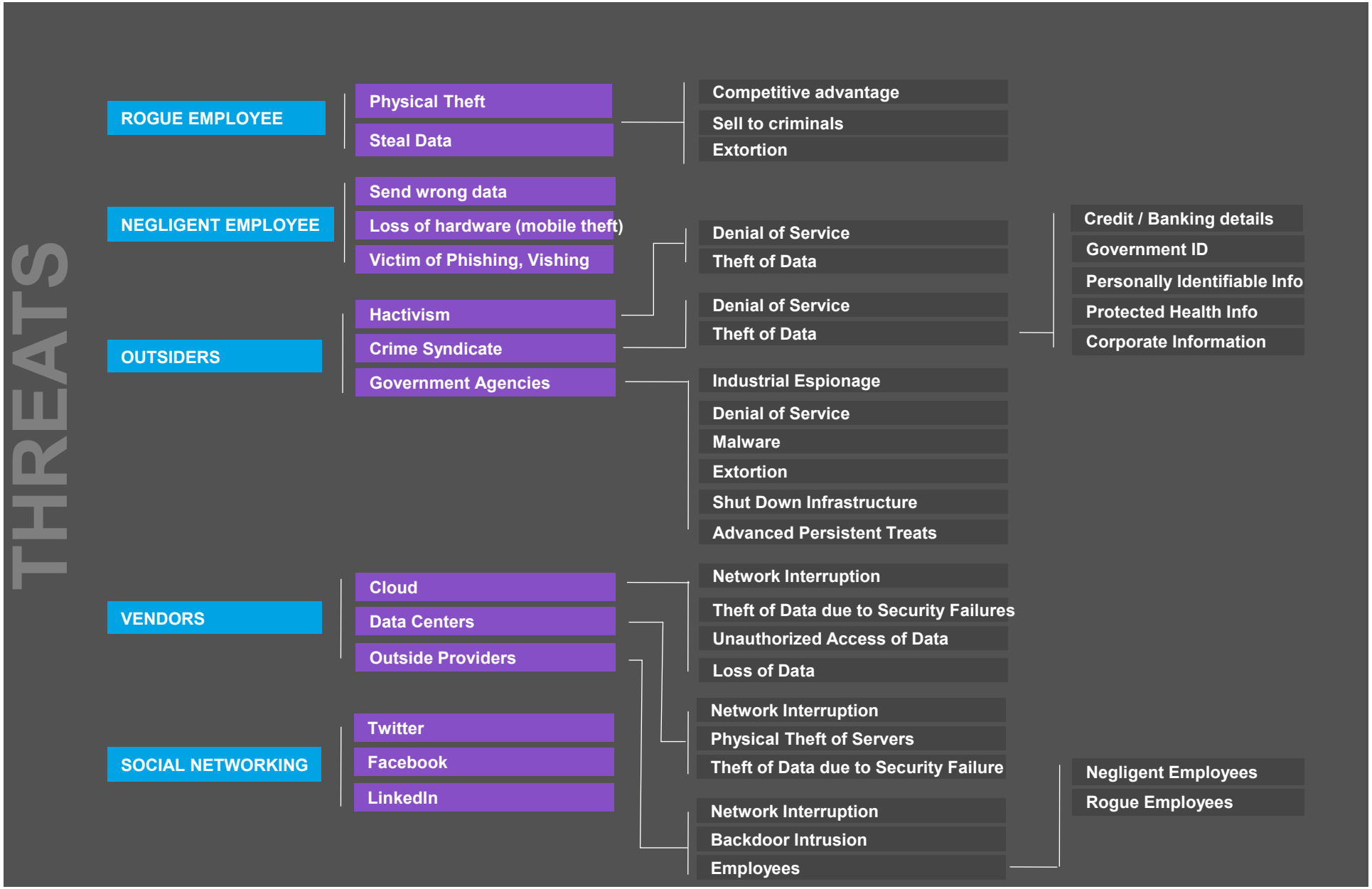
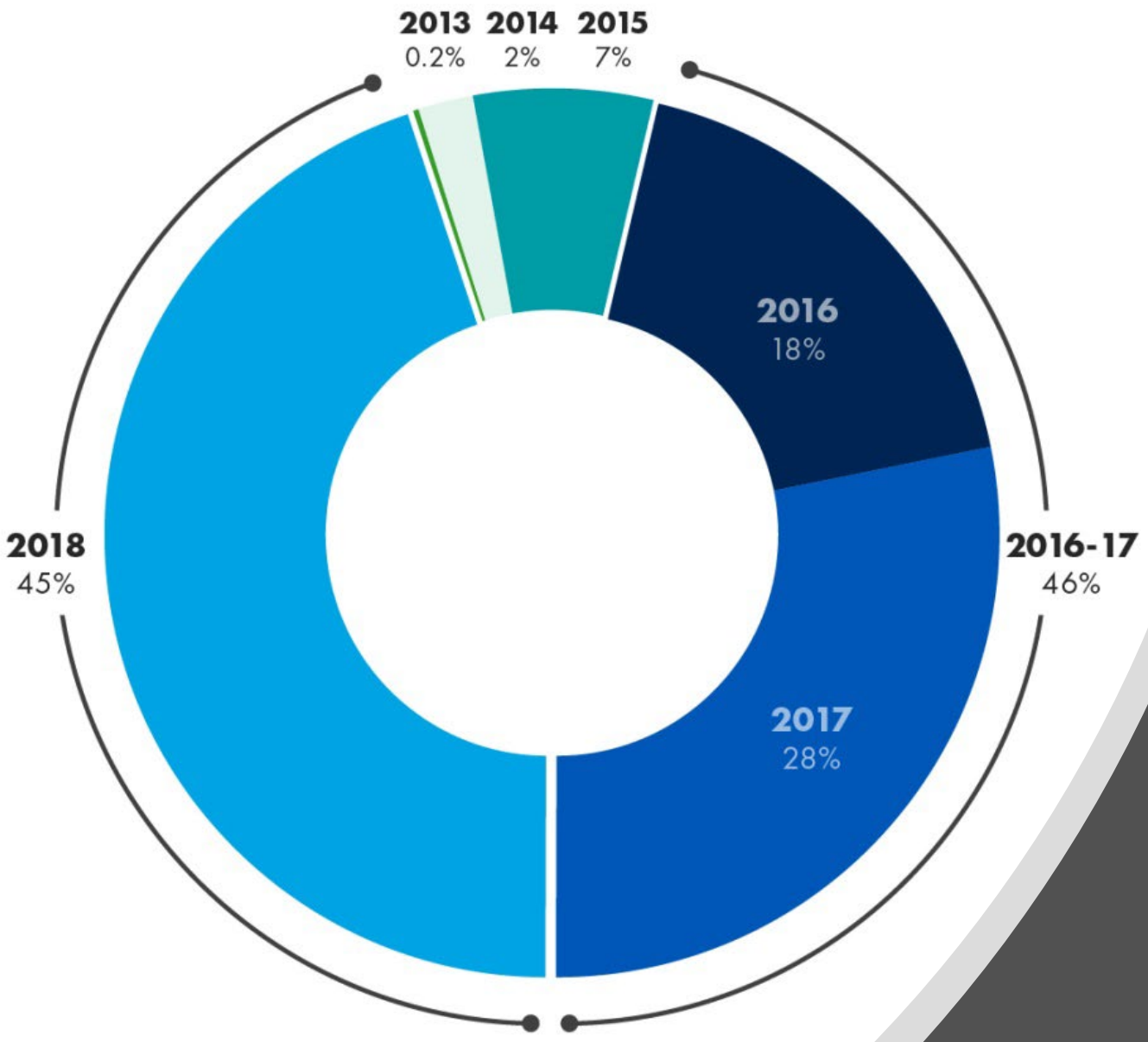

THREATS
ROGUE EMPLOYEE
Physical Theft
Steal Data
Competitive advantage
Sell to criminals
Extortion
NEGLIGENT EMPLOYEE
Send wrong data
Loss of hardware (mobile theft)
Victim of Phishing, Vishing
OUTSIDERS
Hactivism
Crime Syndicate
Government Agencies
Denial of Service
Theft of Data
Denial of Service
Theft of Data
Industrial Espionage
Denial of Service
Malware
Extortion
Shut Down Infrastructure
Advanced Persistent Treats
Credit / Banking details
Government ID
Personally Identifiable Info
Protected Health Info
Corporate Information
VENDORS
Cloud
Data Centers
Outside Providers
Network Interruption
Theft of Data due to Security Failures
Unauthorized Access of Data
Loss of Data
SOCIAL NETWORKING
Twitter
Facebook
LinkedIn
Network Interruption
Physical Theft of Servers
Theft of Data due to Security Failure
Network Interruption
Backdoor Intrusion
Employees
Negligent Employees
Rogue Employees

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



Ζημιές Cyber στην Ευρώπη ανά έτος

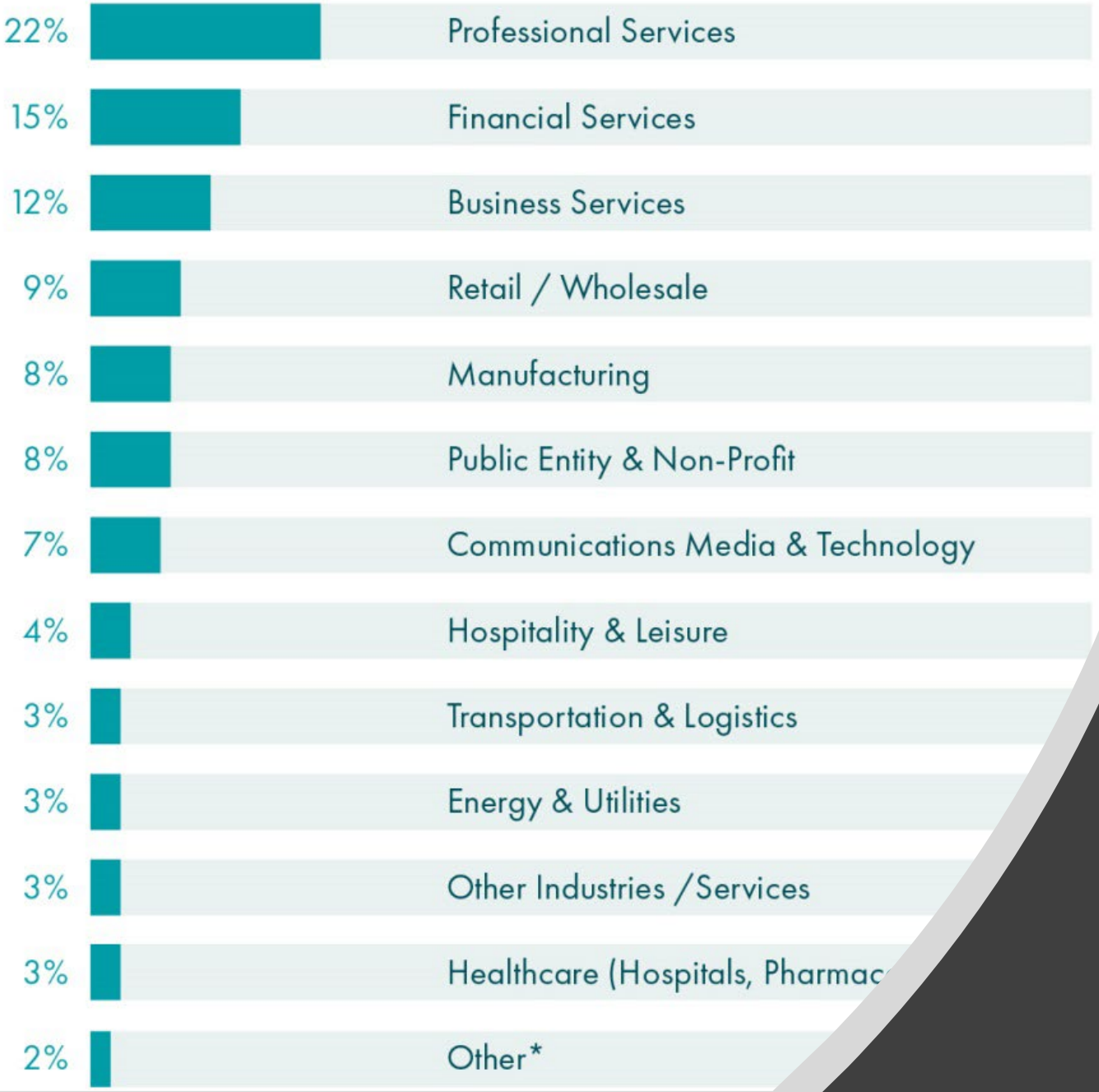
2018 – Ζημίες Cyber ανά κατηγορία περιστατικών

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

AIG

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



2018 – Ζημιές Cyber ανά κατηγορία επιχειρήσεων

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!

AIG

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

AIG

Τι είναι η ασφάλεια των Cyber Risks

- Ασφαλιστικό προϊόν - Ασφάλιση ηλεκτρονικών και διαδικτυακών κινδύνων
- Καταβάλει Αποζημιώσεις προς τρίτους
- Παρέχει Υπηρεσίες αντιμετώπισης κρίσης / περιστατικών
- Αποτελεί Πλήρης ασφαλιστική λύση διαχείρισης ρίσκου

AIG

Ορισμοί

Προσωπικά δεδομένα

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 μη η εξουσιοδοτημένη καταστροφή**
- **Απώλεια**
- **Αλλοίωση**
- **Απαγορευμένη διάδοση / πρόσβαση**

Τι κάνει ο Υπεύθυνος μετά από ένα περιστατικό;

- συγκέντρωση στοιχείων - πραγματογνώμονας για ανάλυση / αξιολόγηση του περιστατικού (αν από το περιστατικό προκύπτουν κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων)
- Ενδεχόμενη υποχρέωση άμεσης ενημέρωσης υποκειμένων των δεδομένων και της Αρχής (ο Υπεύθυνος Επεξεργασίας θα πρέπει να γνωστοποιήσει την παραβίαση, εκτός αν η παράβαση είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων)
- Μέτρα με σκοπό την αντιμετώπιση του περιστατικού παραβίασης ή/και τον περιορισμό των επιπτώσεών του
- Αναβάθμιση πολιτικής ασφάλειας και μέτρων εφαρμογής
- Επανεκπαίδευση προσωπικού
- Πρόγραμμα ανταπόκρισης σε περίπτωση άλλου περιστατικού

Διαρροή δεδομένων και ασφάλεια δικτύου

Καλύπτει απαιτήσεις τρίτων κατά του ασφαλισμένου που προέρχονται από:

- Διαρροή δεδομένων από κακόβουλο λογισμικό και από ιούς ειδικά σχεδιασμένους για το σκοπό αυτό
- Αδυναμία πρόσβασης σε δεδομένα πελατών
- Αλλοίωση δεδομένων τρίτων στα συστήματα του ασφαλισμένου λόγω κακόβουλης ενέργειας
- Κοινολόγηση δεδομένων λόγω παραβίασης συστημάτων
- Απώλεια δεδομένων που βρίσκονταν σε φορητά μέσα

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

CyberEdge - Οι καλύψεις

Α. Διαχείριση Γεγονότων

- 24ώρη πρόσβαση σε τηλεφωνικό κέντρο
- Νομικές υπηρεσίες από εξειδικευμένο νομικό σύμβουλο
- Υπηρεσίες πληροφορικής από εξειδικευμένο σύμβουλο πληροφορικής
- Έξοδα για επαναφορά δεδομένων
- Προστασία της φήμης από εξειδικευμένο σύμβουλο διαχείρισης εταιρικών κρίσεων
- Γνωστοποίηση του περιστατικού

CyberEdge - Οι καλύψεις

Β. Υποχρεώσεις Προστασίας προσωπικών δεδομένων

- Πρόστιμα προστασίας προσωπικών δεδομένων
- Έξοδα υπεράσπισης του ασφαλισμένου στα πλαίσια έρευνας ρυθμιστικής αρχής

Γ. Ευθύνη

- Απαιτήσεις από τρίτους για παραβίαση προσωπικών και εταιρικών Πληροφοριών

Δ. Κάλυψη Ψηφιακών μέσων

- Απαιτήσεις τρίτων και έξοδα υπεράσπισης που σχετίζονται με δραστηριότητες ψηφιακών μέσων (δυσφήμιση, παραβίαση πνευματικών δικαιωμάτων)

Ε. Διακοπή λειτουργίας δικτύου

- Μείωση του καθαρού κέρδους του ασφαλισμένου, δαπάνες για τη συνέχιση της συνήθης δραστηριότητας

ΣΤ. Κάλυψη εκβιασμού αποκάλυψης προσωπικών δεδομένων

- Μετρητά ή άλλα χρηματικά μέσα που κατέβαλε ο Ασφαλισμένος για την αποφυγή ή τον τερματισμό μιας απειλής εκβιασμού

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 ανωτέρω σημεία αυτού του ορισμού στο μέτρο που εγείρεται κατά αυτών **Απαίτηση** σε σχέση με πράξη, σφάλμα ή παράλειψη αυτού

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

Σωματικές Βλάβες και Υλικές Ζημίες

οιαδήποτε:
(i) σωματική βλάβη, ασθένεια, νόσος ή θάνατος και, εάν προκύπτει από τα προαναφερθέντα, νευρικός κλονισμός, συναισθηματική οδύνη, ψυχική οδύνη ή
(i) απώλεια ή καταστροφή ενσώματων αγαθών, εκτός από Δεδομένα.

Ρύπανση

Τρομοκρατία / Πόλεμος

κάθε μορφής:

- πόλεμος, εισβολή, εχθρική ενέργεια ξένου κράτους, εχθροπραξία ή πολεμική επιχείρηση (ανεξαρτήτως εάν έχει κηρυχθεί πόλεμος ή όχι), εμφύλιος πόλεμος, στρατιωτική εξέγερση, στάση ή επανάσταση
- τρομοκρατία (εξαιρουμένης της Τρομοκρατίας στον Κυβερνοχώρο) ή εξέγερση.

Μη Ασφαλίσιμη Ζημία

- κάθε ζήτημα για το οποίο ο **Ασφαλιστής** απαγορεύεται να προβεί σε πληρωμή, βάσει των κανόνων του **Ασφαλιστηρίου** ή της δικαιοδοσίας στην οποία προβάλλεται **Απαίτηση** ή στην οποία προκύπτει για πρώτη φορά **Ασφαλιστικό Γεγονός**.

Παράλειψη Αποκατάστασης

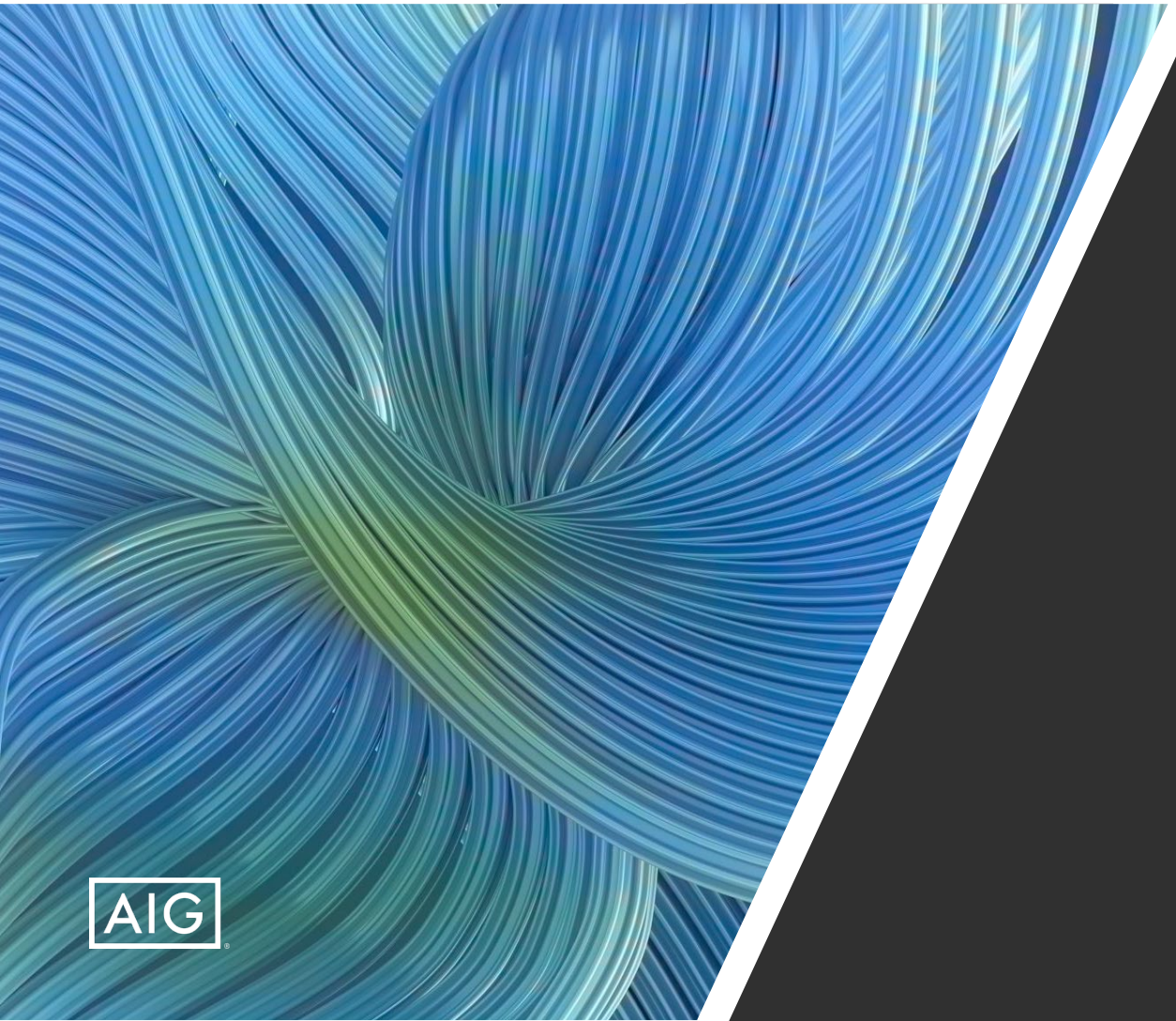
κάθε παράλειψη αποκατάστασης ελαττωματικών συστημάτων, διαδικασιών ή λογισμικού, όπου η ύπαρξη ελαττωμάτων, ελλείψεων ή ευπάθειας σε επίθεση ή παρείσδυση έχει επισημανθεί στο **Αρμόδιο Στέλεχος** αρκετά έγκαιρα πριν από την επέλευση της **Ζημίας**, ώστε να αποφευχθεί ή να μειωθεί ο αντίκτυπός της.

AIG

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

Σε ποιους απευθύνεται



Heat Map…

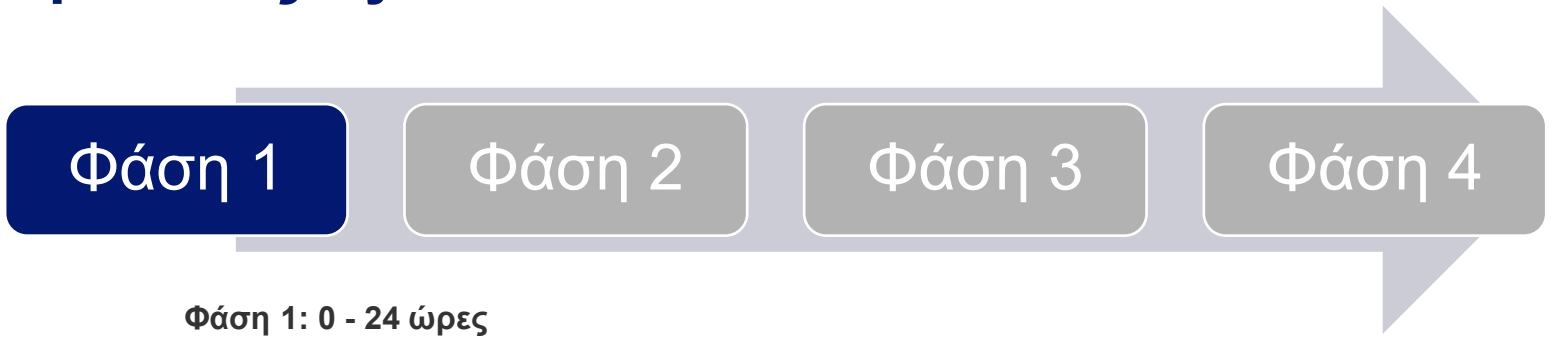
- Βιομηχανία
- Χονδρεμπόριο
- Logistics
- Κατασκευές

- Λιανεμπόριο
- Μεταφορές
- Εκπαίδευση
- Ψυχαγωγία
- Real Estate

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

- Χρηματοοικονομικοί Οργανισμοί

Ανατομία ενός Cyber Claim

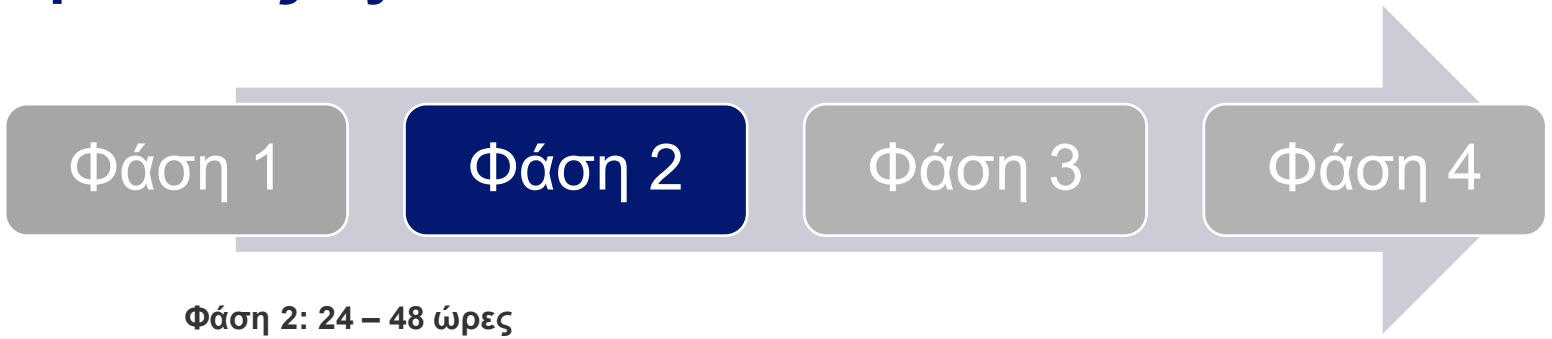


Φάση 1: 0 - 24 ώρες

- 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

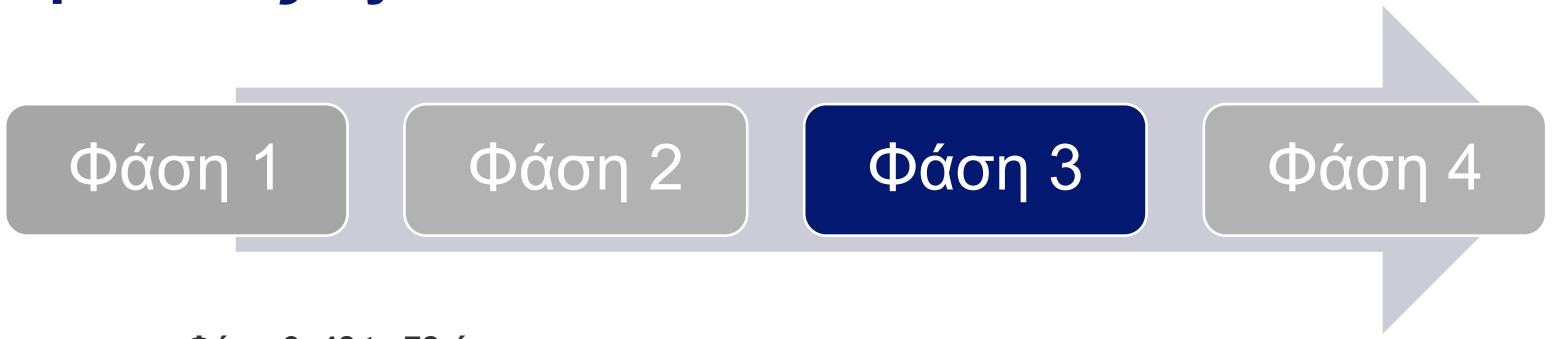


Φάση 2: 24 – 48 ώρες

- 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

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 είδε σε site hackers τα κλεμμένα δεδομένα προς πώληση.

Παραδείγματα Απαιτήσεων

«Κακός» Εργαζόμενος

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

Παραδείγματα Απαιτήσεων

Hacker

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

AIG

CyberEdge

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


Q&As
AIG
www.aig.com.gr/CyberEdge