Πανεπιστήμιο Πειραιώς

Τμήμα: Ψηφιακών Συστημάτων

[Π.Μ.Σ. ΤΔΑΨΔ] – Κατ, ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

“ΑΣΦΑΛΙΣΗ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ”

Εμμανουήλ Καρτέρης

Α.Μ.: MTE1514

Διδάσκων:

Χρήστος Ξενάκης

Φεβρουάριος, 2018

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον Κ. Ξενάκη, τόσο γιατί μου συνέστησε το μεταπτυχιακό πρόγραμμα της Ασφάλειας Ψηφιακών Συστημάτων του Πανεπιστήμιου Πειραιώς, όσο και για την αμέριστη βοήθεια του κατά τη διάρκεια των σπουδών.

Επίσης θα ήθελα να ευχαριστήσω θερμά τη σύζυγο μου για την όλη υπομονή που έδειξε κατά τη διάρκεια των σπουδών και την πολύτιμη στήριξη της.

Μάνος Καρτέρης

Περίληψη

Αντικείμενο της παρούσας εργασίας υπήρξε η μελέτη για περιστατικά ασφαλείας από κυβερνο-επιθέσεις που έχει ως αποτέλεσμα την παραβίαση της ιδιωτικότητας των χρηστών και της ασφάλεια των συστημάτων και των εφαρμογών πάσης φύσεως Οργανισμών. Για τις ανάγκες της υλοποίησης της παρούσας βιβλιογραφικής μελέτης, πραγματοποιήθηκε εκτεταμένη έρευνα και σε βάθος αναζήτηση επιστημονικών δημοσιεύσεων. Συμπερασματικά διαπιστώθηκε ότι η ασφάλεια από των διαφόρων τύπων κυβερνο-επιθέσεων και επειδή μπορεί να επηρεάσει όλων των ειδών των χρηστών, από απλούς χρήστες μέχρι και μεγάλους οργανισμούς, θα γίνεται συνεχώς όλο και πιο απαραίτητη. Είναι ένας σχετικά καινούργιος κλάδος για τον ασφαλιστικό τομέα, ο οποίος τα τελευταία χρόνια παρουσιάζει πολύ μεγάλη αύξηση σε κύκλο εργασιών. Δεδομένο μάλιστα ότι ο αριθμός των επιθέσεων με την πάροδο του χρόνου γίνεται ολοένα και περισσότερος, η ύπαρξη ασφάλειας για τους οργανισμούς θα είναι ακόμα περισσότερο χρήσιμη έως και άκρως απαραίτητη.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Εισαγωγή

Στο σημερινό περίπλοκο και γεμάτο απειλές περιβάλλον το οποίο ζούμε, οι περισσότεροι οργανισμοί και επιχειρήσεις προσπαθούν να υλοποιήσουν συστηματικά και με επιτυχία ένα πλαίσιο για την ασφάλεια και την προστασία των πληροφοριών τους. Υπάρχει όμως ένας τεράστιος και πολύ μεγάλος κίνδυνος σε όλη αυτή την προσπάθεια και αυτό γιατί οι κίνδυνοι στο χώρο του διαδικτύου αυξάνονται συνεχώς και οι εγκληματίες στο χώρο του διαδικτύου συνεχώς εξελίσσονται. Η ψηφιακή επανάσταση, όπως έχει ονομαστεί η ραγδαία ανάπτυξη της τεχνολογίας τις τελευταίες δεκαετίες, έχει επηρεάσει όλες τις πτυχές της καθημερινότητας μας καθώς τόσο η τεχνολογία όσο και το ίντερνετ γενικότερα έχουν γίνει αναπόσπαστα κομμάτια της καθημερινότητας μας. Κατά συνέπεια λοιπόν, όλες οι κύριες και σημαντικές δραστηριότητες της καθημερινότητας ενός ανθρώπου είναι συνεχώς εκτεθειμένες στις συνεχώς αυξανόμενες απειλές και κινδύνους του κυβερνοχώρου.

Αυτό λοιπόν που θα πρέπει να αναρωτηθούν οι οργανισμοί είναι από που θα πρέπει να ξεκινήσουν ότι θα πρέπει να κάνουν για τη θωράκιση τους. Έχοντας να αντιμετωπίσουν ένα σύνθετο περιβάλλον γεμάτο σύνθετες απειλές και στην κορυφή όλων αυτών θα πρέπει ο οργανισμός παράλληλα να είναι πλήρως συμμορφωμένος και κανονιστικές ρυθμίσεις και νόμους καθώς και άλλες απαιτήσεις για να έχει σωστή ασφάλεια πληροφοριών.

Στις μέρες μας οι εταιρείες και οι οργανισμοί αποτελούν σημαντικούς στόχους για τους εγκληματίες του κυβερνοχώρου. Τα δεδομένα που κρατάνε στα συστήματα και την υποδομή τους είναι από σημαντικές ευαίσθητες πληροφορίες για τα υποκείμενα. Τέτοιου είδους δεμένα μπορεί να είναι κοινωνικής και οικονομικής φύσεως καθώς και δεδομένα υγείας.

Θεωρείται λοιπόν απαραίτητη η θωράκιση όλων των οργανισμών πέρα από τα κατάλληλα τεχνολογικά μέτρα ασφαλείας τα οποία θα πρέπει να έχουν και κάποιου είδους ασφαλιστική κάλυψη για την προστασία των δεδομένων τους από κυβερνο-επιθέσεις. Άλλωστε το κόστος σε περίπτωση που υπάρχει παραβίαση των δεδομένων ενός οργανισμού είναι πολύ μεγαλύτερο από τα ετήσια ασφάλιστρα που θα κληθεί να πληρώσει ο εκάστοτε οργανισμός σε περίπτωση που επιλέξει κάτι τέτοιο. Και πολλές φορές το κόστος που θα έχει ένας οργανισμός από πιθανό περιστατικό ασφαλείας μπορεί να είναι ανυπολόγιστο και θα εξαρτηθεί από το πόσο μπορεί να έχει πληγή η φήμη και το κύρος του οργανισμού.

Στη συνέχεια της εργασίας, θα δούμε αναλυτικά, τι εννοούμε με τον όρο cyber security insurance, τους τύπους και τις καλύψεις που προσφέρουν οι ασφαλιστικοί φορείς προς τις εταιρίες και στο τέλος θα δούμε γιατί είναι απαραίτητη μία τέτοιου είδους υπηρεσία για κάθε φύσης οργανισμό και εταιρεία.

1. Τι εννοούμε τον όρο Cyber Security Insurance

Όπως ακριβώς υπάρχουν εδώ και χρόνια γνωστά ασφαλιστικά προϊόντα, όπως τα ασφαλιστικά προγράμματα υγείας, για τα αυτοκίνητα, για τις οικίες των πολιτών ή για τις εγκαταστάσεις και τα γραφεία των επιχειρήσεων, έτσι και η ασφάλεια από κυβερνο-επιθέσεις είναι ένα ασφαλιστικό προϊόν.

Εδώ θα πρέπει να ξεκαθαρίσουμε δύο πολύ σημαντικές έννοιες, τι εννοούμε με τον όρο παραβίαση δεδομένων και τι απώλεια δεδομένων. Παράβαση συστημάτων είναι η μη εξουσιοδοτημένη πρόσβαση σε εταιρικά συστήματα η οποία συνοδεύτε από απώλεια δεδομένων που περιλαμβάνουν οικονομικά στοιχεία, δεδομένα υγείας καθώς και εταιρικά δεδομένα.

Το συγκεκριμένο ασφαλιστικό προϊόν αφορά κατά κύριο λόγο τις επιχειρήσεις και κατά συνέπεια τους εμπλεκόμενους χρήστες, από διαφόρων τύπων επιθέσεων και ρίσκων που προέρχονται από το χώρο του διαδικτύου και γενικότερα από ρίσκα και επιθέσεις που ως στόχο έχουν να προκαλέσουν ζημιά στις υποδομές τεχνολογίας ενός οργανισμού.

Ο όρος γενικά του Cyber Security Insurance χρησιμοποιείται συχνά για να περιγράψει μία μεγάλη γκάμα από καλύψεις, με τον ίδιο τρόπο που χρησιμοποιείται ο όρος κυβερνοχώρος, ο οποίος χρησιμοποιείται για να περιγράψει μια μεγάλη εμβέλεια εργαλείων σχετικών με την προστασία των δεδομένων και των πληροφοριών καθώς και αντίστοιχων υπηρεσιών.

Σήμερα η ασφάλεια από κυβερνο-επιθέσεις που παρέχουν οι ασφαλιστικές εταιρείες περιλαμβάνουν τα εξής χαρακτηριστικά:

- Κάλυψη διαχείρισης κρίσεων από την παραβίαση δεδομένων προσωπικού χαρακτήρα. Τέτοια θα μπορούσαν να ήταν έξοδα σχετικά με τη διαχείριση ενός περιστατικού, την έρευνα, την αποκατάσταση, την ενημέρωση των υποκειμένων των οποίων τα δεδομένα τους παραβιάστηκαν και εκτέθηκαν, νομικά κόστη και πρόστιμα που σχετίζονται με ποινές από ανεξάρτητες αρχές που σχετίζονται με την προστασία των προσωπικών δεδομένων.
- Κάλυψης αστικής ευθύνης πολυμέσων. Ζημιές τρίτων που καλύπτονται και μπορούν να περιλαμβάνουν παραβίαση πχ μίας ιστοσελίδας και παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας.
- Κάλυψη αστικής ευθύνης από εκβιασμούς. Αντικατοπτρίζει τις απώλειες που οφείλονται σε απειλές και εκβιασμούς που προέρχονται από τον κυβερνο-χώρο και την αντιμετώπιση αυτών.
- Ασφάλεια δικτύων. Ζημιές τρίτων που μπορεί να προέλθουν ως αποτέλεσμα της άρνησης πρόσβασης, των δαπανών

Η ασφάλεια από κυβερνο-επιθέσεις (cyber security insurance), καμιά φορά αναφέρεται και ως cyber liability ή data breach liability insurance. Και αυτό γιατί ουσιαστικά οι οργανισμοί μεταφέρουν την ευθύνη ή μέρος αυτής, από μια επίθεση στα προσωπικά δεδομένα που κρατάνε προς τους ασφαλιστικούς φορείς. Βέβαια δεν είναι τόσο απλή διαδικασία γιατί και οι ασφαλιστικοί φορείς θέτουν συγκεκριμένους περιορισμούς, κανόνες και έχουν συγκεκριμένες απαιτήσεις από τους οργανισμούς ως προς τα μέτρα ασφαλείας, για την προστασία των προσωπικών δεδομένων που κρατάει ο εκάστοτε οργανισμός.

1.1 Τι εννοούμε με τον όρο «Cyber Risk»

Ο όρος αυτός, ρίσκα που προέρχονται από το χώρο του διαδικτύου (cyber risk), χρησιμοποιείται όλο και περισσότερο σήμερα στο χώρο των επιχειρήσεων. Θεωρείται οποιοσδήποτε κίνδυνος ο οποίος προέρχεται από την χρήση της τεχνολογίας των πληροφοριών και των επικοινωνιών και υπονομεύει

τα τρία βασικά στοιχεία για την ορθή ποιότητα της πληροφορίας και των δεδομένων και των υπηρεσιών:

- Confidentiality (εμπιστευτικότητα)
- Integrity (ακρίβεια)
- Availability (διαθεσιμότητα)

Έχουν γίνει πολλές προσπάθειες για να οριστεί ο συγκεκριμένος όρος, αλλά ακόμα και μέχρι σήμερα θεωρείται μία αφηρημένη έννοια. Περιλαμβάνει όμως σίγουρα τους κινδύνους των επιχειρηματικών δραστηριοτήτων μέσα στον περιβάλλον του διαδικτύου και προέρχεται από τη χρήση και τη μετάδοση ηλεκτρονικών μέσων μέσα από το διαδίκτυο και τα τηλεπικοινωνιακά δίκτυα.

Στον παρακάτω πίνακα φαίνονται αναλυτικά οι κατηγορίες των Cyber Risks [1], [2]

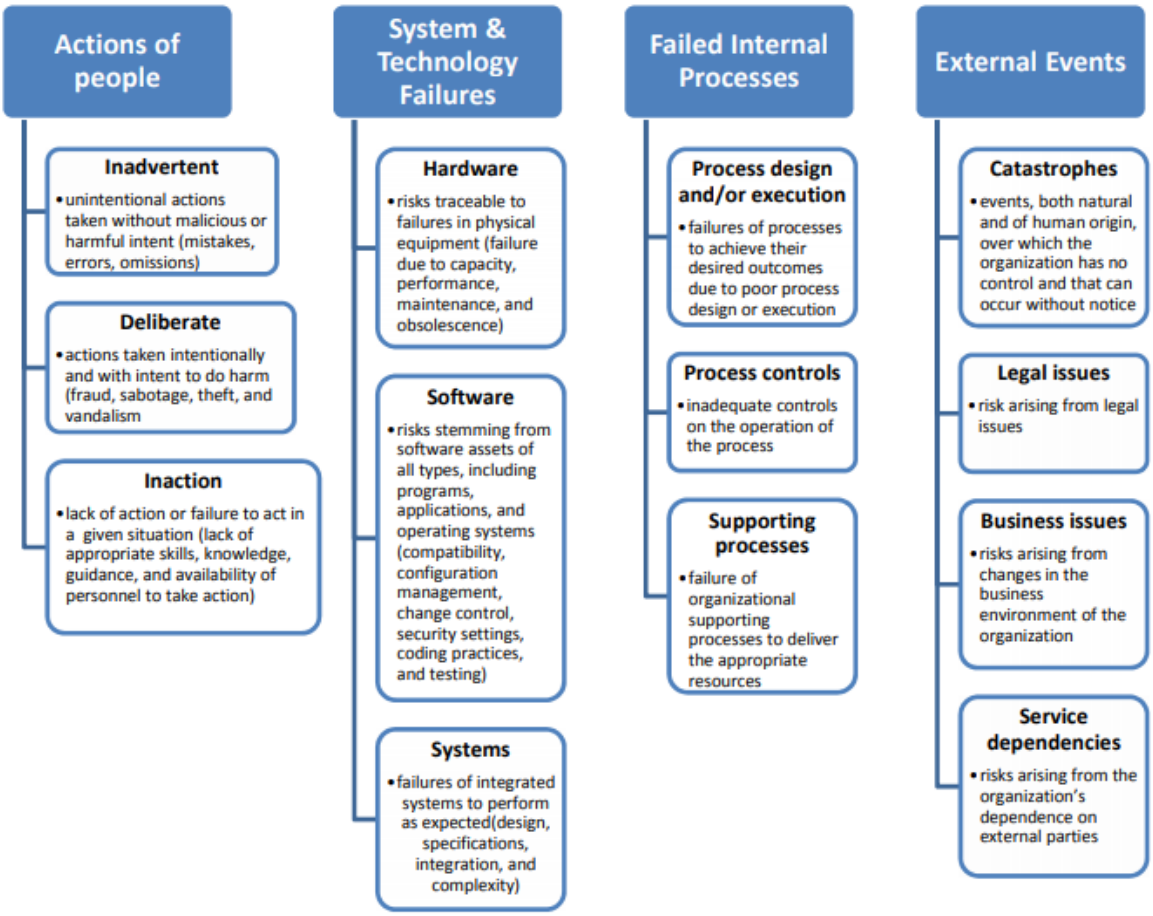

Figure 1 - Cyber Risks

1.2 Γιατί είναι σημαντικό να αποκτήσει ο οργανισμός Cyber Insurance

Τα δεδομένα είναι ένα πολύτιμο περιουσιακό στοιχείο της εταιρίας που δεν ασφαλίζεται από τα παραδοσιακά ασφαλιστήρια

Η ομαλή λειτουργία των συστημάτων μιας επιχείρησης είναι καθοριστική για την οικονομική ανάπτυξή της και το κόστος διακοπής λειτουργίας τους λόγω κυβερνοεπιθέσεων δεν καλύπτεται από τα παραδοσιακά ασφαλιστήρια.

Το κυβερνοέγκλημα είναι το πιο ταχύτατο αναπτυσσόμενο έγκλημα και οι συνέπειες του δεν καλύπτονται από τα παραδοσιακά ασφαλιστήρια.

Τα δεδομένα τρίτων που διατηρεί μια εταιρία λόγω της συνεργασίας της με άλλες εταιρίες είναι πολύτιμά και η απώλειά τους δημιουργεί ευθύνη για αυτή.

Οι εταιρίες που διενεργούν συναλλαγές με χρεωστικές και πιστωτικές κάρτες έχουν ποινές και διοικητικές κυρώσεις σε περίπτωση απώλειας των δεδομένων των κατόχων καρτών και από τις συμβαλλόμενες εταιρίες (VISA, Mastercard, American Express).

Η κανονιστική συμμόρφωση μιας εταιρίας με τους νόμους που διέπουν την συναλλαγή, επεξεργασία και διαχείριση δεδομένων απαιτούν χρόνο και χρήμα.

Η Φήμη μιας εταιρίας είναι το πολυτιμότερο περιουσιακό στοιχείο η ασφάλιση βοηθά στην αποτελεσματική διαχείριση της φήμης σε περίπτωση περιστατικών απώλειας δεδομένων.

Η χρήση των social media από το προσωπικό της εταιρίας δημιουργεί ευθύνη για αυτήν.

Οι φορητές συσκευές που χρησιμοποιούν τα στελέχη της εταιρείας αυξάνουν τον κίνδυνο απώλειας δεδομένων που σχετίζονται με την εταιρία και την πιθανότητα κλοπής τους.

Στόχοι κυβερνοεπιθέσεων δεν είναι αποτελούν μόνο οι μεγάλες εταιρίες.

1.3 Ποιος είναι ο κίνδυνος και στατιστικά στοιχεία

Σε όλο και μεγαλύτερο «πονοκέφαλο» δείχνουν να εξελίσσονται οι κυβερνοεπιθέσεις και οι ψηφιακές απειλές εν γένει για τις επιχειρήσεις διεθνώς, καθώς, σύμφωνα με την έρευνα «The Global State of Information Security Survey 2015» της RSA, για το 2014 η μέση συχνότητα ήταν 117.339 ημερησίως, με οικονομικές απώλειες ύψους 2,7 εκατ. δολαρίων- ποσό κατά 34% από το αντίστοιχο του 2013.

Όπως αναφέρεται σε σχετική ανάρτηση στην ιστοσελίδα του ΣΕΠΕ, σύμφωνα με την έρευνα οι επιθέσεις στις υποδομές IT ενός οργανισμού πληθαίνουν και μαζί τους αυξάνεται και η οικονομική ζημιά που τις συνοδεύει, με τις οικονομικές επιπτώσεις να είναι σημαντικές και να τείνουν να αποκτούν όλο και μεγαλύτερη έκταση.

Συνολικά, ο αριθμός των βεβαιωμένων επιθέσεων σε ολόκληρο τον κόσμο αυξήθηκε το 2014 κατά 48% στα 42,8 εκατομμύρια. Μάλιστα, το πρόβλημα βαίνει διογκούμενο, καθώς από το 2009 τα περιστατικά επιθέσεων αυξάνονται με ρυθμό 66% σε ετήσια βάση.

Η σχετική έκθεση, με τη συμβολή του Northeastern University, διερευνά τους λόγους για τους οποίους ο τομέας της ασφάλειας IT αποτυγχάνει να αντιμετωπίσει αποτελεσματικά τις σύγχρονες επιθέσεις στον κυβερνοχώρο. Δίνει επίσης συστάσεις σχετικά με το τι πρέπει να γίνει, για να ξεπεραστεί η αποτυχία του χώρου να αποτρέψει τις σύγχρονες απειλές.

Η έκθεση διαπιστώνει ότι η έλλειψη συναίσθησης κινδύνου αποτελεί ένα από τα πλέον τρωτά σημεία όσον αφορά την ασφάλεια του IT στις ΗΠΑ. Μάλιστα, τα ποσά που επενδύονται σε τεχνολογίες αποτροπής κυβερνο-επιθέσεων είναι δυσανάλογα υψηλά, σε σχέση με τις δαπάνες για την προμήθεια λύσεων οι οποίες μπορούν να ανιχνεύουν και να αντιμετωπίζουν τις επιθέσεις.

Επιπλέον, σύμφωνα με την έκθεση, η κατάσταση επιδεινώνεται και από ένα «έλλειμμα δεξιοτήτων». Σύμφωνα με τους συντάκτες της έκθεσης, όσοι οργανισμοί δεν διαθέτουν το κατάλληλο προσωπικό ή την εμπειρία να αντιμετωπίσουν τέτοιες καταστάσεις, θα πρέπει να εξετάσουν κατά πόσο χρειάζεται να ενισχύουν την εσωτερική ομάδα ασφάλειας IT, αγοράζοντας εξειδικευμένες cloud-based υπηρεσίες για την πληρέστερη προστασία των υποδομών τους.

Η έκθεση προτείνει ότι το ενδιαφέρον των επιχειρήσεων θα πρέπει, πλέον, να εστιάζεται όχι στο ποιες επιθέσεις εντοπίζονται ή στο πόσο επιτυχημένη είναι η προσπάθεια να αποτραπούν διάφοροι επίδοξοι εισβολείς, αλλά στο ποιοι κατάφεραν να ξεφύγουν, τι ενδέχεται να μην προστατεύεται επαρκώς και ποιες επιθέσεις, ίσως, να μην έχουν γίνει ακόμη γνωστές.

Επιπλέον, κάθε οργανισμός πρέπει να ορίζει τι είναι κρίσιμο για μια συγκεκριμένη λειτουργία (mission critical) και τι για το σύνολο της δραστηριότητας του (business-critical). Ποια επίθεση θα εμπόδιζε την επιχειρηματική εξέλιξη της εταιρείας στο μέλλον και ποια θα την οδηγούσε πολλά χρόνια πίσω ή και εκτός αγοράς.

Την ίδια στιγμή, όσοι ασχολούνται επαγγελματικά με την ασφάλεια του IT, θα πρέπει αρχικά να κατανοήσουν το είδος των αλλαγών, που έχουν συμβεί σε επίπεδο υποδομών - cloud, mobility, BYOD - και στη συνέχεια, να προετοιμάσουν το αμυντικό πλάνο και τις αντίστοιχες τακτικές για την εξουδετέρωση των νέων και εξελιγμένων απειλών. Τέλος, η έκθεση διαπιστώνει ότι δεν πρέπει να υπάρχουν «σκοτεινά» σημεία στις υποδομές IT, όπου θα μπορούσαν να κρυφτούν ή απ’ όπου θα μπορούσαν να διαφύγουν οι εισβολείς.

2. Ιστορική Αναδρομή και στοιχεία

Η εκτενής χρήση του διαδικτύου δημιούργησε καινούργιες επιχειρηματικές ευκαιρίες για όλους σχεδόν τους επιχειρηματικούς τομείς και αυτό κυρίως γιατί παρείχε τη δυνατότητα άμεσης και γρήγορης επικοινωνίας μεταξύ των επιχειρήσεων και του πελάτη. Επιπλέον ο κόσμους του διαδικτύου απλοποιεί σε πολύ μεγάλο βαθμό τις λειτουργικές διαδικασίες ενός οργανισμού και προσφέρει τη δυνατότητα να έχει πρόσβαση άμεσα και εύκολα σε καινούργιους επιχειρηματικούς τομείς με προϊόντα και υπηρεσίες χαμηλότερου κόστους. Παράλληλα όμως και λόγο της φύσης τους ο κυβερνοχώρος δημιουργεί πολύ σημαντικούς λειτουργικούς κινδύνους και εκτός από τα εκάστοτε μέτρα ασφαλείας όπως είναι οι νόμοι που διέπουν τον τεχνολογικό τομέα, οι πολιτικές ασφαλείας και οι βέλτιστες διαδικασίες, ένα νέο εργαλείο εμφανίζεται στα χέρια των ειδικών, η ασφάλεια από κυβερνο-επιθέσεις. Σε ολόκληρο πλέον τον κόσμο, οι οργανισμοί αρχίζουν σιγά σιγά να καταλαβαίνουν ότι οι επιθέσεις μέσω του διαδικτύου είναι καθημερινό φαινόμενο.

Στη συνέχεια θα δούμε την εξέλιξη του προϊόντος τις τελευταίες δεκαετίες.

2.1 Τέλη Δεκαετίας 90

Στα τέλη της δεκαετίας του 90 και με την τεχνολογική ανάπτυξη που γνώριζε τότε ο κόσμος, εμφανίστηκαν και τα πρώτα αντίστοιχα ρίσκα για τις επιχειρήσεις σχετικά με την τεχνολογία. Έτσι λοιπόν παρουσιάστηκε η ανάγκη αυτά τα ρίσκα να μετατεθούν, όπως ακριβώς συμβαίνει και τα υπόλοιπα πράγματα που καλύπτουν οι ασφάλειες των εταιρειών. Οδηγηθήκαμε λοιπόν στην παρουσίαση και την ανάπτυξη των πρώτων πολιτικών. Παράλληλα πολλές από τις τεχνολογικές εταιρίες άρχισαν να έχουν έκθεση σε ευαίσθητά δεδομένα. Γι' αυτό λοιπόν και οι πρώτες πολιτικές γράφτηκαν για να καταγράψουν αυτό το είδος περιεχομένου. Στη συνέχεια και με την πάροδο του χρόνου οι πολιτικές αυτές εξελίχθηκαν και εξελίσσονται συνεχώς.

Οι πρώτες πολιτικές που αφορούν τον τομέα του κυβερνοχώρου – ίντερνετ εμφανίστηκαν στα τέλη της δεκαετίας του 90. Κατά κύριο λόγο ήταν πολιτικές ασφαλείας που αφορούσαν τα μέσα και ξεκινούσαν να καλύπτουν μέσα που ήταν διαθέσιμα στο ίντερνετ και λάθη που συνέβεναν κατά την επεξεργασία των δεδομένων. Γενικά εξελίχθηκαν από τις πολιτικές επαγγελματικής ευθύνης για τους κινδύνους λογισμικού και μέσων.

2.2 Αρχές 2000

Ραγδαία ανάπτυξη παρουσιάστηκε στις αρχές του 2000 και αυτό σχετίζεται κατά κύριο λόγο με την ευρεία ανάπτυξη που παρουσίασε το ίντερνετ. Έτσι λοιπόν σε αυτήν την περίοδο οι νεότερες εκδόσεις των προϊόντων ασφαλείας από κυβερνο- επιθέσεις, άρχισαν να καλύπτουν διαφόρων ειδών περιστατικών επιθέσεων που εμφανίστηκαν στον ασφαλισμένο οργανισμό. Οι κύριες κατηγορίες που άρχισαν να καλύπτουν τα πρώτα ασφαλιστικά προϊόντα κυβερνο-επιθέσεων ήταν:

- Μη εξουσιοδοτημένη πρόσβαση
- Ασφάλεια δικτύων
- Επιθέσεις με Ιούς

Παράλληλα όμως υπήρχαν και πολύ βασικές και σημαντικές εξαιρέσεις όπως είναι:

- Προβλήματα και επιθέσεις μέσα από τον ίδιο τον οργανισμό, πχ κάποιος κακοήθης υπάλληλος
- Θέματα που αφορούσαν τους ισχύοντες τότε νόμους και κανονιστικές ρυθμίσεις
- Ποινές που θα μπορούσαν να επιβληθούν από ανεξάρτητες αρχές

Η βασικότερη όμως εξαίρεση είναι ότι οι πολιτικές εκείνη την εποχή δεν κάλυπταν απ' ευθείας τα βασικά στοιχεία ενός οργανισμού.

2.3 Μέσα Δεκαετίας 2000

Προς τα μέσα της δεκαετίας του 2000 υπήρχαν ραγδαίες εξελίξεις στον τομέα της ασφάλισης των οργανισμών από κυβερνο-επιθέσεις. Οι ασφαλιστικοί οργανισμοί, λόγω των αυξημένων αναγκών των πελατών τους άρχισαν να καλύπτουν τα πλέον βασικά στοιχεία ενός οργανισμού. Συγκεκριμένα αυτές οι καλύψεις περιλαμβάνουν:

- Διακοπή της Επιχειρηματικής συνέχειας ενός οργανισμού σε σχέση με το ίντερνετ
- Διάφορων ειδών εκβιασμών από τον κυβερνοχώρο
- Να προκληθεί ζημιά στα βασικά στοιχεία δικτύου ενός οργανισμού

Η μεγάλη όμως αλλαγή έγινε σε σχέση με τον ανεξάρτητο Αμερικάνικο οργανισμό HIPAA του Υπουργείου Υγείας των ΗΠΑ. Πιο συγκεκριμένα σε περίπτωση λάθους ενός λογισμικού θα μπορούσε ακόμα να γίνει υποβιβασμός του καλυπτόμενου ποσού. Δηλαδή ενώ η κάλυψη μας θα μπορούσε να είναι για παράδειγμα €1 εκατομμύριο, αν το πρόστιμο αφορούσε θέματα σε λάθος λογισμικού σχετικά με την υγεία και των προσωπικών δεδομένων, τότε θα η ασφαλιστική εταιρεία θα μα κάλυπτε πολύ μικρότερο ποσό.

2.4 Έτος 2003

Σημαντικές αλλαγές στον τομέα ασφαλειών από κυβερνο-επιθέσεις, έφερε και ο νόμος με την ονομασία «The California Security Breach and Information Act», ο οποίος τέθηκε σε ισχύ στις αρχές του 2003 (συγκεκριμένα 07/01/2003). Η δημοσίευση αυτού του νόμου έφερε σημαντικές αλλαγές σε θέματα έκθεσης προσωπικών δεδομένων και ασφάλειας. Πιο συγκεκριμένα ο νόμος απαιτούσε από τους οργανισμούς οι οποίοι διαχειρίζονται ευαίσθητα προσωπικά δεδομένα για διάφορα υποκείμενα, να ενημερώσουν τα συγκεκριμένα υποκείμενα άμεσα σε περίπτωση που η ασφάλεια των πληροφοριών αυτών είχε παραβιαστεί. Η δημοσίευση αυτού του νόμου στην Καλιφόρνια έφερε σαν αποτέλεσμα να υιοθετηθεί σταδιακά και από άλλες πολιτείες. Στον τομέα της ασφάλισης των επιχειρήσεων από κυβερνο-επιθέσεις, οι αλλαγές ήταν αρκετά μεγάλες και έφερε καινούριων ειδών καλύψεις, όπως Δημόσιες Σχέσεις, IT Forensics, ειδοποίηση πελατών. Η μεγαλύτερη αλλαγή όμως είναι ότι οι ασφαλιστικές εταιρείες εκείνη την εποχή άρχισαν να καλύπτουν και 3^{ων} μερών πρόστιμα και ποινές που θα μπορούσαν να προκληθούν από ανεξάρτητες ρυθμιστικές αρχές.

2.5 Τέλη Δεκαετίας 2000

Στα τέλη της δεκαετίας του 2000, οι περισσότερες από τις καλύψεις οι οποίες προσφέρονταν στην αγορά, ήταν διαθέσιμες από ένα μικρό αριθμό ασφαλιστικών εταιρειών. Καθώς η ραγδαία ανάπτυξη του διαδικτύου έφερνε παράλληλα συνεχώς καινούργιες απειλές-επιθέσεις για να ευαίσθητα προσωπικά δεδομένα που διατηρούν οι περισσότεροι οργανισμοί, οι ασφαλιστικοί φορείς δεν μπορούσαν να υπολογίσουν και να δώσουν την ανάλογη κάλυψη ανάλογα με τον τύπο επίθεσης που θα μπορούσε να υποστεί ένας οργανισμός.

2.6 Αρχές Δεκαετίας 2010

Το 2010 παρουσιάστηκε αύξηση των φορέων που προσέφεραν ασφαλιστικά πακέτα κάλυψης προς τους οργανισμούς. Παράλληλα αυξήθηκαν και οι αξιώσεις που είχαν οι εταιρείες απέναντι στους ασφαλιστικούς φορείς καθώς τα κρούσματα παραβίασης των δεδομένων των εταιρειών είχαν γίνει

καθημερινό φαινόμενο. Πολλές εταιρείες και μεγάλοι οργανισμοί από διαφορετικά είδη επιχειρήσεων άρχισαν να δέχονται καθημερινά επιθέσεις από το χώρο του διαδικτύου.

2.7 Σήμερα

Τα προϊόντα και οι υπηρεσίες συνεχώς εξελίσσονται. Οι ασφαλιστικοί φορείς πλέον χρησιμοποιούν την τεχνολογία σαν εργαλείο με σκοπό να αξιολογήσουν τον ενδιαφερόμενο για ασφάλιση οργανισμό και κυρίως εξελίσσονται γρήγορα ανταποκρινόμενοι στις αξιώσεις των πελατών τους. Οι ασφαλιστικές εταιρείες είναι πλέον σε θέση να αναλάβουν πολύ μεγαλύτερα ρίσκα βασιζόμενες πλέον στην εμπειρία τους και το μέγεθος τους.

Οι παρακάτω εικόνες παρουσιάζουν συνοπτικά την εξέλιξη του προϊόντος τόσο στην Αμερική όσο και σε Ευρωπαϊκό επίπεδο [3].

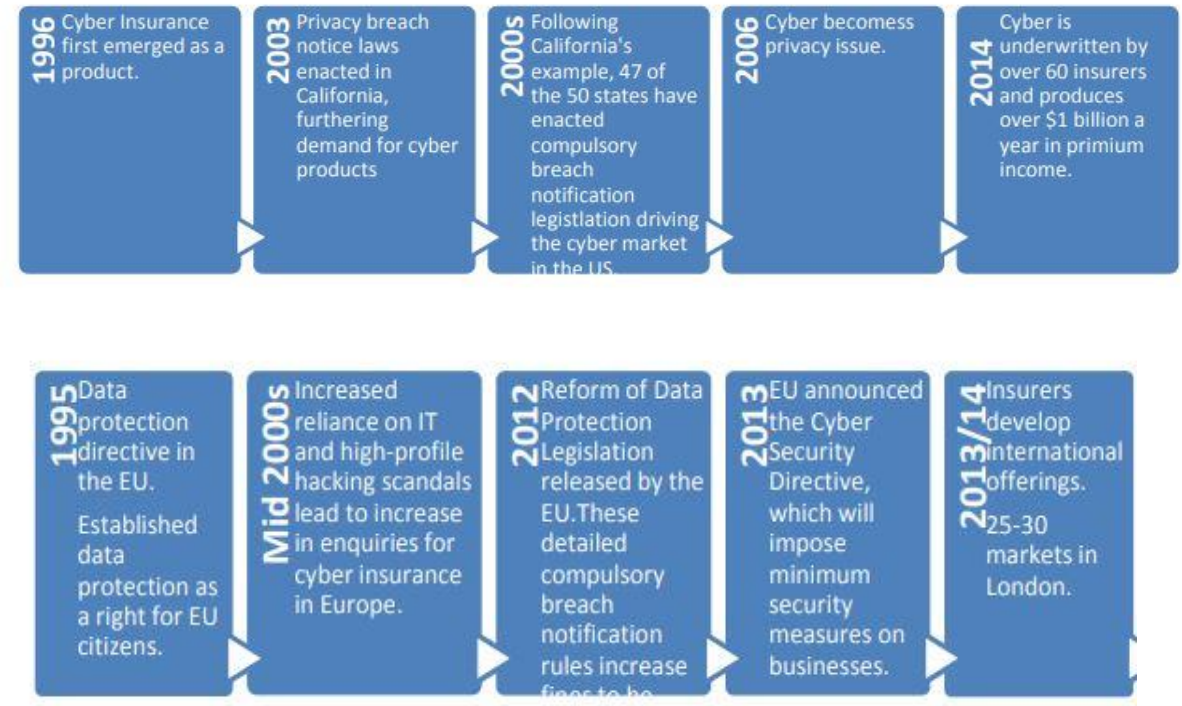

Figure 2 - Εξέλιξη Ασφαλιστικού Προϊόντος

Συμπερασματικά μπορούμε να πούμε ότι η ασφάλεια από κυβερνο-επιθέσεις ξεκίνησε σε πολύ περιορισμένη μορφή και σιγά σιγά αναπτύχθηκε έτσι ώστε σήμερα να καλύπτει τους περισσότερους από τους κινδύνους που προέρχονται από το χώρο του διαδικτύου. Σε σύγκριση με την ανάπτυξη στην πάροδο του χρόνου άλλων ασφαλιστικών προϊόντων, τα βήματα για την ασφάλιση από επιθέσεις από τον κυβερνοχώρο ήταν μικρά και αργά. Αρχικά οι ασφαλιστικοί φορείς άρχισαν να προσφέρουν ξεχωριστά καλύψεις ιδιοκτησίας και αστικής ευθύνης όσο αφορά την κάλυψη για κυβερνο-επιθέσεις, σε αντίθεση με τη σημερινή τάση να το προσφέρουν ως ανεξάρτητο προϊόν.

3. Κατηγορίες Cyber Security Insurance

Το ασφαλιστικό προϊόν για την κάλυψη των επιχειρήσεων από κυβερνο-επιθέσεις είναι ουσιαστικά ένα καινούργιο ασφαλιστικό προϊόν για τον ασφαλιστικό τομέα. Οι περισσότερες από τις καλύψεις είναι σε τόσο πρωταρχικό στδιο, ώστε οι όροι χρήσης να μην έχουν καθιερωθεί ακόμα σε τελειωτικό στάδιο. Και αυτό οφείλεται στο γεγονός ότι οι κίνδυνοι που αντιμετωπίζουν οι οργανισμοί από το χώρο του διαδικτύου είναι καινούργιοι. Είναι ένας καινούργιος τομέας στον ασφαλιστικό κλάδο που συνεχώς εξελίσσεται και γι' αυτό υπάρχει πρόβλημα για τον ακριβή καθορισμό των όρων μεταξύ επιχειρήσεων και ασφαλιστικών φορέων.

Με βάση όμως την κατάσταση που υπάρχει σήμερα και τις ανάγκες της αγοράς, υπάρχουν 3 βασικές κατηγορίες-τύποι:

- Cyber Security
- Cyber Liability
- Technology, Errors and Omissions

Οι δύο πρώτοι τύποι αφορούν κινδύνους που σχετίζονται με την παραβίαση δεδομένων. Ο τρίτος τύπος αφορά επιχειρήσεις που παρέχουν τεχνολογικές υπηρεσίες και προϊόντα. Στη συνέχεια θα παρουσιαστούν εκτενέστερα οι τύπου του Cyber Security Insurance.

3.1 Cyber Security

Είναι ο πιο διαδομένος όρος μέχρι και σήμερα και αναφέρεται σε πρώτου βαθμού καλύψεις προς την επιχείρηση. Το «ασφαλιστικό πακέτο» αυτό δεν προστατεύει τον οργανισμό από επιθέσεις που μπορεί να δεχθεί από τρίτους. Το Cyber Security Insurance ασχολείται ειδικά με το άμεσο κόστος απόκρισης όταν έχει υπάρξει παραβίαση των δεδομένων ενός οργανισμού. Σε πολλές περιπτώσεις αυτό απαιτείται και από την ίδια τη νομοθεσία. Υπάρχουν δηλαδή κανονισμοί, όπως ο Ευρωπαϊκός Κανονισμός Προστασία των Δεδομένων (GDPR – General Data Protection Regulation), ο οποίος ψηφίστηκε το 2016 και θα τεθεί σε ισχύ τον Μάιο του 2018. Ο κανονισμός ορίζει ρητά ότι αν υπάρξει παραβίαση δεδομένων προσωπικού χαρακτήρα σε έναν οργανισμό, τότε ο υπεύθυνος επεξεργασίας των δεδομένων πρέπει να γνωστοποιήσει εντός 72 ωρών από τη στιγμή που αποκτά γνώση για την παραβίαση στην εποπτική αρχή. Παράλληλα όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων των οποίων τα δεδομένα τους παραβιάστηκαν, ο υπεύθυνος επεξεργασίας οφείλει επίσης να ενημερώσει τα ίδια τα υποκείμενα των προσωπικών δεδομένων αυτών.

Μερικά παραδείγματα καλύψεων τα οποία περιλαμβάνει το Cyber Security είναι τα παρακάτω:

- Πρόσληψη ενός ειδικού (forensics expert) ο οποίος θα διερευνήσει την αιτία της παραβίασης και θα προτείνει τα ανάλογα μέτρα ώστε να αποφευχθεί στο μέλλον παρόμοιο συμβάν.
- Πρόσληψη ενός ανεξάρτητου πράκτορα δημοσίων σχέσεων για να βοηθήσει στην αντιμετώπιση της κρίσης και τη διαχείριση ενός συμβάντος παραβίασης δεδομένων.
- Δημιουργία ενός τηλεφωνικού κέντρου μετά την παραβίαση στα δεδομένα του οργανισμού με σκοπό να διαχειριστεί τις κλήσεις και τα παράπονα των πελατών.
- Ειδοποίηση όλων των εμπλεκομένων των οποίων τα ευαίσθητα προσωπικά τους δεδομένα εκτέθηκαν από το συμβάν.
- Να παρακολουθούν τη διάθεση που δείχνουν τα υποκείμενα των οποίων τα δεδομένα παραβιάστηκαν (η συνήθης διάρκεια είναι για ένα χρόνο).

- Να πληρώσει η ασφαλιστική το κόστος της επανάκτησης όλων των δεδομένων τα οποία κλάπηκαν από τον οργανισμό (πχ το κόστος για την ενημέρωση των τραπεζών και των εταιρειών που εκδίδουν πιστωτικές κάρτες).

3.2 Cyber Liability Insurance

Η ασφάλεια αστικής ευθύνης (Cyber Liability Insurance), είναι γνωστή και σαν ασφάλεια προστασίας προσωπικών δεδομένων και ιδιωτικότητας (Information Security and Privacy). Με αυτού το είδος ασφάλειας καλύπτεται η ευθύνη του ασφαλιζόμενου οργανισμού σε περίπτωση που έχουμε παραβίαση δεδομένων και δεν καλύπτει έξοδα που αφορούν το άμεσο κόστος απόκρισης από ένα περιστατικό ασφαλείας.

Το συγκεκριμένο προϊόν αφορά κατά κύριο λόγο εταιρίες και οργανισμούς οι οποίοι πουλούν υπηρεσίες και αγαθά μέσω του διαδικτύου. Ένας τέτοιου είδους οργανισμός έχεις στην κατοχή και στα συστήματα του πολύ σημαντικά και ευαίσθητα προσωπικά δεδομένα των πελατών του. Τέτοια στοιχεία μπορεί να είναι αυστηρά προσωπικά, όπως είναι η διεύθυνση κατοικίας, είτε οικονομική φύσεως, όπως είναι αριθμοί λογαριασμών τραπέζης και αριθμοί πιστωτικών καρτών, αριθμοί κοινωνικής ασφάλισης. Οι κίνδυνοι λοιπόν για έναν τέτοιο οργανισμοί είναι πολλοί και ένας τέτοιος οργανισμός θα πρέπει να έχει λάβει όλα εκείνα τα απαραίτητα μέτρα για την προστασία όλων αυτών των σημαντικών και ευαίσθητων προσωπικών δεδομένων.

Ένα τέτοιου είδους λοιπόν ασφαλιστικό πακέτο καλύπτει τα εξής:

- Κλοπή ενός laptop ενός εργαζομένου (πχ από διάρρηξη του αυτοκινήτου του).
- Περίπτωση που ένα email με ευαίσθητα δεδομένα αποσταλεί σε λάθος παραλήπτη.
- Σημαντικά έγραφα να κλαπούν από τις εγκαταστάσεις του οργανισμού σε περίπτωση διάρρηξης.
- Να κλείσει επιτυχώς ένα περιστατικό ασφαλείας σε εύλογο χρονικό διάστημα.

3.3 Technology Errors and Omissions

Η συγκεκριμένη ασφαλιστική κατηγορία αναφέρεται αλλιώς και ως Επαγγελματική Ευθύνη (Professional Liability) ή σε συντομογραφία E&O. Είναι μία μορφή κάλυψης ευθύνης που προστατεύει τις επιχειρήσεις οι οποίες παρέχουν ή πωλούν τεχνολογικές υπηρεσίες και προϊόντα. Με τις καλύψεις της συγκεκριμένης κατηγορίας αποτρέπει τις επιχειρήσεις να φέρουν το πλήρες κόστος από μία αμέλεια που μπορεί να υποβληθεί από έναν πελάτη και τις αποζημιώσεις που θα πρέπει να δοθούν σε περίπτωση πολιτικής αγωγής. Επίσης μπορεί να καλύπτει διαφημιστικές εταιρείες οι οποίες μπορεί να δημιουργήσουν ψηφιακό περιεχόμενο το οποίοι μπορεί να βλάψει έναν οργανισμό. Παράλληλα μπορεί να καλύψει και προγραμματιστές οι οποίοι μπορεί να έχουν δημιουργήσει έναν κώδικα και να έχει κάποιο λάθος.

Γενικότερα τέτοιου είδους εταιρείες θα πρέπει να σκεφτούν πολύ καλά τι μπορεί να γίνει σε περίπτωση οποιουδήποτε λάθος που μπορεί να υπάρξει στις υπηρεσίες που προσφέρουν προς τους πελάτες τους. Για παράδειγμα:

- Τι θα συμβεί σε περίπτωση που ένα λάθος στο λογισμικό τους (software glitch), οδηγήσει στο να χάσει ο πελάτης τους πολύ σημαντικά δεδομένα.
- Τι θα συμβεί αν μία ανεπαρκής εγκατάσταση του προγράμματος τους (flawed program installation) αποτρέψει τον τελικό τους πελάτη στο να παραλάβει μία παραγγελία του.
- Τι θα συμβεί αν ένα λάθος στον κώδικα οδηγήσει τον χρήστη στο να μην μπορεί να κάνει μία κράτηση μέσω του διαδικτύου.

3.4 Παράδειγμα πως δρα μια ασφαλιστική σε περίπτωση περιστατικού

Οι ειδικοί στη διαχείριση απαιτήσεων ενός ασφαλιστικού φορέα προσφέρουν πολύτιμη βοήθεια προς το τμήμα IT του οργανισμού που δέχθηκε την επίθεση. Αποτελεί ουσιαστικά ένα 2ο επίπεδο άμυνας για τον ίδιο τον οργανισμό.

Συνοπτικά στον παρακάτω πίνακα φαίνεται πως δρα ένας ασφαλιστικός φορέας στην περίπτωση που ασφαλιζόμενος οργανισμός δεχθεί κάποια παραβίαση στα δεδομένα του.

Περιεχόμενο Παραβίασης	**Αντιμετώπιση**
Παραβίαση	Άμεση απόκριση από ειδικό σύμβουλο για τις παραβιάσεις
Εγκληματολόγοι	Εντοπισμός των στοιχείων που έχουν παραβιαστεί, πως μπορεί να γίνει ο περιορισμός τους και προσπάθεια αποκατάστασης
Νομικοί σύμβουλοι κα Σύμβουλοι δημοσίων σχέσεων	Προσπάθεια για την αντιμετώπιση της δυσφήμισης
Κοινοποίηση	Κόστος ενημέρωσης των υποκειμένων των οποίων τα προσωπικά δεδομένα παραβιάστηκαν
Πρόστιμα και έρευνα	Προετοιμασία για έρευνα και αντιμετώπιση ποινών από τις αρμόδιες αρχές.
Αστική Ευθύνη	Κόστος υπεράσπισης για ζημιές (παραβίαση δεδομένων, επηρεασμός αξιοπιστίας τους, κλοπή κωδικών)

4. Επισκόπηση της αγοράς

Παρόλο που τα περιστατικά ασφαλείας που προέχονται από τον κυβερνοχώρο έχουν γίνει μία καθημερινή και τρομακτική καθημερινότητα για τις επιχειρήσεις η αγορά παραμένει μικρή τόσο την Ευρωπαϊκή Ένωση όσο και στο Ηνωμένο Βασίλειο με μικρές διαφοροποιήσεις μεταξύ τους και συνδέονται στενά με τη νομοθεσία για την ασφάλεια στον κυβερνοχώρο. Είναι προφανές ότι περιοχές με καλά δομημένη και καθιερωμένη νομοθεσία μέσα στο πέρασμα του χρόνου έχουν υιοθετήσει πολύ περισσότερο την ασφάλιση από κυβερνο-επιθέσεις. Αντίθετα σε περιοχές με μη καθιερωμένη νομοθεσία υπάρχει πολύ περιορισμένη καθιέρωση και αποδοχή για την ασφάλιση από κυβερνο-επιθέσεις.

Η έγκριση και η επιβολή (Μάιος 2018) του καινούργιου Ευρωπαϊκού Νόμου για την προστασία των προσωπικών δεδομένων GDPR (General Data Protection Regulation), θα φέρει μεγάλη ανάπτυξη και επιτάχυνση για την παγκόσμια αγορά της ασφάλισης από κυβερνο-επιθέσεις και κυρίως στην Ευρώπη. Ακόμα όμως σε σχέση με άλλες ασφαλιστικές κατηγορίες και καλύψεις, μπορούμε να πούμε ότι ο συγκεκριμένος τομέας είναι σε πολύ πρωταρχικό στάδιο.

Ωστόσο, καθώς η αγορά για τον τομέα ασφαλίσεων από κυβερνο-επιθέσεις συνεχώς αναπτύσσεται, το φάσμα καλύψεων θα αυξηθεί. Μέχρι στιγμής όμως και επειδή τα ρίσκα που προέρχονται από το χώρο του διαδικτύου δεν μας είναι 100% γνωστά, τα ασφαλιστικά προϊόντα δεν προωθούνται και διαφημίζονται αναλόγως. Ως εκ τούτου προκύπτει ότι και το μεγαλύτερο ποσοστό των εταιρειών ακόμα και μέχρι σήμερα δεν γνωρίζουν καν της ύπαρξη αυτού του είδους των καλύψεων.

4.1 Τι κοιτάνε οι εταιρείες

Πρωταρχικό βήμα για τις εταιρείες, πριν την υπογραφή των συμβολαίων είναι να γίνουν αρχικά προκαταρκτικές αξιολογήσεις και συνεντεύξεις μεταξύ του ασφαλιστικού φορέα και του οργανισμού που θέλει να ασφαλιστεί. Σε όλη αυτή τη διαδικασία θεωρείται απαραίτητη η απόλυτη συνεργασία και ειλικρίνεια του οργανισμού που θέλει να ασφαλιστεί για όλα τα περιουσιακά του στοιχεία και τα μέτρα ασφαλείας που έχουν παρθεί για την προστασία τους και σε περίπτωση παραβίασης ποια από αυτά επηρεάστηκαν. Παρακάτω παρατίθεται ένα τυπικό τέτοιο ερωτηματολόγιο [4].

Management of privacy exposures

1. Does the Applicant have a written corporate-wide privacy policy? ☐ Yes ☐ No

2. Does the Applicant accept credit cards for goods sold or services rendered? If yes: ☐ Yes ☐ No

   A. Please state the Applicant's approximate percentage of revenues from credit card transactions in the most recent twelve (12) months:____%

   B. If the Applicant accepts credit cards for payment of goods and services, is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)? ☐ Yes ☐ No
   If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:_____

3. Does the Applicant employ a chief privacy officer? If no, what position is responsible for management of, and compliance with Applicant's privacy policies? _____ ☐ Yes ☐ No

4. Within the past two years, has the Applicant undertaken any internal or external privacy or received any privacy certification? If yes, please describe: ☐ Yes ☐ No
   _____

5. Does the Applicant restrict employee access to personally identifiable on a business-need to know basis? ☐ Yes ☐ No

6. Does the Applicant require third parties with which it shares personally identifiable information or confidential information to indemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? ☐ Yes ☐ No

7. Is the Applicant aware of any release, loss or disclosure of personally identifiable information in its care, custody or control, or anyone holding such information on behalf of the Applicant in the most recent three year time period from the of this Application? ☐ Yes ☐ No
   If yes, describe any such release, loss or disclosure:
   _____

Computer Systems Controls

1. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees? ☐ Yes ☐ No

2. Does the Applicant require positive acknowledgement from each employee of their understanding in security issues and agreement with the above policies and procedures?	☐ Yes	☐ No
3. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems? If yes, indicate the frequency of such training:_____	☐ Yes	☐ No
4. Does the Applicant have	☐ Yes	☐ No
a. Disaster Recovery Plan?		
b. Business Continuity Plan?	☐ Yes	☐ No
c. Incident Response Plan for network intrusions and virus incidents?	☐ Yes	☐ No
How often are such plans tested? _____		
5. Does the Applicant have a program in place to periodically test or audit security controls? If yes, please summarize the scope of such audits and/or tests: _____	☐ Yes	☐ No
6. Does the Applicant terminate all the associated computer access and user accounts as part of the regular exit process when an employee leaves the company?	☐ Yes	☐ No
7. Does the Applicant use commercially available firewall protection systems to prevent unauthorized access to internal networks and computer systems?	☐ Yes	☐ No
8. Does the Applicant use intrusion detection software to detect unauthorized access to internal networks and computer systems?	☐ Yes	☐ No
9. Does the Applicant utilize Anti-Virus software? If yes, is how often are virus signatures updated? _____	☐ Yes	☐ No
10. Does the Applicant outsource any of its computer or network system operations or security? If yes: a. Please identify the operations outsourced and vendors:_____	☐ Yes	☐ No
b. Does the Applicant require such vendors to demonstrate adequate security policies and procedures?	☐ Yes	☐ No
11. Is all valuable/sensitive data backed-up by the Applicant on a daily basis? If no, please describe exceptions: _____	☐ Yes	☐ No
12. Is at least one complete back-up file generation stores and secured off-site separate from the Applicant's main operations in a restricted area? If no, describe the procedure used by the Applicant, if any, to store or secure copies of	☐ Yes	☐ No

valuable/sensitive data off-site? _____

13. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted? ☐ Yes ☐ No

    Are all laptop computers and portable media (e.g."thumb drives") protected by encryption? ☐ Yes ☐ No

    Does the Applicant encrypt data "at rest" within computer database? ☐ Yes ☐ No

14. Does the Applicant enforce a software update process including installation of software "patches"? ☐ Yes ☐ No

    If yes, are critical patches installed within 30 days of release? ☐ Yes ☐ No

15. Has the Applicant suffered any known intrusions (i.e., unauthorized access or security breaches) or denial of service attacks relating to its computer systems in the most recent three year time period from the date of this Application? ☐ Yes ☐ No

    If yes, describe any such intrusions or attacks, including any damage caused by any such intrusions, including lost time, lost business income, or costs to repair any damage to systems or to reconstruct data or software, describe the damage that occurred and state value of any lost time, income and the costs of any repair or reconstruction:

    _____

Content exposures

1. Does the Applicant have a procedure for responding to allegations that content created, displayed or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights? ☐ Yes ☐ No

2. Does the Applicant have a qualified attorney review all content prior to posting on the Insured's Internet site? ☐ Yes ☐ No

    If yes, does the review include screening the content for the following :

    Copyright infringement? ☐ Yes ☐ No

    Trademark infringement? ☐ Yes ☐ No

    Invasion of privacy? ☐ Yes ☐ No

    Disparagement Issues? ☐ Yes ☐ No

    If no, please describe procedures to avoid the posting of improper or infringing content:

    _____

3. Within the last 3 years, has the Applicant ever received a complaint or cease and desist ☐ Yes ☐ No

demand alleging trademark, copyright, invasion of privacy, or defamation with regard to any content published, displayed or distributed by or on behalf of the Applicant?
If yes, provide details regarding any such demands:

_____

Prior claims and circumstances

1. Has the Applicant ever received any claims or complaints with respect to allegations of invasion of or injury to privacy, identity theft, theft of information, breach of information security, software copyright infringement or content infringement or been required to provide notification to individuals due to an actual or respected disclosure of personal information? ☐ Yes ☐ No
   If yes, provide details of each such claim, allegation or incident, including costs, losses or damages incurred or paid and any amounts paid as a loss under any insurance policy:

   _____

2. Has the Applicant been subject to any government action or investigation regarding alleged violation of any privacy law or regulation? ☐ Yes ☐ No
   If yes, please provide details of any such action or investigation: _____

3. Has the applicant ever experienced an extortion attempt or demand with respect to its computer systems? ☐ Yes ☐ No
   If yes, please provide details: _____

4. Has the Applicant notified consumers of data breach incident in accordance with a data breach notification law in the past three (3) years? ☐ Yes ☐ No

5. No Applicant, director, officer, employee or other proposed insured has knowledge or information of any fact, circumstance, situation, event or transaction which may give rise to a claim under the proposed insurance except as follows: _____ ☐ None
   If no such knowledge or information, check here:

Prior insurance

1. Does the Applicant currently have insurance in place covering media, privacy or network security exposures? ☐ Yes ☐ No

2. Has any professional liability, privacy, network security or media insurance ever been declined or cancelled? ☐ Yes ☐ No
   If yes, please explain: _____

Figure 3 - Ερωτηματολόγιο

Παρακάτω θα παρουσιάσουμε και ένα ακόμα τυπικό ερωτηματολόγιο [5].

AIG Europe Limited
Υποκατάστημα Ελλάδας
Λεωφ. Κηφισίας 119, 15124 Μαρούσι, Τηλ.: 210 8127.600, Fax: 210-8027.189 e-mail: FLGreece@aig.com
ΥΠ/ΜΑ ΘΕΣ/ΝΙΚΗΣ: Μαρίνου Αντύπα 42, 57001,Πυλαία Θεσσαλονίκης, 57001, Τηλ.: 2310-474999 Fax: 2310-494990
ΝΟΜΙΜΟΣ ΑΝΤΙΠΡΟΣΩΠΟΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ: AIG ΕΛΛΑΣ Α.Ε. ΑΝΤΙΠΡΟΣΩΠΕΥΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ
Α.Φ.Μ.: 997472444, Δ.Ο.Υ ΦΑΕ Αθηνών, Αρ. Μητρ.Γ.Ε.ΜΗ.: 118328300001 URL: http://www.aig.com.gr

CyberEdge

Αίτηση Ασφάλισης

Ασφαλιστικό Πρακτορείο-Κωδικός:_____

1. Πληροφορίες για το Λήπτη της Ασφάλισης

(για τους σκοπούς της ασφάλισης ο Λήπτης της Ασφάλισης και οποιαδήποτε θυγατρική του είναι η εταιρία)

Επωνυμία Λήπτη της Ασφάλισης :	
Α.Φ.Μ.:	**Δ.Ο.Υ.:**
Διεύθυνση έδρας:	
Τηλέφωνο :	**Ιστοσελίδα:**
Έτος ίδρυσης της εταιρίας:	
Περιγραφή εργασιών:	
Κύκλος εργασιών εταιρίας :	**Οικονομικό έτος:**

2. Πληροφορίες για το CyberEdge

Το CyberEdge παρέχει προστασία από τις συνέπειες των ηλεκτρονικών και διαδικτυακών κινδύνων. Έχοντας πρόσβαση σε ανεξάρτητους ειδικούς, συνδυάζει την ασφαλιστική προστασία με τα εργαλεία διαχείρισης κινδύνου. Βοηθάει τις επιχειρήσεις να προστατευτούν ενάντια στις παραβιάσεις ευαίσθητων δεδομένων, τις ηλεκτρονικές παρακολουθήσεις, την απόσπαση και υποκλοπή πληροφοριών, τους ηλεκτρονικούς ιούς, τη δολιοφθορά και τα σφάλματα των εργαζόμενων.

Καλύψεις **(δείτε αναλυτικά τα επιμέρους όρια και τις απαλλαγές στη σελίδα 7-'Έντυπο προσφοράς)**	
Α. Διαχείριση γεγονότων	Α.1 Πρώτη Αντίδραση Α.2 Νομικές Υπηρεσίες Α.3 Υπηρεσίες ΙΤ Α.4 Επαναφορά Δεδομένων Α.5 Προστασία της Φήμης Α.6 Έξοδα Γνωστοποίησης Α.7 Παρακολούθηση Πίστωσης και Ταυτότητας

AIG Europe Limited
Υποκατάστημα Ελλάδας
Λεωφ. Κηφισίας 119, 15124 Μαρούσι, Τηλ.: 210 8127.600, Fax: 210-8027.189 e-mail: FLGreece@aig.com
ΥΠ/ΜΑ ΘΕΣ/ΝΙΚΗΣ: Μαρίνου Αντύπα 42, 57001,Πυλαία Θεσσαλονίκης, 57001, Τηλ.: 2310-474999 Fax: 2310-494990
ΝΟΜΙΜΟΣ ΑΝΤΙΠΡΟΣΩΠΟΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ: AIG ΕΛΛΑΣ Α.Ε. ΑΝΤΙΠΡΟΣΩΠΕΥΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ
Α.Φ.Μ.: 997472444, Δ.Ο.Υ ΦΑΕ Αθηνών, Αρ. Μητρ.Γ.Ε.ΜΗ.: 118328300001 URL: http://www.aig.com.gr

Β. Υποχρεώσεις Προστασίας Προσωπικών Δεδομένων	Β.1 Έρευνα Προστασίας Δεδομένων Β.2 Πρόστιμα Προστασίας Προσωπικών Δεδομένων
Γ. Ευθύνη	Γ.1 Προσωπικές και Εταιρικές Πληροφορίες Γ.2 Αστοχία Ασφάλειας Γ.3 Παράλειψη Γνωστοποίησης Γ.4 Κάτοχος των Πληροφοριών
Δ. Κάλυψη Ψηφιακών Μέσων	
Ε. Κάλυψη Διακοπής Λειτουργίας Δικτύου	Ε.1 Ζημία Διακοπής Λειτουργίας Δικτύου Ε.2 Έξοδα Διακοπής Λειτουργίας Δικτύου και Μετριασμού
ΣΤ.Κάλυψη Εκβιασμού Αποκάλυψης Προσωπικών Δεδομένων στον Κυβερνοχώρο	

3. Πίνακας ασφαλίστρων*

(παρακαλούμε σημειώστε το ασφάλιστρο βάση του κύκλου εργασιών της εταιρίας για την τελευταία οικονομική χρήση και του ορίου ευθύνης που επιθυμείτε)

Όριο ευθύνης (αθροιστικά και ανά γεγονός	Ετήσιος κύκλος εργασιών				
	Έως €1.000.000	€ 1.000.001 – € 5.000.000	€ 5.000.001 – € 10.000.000	€ 10.000.001 – € 25.000.000	Γενική Απαλλαγή (ανά γεγονός)
€ 100.000	☐ €580	☐ €1.100	-	-	€ 2.500
€ 250.000	☐ €950	☐ €1.500	☐ €2.180	☐ €3.050	€ 5.000
€ 500.000	☐ €1.380	☐ €1.950	☐ €2.550	☐ €3.550	€ 5.000
€ 1.000.000	☐ €2.110	☐ €2.850	☐ €3.420	☐ €4.650	€ 5.000
€ 2.000.000	-	☐ €4.220	☐ €4.800	☐ €6.320	€ 7.500
€ 3.000.000	-		☐ €6.040	☐ €7.560	€ 7.500

**Σημείωση:*
Τα παραπάνω ασφάλιστρα είναι τελικά, συμπεριλαμβανομένων φόρων και λοιπών επιβαρύνσεων. Εάν επιθυμείτε όριο ευθύνης μεγαλύτερο από € 3.000.000 ή εάν ο κύκλος εργασιών της εταιρίας είναι μεγαλύτερος από € 25.000.000 επικοινωνήστε με την AIG προκειμένου να εξεταστεί η δυνατότητα έκδοσης ειδικής προσφοράς.

➢ Είναι το αντικείμενο της εταιρίας σχετικό με την υγεία, τις τηλεπικοινωνίες, τις τηλεφωνικές πωλήσεις, τις διαδικτυακές πωλήσεις (e-shop), την επεξεργασία δεδομένων για λογαριασμό τρίτων (Data Processor-outsourcer) ή είναι η εταιρία Call Center ή διενεργεί η εταιρία πάνω από 70.000 συναλλαγές με κάρτες (πιστωτικές, χρεωστικές) το χρόνο;

☐ ΝΑΙ ☐ ΟΧΙ

Εάν ΝΑΙ τα ασφάλιστρα του Πίνακα Ασφαλίστρων θα αυξηθούν κατά 15%.

AIG Europe Limited
Υποκατάστημα Ελλάδας
Λεωφ. Κηφισίας 119, 15124 Μαρούσι, Τηλ.: 210 8127.600, Fax: 210-8027.189 e-mail: FLGreece@aig.com
ΥΠ/ΜΑ ΘΕΣ/ΝΙΚΗΣ: Μαρίνου Αντύπα 42, 57001,Πυλαία Θεσσαλονίκης, 57001, Τηλ.: 2310-474999 Fax: 2310-494990
ΝΟΜΙΜΟΣ ΑΝΤΙΠΡΟΣΩΠΟΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ: AIG ΕΛΛΑΣ Α.Ε. ΑΝΤΙΠΡΟΣΩΠΕΥΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ
Α.Φ.Μ.: 997472444, Δ.Ο.Υ ΦΑΕ Αθηνών, Αρ. Μητρ.Γ.Ε.ΜΗ.: 118328300001 URL: http://www.aig.com.gr

4. Συνολικό ασφάλιστρο/ Έναρξη ασφάλισης

➢ Το συνολικό ασφάλιστρο θα είναι το ασφάλιστρο του Πίνακα Ασφαλίστρων, αυξημένο κατά 15% σε περίπτωση που το αντικείμενο της εταιρίας είναι σχετικό με την υγεία, τις τηλεπικοινωνίες, τις τηλεφωνικές πωλήσεις, τις ηλεκτρονικές πωλήσεις (e-shop), την επεξεργασία δεδομένων για λογαριασμό τρίτων (Data Processor-outsourcer) ή εάν η εταιρία είναι Call Center ή εάν η εταιρία διενεργεί πάνω από 70.000 συναλλαγές με κάρτες (πιστωτικές, χρεωστικές) το χρόνο.

Αναγράψτε το συνολικό ασφάλιστρο: €……..

➢ Τρόπος πληρωμής: Εφάπαξ ☐ Δύο δόσεις ☐

➢ Ημερομηνία Έναρξης Ασφάλισης : ……
(Η ημερομηνία έναρξης της ασφάλισης μπορεί να είναι από την ημερομηνία αποστολής της παρούσας αίτησης ασφάλισης στην AIG έως και 15 ημέρες μεταγενέστερα.)

5. Προϋποθέσεις ισχύος του προγράμματος

➢ **Παρακαλούμε επιβεβαιώστε ότι η Εταιρία :**

- έχει έδρα στην Ελλάδα (ανεξάρτητα από την ύπαρξη θυγατρικών εταιριών σε άλλες χώρες)
- δε διατηρεί θυγατρική εταιρία στη Βόρεια Αμερική (Η.Π.Α, Καναδάς)
- λειτουργεί συνεχόμενα πάνω από 2 έτη
- έχει κύκλο εργασιών που δεν ξεπερνά τα € 25.000.000
- ο κύκλος εργασιών που προέρχεται από Βόρεια Αμερική (Η.Π.Α, Καναδάς) δεν ξεπερνά το 15% του συνολικού κύκλου εργασιών της
- δεν είναι χρηματοοικονομικός οργανισμός, δημόσιος οργανισμός, μέσο κοινωνικής δικτύωσης (social media)

☐ ΝΑΙ ☐ ΟΧΙ

➢ **Παρακαλούμε επιβεβαιώστε ότι η Εταιρία :**

- για την προστασία προσωπικών δεδομένων και εμπιστευτικών εταιρικών πληροφοριών ακολουθεί πολιτική που είναι σύμφωνη με τη Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων
- εφαρμόζει κατάλληλες τεχνικές και μεθόδους για την προστασία προσωπικών δεδομένων (π.χ. antivirus, firewalls) σε όλα τα συστήματα ηλεκτρονικών υπολογιστών, τις κινητές συσκευές και τις ιστοσελίδες της
- έχει ελεγχόμενη πρόσβαση για τους εργαζόμενους σε χώρους και συστήματα με ευαίσθητα δεδομένα
- εφαρμόζει διαδικασίες backup και ανάκτησης δεδομένων για όλα τα σημαντικά εταιρικά συστήματα και προσωπικά δεδομένα
- εάν αναθέτει σε εξωτερικούς συνεργάτες τη συλλογή και διαχείριση δεδομένων(outsourcing) επιλέγει συνεργάτες που δηλώνουν ότι παρέχουν επαρκείς τεχνικές μεθόδους για την προστασία προσωπικών δεδομένων

☐ ΝΑΙ ☐ ΟΧΙ

AIG Europe Limited
Υποκατάστημα Ελλάδας
Λεωφ. Κηφισίας 119, 15124 Μαρούσι, Τηλ.: 210 8127.600, Fax: 210-8027.189 e-mail: FLGreece@aig.com
ΥΠ/ΜΑ ΘΕΣ/ΝΙΚΗΣ: Μαρίνου Αντύπα 42, 57001,Πυλαία Θεσσαλονίκης, 57001, Τηλ.: 2310-474999 Fax: 2310-494990
ΝΟΜΙΜΟΣ ΑΝΤΙΠΡΟΣΩΠΟΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ: AIG ΕΛΛΑΣ Α.Ε. ΑΝΤΙΠΡΟΣΩΠΕΥΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ
Α.Φ.Μ.: 997472444, Δ.Ο.Υ ΦΑΕ Αθηνών, Αρ. Μητρ.Γ.Ε.ΜΗ.: 118328300001 URL: http://www.aig.com.gr

➢ **Παρακαλούμε επιβεβαιώστε ότι η Εταιρία:**

- δεν έχει αποτελέσει αντικείμενο οποιασδήποτε έρευνας ή ελέγχου σχετικά με θέματα προστασίας προσωπικών δεδομένων από την «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» ή οποιαδήποτε άλλη Αρχή
- δεν έχει επιβληθεί ποτέ στην εταιρία οποιαδήποτε ποινή, πρόστιμο ή άλλη κύρωση από την «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» ή οποιαδήποτε άλλη Αρχή για θέματα προστασίας προσωπικών δεδομένων
- δε γνωρίζει η εταιρία κάποιο περιστατικό ή γεγονός που μπορεί να καταλήξει σε απαίτηση για θέματα προστασίας προσωπικών δεδομένων

☐ ΝΑΙ ☐ ΟΧΙ

Προϋπόθεση ισχύος του ασφαλιστικού προγράμματος είναι να έχει σημειωθεί ΝΑΙ σε όλα τα παραπάνω πεδία. Σε διαφορετική περίπτωση θα πρέπει να επικοινωνήσετε με την AIG προκειμένου να εξεταστεί η δυνατότητα έκδοσης ειδικής προσφοράς.

➢ **<u>Μόνο</u> σε περίπτωση που το αντικείμενο της εταιρίας είναι σχετικό με την υγεία, τις τηλεπικοινωνίες, τις τηλεφωνικές πωλήσεις, τις ηλεκτρονικές πωλήσεις (e-shop), την επεξεργασία δεδομένων για λογαριασμό τρίτων (Data Processor-outsourcer) ή εάν η εταιρία είναι Call Center ή εάν η εταιρία διενεργεί πάνω από 70.000 συναλλαγές με κάρτες (πιστωτικές, χρεωστικές) το χρόνο, παρακαλούμε επιβεβαιώστε επιπλέον ότι η εταιρία:**

- έχει διαδικασίες για να εντοπίζει και να ανιχνεύει αδυναμίες στην ασφάλεια των δικτύων της
- έχει μέτρα προστασίας του ηλεκτρονικού εξοπλισμού και των έντυπων αρχείων της από κλοπές
- σε περίπτωση που συλλέγει ή αποθηκεύει αριθμούς πιστωτικών καρτών ακολουθεί το PCI (Payment Card Industry Data Security Standards)
- χρησιμοποιεί μεθόδους κρυπτογράφησης για την προστασία των ευαίσθητων προσωπικών δεδομένων, συμπεριλαμβανομένων δεδομένων σε φορητά μέσα (π.χ. φορητούς υπολογιστές, DVDs, δίσκους, USB κλπ)
- απαιτεί από απομακρυσμένους χρήστες να ταυτοποιούνται πριν τους επιτραπεί να εισαχθούν σε εσωτερικά δίκτυα και συστήματα

☐ ΝΑΙ ☐ ΟΧΙ

Προϋπόθεση ισχύος του ασφαλιστικού προγράμματος είναι να έχει σημειωθεί ΝΑΙ στο παραπάνω πεδίο. Σε διαφορετική περίπτωση θα πρέπει να επικοινωνήσετε με την AIG προκειμένου να εξεταστεί η δυνατότητα έκδοσης ειδικής προσφοράς.

<u>Σημαντικές Σημειώσεις:</u>

- Η ασφαλιστική κάλυψη θα έχει έναρξη την ημερομηνία που αναγράφεται στο στοιχείο 5 της αίτησης ασφάλισης, εφόσον η αίτηση είναι πλήρως συμπληρωμένη και υπογεγραμμένη όχι πριν από 30 ημέρες από την αιτούμενη ημερομηνία έναρξης της κάλυψης και η διάρκεια της θα είναι ετήσια.
- Η πλήρης περιγραφή – έκταση της ασφαλιστικής κάλυψης αναφέρεται στους όρους του ασφαλιστηρίου συμβολαίου. Για κάθε διευκρίνιση μπορείτε να επικοινωνείτε με τον ασφαλιστικό σας σύμβουλο ή απευθείας με την ασφαλιστική εταιρεία.
- Το παρόν έντυπο θα έχει ισχύ έως 30/04/2018.

AIG Europe Limited
Υποκατάστημα Ελλάδας
Λεωφ. Κηφισίας 119, 15124 Μαρούσι, Τηλ.: 210 8127.600, Fax: 210-8027.189 e-mail: FLGreece@aig.com
ΥΠ/ΜΑ ΘΕΣ/ΝΙΚΗΣ: Μαρίνου Αντύπα 42, 57001,Πυλαία Θεσσαλονίκης, 57001, Τηλ.: 2310-474999 Fax: 2310-494990
ΝΟΜΙΜΟΣ ΑΝΤΙΠΡΟΣΩΠΟΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ: AIG ΕΛΛΑΣ Α.Ε. ΑΝΤΙΠΡΟΣΩΠΕΥΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ
Α.Φ.Μ.: 997472444, Δ.Ο.Υ ΦΑΕ Αθηνών, Αρ. Μητρ.Γ.Ε.ΜΗ.: 118328300001 URL: http://www.aig.com.gr

ΕΝΤΥΠΟ ΠΡΟΣΦΟΡΑΣ

(Το έντυπο αυτό συμπληρώνεται προαιρετικά προς διευκόλυνση του Λήπτη της Ασφάλισης)

CyberEdge 2.0
Ασφάλιση Αστικής Ευθύνης για Ηλεκτρονικούς και Διαδικτυακούς Κινδύνους

1. Λήπτης της Ασφάλισης			
2. Διάρκεια ασφαλιστηρίου	12 μήνες από την ημερομηνία που θα συμφωνηθεί		
3. Όριο Ευθύνης	Συνολικό όριο ευθύνης ανά ασφαλιστική περίοδο για όλες τις ζημίες όλων των ασφαλισμένων σύμφωνα με τις ασφαλιστικές καλύψεις (Α, Β, Γ) και κάθε Παράρτημα Πρόσθετης Κάλυψης (Δ, Ε, ΣΤ): €.....		
4. Καλύψεις και επιμέρους όρια (Τα επιμέρους όρια περιλαμβάνονται στο Όριο Ευθύνης και σε καμία περίπτωση δεν το αυξάνουν.)	**Α. Διαχείριση Γεγονότων**		
	Α.1 Πρώτη Αντίδραση	€ 500.000 *	
		Αριθμός έκτακτης Ανάγκης: **Σύμβουλος Απόκρισης:** **Ειδικός IT:**	**+44 (0) 1273 729225** **CMS Legal** **KPMG**
	Α.2 Νομικές Υπηρεσίες	Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων	
	Α.3 Υπηρεσίες IT	Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων	
	Α.4 Επαναφορά Δεδομένων	Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων	
	Α.5 Προστασία της Φήμης	€ 500.000 *	
	Α.6 Έξοδα Γνωστοποίησης	€ 500.000 *	
	Α.7 Παρακολούθηση Πίστωσης	€ 500.000 *	

AIG Europe Limited
Υποκατάστημα Ελλάδας
Λεωφ. Κηφισίας 119, 15124 Μαρούσι, Τηλ.: 210 8127.600, Fax: 210-8027.189 e-mail: FLGreece@aig.com
ΥΠ/ΜΑ ΘΕΣ/ΝΙΚΗΣ: Μαρίνου Αντύπα 42, 57001,Πυλαία Θεσσαλονίκης, 57001, Τηλ.: 2310-474999 Fax: 2310-494990
ΝΟΜΙΜΟΣ ΑΝΤΙΠΡΟΣΩΠΟΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ: AIG ΕΛΛΑΣ Α.Ε. ΑΝΤΙΠΡΟΣΩΠΕΥΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ
Α.Φ.Μ.: 997472444, Δ.Ο.Υ ΦΑΕ Αθηνών, Αρ. Μητρ.Γ.Ε.ΜΗ.: 118328300001 URL: http://www.aig.com.gr

	και Ταυτότητας		
	Β. Υποχρεώσεις Προστασίας Προσωπικών Δεδομένων		
	Β.1 Έρευνα Προστασίας Δεδομένων	€ 500.000 *	
	Β.2 Πρόστιμα Προστασίας Προσωπικών Δεδομένων	€ 500.000 *	
	Γ. Ευθύνη		
	Γ.1 Προσωπικές και Εταιρικές Πληροφορίες	Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων	
	Γ.2 Αστοχία Ασφάλειας	Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων	
	Γ.3 Παράλειψη Γνωστοποίησης	Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων	
	Γ.4 Κάτοχος των Πληροφοριών (Προσωπικές και Εταιρικές Πληροφορίες)	Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων	
5. Πρόσθετες Καλύψεις και επιμέρους όρια (Τα επιμέρους όρια περιλαμβάνονται στο Όριο Ευθύνης και σε καμία περίπτωση δεν το αυξάνουν.)	**Δ. Κάλυψη Ψηφιακών Μέσων**	€ 500.000 *	
	Ε. Κάλυψη Διακοπής Λειτουργίας Δικτύου Ε.1 Ζημία Διακοπής Λειτουργίας Δικτύου Ε.2 Έξοδα Διακοπής Λειτουργίας Δικτύου και Μετριασμού	€ 500.000 *	
	ΣΤ. Κάλυψη Εκβιασμού Αποκάλυψης Προσωπικών Δεδομένων στον Κυβερνοχώρο	€ 500.000 *	
		Σύμβουλος σε θέματα εκβιασμού στον κυβερνοχώρο **Αριθμός επικοινωνίας**	**NYA Neil Young Associates** **+ 44 208 242 6449**
6. Απαλλαγές**	**Γενική Απαλλαγή Ασφαλιστηρίου**		€.....
	Α.5 Προστασία της Φήμης		Γενική Απαλλαγή

8

AIG Europe Limited
Υποκατάστημα Ελλάδας
Λεωφ. Κηφισίας 119, 15124 Μαρούσι, Τηλ.: 210 8127.600, Fax: 210-8027.189 e-mail: FLGreece@aig.com
ΥΠ/ΜΑ ΘΕΣ/ΝΙΚΗΣ: Μαρίνου Αντύπα 42, 57001,Πυλαία Θεσσαλονίκης, 57001, Τηλ.: 2310-474999 Fax: 2310-494990
ΝΟΜΙΜΟΣ ΑΝΤΙΠΡΟΣΩΠΟΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ: AIG ΕΛΛΑΣ Α.Ε. ΑΝΤΙΠΡΟΣΩΠΕΥΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ
Α.Φ.Μ.: 997472444, Δ.Ο.Υ ΦΑΕ Αθηνών, Αρ. Μητρ.Γ.Ε.ΜΗ.: 118328300001 URL: http://www.aig.com.gr

	Α.6 Έξοδα Γνωστοποίησης	Γενική Απαλλαγή
	Β.2 Πρόστιμα Προστασίας Προσωπικών Δεδομένων	Γενική Απαλλαγή
	Γ. Ευθύνη	Γενική Απαλλαγή
	Δ. Κάλυψη Ψηφιακών Μέσων	Γενική Απαλλαγή
	Ε.1 Ζημία Διακοπής Λειτουργίας Δικτύου	8 ώρες αναμονή
	Ε.2 Έξοδα Διακοπής Λειτουργίας Δικτύου και Μετριασμού	4 ώρες αναμονή
	ΣΤ. Κάλυψη Εκβιασμού Αποκάλυψης Προσωπικών Δεδομένων στον Κυβερνοχώρο	Γενική Απαλλαγή
	Λοιπές καλύψεις	Καμία απαλλαγή
7. Συνολικό Ετήσιο Ασφάλιστρο	€.....	
8. Τρόπος πληρωμής		
9. Ημερομηνία Αναδρομικής Ισχύος	Έναρξη ασφαλιστηρίου	
10. Γεωγραφικά όρια/ Δωσιδικία	Παγκόσμια	
11. Όροι	Σύμφωνα με το ασφαλιστήριο CyberEdge 2.0 της AIG στην ελληνική γλώσσα	
12. Ασφαλιστής	AIG Europe Limited Λεωφόρος Κηφισίας 119 15124, Μαρούσι-Αθήνα, Ελλάδα Τηλ: +30 2108127600	
13. Ισχύς της παρούσας προσφοράς	Η παρούσα προσφορά είναι ενδεικτική και μη δεσμευτική και εκδόθηκε με βάση τις πληροφορίες που γνωρίστηκαν στον Ασφαλιστή. Ο Ασφαλιστής διατηρεί το δικαίωμα να τροποποιήσει ή / και αποσύρει την παρούσα προσφορά σε περίπτωση επίτασης του κινδύνου. Η παρούσα προσφορά ΔΕΝ αποτελεί ασφαλιστική κάλυψη και θα παραμείνει σε ισχύ για ένα μήνα.	

Σημείωσεις:

*Σε περίπτωση που το Όριο Ευθύνης που έχει επιλεγεί στον Πίνακα Ασφαλίστρων είναι μικρότερο από € 500.000, τότε το επιμέρους όριο της κάλυψης θα ισούται με το Όριο Ευθύνης .

**Για περιστατικά που θα ενεργοποιήσουν περισσότερες από μία καλύψεις θα εφαρμοστεί μία φορά η Γενική Απαλλαγή σε συνδυασμό με τις απαλλαγές των ωρών αναμονής για τις καλύψεις Ε1 και Ε2.

9

Figure 4 - Τυπικό ερωτηματολόγιο νο2

Ένα ακόμα πολύ σημαντικό στοιχείο που εξετάζουν οι ασφαλιστικοί φορείς είναι το γεγονός ότι οι όροι για τις πολιτικές και οι οικονομικές ανάγκες χρειάζονται συνεχώς προσαρμογή και αυτό γιατί οι κίνδυνοι που προέρχονται από το χώρο του διαδικτύου είναι διαφορετική ανά κατηγορία επιχείρησης και ανάλογα με το μέγεθος του οργανισμού και του τύπου των δεδομένων που επεξεργάζεται και αποθηκεύει. Αλλά για να παραμείνουν μπροστά στην ψηφιακή εποχή καλούνται να αλλάξουν και για να συμμετάσχουν ενεργά στην αγορά των ασφαλίσεων από επιθέσεις από τον κυβερνοχώρο, πρέπει να ανακατασκευάσουν την όλη λειτουργία και φιλοσοφία τους. Απαιτείται μια σειρά τεχνικών γνώσεων και γνώσεων για να ασφαλίσουν αυτά τα είδη κινδύνων, αλλά εξακολουθούν να είναι επαγγελματίες που συνδυάζουν ασφάλιση και τεχνικές δεξιότητες είναι δύσκολο να βρεθούν.

Οι περισσότεροι ασφαλιστικοί φορείς ακολουθούν τις παρακάτω πληροφορίες μια βασική μορφή αξιολόγησης των οργανισμών όλων των τομέων και αναλόγως με τα αποτελέσματα μια εκτεταμένη αξιολόγηση θα διεξαχθεί:

- Αρίθμηση και γεωγραφική εξάπλωση των επιχειρήσεων:
  - Μέγεθος
  - Λειτουργία
  - Έσοδα
- Λεπτομέρειες της επιχειρηματικής λειτουργίας τους:
  - Τομέας
  - Δραστηριότητες
  - Υπηρεσίες
  - Εξωτερικές λειτουργίες
  - Έκθεση σε ρίσκα
- Εξαρτήσεις από την υποδομή της Πληροφορικής
- Τη χρήση, την αποθήκευση και το διαμοιρασμό των δεδομένων:
  - Δίσκοι δεδομένων
  - Ευαισθησία των δεδομένων (π.χ. προσωπικά δεδομένα, πνευματική ιδιοκτησία)
  - Υποχρεωτική ευθύνη
- Ιστορικό συμβάντων (στην περίπτωση που έχουν υπάρξει τέτοια)
- Εταιρική παρουσία στα μέσα κοινωνικής δικτύωσης
- Ιστορία των πολιτικών και των διεκδικήσεων (εάν υπήρχαν αξιώσεις εναντίον της)

Θα πρέπει να γίνει κατανοητό και ξεκάθαρο ότι η ασφάλεια από κυβερνο-επιθέσεις δεν παίρνει σε καμία περίπτωση τη θέση όλων των απαραίτητων μέτρων ασφαλείας που θα πρέπει να έχει ένας οργανισμός για την ασφάλεια των πληροφοριών και των δεδομένων που διαχειρίζεται. Απλά δημιουργεί μία δεύτερη γραμμής ασφαλείας στην άμυνα ενός οργανισμού με σκοπό να ελαχιστοποιήσει το ρίσκο από περιστατικά ασφαλείας που προέρχονται από το χώρο του διαδικτύου.

4.2 Καλύψεις

Στον παρακάτω πίνακα παρουσιάζονται συνοπτικά οι συνήθεις καλύψεις που παρέχουν οι ασφαλιστικοί φορείς προς τις εταιρείες.

Covered Risk	Details
Privacy and Data Breach cover	Defense costs and damages for which the Insured or Outsourced Service Provider is liable, arising from a loss of data.
Business Interruption and Restoration costs cover	Loss of business income (and restoration costs) caused by a targeted attack against the company's computer system.
Network security claims cover	Defense costs and damages for which the Insured is liable, arising from a targeted cyber-attack.
Media liability claims cover	Defense costs and damages for which the Insured is liable, arising from the publication or broadcasting of digital media content.
Regulatory costs cover	Defense costs for a claim by a regulator arising out of the loss of data.
Regulatory fines and penalties cover	Monetary fines and penalties levied by regulators (to the extent that they are insurable) arising from a loss of data.
Notification costs	In accordance with legal and regulatory requirements following a loss of data.
Response costs	Fees and expenses for: • Forensic investigation following a loss of data • Identifying and preserving lost data • Advice on legal and regulatory duties • Determining the extent of indemnification obligations in contracts with third party service providers • Credit monitoring services and other remedial actions required after a loss of data.
Hacker theft cover	Indemnity for stolen funds due to malicious activities of a third party.
Cyber extortion cover	Indemnity for the resolution of a credible threat to compromise the Insured's data or systems.
E-payments cover	Defense costs, damages and contractual penalties in respect of a breach of Payment Card Industry Data Security Standards.
Crisis Communication cover	Public relations expenses of a panel of experts to mitigate any negative publicity from a covered event.
Consultant services cover	The expenses of an IT expert to determine the amount and extent of a loss covered under this policy.

Figure 5 - Ασφαλιστικές καλύψεις

Στην παρακάτω εικόνα θα δούμε μία σύγκριση των παροχών Cyber insurance σε σχέση με τα παραδοσιακά ασφάλιστρα.

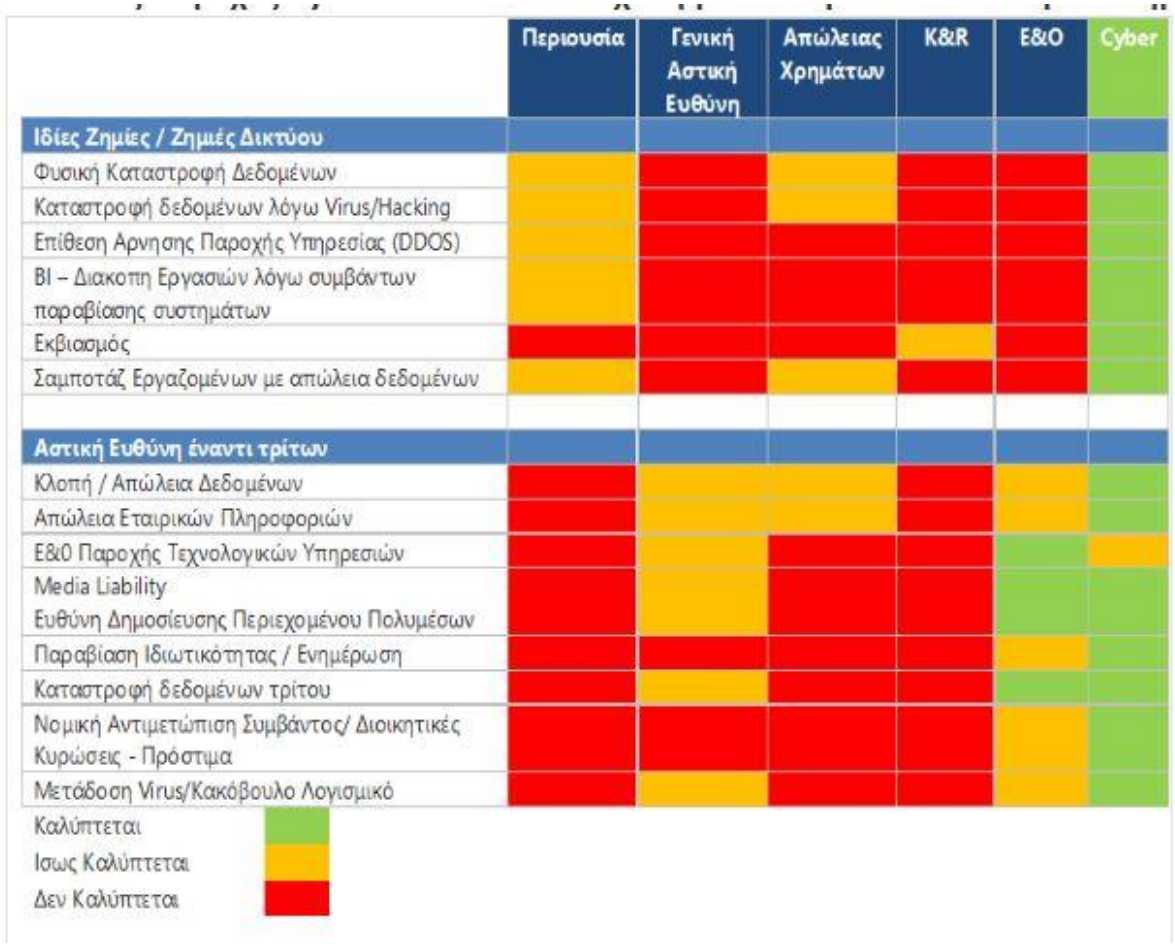

Figure 6 - Συγκριση Cyber insurance με παραδοσιακά συμβόλαια

Η καινοτομία των νέων ασφαλιστικών προϊόντων προέρχεται από την παροχή υπηρεσιών διαχείρισης συμβάντων σε συνεργασία με εγνωσμένης αξίας παρόχους υπηρεσιών ψηφιακής εγκληματολογίας, νομικούς, επικοινωνιολόγους με σκοπό την αποτελεσματική διαχείριση των συμβάντων και την μείωση των συνεπειών στην εταιρική φήμη.

Κύριες κατηγορίες των καλύψεων είναι:

- Οικονομικό κόστος
- Συμβουλευτικές Υπηρεσίες

Παράλληλα υπάρχουν και καλύψεις που μπορούν να χαρακτηριστούν ως προαιρετικές, όπως:

- Διακοπή λειτουργίας δικτύου
- Κάλυψη εκβιασμού
- Ευθύνη ψηφιακών πολυμέσων

4.2.1 Οικονομικός Κόστος

Ίσως το πιο βασικό σκέλος των καλύψεων είναι αυτό του οικονομικού κόστους.

- Ένα κομμάτι αφορά τα υποκείμενα των οποίων τα δεδομένα παραβιάστηκαν. Παρέχεται κόστους για την ειδοποίησης τους, όσο και για την ειδοποίηση των ανάλογων ρυθμιστικών αρχών. Παράλληλα παρέχεται και κάλυψη των εξόδων για παρακολούθηση της όποιας χρήσης μπορεί να γίνει στα δεδομένα που κλάπηκαν.
- Κόστος υπεράσπισης και ζημιές σε περίπτωση που η επιχείρηση προκαλέσει παραβίαση προσωπικών ή εταιρικών δεδομένων.
- Κόστος υπεράσπισης και ζημιές σε περίπτωση που η επιχείρηση προσβάλει τα δεδομένα τρίτων με ιό.
- Κόστος υπεράσπισης και ζημιές σε περίπτωση που η επιχείρηση υποστεί κλοπή κωδικών πρόσβασης στα συστήματα με μη ηλεκτρονικά μέσα.
- Κόστος υπεράσπισης και ζημιές σε περίπτωση που κάποιος εργαζόμενος του οργανισμού αποκαλύψει δεδομένα σε τρίτους.

Επίσης σημαντικό κομμάτι είναι και το οικονομικό κόστος για την παροχή νομικής προστασίας.

- Το κόστος για την παροχή νομικών συμβούλων και εκπροσώπηση στη σχετική έρευνα που θα διεξαχθεί για την προστασία των δεδομένων.
- Πρόστιμα και κυρώσεις που επιβάλλονται από ανεξάρτητες αρχές προστασίας των προσωπικών δεδομένων.

4.2.2 Συμβουλευτικές Υπηρεσίες

Ειδικοί σύμβουλοι παρέχονται προς την επιχείρηση κατά τη διάρκεια και μετά από το περιστατικό ασφαλείας.

- Βοήθεια προς τον οργανισμό με ομάδες αντιμετώπισης περιστατικών
- Βοήθεια μετά από τη διαπίστωση του περιστατικού ασφαλείας και καθοδήγηση για την αποκατάσταση συστημάτων και υποδομής.
- Κάλυψη του κόστους και παροχή συμβουλευτικών υπηρεσιών προς τον οργανισμό για να προσδιοριστεί αν τα δεδομένα μπορούν να αποκατασταθούν και να επανασυλλεχθούν.

Επίσης σημαντικό ρόλο παίζει και η βοήθεια προς τον οργανισμός για την αποκατάσταση της φήμης του μετά από τη διαπίστωση ενός περιστατικού ασφαλείας.

- Πρόληψη ή ελαχιστοποίηση ενδεχόμενων αρνητικών επιπτώσεων μετά από τη διαπίστωση ενός σοβαρού περιστατικού ασφαλείας.
- Κόστος για την ελαχιστοποίηση ενδεχόμενης ζημιάς στη φήμη οποιουδήποτε ατόμου στην εταιρεία.

4.3 Κριτήρια και όρια ασφαλιστικότητας

Είναι γνωστό ότι κάθε περιστατικό παραβίασης των δεδομένων ενός οργανισμού, συνοδεύεται είτε από ζημιά στο οργανισμό που είχε το περιστατικό ασφαλείας. Η ζημιά αυτή μπορεί να είναι είτε οικονομικής φύσεως (να χαθούν πελάτες ή να ακυρωθούν παραγγελίες) ή ακόμα χειρότερα να είναι στη φήμη του οργανισμού. Στη δεύτερη περίπτωση μάλιστα το κόστος δεν μπορεί να αποτιμηθεί άμεσα, αλλά σε βάθος χρόνου. Ενώ παράλληλα τα τρέχοντα ασφαλιστικά συμβόλαια που προσφέρουν οι ασφαλιστικοί φορείς δεν καλύπτουν επαρκώς όλους του κινδύνους προερχόμενους από το ίντερνετ. Δε θα ήταν υπερβολή να χαρακτηρίσουμε τους κινδύνους από τον κυβερνοχώρο σαν μία κοινή απειλή για την παγκόσμια οικονομία και ο μόνος τομέας που θα μπορούσε να μειώσει σημαντικά αυτή την απειλή είναι ο ασφαλιστικός.

Ωστόσο μέχρι και σήμερα οι προτάσεις, οι λύσεις και τα τελικά προϊόντα που προσφέρουν οι ασφαλιστικοί φορείς προς τους οργανισμούς είναι περιορισμένα και παραμένουν κάτω από σοβαρή κριτική. Και αυτό γιατί οι περισσότεροι από τους τύπους των ρίσκων χαρακτηρίζονται ως μη ικανοί προς ασφάλιση (uninsurable) ενώ κάποιοι λίγοι ικανοί προς ασφάλιση (insurable).

Προκειμένου λοιπόν ο ασφαλιστικός τομέας να είναι σε θέση να προσφέρει λειτουργικά και βιώσιμα προϊόντα προς τους οργανισμούς θα πρέπει να θέσει κάποια σημαντικά κριτήρια για την ασφάλιση τους. Με την ανάλυση των κριτηρίων αυτών κάποιον μπορεί να έρθει αντιμέτωπος με τα προβλήματα που αντιμετωπίζει η αγορά. Στον παρακάτω πίνακα παρατίθενται συνοπτικά τα κριτήρια αυτά [1].

Insurability Criteria	Observations	Insurance Market Considerations
Frequency & Severity of losses	Cyber Incidents, especially after 2000, continuously increased as well as the losses and Cyber risk is considered the number one operational risk.	Self-protective measures have been increased but the losses still remain huge. How cyber insurance products can remain viable and effective?
Risk Pooling	Cyber risk compared to other operational risks is relatively high, making efficient risk pooling problematic and unachievable.	How the increasing reinsurance capacity can be achieved to better spread the exposure?
Scarcity of Data	The scarcity of Data and the lack of understanding all types and sources of this risk is a global phenomenon.	Insurers treat this uncertainty by setting high deductibles and low maximum coverage that seems not appealing at all to potential customers.
Risk of change	Cyber exposures are changing dynamically, drastically and fast.	Loss estimates are not stable due to HW & SW technical progress and the analysis of historical cyber risk data may be misleading not to say of any value at all. In addition, cyber risk insurance policies are not keeping pace with evolving cyber risks.
Information Asymmetries	The interrelated nature of information systems makes it difficult to discover, much less prove, sources of losses and identity of perpetrators.	The vulnerability of information systems complex interrelations is unpredictable. Furthermore, moral hazard and adverse selection add insurmountably impediments.

Insurance Product add value	Cyber Insurance products contain significant exclusions and relatively low cover limits.	These exclusions form one hand make customers question the value of these products and on the other hand if insurers slide over this exclusions or increase the cover limits may be not able to sustain such a risk.

Figure 7 - Κριτήρα Ασφαλιστικότητας

Στα παραπάνω κριτήρια μπορούμε επιπλέον να προσθέσουμε επιπλέον και τα:

- Randomness of loss occurrence (τυχαία εμφάνιση ζημιών)
- Maximum possible loss (μέγιστη πιθανή απώλεια)
- Average loss per event (μέγιστη απώλεια ανά συμβάν)
- Loss exposure (απώλεια έκθεσης)
- Insurance premium (ασφάλιστρο)
- Cover limits (όρια καλύψεων)
- Public policy (δημόσιες πολιτικές)
- Legal restrictions (νομικοί περιορισμοί)

4.3.1. Randomness of loss occurrence

Μία απαίτηση για την παροχή ασφάλειας απέναντι από ένα συγκεκριμένο ρίσκο είναι η ανεξαρτησία των κινδύνων. Σύμφωνα με το νόμο των μεγάλων αριθμών, όσο μεγαλύτερος είναι ο αριθμός των αμοιβαία εξαρτώμενων κινδύνων στον τομέα της ασφάλειας, τόσο πιο πιθανό είναι οι μέσες συνολικές απώλειες να αντιστοιχούν στις αναμενόμενες απώλειες. Με αυτό τον τρόπο επιτυγχάνεται η μείωση των φορτίων ασφαλείας. Επομένων η προϋπόθεση της ανεξαρτησίας των κινδύνων είναι μια σημαντική προϋπόθεση για την ασφάλιση κάθε τύπου κινδύνου.

Τα περισσότερα από τα συστήματα του κυβερνοχώρου έχουν σχεδιαστεί με πανομοιότυπο τρόπο. Κατά συνέπεια είναι ευάλωτα στα ίδια περιστατικά και κινδύνους. Γι’ αυτό και δικαιολογείται η υπόθεση ότι οι κίνδυνοι που αντιμετωπίζουν οι οργανισμοί μπορούν να συσχετιστούν άμεσα. Γενικότερα ένα μεγάλο ποσοστό των απωλειών που μπορεί να συμβούν σε έναν οργανισμό σχετίζονται άμεσα με πιθανές απώλειες ενός άλλου οργανισμού.

Εδώ είναι σημαντικό να σημειωθεί όμως ότι ο συσχετισμός δε συμβαίνει απαραιτήτως σε όλες τις κατηγορίες των ρίσκων. Ένα τέτοιο παράδειγμα μπορεί να είναι η φυσική απώλεια δεδομένων από έναν οργανισμό.

4.3.2 Maximum Possible Loss

Το κριτήριο αυτό ικανοποιείται εάν η μέγιστη δυνατή απώλεια ανά συμβάν είναι διαχείρισιμη από άποψη ασφαλιστικής φερεγγυότητας. Οι μέγιστες ιστορικές απώλειες από ρίσκα του κυβερνοχώρου είναι σημαντικά χαμηλότερες από εκείνες που προέρχονται από γενικά λειτουργικά ρίσκα. Γι’ αυτό και οι ασφαλιστικοί φορείς καλύπτουν τους εαυτούς τους με όρια στις καλύψεις προς τους οργανισμούς. Έτσι οι μέγιστες απώλειες από τους κινδύνους και τα ρίσκα από τον κυβερνοχώρο φαίνεται να γίνονται διαχειρίσιμες.

4.3.3 Average Loss per Event

Υπάρχουν πολλές μελέτες που έχουν υπολογίσει πόσο περίπου είναι το μέσο κόστος για κάθε περιστατικό ασφαλείας. Το σίγουρο είναι ότι το κόστος αυτό ανέρχεται σε αρκετά εκατομμύρια.

Γενικά παρατηρείται ότι οι μικροί και οι πολύ μεγάλοι οργανισμοί έχουν μεγαλύτερα κόστη ανά περιστατικό από μεσαίους οργανισμούς. Αυτό πιθανότατα οφείλεται στο ότι οι μικροί οργανισμοί είναι λιγότερο ενημερωμένοι και σε εγρήγορση σε είναι λιγότερο διαθέσιμοι στο να αντιμετωπίσουν την έννοια των ρίσκων από τον κυβερνοχώρο. Ενώ παράλληλα οι μεγάλοι οργανισμοί είναι δύσκολο λόγο της πολυπλοκότητας της δομής που έχουν.

Ένα άλλο σημαντικό οικονομικό στοιχείο είναι ότι εταιρείες που έχουν στο δυναμικό τους εργαζόμενο με την ειδικότητα του CISO (Chief Information Security Officer) έχουν μικρότερο κόστος ανά περιστατικό. Η θεσμική δέσμευση που επιδεικνύει ένα τέτοιο άτομο με την αντίστοιχη εμπειρία του φαίνεται να επηρεάζει τη μέση απώλεια ανά συμβάν.

4.3.4 Loss exposure

Παρατηρείται συνεχώς ότι έχουμε έναν αυξανόμενο αριθμό συμβάντων προερχόμενα από τον κυβερνοχώρο με την πάροδο του χρόνου. Η συχνότητα αυτή ωστόσο εξαρτάται από την κατηγορία που ανήκει το συμβάν. Για παράδειγμα η δραστηριότητα του ανθρώπου εντοπίζεται πολύ πιο συχνά από απώλειες που προέρχονται πχ από φυσικά αίτια και καταστροφές. Επιπλέον η έκθεση εξαρτάται από τον τύπο του οργανισμού και από το μέγεθος του. Το κριτήριο όμως αυτό δείχνει πολλές φορές να είναι αναποτελεσματικό.

4.3.5 Insurance Premium

Τα ασφαλιστήρια συμβόλαια συχνά χαρακτηρίζονται ως δαπανηρά και ακριβά. Οι τέσσερις κύριοι λόγοι που καθορίζουν την αξία ενός συμβολαίου είναι:

- Η καινοτομία του προϊόντος. Όσο καινούργιο είναι ένα προϊόν τόσο λιγότερους κινδύνους αντιμετωπίζει.
- Όσο καινούργιο είναι ένα προϊόν τόσο μικρότερος είναι και ο αριθμός στους οποίους είναι διαθέσιμο.
- Όσο καινούργιο είναι ένα προϊόν τόσο λιγότερο στοιχεία είναι διαθέσιμα γι’ αυτό.
- Οι μη έγκυρες διαθέσιμες πληροφορίες για ένα προϊόν απαιτούν δαπανηρή έρευνα για την εκ των προτέρων αξιολόγηση του κινδύνου, πριν δηλαδή παρουσιαστεί κάποιο ρίσκο.

4.4 Γενικά στοιχεία της αγοράς

Η έκθεση στον κυβερνοχώρο είναι μία από τις μεγαλύτερες πηγές ανησυχίας για τις επιχειρήσεις. Η παγκόσμια αγορά στον κυβερνοχώρο σήμερα υπολογίζεται σε εκατοντάδες εκατομμύρια ευρώ, ενώ αναμένεται ακόμα πιο ισχυρή και ραγδαία ανάπτυξη μέσα στα επόμενα χρόνια με τη διάδοση της τεχνολογίας και των υπολογιστών. Όλο αυτό έχει προσφέρει μια μεγάλη ευκαιρία πωλήσεων για τους ασφαλιστικούς φορείς καθώς ελάχιστοι οργανισμοί είναι ασφαλισμένοι έναντι των κυβερνοεπιθέσεων. Παρόλο λοιπόν που οι περισσότεροι οργανισμοί βασίζονται στα δίκτυα των

υπολογιστών και τα περισσότερα συστήματα τους είναι διαθέσιμα στο ίντερνετ, λίγοι οργανισμοί έχουν τέτοιου είδους ασφαλιστικά πακέτα.

4.4.1 Ποιοι μπορεί να είναι οι πελάτες

Κάθε εταιρεία η οποία αποθηκεύει, διαχειρίζεται ή μεταφέρει οποιασδήποτε μορφή δεδομένα και προσωπικά δεδομένα κινδυνεύει είτε από τη φυσική είτε από τη διαδικτυακή κλοπή τους. Στη συνέχεια θα δούμε ενδεικτικά μερικούς κλάδους εταιρειών που θα μπορούσαν να είναι υποψήφιοι πελάτες για τους ασφαλιστικούς φορείς.

- Εταιρείες με δραστηριότητες στις ΗΠΑ.
  Όσες εταιρείες δραστηριοποιούνται στις ΗΠΑ είναι υποχρεωμένες να συμμορφώνονται με την εκεί νομοθεσία σε περίπτωση που διαπιστωθεί περιστατικό ασφαλείας των δεδομένων τους. Οι κανονισμοί και οι ειδικές νομοθεσίες που διέπουν τους διάφορους κλάδους της αγοράς θα πρέπει να τηρούνται. Παράλληλα για τις ΗΠΑ κάθε εταιρεία που είναι εισηγμένη στο χρηματιστήριο θα πρέπει να δημοσιοποιεί τις όποιες συνέπειες λειτουργικές και οικονομικές, μια επίθεσης προερχόμενης από τον κυβερνοχώρο.
- Πανεπιστήμια
  Τα πανεπιστημιακά ιδρύματα συλλέγουν πολλά ευαίσθητα προσωπικά δεδομένα ειδικά των αιτούντων (οικονομικά δεδομένα, στοιχεία για την υγεία τους, προσωπικά έγγραφα, τίτλους σπουδών κλπ

- Κλάδος Υγείας
  Η τεχνολογία δεν άφησε ανεπηρέαστο τον συγκεκριμένο κλάδο. Η ανάπτυξη ηλεκτρονικών βάσεων δεδομένων με ευαίσθητα προσωπικά δεδομένα καταχωρημένα για κάθε ασθενή καθώς και η ανάπτυξη ψηφιακών πλατφορμών (πχ για ηλεκτρονική συνταγογράφηση φαρμάκων), καθιστά τον συγκεκριμένα κλάδο επιρρεπή σε παραβιάσεις ασφαλείας.
- Επιχειρήσεις λιανικής πώλησης και εμπορίου
  Επίσης ένας κλάδος επιχειρήσεων που εμπεριέχει ευαίσθητα προσωπικά δεδομένα των πελατών τους. Τέτοια μπορεί να είναι οικονομικής φύσεως (τραπεζικοί λογαριασμοί και αριθμοί πιστωτικών καρτών για την αγορά των προσφερόμενων προϊόντων). Παράλληλα μιλάμε σήμερα για έναν κλάδο ο οποίος βρίσκεται σε ανοδική τάση και ανάπτυξη. Οπότε μιλάμε για έναν κλάδο ελκυστικό για επιθέσεις από τον κυβερνοχώρο με ανυπολόγιστες ζημιές για τον εκάστοτε οργανισμό, αλλά και πρόστιμα και πιθανές κυρώσεις από τη νομοθεσία που διέπει τις χώρες που λειτουργούν.
- Ξενοδοχειακές και Τουριστικές επιχειρήσεις
  Επίσης ένας πολύ ελκυστικός στόχος για επιθέσεις από τον κυβερνοχώρο. Η ανάπτυξη της τεχνολογίας και του ιντερνέτ έχει φέρει σημαντικές αλλαγές στον τομέα τον κρατήσεων. Οι πελάτες των οργανισμών αυτών μέσω ειδικών πλατφορμών μπορούν να κάνουν κρατήσεις ηλεκτρονικά και να πραγματοποιούν τις πληρωμές τους.
- Τηλεπικοινωνίες
  Οι οργανισμοί τηλεπικοινωνιών διαχειρίζονται τεράστιο όγκο δεδομένων και ευαίσθητων προσωπικών πληροφοριών των πελατών τους. Είναι από τους πλέον ελκυστικούς στόχους επιθέσεων και η φήμη τους μπορεί να επηρεαστεί σε πολύ μεγάλο βαθμό σε περίπτωση περιστατικού παραβίασης ασφαλείας.
- Εταιρείες κοινής ωφέλειας
  Η ανάπτυξη της τεχνολογίας έχει επιφέρει σημαντικές αλλαγές στις υποδομές τέτοιου είδους οργανισμών. Πολλά αυτοματοποιημένα συστήματα υπάρχουν πλέον στις υποδομές τους,

αυξάνοντας όμως παράλληλα την έκθεση ευαίσθητων πληροφοριών και κρίσιμων υποδομών στο διαδίκτυο.

- Χρηματοπιστωτικά ιδρύματα
  Από τη φύση και μόνο του κλάδου καταλαβαίνουμε πόσο πολύ σημαντικός και επικίνδυνος στόχος αποτελεί. Οι πληροφορίες που συλλέγουν είναι πολύ μεγάλες σε όγκο και πολύ κρίσιμες και ευαίσθητες για τα υποκείμενα.

Βλέπουμε λοιπόν ότι η αγορά ασφαλειών για κυβερνοεπιθέσεις είναι μια αγορά που βρίσκεται σε πολύ αρχικό στάδιο με συνεχόμενη και ραγδαία ανάπτυξη. Από την πλευρά των οργανισμών θα πρέπει να γίνει πλήρης κατανόηση των κινδύνων του κυβερνοχώρου. Οι κίνδυνοι είναι πολύ και παράλληλα εκτός από τεχνολογικά μέτρα χρειάζεται επιπλέον μία σαφής και δομημένη προστασία όπως αυτή που παρέχουν τα ασφαλιστικά προγράμματα.

Εκτός από τους κινδύνους οι οργανισμοί θα πρέπει να κατανοήσουν και τις δαπάνες που θα χρειαστούν σε περίπτωση που προκύψει κάποιο περιστατικό ασφαλείας, καθώς μία τέτοια παραβίαση μπορεί να προκαλέσει πολλαπλές επιπτώσεις και οικονομικές συνέπειες να είναι σοβαρές έως και δυσβάσταχτες.

4.4.2 Οικονομικά Στοιχεία της Αγοράς

Θα δούμε συνοπτικά 2 εικόνες με οικονομικά στοιχεία για την αγορά της ασφάλισης από περιστατικά παραβίαση τόσο στην Αμερική όσο και στην Ευρώπη [7].

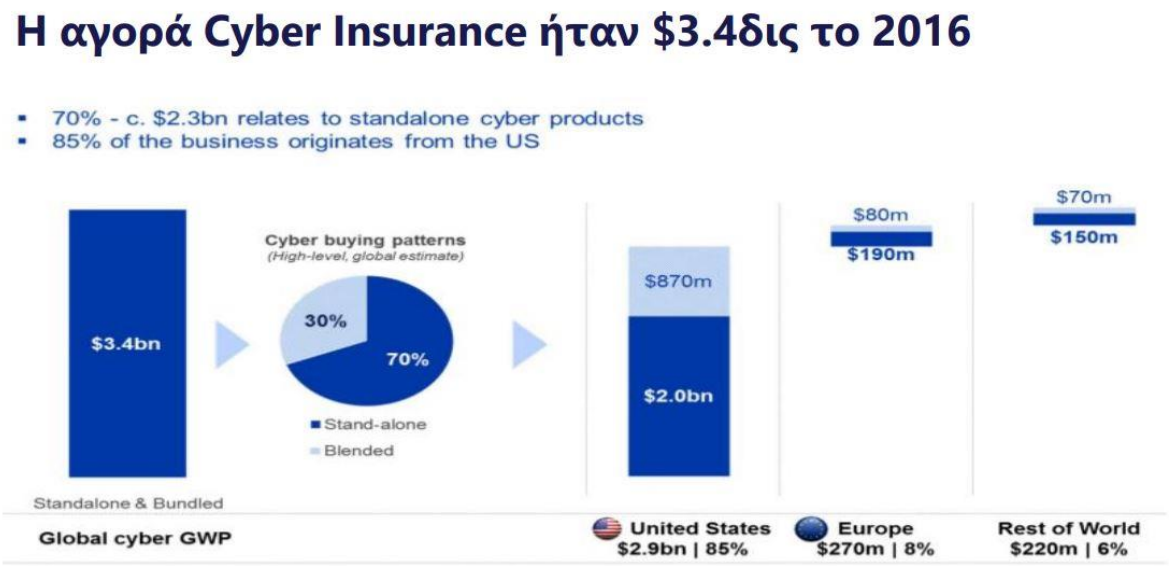

Figure 8 - Αγορά στις ΗΠΑ

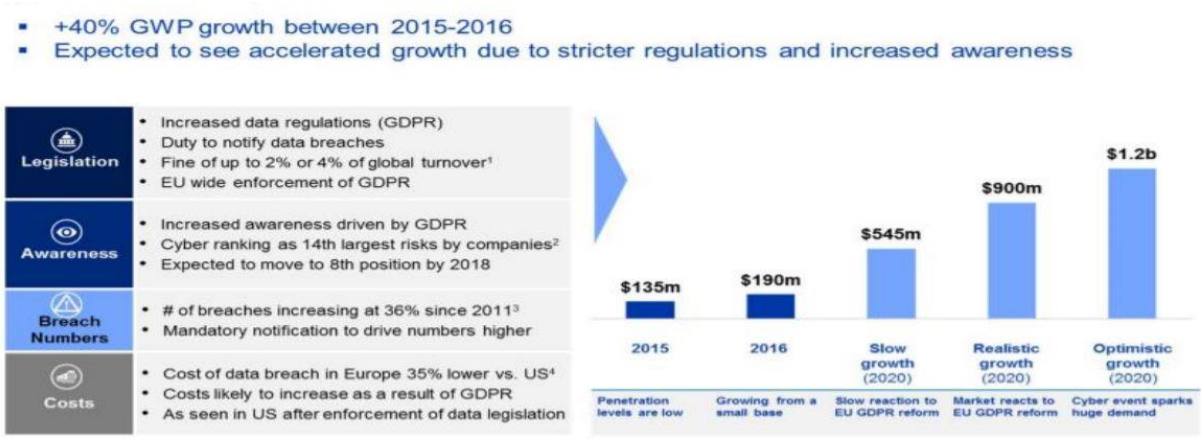

Figure 9 - Αγορά στην Ευρώπη

4.4.3 Εξέλιξη της αγοράς

Το μέγεθος της ασφαλιστικής αγοράς που αναπτύσσεται είναι πολύ μεγάλο όπως αποδεικνύεται από την ανάπτυξη που παρουσιάζει η αγορά του Cyber Insurance στην Αμερική [7].

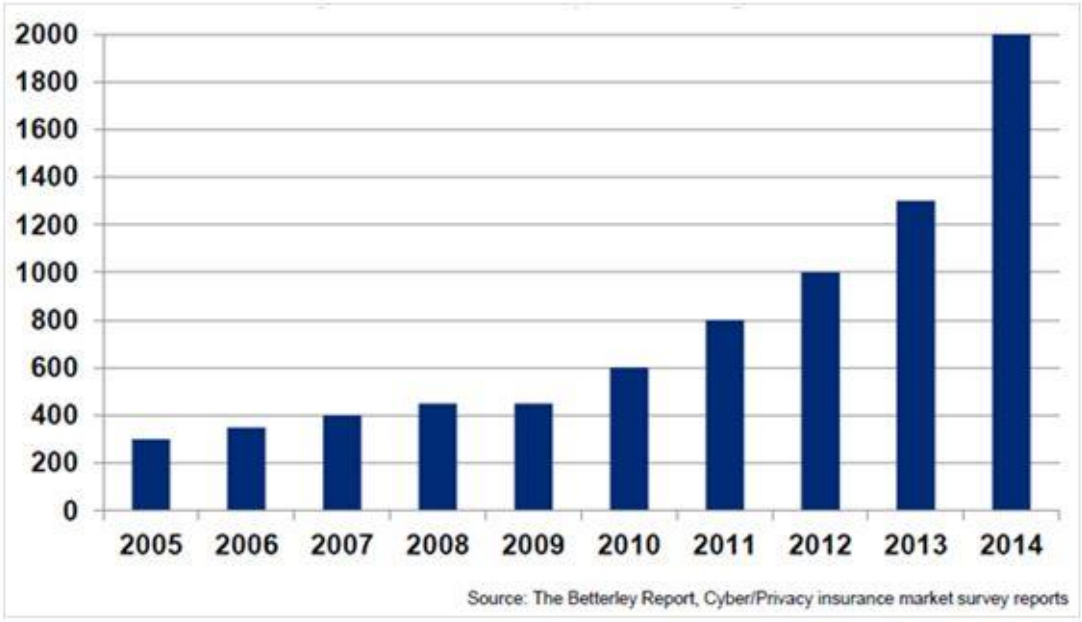

Figure 10 - Εξέλιξη της αγοράς στις ΗΠΑ

Η νέα νομοθεσία της Ευρωπαϊκής Ένωσης περί προστασίας προσωπικών δεδομένων που πρόκειται να ενσωματωθεί στο Ευρωπαϊκό δίκαιο θα φέρει μαζί της εκτός από την αναγκαία ενημέρωση εντός 24 ωρών των Αρχών Προστασίας Προσωπικών Δεδομένων, επίσης την υποχρεωτική ενημέρωση των υποκείμενων των οποίων χάθηκαν τα προσωπικά δεδομένα καθώς και διοικητικές κυρώσεις και πρόστιμα για τις εταιρίες που λόγω εσφαλμένου χειρισμού τους χάνουν δεδομένα.

Οι αλλαγές στην νομοθεσία θα μπορούσαν να αποτελέσουν καταλύτη αλλαγής της Ευρωπαικής Αγοράς του cyber insurance και να αυξήσουν σημαντικά το μέγεθός της, το οποίο μπορεί να φθάσει τα €780εκ το 2018 (Πηγή AGCS, Allianz).

Το εκτιμώμενο μέγεθος της ευρωπαϊκής αγοράς σύμφωνα με τα στοιχεία της ADVISEN είναι €224,2 εκ. για το 2015 και € 426εκ για το 2016 [7].

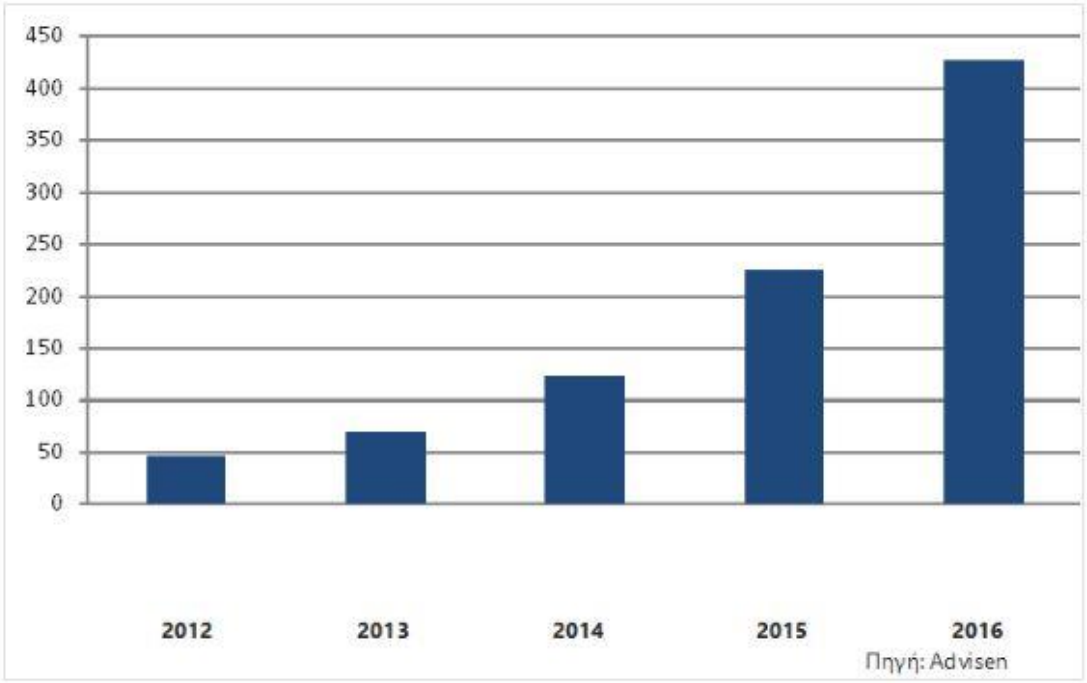

Figure 11 - Εξέλιξη της αγορά στην ΕΕ

5. Συμπεράσματα

Ο χώρος της ασφάλισης από επιθέσεις που προέρχονται από τον κυβερνοχώρο είναι μια καινούργια αγορά η οποία τα τελευταία χρόνια παρουσιάσει σημαντική ανάπτυξη παράλληλα με την ανάπτυξη που έχει η τεχνολογία και τι διαδίκτυο. Είναι μια αγορά που εμπεριέχει μεγάλο ρίσκο κυρίως γιατί ο «εχθρός» εξελίσσεται ραγδαία και καθημερινά παρουσιάζονται συνεχώς καινούργιες απειλές και αδυναμίες στα συστήματα και στις υποδομές. Όσος λοιπόν ασφαλής και να θεωρεί ότι είναι ένας οργανισμός, τέτοια προϊόντα όπως αυτά των ασφαλιστικών φορέων προσφέρουν μία δεύτερη σημαντική γραμμή άμυνας.

Σημαντικό θα ήταν να τονίσουμε ότι και η ίδια η κατεύθυνση που ορίζουν οι εκάστοτε νομοθεσίες και κανονισμοί (πχ η ψήφιση του κανονισμού GDPR), οδηγούν την αγορά και κατά συνέπεια τους οργανισμούς σε λήψη οργανωτικών μέτρων για την ασφάλεια όλων των εμπιστευτικών δεδομένων που κρατάνε στις υποδομές τους.

Η ασφάλιση Cyber Insurance αποτελεί ένα αποτελεσματικό εργαλείο διαχείρισης του υπολοιπόμενου κινδύνου (residual risk) και οι υπηρεσίες διαχείρισης περιστατικών παραβίασης ασφάλειας που παρέχει μπορούν να καταστήσουν λειτουργικό το Πλάνο Αντιμετώπισης Περιστατικών που απαιτεί ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) να έχει κάθε εταιρία.

Να μην ξεχνάμε άλλωστε ότι [8]:

«οι οργανισμοί χωρίζονται σε δύο κατηγορίες, σε αυτές που έχουν υποστεί παραβίαση και το γνωρίζουν και σε αυτές που έχουν υποστεί παραβίαση και δεν το γνωρίζουν»

Επίσης [8]:

«Χρειάζονται 20 χρόνια για να δημιουργηθεί η φήμη μιας εταιρίας και μόνο 5 λεπτά για να καταστραφεί»

Πηγές

[1]. Biener, C., Eling, M. and Wirfs, J. (2014). Insurability of Cyber Risk. 1st ed. [eBook] The Geneva Association. Available at: https://www.genevaassociation.org/media/891047/ga2014-if14-biener_elingwirfs.pdf, 2014.

[2]. LinkedIn, (2017). Cyber Risks [online] Available at: https://www.linkedin.com/pulse/cyber-risks-whatsinsurableprince-riley.

[3]. Cyber Insurance: Recent Advances, Good Practices and Challenges. (2016).1st ed. [eBook] ENISA. Available at: https://enisa.europa.eu/publilcations/cyber-insurance-recent-advances-good-practices-andchallenges

[4] Cromar Insurance brokers LTD, application form

[5] AIG, application form Greece

[6] John Robles, R., Choi, M., Cho, E., Kim, S., Park, G. and Lee, J. (2008). Common Threats and Vulnerabilities of Critical. [ebook] International Journal of Control and Automation. Available at: http://sersc.org/journals/IJCA/vol1_no1/papers/03.pdf

[7] https://www.insurancedaily.gr/dierrefsan-prosopika-dedomena-pelat/

[8] https://www.cyberinsurancegreece.com