Η Διαδικτυακή Ασφάλεια στη Πράξη

Μαργαρίτα Γκολφινοπούλου
Director, Commercial Lines & Risk Champion AIG Greece

Σεπτέμβριος 2018

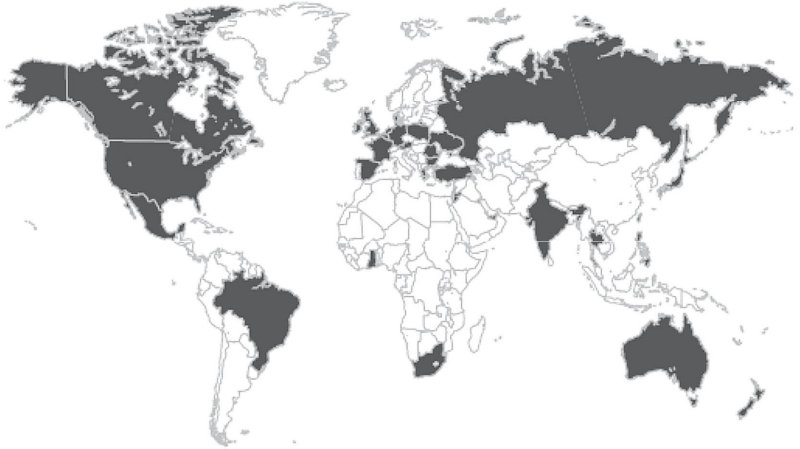
Η ασφάλιση των Διαδικτυακών & Ηλεκτρονικών κινδύνων δεν είναι απλά ένα ασφαλιστικό προϊόν, είναι ένα εργαλείο **Risk Management** (3-5LoDs), παρέχοντας κυρίως υπηρεσίες **προετοιμασίας για την αποφυγή / περιορισμό των συνεπειών** περιστατικών παραβίασης συστημάτων και φυσικά, αποζημιώσεις

AIG

Ευρωπαϊκές & Διεθνείς Εξελίξεις

- EE - General Data Protection Regulation (GDPR)
  - Προστασία Καταναλωτή
  - Υψηλές Χρηματικές ποινές
  - Υποχρέωση Ενημέρωσης

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	
Denmark	Japan	Philippines	Turkey	

AIG

Κόστος ανά χώρα

Ηνωμένο Βασίλειο
£27 δις
Κόστος κυβερνο-εγκλήματος

Ιρλανδία:
37 διαρροές/ έτος

Σκωτία:
£5 δις
Κόστος Κυβερνο-εγκλήματος

Κόστος για Βρετανικές επιχειρήσεις
£21 δις

£2,04
εκατ.
Μέσο κόστος διαρροής

AIG

Κόστος ανά χώρα

Ιταλία
16,456 επιθέσεις hackers εις βάρος οργανισμών σε 6 μήνες, ανεβασμένο 57% από τη περσινή χρονιά

Γερμανία:
Κόστος για τις επιχειρήσεις **EUR 43δις**

Ρωσία:
αύξηση κυβερνο – εγκλήματος κατά 33%

Βέλγιο:
Κόστος κυβερνο - εγκλήματος **EUR 5δις**

AIG

Συνέπειες που επέρχονται

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

Αδυναμία πραγματοποίησης πωλήσεων
- Απώλεια πωλήσεων
- Αθέτηση πιθανών service agreements

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

Απρόβλεπτα κόστη
- Δαπάνες για συνέχιση παραγωγής
- Ανάγκη επισκευών μηχανογραφικών υποδομών
- Έξοδα συμβούλων
- Ανάκτηση ή Αντικατάσταση δεδομένων
- Έξοδα ενημέρωσης πελατών / συνεργατών

Κρίση εταιρικής Φήμης
- Κόστος για την εταιρία
- Ενόχληση καταναλωτών
- Απώλεια υφιστάμενων συμβάσεων 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
- Εσωτερικές
- Ελεγκτικών Αρχών
- Μετόχων

AIG

The Cyber Landscape

Οι Διαδικτυακές απειλές δεν είναι πια προνόμιο των μεγάλων επιχειρήσεων

- Ολοένα και αυξανόμενο ποσοστό μικρομεσαίων επιχειρήσεων πιστεύει ότι οι διαδικτυακοί κίνδυνοι αποτελούν μια σοβαρή απειλή για τις ίδιες και σχεδόν όλες παίρνουν πλέον κάποια μέτρα προστασίας, αλλά και πάλι σχεδόν όλες δεν καταφέρνουν να δουν το θέμα ολικά και να προετοιμαστούν σφαιρικά.

- Οι ΜΜΕ είναι επίσης πιο εκτεθειμένες σχετικά με τη χρήση φορητών ηλεκτρονικών συσκευών από τους υπαλλήλους τους και γι' αυτό καταφεύγουν όλο και συχνότερα στη λύση εξωτερικών παρόχων (cloud).

- Παρόλο που όλοι συμφωνούν για την ύπαρξη των διαδικτυακών και ηλεκτρονικών κινδύνων, λίγες μικρομεσαίες επιχειρήσεις προετοιμάζονται και έτσι είναι πιο εύκολος στόχος.

Advisen study 2013

AIG

Παραδείγματα Απαιτήσεων

Πραγματικές περιπτώσεις που έχει χειριστεί η AIG

Παραδείγματα Απαιτήσεων

Παραβίαση Ασφάλειας

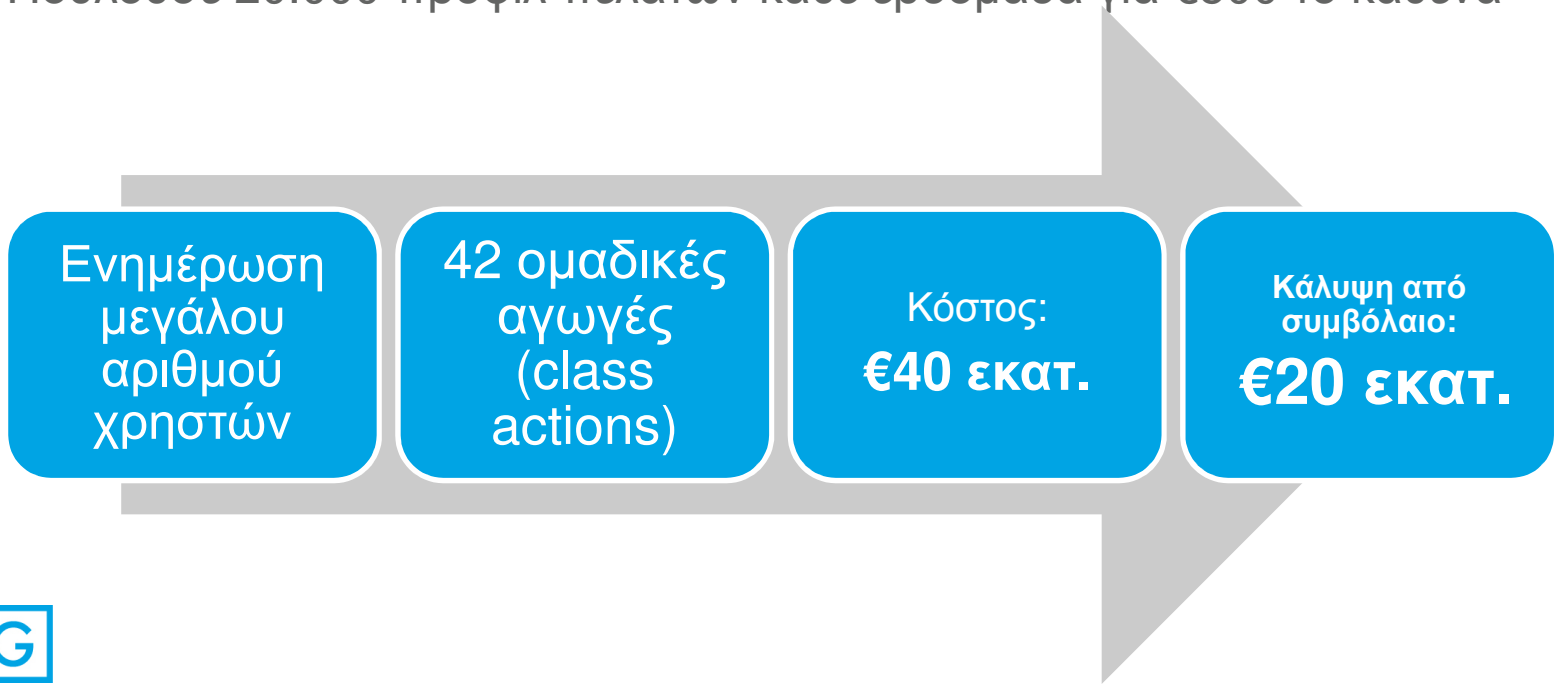
- Η ασφαλισμένη προσφέρει ιατρική και ταξιδιωτική βοήθεια σε 70 χώρες
- Συνεργάζεται με κυβερνήσεις, εταιρίες και ΜΚΟ
- Ενημερώθηκε από εταιρία συμβούλων που το είδε σε site hackers

AIG

Παραδείγματα Απαιτήσεων

Απιστία Εργαζομένου

- Η ασφαλισμένη είναι τράπεζα με δραστηριότητα σε πολλές χώρες
- Ένας υψηλόβαθμος Οικονομικός Αναλυτής στο τμήμα δανείων της ασφαλισμένης «κατέβασε» 2εκ φακέλους πελατών
- Πουλούσε 20.000 προφίλ πελατών κάθε εβδομάδα για €500 το καθένα



AIG

Παραδείγματα Απαιτήσεων

Παραβίαση Ασφάλειας

- Μεγάλη εμπορική αλυσίδα καταναλωτικών ειδών
- Η διαρροή έγινε τον Δεκέμβριο του 2013
- Η ασφαλισμένη ενημερώθηκε 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

AIG

Ανατομία ενός Cyber Claim

Τι συμβαίνει και πότε;

AIG

Ανατομία ενός Cyber Claim

Πριν

- Αναγνωρίστε ότι τα δεδομένα σας είναι σε κίνδυνο και φτιάξτε ένα σχέδιο δράσης!

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 – Διαφορετικά,

  …. 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

AIG

Ανατομία ενός Cyber Claim

1ο Στάδιο : 0 - 24 ώρες

- Ειδοποιήστε τον ασφαλιστή σας!
- Οι Σύμβουλοι Ασφαλείας Πληροφορικής και οι Νομικοί μας Σύμβουλοι θα επικοινωνήσουν μαζί σας σε 1 ώρα
- 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

2ο Στάδιο : 24 – 48 ώρες

- Εκτίμηση του προβλήματος και δημιουργία σχεδίου αντίδρασης
- Συμβουλές σχετικά με την ενημέρωση των ανθρώπων που χάθηκαν τα δεδομένα τους
- Συμβουλές σχετικά με την επικοινωνία με εποπτεύουσες αρχές
- Συνέχιση της ανάλυσης του περιστατικού
- Επιλογή συμβούλου επικοινωνίας και διαχείρισης του γεγονότος
- Διαχείριση περιστατικών εκβιασμού

AIG

Ανατομία ενός Cyber Claim

3ο Στάδιο : 48 - 72 ώρες

- Αναλυτικό σχέδιο για την ενημέρωση των παθόντων
- Ενημέρωση Αρχής Προστασίας και «διαπραγμάτευση» μαζί τους
- Συνέχιση των ενεργειών από της ομάδες των Συμβούλων (PR /IT forensic/ διαχείρισης εκβιασμού) σύμφωνα με τις ανάγκες
- Συμβουλές για την παρακολούθηση των συστημάτων και την ενίσχυση της ασφάλειας τους

AIG

Ανατομία ενός Cyber Claim

4ο Στάδιο: 72+ ώρες

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

AIG

Σύνοψη της ανατομία μιας ζημιάς και της αντίδρασης ενός ασφαλιστικού προγράμματος

1. **Παραβίαση** → Άμεση αντίδραση μέσα σε 1 ώρα
2. **IT Forensics** → Ειδικοί εντοπίζουν τι έχει επηρεαστεί, πώς μπορεί να περιοριστεί η διαρροή και πώς να αποκατασταθεί η ζημιά
3. **Νομική Υποστήριξη και Δημόσιες Σχέσεις** → Ειδικοί αναλαμβάνουν να περιορίσουν την νομική έκθεση σε κίνδυνο και να προστατέψουν τη φήμη της εταιρίας
4. **Ενημερώσεις** → Κόστος ενημέρωσης όσων επηρεάστηκαν
5. **Πρόστιμα και Έρευνες** → προετοιμασία για έρευνες από αρχές και κάλυψη ασφαλίσιμων προστίμων
6. **Ευθύνες** → Έξοδα υπεράσπισης και αποζημιώσεις για διαρροή δεδομένων
7. **Εκβιασμός** → Διαπραγμάτευση και κάλυψη «λύτρων» εκβιασμού
8. **Διακοπή Εργασιών** → Αποζημίωση απώλειας κερδών / κόστους εργασίας

AIG

Complimentary Tools and Services

- **Employee Cybersecurity eLearning** – Available in 11 languages
- **Blacklist IP Blocking and Domain Protection** – Reduces the attack surface up to 90% ahead of the firewall
- **Infrastructure Vulnerability Scan** – Identification of high risk infrastructure vulnerabilities
- **Insurance Portfolio Diagnostic** – Cyber as a peril analysis against insurance portfolio
- **Cybersecurity Information Portal** – Online access to cybersecurity Information

AIG

AIG Risk Consulting Services

AIG's team of cyber risk consultants brings over 50 years combined experience in IT security to help our clients stay ahead of their cyber risk. Our team works directly with insureds to provide detailed, technical expertise and consulting services

through:

- **Cyber Defense Review**, designed to take a look at an insured's people, processes, and tools comprising their cybersecurity program and identify strengths and weaknesses.
- **Internet Facing System Examination**, designed to help insureds identify risks and exposures in their public facing infrastructure from an attacker's perspective.
- **Incident Simulation Workshop**, designed to help clients ensure their incident response plan will respond efficiently and help them better maximize their CyberEdge benefits.
- **Executive Threat Brief**, designed to help clients better understand the current security threat landscape specific to their industry and current methods attackers are using.
- **Cyber Engineering Study**, designed to look at an insured's people, processes, and tools that protect critical systems and industrial controls within their environment.

AIG

Preferred Vendor Partner Services

We have partnered with experts in cyber risk to bring our clients additional options to add to their line of defense. Available services include:

- **Dark Net Intelligence**, powered by K2-Intelligence, helps clients stay apprised of what the latest chatter is inside the dark net.
- **Cybersecurity Maturity Assessment**, powered by RSA, helps organisations assess their cybersecurity risk.
- **BitSight Security Ratings**, powered by BitSight Technologies, and Vendor Security Ratings, powered by SecurityScorecard, let companies measure and monitor their own network and those of their third-party vendors.
- **Security Awareness Training**, powered by Wombat Security, provides phishing training and simulations for an insured's employees.
- **Quantification Workshop and Insurance Portfolio**
- **Stress Test**, powered by AXIO, helps clients understand their cyber exposure in financial terms and subsequently, how a variety of representative cyber loss scenarios might be treated by the client's entire insurance portfolio.

AIG

Η σημασία της ασφάλισης

Τα προγράμματα που υπάρχουν στην αγορά προσφέρουν:

- Πρωτοποριακά εργαλεία προστασίας από ζημιές
- Ειδικούς συμβούλους διαχείρισης της κρίσης σε όλα τα επίπεδα
- Οικονομική αποζημίωση για μια σειρά από έξοδα και απαιτήσεις και
- Αποτελούν ένα πολύτιμο επιπλέον δίχτυ προστασίας ακόμα και για τα δυνατότερα συστήματα ασφαλείας.

AIG

Contact us today to take advantage our Complementary services and improve your organization's protection against a cyber attack:
www.aig.com/CyberRiskConsulting
and complete the contact form, or email us at **CyberRiskConsulting@aig.com**

Or visit : www.aig.com.gr/CyberEdge for more information

AIG