ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΔΙΟΙΚΗΣΗ
ΕΠΙΧΕΙΡΗΣΕΩΝ

<u>Διπλωματική Εργασία</u>

ΕΥΡΩΠΑΙΚΟΣ ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ, ΚΙΝΔΥΝΟΙ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ΚΑΙ Ο ΡΟΛΟΣ ΤΗΣ ΑΣΦΑΛΙΣΗΣ ΕΝΑΝΤΙ ΤΩΝ ΔΙΑΔΙΚΤΥΑΚΩΝ ΚΙΝΔΥΝΩΝ

της

ΒΑΣΙΛΕΙΑΔΟΥ ΧΡΙΣΤΙΝΑΣ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του
μεταπτυχιακού διπλώματος ειδίκευσης στη
Διοίκηση Επιχειρήσεων

Ιανουάριος 2019

Αφιερώσεις

Σε όλους όσους με στήριξαν
κατά την διάρκεια των σπουδών μου

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κ. Ελευθεριάδη Ιορδάνη, για την αμέριστη συμπαράστασή του και την έμπρακτη βοήθειά του.

Θα ήθελα επίσης να ευχαριστήσω την οικογένειά μου αλλά και τους φίλους μου, για την ηθική υποστήριξη που μου προσέφεραν σε αυτό το ταξίδι.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας διπλωματικής εργασίας είναι η επισκόπηση τριών βασικών θεμάτων: α) του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), β) των Κινδύνων του Κυβερνοχώρου (Cyber Risks) και γ) της Ασφάλισης έναντι των Κινδύνων του Κυβερνοχώρου (Cyber Risk Insurance). Μέσα από την ενδελεχή εξέταση ορισμένων εκ των πιο καίριων ζητημάτων που αναδύονται, αποσκοπούμε σε μια, όσο το δυνατόν πιο, ολιστική περιγραφή των ανωτέρω αυτών θεμάτων. Η ανασκόπηση της παγκόσμιας βιβλιογραφίας εξυπηρετεί ακόμα περισσότερο τον στόχο της εργασίας, καθότι δίδεται η ευκαιρία στον αναγνώστη να αποκτήσει άποψη για τις πιο σύγχρονες εξελίξεις, καθώς και τους προβληματισμούς που ελλοχεύουν, τόσο για τη σοβαρότητα των κινδύνων του κυβερνοχώρου, όσο και για τους τρόπους διαχείρισης και αντιμετώπισής τους. Στο πλαίσιο αυτό, η ασφάλιση έναντι αυτής της μορφής των κινδύνων, αποτελεί ένα θέμα που προσελκύει το αυξανόμενο ενδιαφέρον της επιστημονικής και επαγγελματικής παγκόσμιας κοινότητας, δεδομένου ότι δείχνει πολλά υποσχόμενη, ως μια αποδοτική εναλλακτική μορφή διαχείρισης των κινδύνων του κυβερνοχώρου.

ΕΙΣΑΓΩΓΗ

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι διττός. Πιο συγκεκριμένα, αποσκοπεί στην παρουσίαση των σχετικών, με τους κινδύνους του κυβερνοχώρου, πληροφοριών, καθώς και στην λεπτομερή επισκόπηση των διαδικασιών και των πρακτικών που εφαρμόζονται προκειμένου να αποκτήσει μια επιχείρηση την απαιτούμενη διασφάλιση ότι είναι επαρκώς προστατευμένη έναντι των κινδύνων αυτών.

Προκειμένου να επιτευχθούν οι σκοποί της εργασίας, προχωράμε σε μια εκτενή επισκόπηση της παγκόσμιας βιβλιογραφίας που άπτεται των θεμάτων της προστασίας των προσωπικών δεδομένων, των κινδύνων του κυβερνοχώρου και της στάσης των επιχειρήσεων προς αυτούς, καθώς και της σημασίας της ασφάλισης έναντι αυτής της μορφής των κινδύνων.

Η παρούσα διπλωματική εργασία είναι χωρισμένη σε πέντε επιμέρους βασικές θεματικές ενότητες. Σε κάθε μια από αυτές παρουσιάζονται, με τρόπο διακριτό, οι πληροφορίες που σχετίζονται με τα επί μέρους ζητήματα που άπτονται του θέματος της εργασίας. Οι ενότητες της εργασίας περιλαμβάνουν, συνοπτικά, τα εξής:

1ο Κεφάλαιο

Στο πρώτο κεφάλαιο της εργασίας πραγματοποιείται μια σύντομη εισαγωγή στο θέμα της διατριβής, μέσα από την περιληπτική αναφορά στις θεματικές ενότητες του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), του Κινδύνου του Κυβερνοχώρου (Cyber Risk) και της Ασφάλισης έναντι των Κινδύνων του Κυβερνοχώρου (Cyber Insurance). Εν συνεχεία, γίνεται μια αναλυτικότερη παράθεση ορισμένων άρθρων από τον κανονισμό περί προστασίας των προσωπικών δεδομένων. Το κεφάλαιο ολοκληρώνεται με την παρουσίαση του σκοπού και των στόχων της εργασίας, καθώς και της δομής της.

2ο Κεφάλαιο

Το δεύτερο κεφάλαιο της εργασίας είναι αφιερωμένο στην επισκόπηση της παγκόσμιας βιβλιογραφίας και επιστημονικής αρθρογραφίας που άπτεται των τριών βασικών θεματικών ενοτήτων της παρούσας διατριβής, δηλαδή της συμμόρφωσης των επιχειρήσεων με τον Γενικό Κανονισμό της Προστασίας Δεδομένων, των κινδύνων που τις απειλούν και σχετίζονται με τον κυβερνοχώρο, καθώς και τον ασφαλιστικών μέτρων που λαμβάνουν έναντι των κινδύνων αυτών.

3ο Κεφάλαιο

Στο τρίτο κεφάλαιο παρουσιάζεται η θεματική ενότητα περί των κινδύνων του κυβερνοχώρου. Πιο συγκεκριμένα, επισκοπούνται πληροφορίες που σχετίζονται με την φύση και τη μορφή των κινδύνων αυτών, τις απειλές που συνεπάγονται για τις επιχειρήσεις, τον τρόπο της αναγνώρισης, της ανάλυσης, της εκτίμησης και της αντιμετώπισής τους, καθώς και το γενικότερο πλαίσιο διαχείρισής τους.

4ο Κεφάλαιο

Στο τέταρτο κεφάλαιο παρουσιάζεται η θεματική ενότητα περί της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου. Πιο συγκεκριμένα, επισκοπούνται ποικίλα μοντέλα εκτίμησης των πιθανών κινδύνων και απειλών που αφορούν τον κυβερνοχώρο, καθώς και τον τρόπο με τον οποίο μια επιχείρηση μπορεί να τα εκμεταλλευτεί προς όφελός της, αυξάνοντας την αποδοτικότητά της μέσω της αποτελεσματικότερης διαχείρισης των κινδύνων αυτών.

5ο Κεφάλαιο

Στο πέμπτο κεφάλαιο παρουσιάζονται τα συμπεράσματα της εργασίας, ο σχολιασμός των συμπερασμάτων αυτών, καθώς και οι περιορισμοί της εργασίας και οι προτάσεις για περαιτέρω έρευνα.

Η εργασία ολοκληρώνεται με την παράθεση της βιβλιογραφίας που χρησιμοποιήθηκε για την συγγραφή της.

ΚΕΦΑΛΑΙΟ 1

1.1 Θεωρητικό Υπόβαθρο της Εργασίας

Είναι κοινή πρακτική των καιρών μας ότι οι επιχειρήσεις χρησιμοποιούν όλο και περισσότερο τα προσωπικά δεδομένα των μεμονωμένων ατόμων για την παροχή υπηρεσιών, ιδίως στο διαδίκτυο, σε διάφορες μορφές, όπως για εξατομικευμένα παρεχόμενες υπηρεσίες και στοχοθετημένες διαφημίσεις. Κατά συνέπεια, πάγια απαίτηση των νομοθετικών οργάνων και των ρυθμιστικών φορέων είναι ότι οι υπηρεσίες αυτές θα πρέπει να συμμορφώνονται με τους νόμους περί προστασίας δεδομένων που διέπουν τη συλλογή και τη μετέπειτα χρήση και ανταλλαγή των προσωπικών αυτών δεδομένων. Για τον λόγο αυτό, η Ευρωπαϊκή Επιτροπή με τον Κανονισμό 2016/679, της 27ης Απριλίου 2016, προχώρησε στην ανακοίνωση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Το GDPR εφαρμόστηκε καθολικά αρχής γενομένης της 25ης Μαΐου 2018.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων είναι ένας κανονισμός της νομοθεσίας της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των δεδομένων και της ιδιωτικής ζωής για όλα τα άτομα εντός της Ευρωπαϊκής Ένωσης (Ε.Ε.) και του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ.). Αφορά επίσης την εξαγωγή δεδομένων προσωπικού χαρακτήρα εκτός των περιοχών της ΕΕ και του ΕΟΧ. Το GDPR αποσκοπεί πρωτίστως στον να δώσει στα μεμονωμένα πρόσωπα τον έλεγχο των προσωπικών δεδομένων τους και στην απλούστευση του ρυθμιστικού περιβάλλοντος για τις διεθνείς επιχειρήσεις με την ενοποίηση του κανονισμού εντός της ΕΕ (Pandit et al., 2018)[1].

Επιγραμματικά, ο κανονισμός GDPR δίνει στους πολίτες της ΕΕ νέα δικαιώματα σε σχέση με τα προσωπικά τους δεδομένα, όπως, μεταξύ άλλων, το δικαίωμα να αποσύρουν τη συγκατάθεσή τους, καθώς και ευκολότερη πρόσβαση στα δεδομένα που τους ανήκουν. Αναγκάζει τις

[1] Pandit, H., J., O' Sullivan, D. and Lewis, D. (2018), "Queryable Provenance Metadata For GDPR Compliance", *SEMANTiCS 2018 – 14th International Conference on Semantic Systems*, Procedia Computer Science

επιχειρήσεις να αναλάβουν μεγαλύτερη ευθύνη για τα δεδομένα χρηστών τα οποία συλλέγουν και να εξασφαλίσουν ότι κάνουν ό,τι καλύτερο μπορούν για την προστασία των δεδομένων αυτών. Δύο είναι οι λόγοι που οδήγησαν στη δημιουργία αυτού του κανονισμού. Ο πρώτος είναι οι ίδιοι οι πολίτες να έχουν τον έλεγχο των δεδομένων τους. Οι εταιρείες δεν μπορούν πλέον να συλλέγουν οποιαδήποτε πληροφορία επιθυμούν, αν δεν συντρέχει σοβαρός λόγος. Δεύτερον, κάθε χώρα έχει χωριστή νομοθεσία για τον έλεγχο των δεδομένων των χρηστών.

Σύμφωνα με την Ευρωπαϊκή Επιτροπή[2], τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα. Επιπλέον, τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (European General Data Protection Regulation – GDPR).

Στο άρθρο 4 του Κανονισμού 2016/679, αναφέρεται ότι με τον όρο δεδομένα προσωπικού χαρακτήρα νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα με τέτοιον τρόπο ώστε το άτομο να μην είναι ή να μην είναι πια ταυτοποιήσιμο δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη. Ο Γενικός Κανονισμός Προστασίας Δεδομένων προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την

[2] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή. Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει το GDPR.

Δεδομένης της σημασίας της προστασίας των προσωπικών δεδομένων, το εύλογο ζήτημα που ανακύπτει είναι αυτό της επεξήγησης, της κατανόησης, του εντοπισμού και της αντιμετώπισης του κινδύνου από τον οποίο απειλούνται οι πληροφορίες αυτές, με άλλα λόγια του κινδύνου του κυβερνοχώρου (cyber risk). Στις ανεπτυγμένες και αναπτυσσόμενες οικονομίες η χρήση της τεχνολογίας των πληροφοριών και των επικοινωνιών έχει αυξηθεί τα τελευταία 30 χρόνια για να καλύψει τις περισσότερες πτυχές της καθημερινής ζωής. Τα άτομα, οι επιχειρήσεις και οι κυβερνήσεις βασίζονται σε διασυνδεδεμένες ψηφιακές συσκευές οι οποίες φαινομενικά αγγίζουν κάθε βιομηχανία και κάθε έκφανση της καθημερινότητας. Η τεχνολογία έχει γνωρίσει μια εκρηκτική άνθιση με τον πολλαπλασιασμό των διάφορων συσκευών, καθώς και με τις συνεχείς και αλληλοσυνδεόμενες ιδιότητες τους.

Όπως χαρακτηριστικά αναφέρει ο Geer (2010)[3], φαίνεται ότι προτιμούμε να βασιζόμαστε ολοένα και περισσότερο στο Διαδίκτυο των Πραγμάτων (Internet of Things) επειδή τα οφέλη της χρήσης του αντισταθμίζουν τους συγκεντρωτικούς κινδύνους που αυτό εγκυμονεί, ενώ συμπληρώνει επίσης ότι «μια τεχνολογία που μπορεί να μας δώσει ό,τι επιθυμούμε μπορεί πολύ εύκολα να μετατραπεί και σε μια τεχνολογία που μπορεί μας πάρει όλα όσα έχουμε».

Ένας τρόπος προστασίας έναντι των κινδύνων του κυβερνοχώρου είναι η ασφάλιση έναντι των κινδύνων αυτών (cyber insurance). Σύμφωνα με τον Marsh (2014)[4], οι πρώτες ρυθμιστικές πολιτικές περί προσδιορισμού, αντιμετώπισης και ασφάλισης έναντι των κινδύνων του κυβερνοχώρου, σχεδιάστηκαν κατά τη δεκαετία του 1990 και επί της ουσίας εστίαζαν στην κάλυψη της ευθύνης τρίτων για τις αρνητικές επιπτώσεις από τη χρήση κακόβουλου λογισμικού. Έκτοτε, τα πράγματα έχουν αλλάξει σημαντικά και έχουν πραγματοποιηθεί γενναία βήματα προς την

[3] Geer, D., E. (2010), "Cybersecurity and National Policy," *Cybersecurity National Policy,* Vol. 1, pp: 203–215

[4] Marsh. (2014), "Cyber gap insurance," *Global Energy Practice*

ουσιαστικότερη νομοθετική ρύθμιση περί της ασφάλισης των κινδύνων του κυβερνοχώρου. Η ζήτηση για παροχή υπηρεσιών ασφάλισης έναντι των κινδύνων του κυβερνοχώρου, υψηλών προδιαγραφών και ποιότητας, έχει οδηγήσει στην ραγδαία άνθιση του επαγγέλματος αυτού. Σύμφωνα με σχετική έκθεση της Allianz (2015)[5], η αγορά αυτή, στο σύνολό της, προβλέπεται να φθάσει τα 20 δισεκατομμύρια δολάρια μέχρι το 2025. Σύμφωνα με την έκθεση αυτή, οι ΗΠΑ κατέχουν το μερίδιο του λέοντος στην αγορά ασφάλισης στον κυβερνοχώρο σε ποσοστό που ανέρχεται, περίπου, στο 90% της παγκόσμιας αγοράς των 2 δισεκατομμυρίων δολαρίων. Ωστόσο, υπογραμμίζεται ότι η εικόνα αυτή ενδεχομένως να αλλάξει κατά την επόμενη δεκαετία, δεδομένου ότι ο ευρωπαϊκός κανονισμός για την προστασία των προσωπικών δεδομένων, ο οποίος συνεπάγεται αυστηρές κυρώσεις για τη μη συμμόρφωση, θα τεθεί σε ισχύ από το 2018.

1.2 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Όπως έχει αναφερθεί και ανωτέρω, ο Γενικός Κανονισμός Προστασίας Δεδομένων θεσπίζει τους κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα. Βασικό στόχος του κανονισμού είναι η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα του δικαιώματός τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Στο άρθρο 1 του Κανονισμού 2016/679, αναφέρεται χαρακτηριστικά ότι η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Στο άρθρο 2 προσδιορίζεται ότι ο Κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. Η παραπάνω φράση συμπληρώνεται από τις αναφορές στο τρίτο άρθρο του σχετικού κανονισμού στο οποίο αναφέρεται ότι το πεδίο εφαρμογής του εμπίπτει στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων

[5] Allianz Global Corporate Specialty. (2015), “A Guide to Cyber Risk”

μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ευρωπαϊκή Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ευρωπαϊκής Ένωσης. Επιπλέον, ο κανονισμός εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ευρωπαϊκή Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου. Ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ευρωπαϊκή Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ευρωπαϊκή Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:

- Την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ευρωπαϊκή Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή
- Την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ευρωπαϊκής Ένωσης.

1.2.1 Αρχές που Διέπουν την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

Στο άρθρο 5 του κανονισμού παρατίθενται οι αρχές που διέπουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Βάσει αυτού, τα δεδομένα προσωπικού χαρακτήρα:

- Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»).
- Συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς. («περιορισμός του σκοπού»).
- Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»).
- Είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται. Πρέπει επίσης να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»).

- ❖ Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»).
- ❖ Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).
- ❖ Τέλος, ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τα όσα προβλέπονται στον σχετικό κανονισμό («λογοδοσία»).

1.2.2 Νομιμότητα της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις, σύμφωνα με το άρθρο 6 του κανονισμού:

- ✓ Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.
- ✓ Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.
- ✓ Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας.
- ✓ Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.

- ✓ Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
- ✓ Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

1.2.3 Διαφανής Ενημέρωση

Μεταξύ των σημαντικότερων προϋποθέσεων για την συγκατάθεση του υποκείμενου των δεδομένων του δικαιώματος χρήσης και επεξεργασίας των προσωπικών του δεδομένων, το άρθρο 7 του κανονισμού αναφέρει ότι, όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα. Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση.

Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της. Επιπροσθέτως, κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

Στο άρθρο 12, περί της διαφανούς ενημέρωσης, ανακοίνωσης και των ρυθμίσεων για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων, επεξηγείται περαιτέρω ότι ο υπεύθυνος επεξεργασίας των προσωπικών δεδομένων λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία των δεδομένων του, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά. Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα.

Στα άρθρα 13 και 14 του κανονισμού προσδιορίζονται οι πληροφορίες που θα πρέπει να παρέχονται προς το υποκείμενο των δεδομένων, είτε εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων (άρθρο 13), είτε εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων (άρθρο 14). Βάσει των όσων αναφέρονται, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες:

- Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας.
- Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση.
- Τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία.
- Τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο.
- Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν.
- Κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής.

Εκτός από τις ανωτέρω πληροφορίες, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων τις εξής επιπλέον πληροφορίες που είναι αναγκαίες για την εξασφάλιση θεμιτής και διαφανούς επεξεργασίας:

- Το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα.
- Την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων.
- Την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της.
- Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.
- Κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών.
- Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ και σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

1.2.4 Δικαίωμα Διόρθωσης, Διαγραφής, Εναντίωσης και Περιορισμού της Επεξεργασίας

Στο άρθρο 16 αναφέρεται ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

Όσον αφορά την διαγραφή των προσωπικών δεδομένων, στο άρθρο 17 αναφέρεται ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

A. Τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
B. Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία.
C. Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία.
D. Τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα.
E. Τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.
F. Τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών.

Σχετικά με το δικαίωμα εναντίωσης περί της χρήσης και επεξεργασίας των προσωπικών δεδομένων, το άρθρο 21 αναφέρει ότι το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, περιλαμβανομένης της κατάρτισης προφίλ. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση. Επιπλέον, όταν τα υποκείμενα των δεδομένων

αντιτίθενται στην επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς.

Αναφορικά με το δικαίωμα του περιορισμού της επεξεργασίας των προσωπικών δεδομένων, στο άρθρο 18 προσδιορίζεται ότι το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα:

- Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα.
- Η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους.
- Ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.
- Το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 του κανονισμού, παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

ΚΕΦΑΛΑΙΟ 2

ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΒΙΒΛΙΟΓΡΑΦΙΑΣ

2.1 Εισαγωγή

Στο παρόν κεφάλαιο επικεντρωνόμαστε στην επισκόπηση της παγκόσμιας αρθρογραφίας και βιβλιογραφίας που άπτεται τριών βασικών θεμάτων: α) των προκλήσεων που αναδύονται από τον ερχομό και την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), β) των κινδύνων του κυβερνοχώρου (cyber risks) και γ) της προστασίας-ασφάλισης έναντι των κινδύνων του κυβερνοχώρου (cyber risk insurance).

2.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων

Σε μια προσπάθεια επισκόπησης των συζητήσεων, καθώς και τον προκαταρκτικών εγγράφων που προηγήθηκαν της δημοσίευσης του GDPR, οι Hert και Papakonstantinou (2016)[6], παρέθεσαν τις θέσεις τους αναφορικά με την αποτελεσματικότητα του νέου αυτού Κανονισμού για την προστασία των προσωπικών δεδομένων, συγκρίνοντας, κατά κύριο λόγο, τα αρχικά κείμενα της Κομισιόν επί του θέματος και τις μεταγενέστερες σχετικές δημοσιεύσεις. Σύμφωνα με τους συγγραφείς, αν και ορισμένες αλλαγές και τροποποιήσεις στο κείμενο του Κανονισμού, εγείρουν σημαντικά ερωτήματα και συζητήσεις, εντούτοις ο αυτοσκοπός του παρέμεινε αναλλοίωτος και για τον λόγο αυτό επικροτούν τόσο τον ερχομό του, όσο και τις θετικές αλλαγές που θα επιφέρει στην παγκόσμια κοινότητα. Ωστόσο, η πάγια θέση των επιστημόνων είναι ότι η Κομισιόν δεν θα πρέπει να επαναπαυθεί από την όποια επιτυχία και αποδοχή γνωρίσει ο νέος αυτός Κανονισμός, αλλά οφείλει να βρίσκεται σε συνεχή επαγρύπνηση προκειμένου να επιτυγχάνει συνεχείς βελτιώσεις και να μετριάζει τις όποιες αμβλώσεις προκληθούν στην πορεία.

[6] De Hert, P. and Papakonstantinou, V. (2016), "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", *Computer Law & Security Review,* 32 (2), pp. 179-194

Σε μια προσπάθεια να επισημάνουν τις νέες αλλαγές που φέρνει ο GDPR, οι Ryz και Crest (2016)[7], αναφέρουν ότι λόγω της πολυπλοκότητάς του, το χρονοδιάγραμμα, μέχρι και την τελική του προώθηση και επίσημη εφαρμογή, δεν αφήνει αρκετό χρόνο για τις ίδιες τις επιχειρήσεις, τις δικηγορικές και συμβουλευτικές εταιρίες, καθώς και τους παρόχους ηλεκτρονικών υπηρεσιών να προκειμένου να κατανοήσουν πλήρως τις απαιτήσεις του Κανονισμού και να αποκτήσουν μια πιο αποκρυσταλλωμένη εικόνα σχετικά με τις προκλήσεις της εφαρμογής του. Μεταξύ των τριών βασικών σημείων που σχολιάζουν, αναφέρουν ότι το γεγονός του ότι πρόκειται για έναν ενιαίο κανονισμό συνεπάγεται μια πιο ταχεία ενσωμάτωση και υιοθέτηση από τις κατά τόπους εγχώριες νομοθεσίες των χωρών της Ε.Ε. Σχετικά με τις επιπτώσεις του Κανονισμού στην ηλεκτρονική ανακάλυψη (e-discovery) αναφέρουν ότι ακόμα η κατάσταση είναι σχετικά θολή προκειμένου να μπορούν να εξαχθούν συμπεράσματα, ενώ όσον αφορά την πιο άμεση ταυτοποίηση των χρηστών αναγνωρίζουν το πρόκειται για ένα θετικό βήμα καθόσον έτσι θα μειωθεί η απαίτηση για περιττή διακίνηση προσωπικών δεδομένων, πράγμα που μειώνει και τον δυνητικό κίνδυνο απώλειας των δεδομένων αυτών.

Με σαφή προσανατολισμό υπέρ της υπεράσπισης του GDPR, καθώς και των όσων εισαγάγει και προωθεί ο νέος αυτός κανονισμός, ο Zerlang (2017)[8], επεξηγεί στο σχετικό του άρθρο, συνοπτικά, τις επιπτώσεις του κανονισμού στο επιχειρηματικό γίγνεσθαι. Σύμφωνα με τα όσα αναφέρει, ένα από τα σημαντικότερα οφέλη του GDPR είναι το ότι άπτεται ενός μεγάλου φάσματος εννοιών και ζητημάτων που χρήζουν αντιμετώπισης. Ο κανονισμός έχει σχεδιαστεί με γνώμονα το μέλλον, καθορίζοντας την ελάχιστη βασική γραμμή ασφάλειας στην οποία θα υπόκεινται τα δεδομένα, σε αντίθεση με την ελάχιστη απαίτηση για την εξασφάλισή τους. Το επίκεντρο είναι πολύ ευρύτερο (από αυτό που όριζε ο προηγούμενος κανονισμός), υποκινώντας τις εταιρείες να εξασφαλίσουν τα συστήματά τους για να αποφευχθούν οι παραβιάσεις δεδομένων όπου είναι δυνατόν. Αυτό σημαίνει ότι σε ένα συνεχώς εξελισσόμενο ψηφιακό τοπίο, ο κανονισμός θα πρέπει να παραμείνει σχετικός με τις σύγχρονες επιχειρηματικές πρακτικές για τα επόμενα χρόνια. Επιπροσθέτως, ο συγγραφέας σχολιάζει ότι ένα βασικό αποτέλεσμα αυτής της προσέγγισης είναι η υιοθέτηση ανθεκτικών και συνεκτικών δομών στον κυβερνοχώρο (cyber-

[7] Ryz, L. and Crest, L. (2016), "A new era in data protection", *Computer Fraud & Security*, 2016 (3), pp. 18-20

[8] Zerlang, J. (2017), "GDPR: a milestone in convergence for cybersecurity and compliance", *Network Security*, 17 (6), pp. 8-11

resilience), μιας αλλαγής στην αντίληψη που αναγνωρίζει ότι θα υπάρξουν επιθέσεις στον κυβερνοχώρο και συνεπώς οι επιχειρήσεις θα πρέπει να είναι κατάλληλα προετοιμασμένες για αυτό το ενδεχόμενο. Σύμφωνα με τα όσα προβλέπει το GDPR, αποτελεί αδιαπραγμάτευτη ευθύνη της κάθε επιχείρησης να προετοιμαστεί και να μετριάσει τις προκλήσεις που δύναται να προκληθούν από μια επίθεση στον κυβερνοχώρο της, επιστρέφοντας στη συνήθη επιχειρηματική της πρακτική όσο το δυνατόν συντομότερα και παρέχοντας την απαιτούμενη διασφάλιση ότι τα προσωπικά δεδομένα των χρηστών δεν απειλούνται από εγγενείς κινδύνους.

Ο Krystlik (2017)[9], εστιάζει στην απαραίτητη προετοιμασία των επιχειρήσεων προκειμένου να επιτύχουν όλες τις αναγκαίες προεργασίες έτσι ώστε να μπορούν να υποδεχθούν όσο πιο ομαλά γίνεται τον νέο Κανονισμό. Μεταξύ άλλων, αναφέρει τις πέντε βασικές υποχρεώσεις των επιχειρήσεων που απαιτούνται προκειμένου να συμμορφωθούν με τις απαιτήσεις του GDPR. Αυτές είναι: α) να διασφαλίσουν ότι το δικαίωμα του κάθε χρήστη στη λήθη είναι εύκολο να εντοπισθεί και να επιλεχθεί, εφόσον ο χρήστης το επιθυμεί, β) να παρέχουν μια σαφή φόρμα μέσω της οποίας ο ενδιαφερόμενος να μπορεί να δώσει την ρητή του συγκατάθεση για την επεξεργασία των προσωπικών του δεδομένων, γ) να εξασφαλίσουν τις απαιτούμενες διαδικασίες έτσι ώστε τα δεδομένα να μεταφέρονται από έναν πάροχο υπηρεσιών σε άλλο γρήγορα, εύκολα και πρωτίστως με ασφάλεια, δ) να ορίσουν έναν υπεύθυνο επεξεργασίας δεδομένων, ο οποίος θα πρέπει να είναι σε επαφή με οποιαδήποτε εποπτική αρχή, εφόσον παραστεί μια τέτοια ανάγκη και ε) να εξασφαλίσουν ότι η επεξεργασία δεδομένων πραγματοποιείται μέσω τεκμηριωμένων διαδικασιών, είτε η επιχείρηση διεξάγει αυτές τις διαδικασίες η ίδια είτε αυτές διενεργούνται για λογαριασμό της επιχείρησης.

Με θέμα την διερεύνηση των επιπτώσεων του GDPR, καθώς και των αλλαγών που επιφέρει για τις εταιρείες συλλογής προσωπικών δεδομένων και οι οποίες δύναται να επηρεάσουν την διαχείριση των δεδομένων αυτών καθώς και να διαταράξουν την επιχειρηματική τους δραστηριότητα, ασχολήθηκαν στην εργασία τους οι Tikkinen et al. (2018)[10]. Για τον σκοπό αυτό, προσδιόρισαν και ταξινόμησαν τις βασικές πρακτικές συνέπειες των επερχόμενων αυτών αλλαγών, αναπτύσσοντας ένα πλαίσιο στο οποίο παρουσίασαν 12 πτυχές αυτών των επιπτώσεων και τις

[9] Krystlik, J. (2017), "With GDPR, preparation is everything", *Computer Fraud & Security*, 2017 (6), pp. 5-8

[10] Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review*, 34 (1), pp. 134-153

αντίστοιχες οδηγίες για τον τρόπο προετοιμασίας για τις νέες απαιτήσεις του Κανονισμού. Σύμφωνα με τις αρθρογράφους, αυτές οι πτυχές καλύπτουν επιχειρηματικές στρατηγικές και πρακτικές, καθώς και οργανωτικά και τεχνικά μέτρα. Τέλος, προτρέπουν τις εταιρείες να συμβουλευθούν και να χρησιμοποιήσουν ορισμένες από τις υπάρχουσες κατευθυντήριες γραμμές που άπτονται των ιδιαίτερων επιχειρηματικών τους δραστηριοτήτων τους έτσι ώστε να υποστηρίξουν αποτελεσματικότερα την προετοιμασία τους για τις επερχόμενες αλλαγές του θα επιφέρει ο GDPR.

Σε σχετικό άρθρο με κεντρικό θέμα το βαθμό ετοιμότητας των αμερικάνικων, κυρίως, επιχειρήσεων, ως προς τις επερχόμενες αλλαγές που θα επέφερε ο Γενικός Κανονισμός Προστασίας Δεδομένων, δημοσίευσε τις θέσεις του ο Miglicco (2018)[11]. Σύμφωνα με τα όσα αναφέρει, δεν είναι λίγοι οι ερευνητές που επισημαίνουν το γεγονός ότι δεκάδες αμερικάνικες επιχειρήσεις έχουν σοβαρή έλλειψη ενημέρωσης ή ανησυχίας σχετικά με αυτούς τους κανονισμούς, ενώ αντίστοιχα μεγάλος είναι και ο αριθμός των όσων διοικούντων πιστεύουν ότι είναι ένας ευρωπαϊκός νόμος που ισχύει μόνο για την Ευρωπαϊκή Ένωση, όχι για τις ΗΠΑ και τις υπόλοιπες χώρες του κόσμου. Τέλος, ο αρθρογράφος υπογραμμίζει το ότι υπάρχουν οφέλη, ειδικά για τις μικρές και μεσαίες επιχειρήσεις, από την άμεση συμμόρφωση με τα όσα προβλέπει το GDPR, αφού μέσω αυτής δύναται να βελτιωθεί η επιχειρησιακή αποτελεσματικότητα, τόσο μέσω της προδραστικότητας στις νέες μεγάλες επερχόμενες αλλαγές, όσο και μέσω της μακροπρόθεσμης εξοικονόμησης σημαντικών κονδυλίων, ενώ παράλληλα αναγνωρίζει το ότι αργά ή γρήγορα, ένας αντίστοιχος κανονισμός θα έρθει και στις ΗΠΑ.

Σε μια έρευνα αναφορικά με το τι συνεπάγεται ο GDPR για την ιατρική κοινότητα, η McCall[12] προχώρησε στην διενέργεια προσωπικών συνεντεύξεων με υψηλόβαθμα στελέχη μεγάλων ιατρικών εταιριών, τις οποίες και παρουσίασε στο δημοσιευμένο άρθρο της. Το βασικό συμπέρασμα της δημοσίευσης είναι ότι η ιατρική κοινότητα φαίνεται αρκετά προβληματισμένη ως προς τις απαιτήσεις του Κανονισμού για την διαχείριση των πραγματικών δεδομένων (real world data), τα οποία όμως είναι ανυπολόγιστης αξίας για την μακροπρόθεσμη παροχή προϊόντων και υπηρεσιών υψηλής ποιότητας και στην οποία μπορεί οι μεμονωμένοι χρήστες να μην παρέχουν

[11] Miglicco, G. (2018), "GDPR is here and it is time to get serious", *Computer Fraud and Security*, 2018 (9), pp. 9-11

[12] McCall, B. (2018), "What does the GDPR mean for the medical community?", *The Lancet*, 391 (20127), pp. 1249-1250

την συγκατάθεσή τους, γεγονός που δημιουργεί προβλήματα και εγείρει ουσιώδεις αντιφάσεις μεταξύ της συμμόρφωσης με την ισχύουσα νομοθεσία και την προστασία και βελτίωση της ανθρώπινης ζωής.

Σύμφωνα με τον Gellert (2018)[13], ένα ιδιαίτερα σημαντικό στοιχείο που αναφέρεται στον GDPR και πιο συγκεκριμένα στην παράγραφο 35 αυτού, περί της υποχρέωσης διενέργειας αξιολογήσεων των επιπτώσεων για την προστασία των δεδομένων, είναι αυτό της έννοιας του ρίσκου-κινδύνου, καθώς και της διαχείρισής του. Βάσει των όσων αναφέρει, η υιοθέτηση αυτής της προσέγγισης με βάση τον κίνδυνο δεν έρχεται χωρίς αρκετές συζητήσεις και αμφισβητήσεις, κυρίως σχετικά με το πεδίο εφαρμογής και την έννοια της προσέγγισης που βασίζεται στον κίνδυνο. Ωστόσο, αυτό που έχει μείνει μέχρι στιγμής εκτός συζήτησης είναι η ίδια η έννοια του κινδύνου, από την οποία πηγάζει την όλη προσέγγιση που βασίζεται στον κίνδυνο. Ο αρθρογράφος υπογραμμίζει το γεγονός ότι είναι υποδεέστερης σημασίας το πως ορίζεται ο κίνδυνος στις κανονιστικές διατάξεις του GDPR, ενώ βασική προτεραιότητα όλων θα πρέπει να είναι ο προσδιορισμός της βέλτιστης μεθοδολογίας για την προσέγγιση του αντιληπτού κινδύνου (perceived risk), καθώς και η αναγνώριση των ουσιωδών κινδύνων που συνεπάγεται η καθημερινή πρακτική.

Η Wachter (2018)[14], επισκόπησε στην εργασία της το κατά πόσο ο Γενικός Κανονισμός Προστασίας Δεδομένων μπορεί να παράσχει ουσιαστική καθοδήγηση για την επίτευξη της ισορροπίας μεταξύ των συμφερόντων των παρόχων του Διαδικτύου των Πραγμάτων (Internet of Things) και των χρηστών του Διαδικτύου, εστιάζοντας σε δύο βασικά ζητήματα, αυτά της ιδιωτικότητας και της αναγνωρισιμότητας στο διαδίκτυο. Σύμφωνα με την συγγραφέα, εντοπίζονται τέσσερις πυλώνες πάνω στους οποίους μπορεί να οικοδομηθεί αποτελεσματικά αυτή η ισορροπία και είναι: α) σαφής προσδιορισμός του προφίλ των χρηστών, β) οριοθέτηση του ελέγχου της χρήσης των προσωπικών δεδομένων και ουσιαστική κατανόηση της ευαισθησίας της ταυτότητας του κάθε μεμονωμένου χρήστη, γ) ξεκάθαρες διαδικασίες ως προς τη συναίνεση του χρήστη για την επεξεργασία των προσωπικών του δεδομένων και ελαχιστοποίηση της

[13] Gellert, R. (2018), "Understanding the notion of risk in the General Data Protection Regulation", *Computer Law & Security Review,* 34 (2), pp. 279-288

[14] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR*", Computer Law & Security Review,* 34 (3), pp. 436-449

αβεβαιότητας μέσω διαφανών πρακτικών και δ) επένδυση στην ειλικρίνεια, την εμπιστοσύνη και την διαφάνεια.

Στο πολύ ενδιαφέρον άρθρο των Politou et al. (2018)[15], επισκοπείται το θέμα της δημιουργίας αντιγράφων ασφαλείας (backups) και του δικαιώματος στη λήθη (right to be forgotten). Σύμφωνα με τα όσα αναφέρουν οι συγγραφείς, η πρόσφατη εφαρμογή του GDPR έχει επιβάλει πρόσθετα βάρη στους υπεύθυνους επεξεργασίας δεδομένων που λειτουργούν εντός της ΕΕ. Πέραν των άλλων προκλήσεων, η άσκηση του δικαιώματος της λήθης από άτομα που ζητούν τη διαγραφή των προσωπικών τους πληροφοριών έχει επίσης γίνει ένα ακανθώδες ζήτημα όταν εφαρμόζεται σε αντίγραφα ασφαλείας και αρχεία, έτσι όπως τουλάχιστον αυτά καθορίζονται από τα σύγχρονα πρότυπα ασφαλείας. Μέσα από την εξέταση των πιθανών συνεπειών που συνεπάγεται η εξάσκηση του δικαιώματος της λήθης, σύμφωνα με τα τρέχοντα συστήματα δημιουργίας αντιγράφων ασφαλείας, οι συγγραφείς επισημαίνουν ορισμένες προτεινόμενες οργανωτικές, επιχειρηματικές και τεχνικές προκλήσεις που σχετίζονται με τα ευρέως γνωστά πρότυπα δημιουργίας αντιγράφων ασφαλείας, τις πολιτικές διατήρησης δεδομένων, τα εφεδρικά μέσα, τις υπηρεσίες αναζήτησης και τα συστήματα ERP.

Με κεντρικό θέμα τις αντιδράσεις ορισμένων επιχειρήσεων μετά την υποχρεωτική εφαρμογή του GDPR, ασχολήθηκε στο άρθρο του ο Datoo (2018)[16], κάνοντας ειδική αναφορά στην επιχειρηματική πρακτική των Chicago Times και LA Times (επιχειρήσεις που δραστηριοποιούνται στον χώρο της έντυπης και ηλεκτρονικής ενημέρωσης, με έδρα τις ΗΠΑ). Σύμφωνα με τα όσα αναφέρει, δεδομένου ότι οι ανωτέρω επιχειρήσεις διαπίστωσαν ότι δεν έχουν κάνει όλες τις απαραίτητες ενέργειες προκειμένου να συμμορφωθούν με τις απαιτήσεις του GDPR – και υπό τον πανικό και τον φόβο επικείμενων κυρώσεων σε περίπτωση που έρχονταν αντιμέτωπες μηνύσεις χρηστών – αποφάσισαν να μπλοκάρουν την είσοδο στις υπηρεσίες τους για τους χρήστες της Ε.Ε., θεωρώντας πως έτσι δεν θα είναι πλέον υπόλογες προς τις απαιτήσεις του νόμου αυτού. Κάτι τέτοιο ωστόσο, σύμφωνα με τον αρθρογράφο χαρακτηρίζεται ως μια έντονα τοξική και εσφαλμένη επιχειρηματική πρακτική, που μόνο αρνητικές συνέπειες (οικονομικές,

[15] Politou, E., Michota, A., Alepis, E., Pocs, M. and Patsakis, K. (2018), "Backups and the right to be forgotten in the GDPR: An uneasy relationship", *Computer Law & Security Review*, 34 (6), pp. 1247-1257

[16] Datoo, A. (2018), "Data in the post-GDPR world", *Computer Fraud & Security*, 2018 (9), pp. 17-18

φήμης, υποψίες για παράνομες ενδεχομένως πρακτικές που η επιχείρηση δεν θέλει να σταματήσει ή να έρθουν στο φως της δημοσιότητας κ.λπ) μπορεί να έχει για όποιον την ακολουθήσει.

Οι Bendiek και Romer (2018)[17], επιχειρούν να εξηγήσουν στην δημοσίευσή τους, το πώς η ΕΕ σχεδιάζει να προωθήσει το δικό της καθεστώς προστασίας δεδομένων σε τρίτα κράτη και ειδικότερα στις ΗΠΑ. Σύμφωνα με τους συγγραφείς, δεδομένου ότι οι ψηφιακές υπηρεσίες έχουν καταστεί κεντρικό στοιχείο της διατλαντικής οικονομίας, ένα σημαντικό μέρος αυτού του διεθνούς εμπορίου συνδέεται με τη μεταφορά δεδομένων, απαιτώντας πολλά από τα νέα προϊόντα και υπηρεσίες που αναδύονται να τηρούν ορισμένα βασικά πρότυπα προστασίας δεδομένων.

Τέλος, ο Garber (2018)[18], προσπαθεί να διερευνήσει στο άρθρο του, το κατά πόσο ο νέος αυτός Κανονισμός αποτελεί τροχοπέδη ή μια ουσιαστική ευκαιρία για τις επιχειρήσεις. Σύμφωνα με τα όσα αναφέρει, δεν είναι λίγες οι επιχειρήσεις που υποστηρίζουν ότι ο GDPR είναι είτε αρκετά περιοριστικός, είτε προσδοκά δυσανάλογα πολλά (σε σχέση με το υπάρχον τουλάχιστον καθεστώς) από αυτές. Από την άλλη πλευρά, μπορεί ναι μεν να γνωρίζουν και να κατανοούν τις απαιτήσεις που εισάγονται στο προσκήνιο, ωστόσο δεν δίδονται σαφείς διευκρινιστικές οδηγίες ως προς το πως θα πρέπει να υλοποιηθούν οι απαιτούμενες αλλαγές. Παρόλα αυτά, ο αρθρογράφος προτρέπει όλους τους ενδιαφερόμενους να στηρίξουν το νέο αυτό Κανονισμό, υπογραμμίζοντας το γεγονός ότι το πρώτο – και δυσκολότερο – βήμα για την πλήρη συμμόρφωση με αυτόν, είναι ο σαφής προσδιορισμός των κινδύνων που σχετίζονται με την επιχείρηση. Από εκεί και πέρα, ο σχεδιασμός του επιχειρησιακού τεχνολογικού πλάνου πορείας θα πρέπει να υλοποιηθεί από ανθρώπους που έχουν βαθιά γνώση των ζητημάτων που δύναται να ανακύψουν προκειμένου να επιτευχθεί η πλήρης συμμόρφωση με τις απαιτήσεις του Κανονισμού.

---

[17] Bendiek, A. and Römer, M. (2018), "Externalizing Europe: the global effects of European data protection", Digital Policy, Regulation and Governance, [online], Διαθέσιμο στο: https://doi.org/10.1108/DPRG-07-2018-0038, (Ημερομηνία Πρόσβασης, 18/11/2018)

[18] Garber, J. (2018), "GDPR – compliance nightmare or business opportunity?", *Computer Fraud & Security*, 2018 (6), pp. 14-15

2.3 Οι Κίνδυνοι του Κυβερνοχώρου (Cyber Risks) και η Προστασία έναντι αυτών (Cyber Security)

Μια ενδιαφέρουσα επισκόπηση πάνω στο ζήτημα των κινδύνων του κυβερνοχώρου έρχεται από τους Garg et al. (2003)[19], οι οποίοι ορμώμενοι από την αποτελεσματική θεωρία της αγοράς, χρησιμοποίησαν μια μεθοδολογία μελέτης γεγονότων για να μετρήσουν έμμεσα τον οικονομικό αντίκτυπο των παραβιάσεων ασφαλείας του Διαδικτύου στην πορεία της απόδοσης των μετοχών, των παραβιαζόμενων επιχειρήσεων (και επίσης στους παρόχους ασφάλειας στο Διαδίκτυο). Όπως αναφέρουν οι ερευνητές, σύμφωνα με την αποτελεσματική υπόθεση της αγοράς, όλες οι πληροφορίες για παρελθόντα και μελλοντικά γεγονότα εντός μιας επιχείρησης (ή της βιομηχανίας) θα πρέπει να αντικατοπτρίζονται στην τιμή των μετοχών, η οποία αντανακλά τις πεποιθήσεις των επενδυτών σχετικά με τις μελλοντικές ταμειακές ροές προς τους επενδυτές. Η παραβίαση της ασφάλειας μπορεί να οδηγήσει σε επανεξέταση της μελλοντικής ευπάθειας καθώς και του μελλοντικού νομικού κινδύνου και, ως εκ τούτου, αντικατοπτρίζει μια αξιολόγηση της επίδρασης της αγοράς στις ταμειακές ροές διαφορετική από την αναφερθείσα οικονομική ζημία (η οποία μπορεί να είναι και προκατειλημμένη). Χρησιμοποιώντας τη μεθοδολογία της μελέτης συμβάντων την οποία και εφάρμοσαν σε 22 γεγονότα παραβίασης της ασφάλειας στον κυβερνοχώρο, διαπίστωσαν ότι οι διαρκείς επιδράσεις στις τιμές των μετοχών των παραβιάσεων ασφαλείας είναι μεγαλύτερες από τις λοιπές ζημίες (17-28 εκατομμύρια δολάρια σε αντίθεση με άλλες αναφερόμενες εκτιμήσεις που κυμαίνονταν μεταξύ 50.000 δολαρίων έως και 2 εκατ. δολαρίων ανά συμβάν).

Σύμφωνα με τους Brockett et al. (2012)[20], ο κίνδυνος στον κυβερνοχώρο αντιπροσωπεύει μια συνεχώς αυξανόμενη απειλή για τα δημόσια και ιδιωτικά ιδρύματα εξαιτίας των δυνητικά καταστροφικών επιπτώσεών του στα οργανωτικά συστήματα πληροφοριών, τον κίνδυνο φήμης και τη δυνητική απώλεια εμπιστοσύνης των καταναλωτών και των επενδυτικού κοινού. Με την

[19] Garg, A., Curtis, J. and Halper, H. (2003), "Quantifying the financial impact of IT security breaches", *Information Management and Computer Security*, 11 (2), pp. 74-83

[20] Brockett, L., P., Golden, L., L. and Wolman, W. (2012), "Enterprise Cyber Risk Management, Risk Management for the Future - Theory and Cases", [online], Διαθέσιμο στο: http://www.intechopen.com/books/risk management-for-the-future-theory-andcases/enterprise-cyber-risk-management, (Ημερομηνία Πρόσβασης: 24/11/2018)

εμφάνιση του Διαδικτύου και τον αντίστοιχο πολλαπλασιασμό της τεχνολογίας της πληροφορίας, οι επιχειρήσεις, τα μη κερδοσκοπικά ιδρύματα και οι κυβερνητικές οντότητες ήταν γενικά απροετοίμαστες για τον εντοπισμό και την αντιμετώπιση αυτού του κινδύνου, αλλά οι απειλές έχουν αυξηθεί τόσο σε συχνότητα όσο και σε σοβαρότητα με την πάροδο του χρόνου, ενώ η ίδια η φύση των επιθέσεων έχει επίσης αλλάξει στο πέρασμα των ετών.

Για το θέμα αυτό είχε μιλήσει και ο Baker (2008)[21], στην εργασία του λίγα μόλις χρόνια πριν, αναφέροντας ότι σε πολλά παλαιότερα περιστατικά επιθέσεων στον κυβερνοχώρο, οι δράστες υποκινούνταν σε πολλές περιπτώσεις από προσωπικά εγωιστικά κίνητρα (κυρίως για λόγους προσωπικής διασκέδασης) ή θεωρούσαν ότι η υπονόμευση των εταιρικών τεχνολογιών πληροφορικής ήταν κάποια πρόκληση προκειμένου να αξιολογήσουν τις προσωπικές τους δεξιότητες. Παρόλα αυτά, καθώς το Διαδίκτυο έχει αυξηθεί εκθετικά και το ηλεκτρονικό εμπόριο έχει αναπτυχθεί, η πρόσβαση των εργαζομένων στα δεδομένα των εταιρειών έχει αυξηθεί και η απομακρυσμένη πρόσβαση στα εσωτερικά συστήματα υπολογιστών έχει γίνει συνηθισμένη, με συνέπεια οι επιθέσεις στον κυβερνοχώρο όχι μόνο να έχουν εξελιχθεί, αλλά και να γίνονται ακόμα πιο περίπλοκες και τα αποτελέσματά τους να γίνονται, κατά συνέπεια και πιο καταστροφικά (Rhemann, 2011)[22].

Με αυτή την εξέλιξη των προσωπικών κινήτρων, της έντασης και της πολυπλοκότητας των επιθέσεων στον κυβερνοχώρο φαίνεται ότι συντάσσονται και οι Maillart και Sornette (2010)[23], οι οποίοι αναφέρουν ότι οι δράστες των διαδικτυακών επιθέσεων επικεντρώνονται όλο και περισσότερο στο να επωφελούνται από τις συνέπειες των επιθέσεων τους και είτε να εκμεταλλεύονται τα δεδομένα που λαμβάνουν παράνομα για ιδιωτικό κέρδος είτε να απαιτούν πληρωμές από τις θυματοποιημένες επιχειρήσεις για να αποκαταστήσουν τις ζημίες που έχουν προκαλέσει.

---

[21] Hallam-Baker, P. (2008), "Famous for Fifteen Minutes: A History of Hacking Culture, In: CSO Online-Security and Risk", [online], Διαθέσιμο στο: http://www.csoonline.com/article/217058/famous-for-fifteen-minutes-a historyofhacking-culture, (Ημερομηνία Πρόσβασης: 24/11/2018)

[22] Rhemann, M. (2011). "Cyber Trends", *Trends Digest*, [online], Διαθέσιμο στο: http://trendsdigeststore.com/CyberTrends.aspx, (Ημερομηνία Πρόσβασης: 24/11/2018)

[23] Maillart, T. and Sornette, D. (2010), "Heavy-tailed distribution of cyber-risks", *European Physical Journal B*, 75 (3), pp. 357–364

Ο Hall (2016)[24], επισκόπησε κριτικά την στάση πολλών επιχειρήσεων απέναντι στην ελλιπή οικοδόμηση επαρκών δομών προκειμένου να είναι προστατευμένες έναντι των κινδύνων του κυβερνοχώρου. Σύμφωνα με τα όσα αναφέρει, δεν είναι λίγες οι οργανώσεις που εφαρμόζουν πολύ κακές πρακτικές διαχείρισης και ελέγχου των κινδύνων του κυβερνοχώρου, ενώ παράλληλα έχουν αδύναμες ή ανύπαρκτες δομές αξιολογήσεων του κινδύνου, καθώς και προληπτικών μέτρων αντιμετώπισής του. Ταυτόχρονα, η επικοινωνία μεταξύ των στελεχών που είναι υπεύθυνα για την ασφάλεια στον κυβερνοχώρο και των υπολοίπων εργαζομένων είναι, σε πολλές περιπτώσεις, μηδαμινή ή ακόμα και σχεδόν ανύπαρκτη. Πολλοί διοικούντες θεωρούν την ασφάλεια στον κυβερνοχώρο ως ακόμα έναν θόρυβο του περιβάλλοντος που πρέπει να αντιμετωπίσουν, δίχως να αναγνωρίζουν τη σημαντικότητά της και αποφεύγοντας έτσι να επενδύσουν υπεύθυνα στην ενδυνάμωσή της. Ο αρθρογράφος ολοκληρώνει εστιάζοντας στην ενδυνάμωση της οργανωτικής κουλτούρας, ως βασικό συστατικό της επιτυχημένης ενσωμάτωσης όλων εκείνων των απαραίτητων χαρακτηριστικών, καθώς και της αποδοχής αυτών από ολόκληρη την οργάνωση, που θα εξασφαλίσουν μια επαρκή προστασία έναντι των ποικίλων κινδύνων του κυβερνοχώρου.

Με την αποτελεσματικότητα των στρατηγικών λήψεων αποφάσεων για επένδυση σε πόρους ασφάλειας στον κυβερνοχώρο ασχολήθηκαν στην εργασία τους οι Fielder et al. (2016)[25]. Μέσα από την εξέταση τριών μεθοδολογιών υποστήριξης αποφάσεων που βασίζονται στη θεωρία παιγνίων, τη θεωρία της συνδυαστικής βελτιστοποίησης, καθώς και σε ένα υβριδικό μοντέλο βάσει των δύο προαναφερθέντων μεθόδων, επιχείρησαν να διερευνήσουν την αποτελεσματικότητα των ελέγχων ασφάλειας στον κυβερνοχώρο σχετικά με την προστασία των διαφόρων περιουσιακών στοιχείων που θεωρούνται στόχοι σε περίπτωση απειλών του κυβερνοχώρου. Τα αποτελέσματα της συγκριτικής επισκόπησης των στοιχείων τους είναι ιδιαίτερα ενθαρρυντικά, δεδομένου ότι κατέληξαν σε παρόμοια συμπεράσματα με αυτά που υποστηρίζει η κυβέρνηση του Ηνωμένου Βασιλείου όσον αφορά τις απαιτήσεις για τη βασική προστασία από επιθέσεις στον κυβερνοχώρο για τις μικρομεσαίες επιχειρήσεις.

[24] Mark, H. (2016), "Why people are key to cyber-security", *Network Security*, 2016 (6), pp. 9-10

[25] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F. (2016), "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol. 86, pp. 13-23

Σε παρόμοιο μήκος κύματος κινήθηκαν και οι Molina et al. (2017)[26], οι οποίοι προχώρησαν σε μια συγκριτική επισκόπηση των σημαντικότερων εργαλείων ανάλυσης των κινδύνων του κυβερνοχώρου. Για τον σκοπό της εργασίας τους ανέλυσαν και αξιολόγησαν τις ιδιότητες, τις μετρήσεις, τις στρατηγικές, καθώς και την υποστήριξη του κάθε εργαλείου, για την ανάλυση του κινδύνου, της λήψης αποφάσεων και της πρόληψης για την ασφάλεια του κυβερνοχώρου για την προστασία των πληροφοριακών στοιχείων ενός οργανισμού.

Σύμφωνα με τα όσα αναφέρει ο McKenna (2018)[27], στο άρθρο του με κεντρικό θέμα την μέτρηση του κινδύνου του κυβερνοχώρου, τα πιο πρόσφατα δεδομένα υπογραμμίζουν την πραγματική και αυξανόμενη απειλή των επιθέσεων στον κυβερνοχώρο. Μία από τις προκλήσεις που θέτει ο κυβερνοχώρος για τις επιχειρήσεις είναι ότι η έλλειψη γεωγραφικών συνόρων επέτρεψε να εξαπλωθούν οι επιθέσεις στον κυβερνοχώρο γρήγορα και σε πολλές – αν όχι στις περισσότερες των περιπτώσεων – δίχως να μπορούν να ελεγχθούν ή και να εντοπιστούν εγκαίρως. Συνεχίζει αναφέροντας ότι είναι πλέον σαφές ότι οι επιχειρήσεις πρέπει να λάβουν μέτρα για την ελαχιστοποίηση του κινδύνου αυτού του γεγονότος και να είναι προετοιμασμένες να μετριάσουν γρήγορα τον αντίκτυπο σε περίπτωση εμφάνισης επιθέσεων στον κυβερνοχώρο. Για τον λόγο αυτό προτρέπει τις διοικήσεις των επιχειρήσεων να αναγνωρίσουν την σημαντικότητα αυτού του θέματος και να λάβουν όσο το δυνατόν γρηγορότερα όλα τα αναγκαία μέτρα προστασίας και θωράκισης των εταιρικών δομών.

Ο καιρός που οι επιχειρήσεις υποτιμούσαν τη σοβαρότητα της προστασίας έναντι των κινδύνων του κυβερνοχώρου έχει περάσει ανεπιστρεπτί, σύμφωνα με τον James (2018)[28], ο οποίος επισημαίνει ότι η ασφάλεια στον κυβερνοχώρο θα πρέπει να αποτελεί βασική στρατηγική επιχειρηματική προτεραιότητα για τις σύγχρονες οργανώσεις. Το επόμενο, καθοριστικής σημασίας, βήμα απέναντι στην πιο αποτελεσματική κοινωνική θωράκιση έναντι των κινδύνων του κυβερνοχώρου είναι η ενθάρρυνση των εταιρειών προκειμένου να διαμοιράζονται τις πληροφορίες που αφορούν τις προσωπικές τους εμπειρίες στις οποίες έπεσαν θύματα ηλεκτρονικών επιθέσεων (ή βρέθηκαν αντιμέτωπες με αντίστοιχα περιστατικά), έτσι ώστε η ευρύτερη κοινότητα να

[26] Roldan-Molina, G., Almache-Cueva, M., Silva-Rabadao, C., Yevseyeva, I. and Basto-Fernandez, V. (2017), "A Comparison of Cybersecurity Risk Analysis Tools", *Procedia Computer Science*, Vol. 121, pp. 568-575

[27] McKenna, B. (2018), "Measuring Cyber-Risk", *Network Security*, 2018 (4), pp. 12-14

[28] James, L. (2018), "Making cyber-security a strategic business priority", *Network Security*, 2018 (5), pp. 6-8

επωφεληθεί από τα διδάγματα και τις επακόλουθες πληροφορίες σχετικά με τον τρόπο με τον οποίο οι δράστες των επιθέσεων έδρασαν, πως οι ίδιες οι επιχειρήσεις αντιμετώπισαν αυτές τις απειλές και σε ποιον βαθμό επηρεάστηκαν. Σύμφωνα με τον αρθρογράφο, η βελτίωση της ανταλλαγής πληροφοριών, ιδίως στον τομέα της σύμπραξης δημόσιου και ιδιωτικού τομέα, θα ενισχύσει επίσης την ευαισθητοποίηση έναντι των κινδύνων και θα επιτρέψει στις επιχειρήσεις να βελτιώσουν τη στάση τους όσον αφορά την ασφάλεια, περιορίζοντας έτσι τον κίνδυνο και τον αντίκτυπο της παραβίασης των δεδομένων τους. Όπως χαρακτηριστικά αναφέρει, δεν αρκεί απλά να υπάρχουν τα μέσα για την ανίχνευση ενός προβλήματος - το πιο σημαντικό είναι ότι μια επιχείρηση πρέπει να έχει τα κατάλληλα μέσα για να ανταποκριθεί σε μια επίθεση και να απομακρύνει την απειλή. Τα τέσσερα βασικά βήματα που πρέπει να ακολουθήσουν οι επιχειρήσεις προς την κατεύθυνση αυτή είναι: α) παρακολούθηση, ανίχνευση, αντιμετώπιση και αποκατάσταση, β) έγκαιρος εντοπισμός της επίθεσης και απομόνωση της απειλής, γ) περιορισμός των επιπτώσεων του κινδύνου και δ) αντιμετώπιση του προβλήματος.

Οι Eling και Wirfs (2019)[29], έστρεψαν το ερευνητικό τους ενδιαφέρον στον προσδιορισμό του πραγματικού κόστους που συνεπάγονται οι απειλές του κυβερνοχώρου. Για το σκοπό αυτό, συγκέντρωσαν 1579 περιστατικά απειλών-επιθέσεων στον κυβερνοχώρο από ένα σύνολο δεδομένων λειτουργικού κινδύνου και τα ανέλυσαν με μεθόδους από τον τομέα των στατιστικών και της αναλογιστικής επιστήμης. Έπειτα, προχώρησαν στο διαχωρισμό των κινδύνων του κυβερνοχώρου σε δύο κατηγορίες: α) στους καθημερινούς κινδύνους του κυβερνοχώρο και β) στους ακραίους κινδύνους του κυβερνοχώρου. Σύμφωνα με τα ευρήματά τους, ο κυβερνοχώρος δεδομένης της μεγάλης σπουδαιότητάς τους για την οικονομία και την κοινωνία. Τα αποτελέσματα της εργασίας τους υποδηλώνουν ότι η ανθρώπινη συμπεριφορά, είτε είναι εγκληματική είτε όχι, είναι η κύρια πηγή των κινδύνων του κυβερνοχώρου.

Μια ιδιαίτερα σημαντική και ενδιαφέρουσα θεματολογία αναφορικά με τους κινδύνους του κυβερνοχώρου, εστιάζει στην προστασία των μικρομεσαίων επιχειρήσεων έναντι των απειλών του διαδικτύου. Σε σχετικό της άρθρο η Goucher (2011)[30], ανέφερε ότι η ασφάλεια των ηλεκτρονικών

[29] Eling, M. and Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research,* Vol. 272, pp. 1109-1119

[30] Goucher, W. (2011), "Do SMEs have the right attitude to security?", *Computer & Fraud Security,* 2011 (7), pp. 18-20

πληροφοριών των μικρομεσαίων επιχειρήσεων είναι σημαντικά χαμηλά στη λίστα των οργανωτικών τους προτεραιοτήτων. Οι τέσσερις βασικοί λόγοι που οδηγούν σε αυτή τη συμπεριφορά είναι: α) περιορισμένος προϋπολογισμός, β) λιγοστός διαθέσιμος χρόνος προκειμένου οι ιδιοκτήτες και οι εργαζόμενοι να αποκτήσουν επαρκείς γνώσεις για το θέμα αυτό, γ) μικρή ή αμελητέα εκτίμηση των δυνητικών προβλημάτων που μπορούν να προκαλέσουν οι κίνδυνοι του κυβερνοχώρου και δ) απουσία επαρκών νομοθετικών ρυθμίσεων που να απαιτούν την συμμόρφωση με συγκεκριμένα πρότυπα. Παρόλα αυτά, υπογραμμίζει το ότι η οποιαδήποτε λύση που θα βοηθήσει προς την βελτιστοποίηση της οργάνωσης των μικρομεσαίων επιχειρήσεων έναντι των διαδικτυακών κινδύνων, θα πρέπει να είναι σαφώς προσανατολισμένη προς την ελαχιστοποίηση του κόστους που συνεπάγεται ένα τέτοιο εγχείρημα, δεδομένων των περιορισμένων πόρων που έχουν στη διάθεσή τους οι επιχειρήσεις αυτού του βεληνεκούς.

Ο Kurpjuhn (2015)[31], αναφέρει ότι ο κίνδυνος κακόβουλων απειλών από τους εγκληματίες στον κυβερνοχώρο είναι εξίσου σημαντικός για τις μικρές και μεσαίες επιχειρήσεις, όπως και για τους μεγαλύτερους οργανισμούς. Οι μικρότερες εταιρείες χρησιμοποιούν, παράγουν και αποθηκεύουν μεγάλα ποσά δεδομένων, καθιστώντας τα πιθανά κέρδη από μια επιτυχή παραβίαση της ασφαλείας τους, πολύ υψηλότερη από ό,τι ήταν πριν από τουλάχιστον πέντε χρόνια. Συνεπώς, αποτελούν, πλέον, έναν ιδιαίτερα ελκυστικό στόχο για τους επίδοξους δράστες του κυβερνοχώρου. Όπως χαρακτηριστικά αναφέρει, η πραγματικότητα για τις μικρομεσαίες επιχειρήσεις είναι ότι πρέπει να αντιμετωπίσουν ένα παρόμοιο επίπεδο κινδύνου, με αυτό που αντιμετωπίζουν οι συγκριτικά μεγαλύτεροι οργανισμοί, αλλά με πολύ πιο περιορισμένους πόρους. Μπορεί να είναι δύσκολο για τους υπευθύνους λήψης αποφάσεων να δουν πώς μπορεί να επωφεληθεί πραγματικά μια μικρομεσαία επιχείρηση από μια επένδυση σε τεχνολογίες ασφάλειας, γεγονός που οδηγεί, πολύ συχνά, στην λανθασμένη αντίληψη ότι μια τέτοια ενέργεια είναι περιττή.

Την σημασία της προστασίας των ηλεκτρονικών δεδομένων των μικρομεσαίων επιχειρήσεων, ως βασικά συστατικά στοιχεία της επιτυχημένης και απρόσκοπτης λειτουργία των εφοδιαστικών αλυσίδων, υπογράμμισε στο άρθρο της η Caldwell (2015)[32]. Σύμφωνα με τα στοιχεία που παραθέτει, σχεδόν οι μικρομεσαίες επιχειρήσεις που πέφτουν θύματα διαδικτυακών

[31] Kurpjuhn, T. (2015), "The SME security challenge", *Computer Fraud & Security*, 2015 (3), pp. 5-7

[32] Caldwell, T. (2015), "Securing small businesses – the weakest link in a supply chain?", *Computer & Fraud Security*, 2015 (9), pp. 5-10

επιθέσεων, παύουν τις επιχειρηματικές τους δραστηριότητές τους εντός έξι μηνών. Κάθε επιχείρηση πρέπει να αναλάβει την ευθύνη για την εξασφάλιση των βασικών διαδικασιών που θα της παρέχουν τα απαιτούμενα μέτρα ασφαλείας στον κυβερνοχώρο. Επιπροσθέτως, αναφέρει ότι ενώ οι περισσότερες μικρές και μεσαίες επιχειρήσεων χρησιμοποιούν, στις περισσότερες περιπτώσεις, κάποιο είδος τείχους προστασίας, αυτό το εργαλείο δεν επαρκεί για την προστασία ενός δικτύου από τις σημερινές προηγμένες απειλές του κυβερνοχώρου. Για το λόγο αυτό, θα πρέπει να διενεργούνται έλεγχοι ασφαλείας σε όλους τους εμπλεκομένους των εφοδιαστικών αλυσίδων, έτσι ώστε να διασφαλίζεται ότι πληρούν τουλάχιστον τα ελάχιστα πρότυπα που ορίζει η ηγέτιδα εταιρεία. Δεδομένου των περιορισμένων οικονομικών πόρων που μια μικρομεσαία επιχείρηση μπορεί να διαθέσει για την θωράκισή της έναντι των κινδύνων του κυβερνοχώρου, αποτελεί βασική ευθύνη της, υπεύθυνης για την διασφάλιση της απρόσκοπτης λειτουργίας της εφοδιαστικής αλυσίδας, επιχείρησης να παρέχει την κατάλληλη καθοδήγηση και εκπαίδευση προς κάθε εμπλεκόμενο μέρος της αλυσίδας, έτσι ώστε να επιτευχθούν τα επιθυμητά αποτελέσματα.

Αντίστοιχο είναι και το ενδιαφέρον της Paul (2017)[33], η οποία επισημαίνει τη σημασία της ενδυνάμωσης των αμυντικών μηχανισμών των μικρομεσαίων επιχειρήσεων έναντι των απειλών του κυβερνοχώρου. Σύμφωνα με την αρθρογράφο, αυτό μπορεί να επιτευχθεί μέσω της συντεταγμένης διενέργειας των ακόλουθων διαδικασιών: α) έλεγχος και ανάλυση των δεδομένων καταγραφής, β) βελτίωση των πρακτικών του εσωτερικού ελέγχου, γ) προληπτική επιτήρηση, δ) ενίσχυση των ασφαλιστικών δικλίδων των διαδικτυακών υπηρεσιών, ε) διαχείριση κωδικών πρόσβασης και στ) εκτενής ανάλυση του τείχους προστασίας. Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι κοινός παρονομαστής όλων των άρθρων που σχετίζονται με τις απειλές και τους κινδύνους του κυβερνοχώρου είναι ότι σε μεγάλο βαθμό φαίνεται ότι προέρχονται από το εσωτερικό της επιχείρησης (internal cyber threat), γεγονός που θα πρέπει να προβληματίζει τους διοικούντες των επιχειρήσεων, καθώς και τους υπευθύνους διαχείρισης των εταιρικών κινδύνων.

[33] Paul, S. (2017), "Reinforcing your SME against cyberthreats", *Computer Fraud & Security*, 2017 (10), pp. 13-15

2.4 Η Ασφάλιση έναντι των Κινδύνων του Κυβερνοχώρου

Η αναγκαιότητα για ασφάλιση έναντι των κινδύνων του κυβερνοχώρου (cyber risk insurance) είναι μια έννοια σχετικά πρόσφατη. Παρόλα αυτά, οι επιχειρήσεις στρέφονται ολοένα και περισσότερο προς την απόκτηση επαρκούς ασφάλισης έναντι των κινδύνων του κυβερνοχώρου προκειμένου να επιτύχουν την όσο το δυνατόν καλύτερη διαχείριση των απειλών του διαδικτύου, καθώς και να διασφαλιστούν ισχυρότερα απέναντι σε κάθε προκύπτουσα νομική ευθύνη από παραβιάσεις δεδομένων. Δεδομένου ότι οι ηλεκτρονικές επιχειρήσεις (e-Businesses), έχουν αυξηθεί εκθετικά παγκοσμίως την τελευταία τουλάχιστον δεκαετία, χρησιμοποιώντας ηλεκτρονικές συναλλαγές για να αυξήσουν την πελατειακή τους βάση και τα έσοδά τους, καθίσταται πλέον αντιληπτό από όλους ότι ο κίνδυνος της ηλεκτρονικής πειρατείας και των επιθέσεων στον κυβερνοχώρο είναι όχι απλά υπαρκτός, αλλά και μεγάλος.

Μια από τις πρώτες και πολύ ενδιαφέρουσες εργασίες πάνω στο θέμα της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου έρχεται από τους Gordon et al. (2003)[34], οι οποίοι επισκόπησαν στην έρευνά τους τρεις πτυχές της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου, της τιμολόγησης των ασφαλιστικών υπηρεσιών (pricing), της δυσμενούς επιλογής (adverse selection) και του ηθικού κινδύνου (moral hazard). Σύμφωνα με τους συγγραφείς, δεδομένου ότι η τιμολόγηση εξαρτάται σε μεγάλο βαθμό από τις αναλογιστικές εκτιμήσεις και τα ιστορικά δεδομένα, η πολιτική τιμολόγησης για την κάλυψη των ζημιών από διαδικτυακές επιθέσεις στηρίζεται σε πολύ πιο σαθρά θεμέλια από ότι η τιμολόγηση των πιο συμβατικών ασφαλιστικών πακέτων. Όσον αφορά το θέμα της δυσμενούς επιλογής, σημειώνουν ότι όσο μεγαλύτερος είναι ο κίνδυνος για μια εταιρία να πέσει θύμα διαδικτυακών επιθέσεων, τόσο περισσότερες είναι και οι πιθανότητες να αναζητήσουν κάποιας μορφής ασφαλιστική κάλυψη έναντι αυτού του σεναρίου. Οι ασφαλιστικές εταιρίες ωστόσο δεν μπορούν να γνωρίζουν προκαταβολικά το κατά πόσο μια επιχείρηση έχει επαρκή συστήματα διαχείρισης των κινδύνων ή ικανοποιητικές δομές προστασίας έναντι των κινδύνων του κυβερνοχώρου. Για το λόγο αυτό, οι συγγραφείς προτείνουν προς τις ασφαλιστικές εταιρίες να διατηρούν μια καρτέλα με το προφίλ κινδύνου της κάθε επιχείρησης, στην οποία θα πρέπει να αναφέρεται τουλάχιστον, μεταξύ άλλων, το κατά πόσο ο πελάτης έχει ελεγχθεί για την επάρκεια των αμυντικών συστημάτων που διατηρεί για την προστασία του έναντι

[34] Gordon, L., Loeb, M. and Sohail, T. (2003), "A Framework for Using Insurance for Cyber Risk Management", *Communications of the Association of Computing Machinery*, 46 (3), pp. 81-85

των κινδύνων του κυβερνοχώρου. Τέλος, όσον αφορά τον ηθικό κίνδυνο, ο οποίος αναφέρεται στο ότι μια επιχείρηση δύναται να επαναπαυθεί εξαιτίας των ασφαλιστικών υπηρεσιών που λαμβάνει και να μην προσπαθεί τα δέοντα προκειμένου να θωρακίσει επαρκώς τις εταιρικές της δομές έναντι των κινδύνων του κυβερνοχώρου, οι συγγραφείς προτείνουν ότι θα πρέπει να δίδονται οικονομικά κίνητρα μείωσης των ασφαλίστρων προς τις επιχειρήσεις προκειμένου να επηρεαστούν θετικά οι αποφάσεις της για να διαθέσει ίδιους πόρους για τον περιορισμό του υπαρκτού κινδύνου από μόνη της. Με την άποψη αυτή συντάσσονται και οι Schwartz et al. (2010)[35], οι οποίοι αναφέρουν ότι τα εκπτωτικά ποσά, τα πιο αυστηρά ασφαλιστικά όρια κάλυψης ζημιών και η συνασφάλιση είναι τυποποιημένα εργαλεία που χρησιμοποιούνται από τις ασφαλιστικές εταιρείες όταν υπάρχει ασυμμετρία πληροφόρησης και μπορούν να εφαρμοστούν και για την περίπτωση της κάλυψης των κινδύνων του κυβερνοχώρου. Αυτό συνεπάγεται υψηλότερο οικονομικό βάρος για τον ασφαλισμένο για τον μετριασμό των επιπτώσεων της δυσμενούς επιλογής που προκύπτει από την ασυμμετρία της πληροφόρησης και της αδράνειας που προκαλείται από την αδυναμία του ασφαλιστή να παρακολουθεί επαρκώς τη συμπεριφορά του πελάτη του.

Οι Mukhopadhyay et al. (2005)[36], διατείνονται στην εργασία τους ότι οι ποικίλες επιλογές λογισμικού και φυσικού εξοπλισμού που χρησιμοποιούνταν για την προστασία των ενδιαφερομένων από τις κακόβουλες επιθέσεις στον κυβερνοχώρο δεν έχουν αποδώσει τα αναμενόμενα οφέλη (αυτό αφορά φυσικά την εποχή κατά την οποία γράφτηκε η εν λόγω εργασία, δηλαδή σχεδόν 15 χρόνια πριν). Για να μειωθούν οι οικονομικές απώλειες που οφείλονται σε ηλεκτρονικούς κινδύνους, η χρήση ενός ασφαλιστικού προϊόντος ως συμπληρωματικού εργαλείου είναι μια βιώσιμη επιλογή, όπου η απώλεια εσόδων μπορεί να μειωθεί ή ακόμα και να αντισταθμιστεί με τα όποια οφέλη μπορούν να προκύψουν από την ασφάλιση αυτή. Για τον λόγο αυτό, χρησιμοποίησαν τη θεωρία χρησιμότητας (utility theory), έτσι ώστε να διαμορφώσουν το αναμενόμενο ασφάλιστρο που ένας οργανισμός-επιχείρηση υποχρεούται να πληρώσει, ανάλογα με το προφίλ κινδύνου του, επισημαίνοντας παράλληλα τα γνωρίσματα και τα πιθανά οφέλη ενός

[35] Schwartz, G., Shetty, N. and Walrand, J. (2010), "Cyber-Insurance: Missing Market Driven by User Heterogeneity", *Submission to Workshop on the Economics of Information Security (WEIS)*, [online], Διαθέσιμο στο: https://pdfs.semanticscholar.org/d1db/6af4b7c93315e48c8ab407f1f75187a88687.pdf, (Ημερομηνία Πρόσβασης: 27/11/2018)

[36] Mukhopadhyay, A., Saha, D., Chakrabarti, B., B., Mahanti, A. and Podder, A. (2005), "Insurance for Cyber-risk: A Utility Model", *Decision*, 32 (1), pp. 1-19

πιθανού ασφαλιστικού προϊόντος με σαφή προσανατολισμό για την κάλυψη των ζημιών-απωλειών από επιθέσεις στον κυβερνοχώρο.

Οι Anderson και Moore (2006)[37], υποστηρίζουν ότι η ασφάλιση έναντι των κινδύνων του κυβερνοχώρου είναι εξαιρετικά δύσκολη, δεδομένης της διασυνδεσιμότητας (interconnectedness) της υποδομής ασφάλειας των πληροφοριών και της αλληλεξάρτησης από ένα κομμάτι δημοφιλούς λογισμικού, με το οποίο μια γενική ευπάθεια σε ένα προϊόν μπορεί να εκθέσει κάθε επιχείρηση που χρησιμοποιεί αυτό το λογισμικό σε απειλές στον κυβερνοχώρο. Σύμφωνα με τους αρθρογράφους, το μεγάλο ερώτημα που γεννάται από την παραπάνω περίπτωση, είναι το γιατί θα πρέπει μια ασφαλιστική εταιρεία να πληρώσει για ζημίες που προκλήθηκαν από μια άλλη εταιρεία που έπεσε θύμα μιας διαδικτυακής επίθεσης ή προκάλεσε τη ζημία της καλυπτόμενης επιχείρησης; Όπως χαρακτηριστικά αναφέρουν, ο νόμος των μεγάλων αριθμών, που συχνά χρησιμοποιείται για να δικαιολογήσει την κάλυψη των ασφαλιστικών εταιρειών, θα μπορούσε να αποδυναμωθεί από το εύρος και τον αντίκτυπο τέτοιων ζημιών οδηγώντας έτσι στην αδυναμία πληρωμής των απαιτήσεων του ασφαλιστή. Εάν ένα ελάττωμα σε ένα πολύ συνηθισμένο σύστημα λογισμικού επηρεάζει εκατομμύρια χρήστες και διαδίδεται μέσω διαφόρων εταιρειών, ο ασφαλιστής μπορεί να δυσκολεύεται να πληρώσει όλες τις επακόλουθες ζημίες. Παρόμοια είναι και η θέση των Bohme και Kataria (2006)[38], οι οποίοι αναφέρουν ότι οι ασφαλιστικές υπηρεσίες για την κάλυψη των κινδύνων του κυβερνοχώρου δεν μπορούν να λειτουργήσουν αποτελεσματικά όταν οι κίνδυνοι που αντιμετωπίζουν μεμονωμένοι πελάτες είναι υπερβολικά συσχετισμένοι ή όταν οι ασφαλιστές δεν μπορούν να παρακολουθούν τα επίπεδα ασφαλείας των πελατών τους και επιπλέον οι πολιτικές τείνουν να είναι υπερτιμημένες επειδή οι ασφαλιστές δεν είναι σε θέση να προβλέψουν τις δευτερεύουσες ζημίες των ασφαλισμένων τους, όπως για παράδειγμα την απώλεια της καλής φήμης και πελατείας. Με την άποψη αυτή συντάσσονται και οι Shetty et al. (2010)[39].

[37] Anderson, R. and Moore, T. (2006), "The Economics of Information Security", *Science*, 314 (5799), pp. 610-613

[38] Böhme, R. and Kataria, G. (2006), "Models and measures for correlation in cyber-insurance", *Workshop on Economics of Information Security (WEIS)*, [online], Διαθέσιμο στο: https://www.econinfosec.org/archive/weis2006/docs/16.pdf, (Ημερομηνία Πρόσβασης: 27/11/2018)

[39] Shetty, N., Schwartz, G., Felegyhazi, M. and Walrand, J. (2010), "Competitive Cyber-Insurance and Internet Security", *Economics of Information Security and Privacy*, Springer, Boston, MA, pp. 229-247

Η χρησιμότητα της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου προβλημάτισε τον Shackelford (2012)[40], ο οποίος προχώρησε στην ανάλυση: α) του αντίκτυπου των επιθέσεων στον κυβερνοχώρο σε επιλεγμένες επιχειρήσεις των ΗΠΑ, β) της τότε ισχύουσας νομοθεσίας των ΗΠΑ που αφορούσαν τις ευθύνες των ιδιωτικών επιχειρήσεων σε περιπτώσεις παραβίασης δεδομένων και γ) του βαθμού στον οποίο η ασφάλιση έναντι των κινδύνων του κυβερνοχώρου συμβάλλει στην άμβλυνση των απειλών του κυβερνοχώρου. Σύμφωνα με τα όσα υποστηρίζει ο συγγραφέας, οι επιχειρήσεις πρέπει να υιοθετήσουν μια προορατική στάση απέναντι στις επιθέσεις στον κυβερνοχώρο - όχι μόνο για την ευημερία τους αλλά και για να ενισχύσουν τη συνολική ασφάλεια στον κυβερνοχώρο και να βοηθήσουν στην εξασφάλιση μιας κρίσιμης εθνικής υποδομής έναντι των απειλών αυτής της μορφής.

Στην εξίσου ενδιαφέρουσα εργασία τους οι Biener et al. (2015)[41], χρησιμοποίησαν δεδομένα σχετικά με τις ζημίες που συνδέονται με τις διαδικτυακές επιθέσεις από μια βάση δεδομένων λειτουργικού κινδύνου για την εμπειρική ανάλυση του κατά πόσο αυτές οι ζημίες μπορούν να καλυφθούν από τις ασφαλιστικές εταιρίες, σύμφωνα με ορισμένα τυποποιημένα κριτήρια που συμπεριλαμβάνονται στα συνήθη ασφαλιστικά συμβόλαια. Αν και εντοπίζουν τις συνήθεις δυσχέρειες που αναγνωρίζονται από την παγκόσμια βιβλιογραφία, όπως τη συσχέτιση μεταξύ των ζημιών, την έλλειψη στοιχείων και τις σοβαρές ασυμμετρίες πληροφόρησης, οι συντάκτες συμπεραίνουν ότι η ασφαλιστική κάλυψη αυτής της μορφής κινδύνων μπορεί να φέρει θετικό πρόσημο για τις ασφαλιστικές εταιρίες. Σε παρόμοιο μήκος κύματος κινούνται και οι εργασίες των Sinanaj and Muntermann (2013)[42] Edwards et al. (2016)[43], οι οποίοι επισκοπούν αντίστοιχες περιπτώσεις διαδικτυακών επιθέσεων.

[40] Shackelford, S., J. (2012), "Should your firm invest in cyber risk insurance?", *Business Horizons,* 55 (4), pp. 349-356

[41] Biener, C., Eling, M. and Wirfs, J., H. (2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance - Issues and Practice,* 40 (1), pp. 131-158

[42] Sinanaj, G. and Muntermann, J. (2013), "Assessing corporate reputational damage of data breaches: an empirical analysis", *Proceedings of the 26th International Bled eConference,* pp. 78–89

[43] Edwards, B., Hofmeyr, S. and Forrest, S. (2016), "Hype and heavy tails: a closer look at data breaches", *Journal of Cybersecurity,* 2 (1), pp. 3-14

Στην πολύ περιεκτική τους εργασία, οι Eling και Schnell (2016)[44], επισκοπούν την διαθέσιμη παγκόσμια βιβλιογραφία προκειμένου να διαπιστώσουν την παρούσα κατάσταση των κινδύνων του κυβερνοχώρου, καθώς και των ασφαλιστικών μέτρων έναντι αυτών. Η εργασία τους είναι χωρισμένη σε επτά βασικές ενότητες, η τελευταία εκ των οποίων, άπτεται του ζητήματος της ασφαλιστικής κάλυψης για τους κινδύνους του κυβερνοχώρου. Το γενικό συμπέρασμα των αρθρογράφων είναι ότι η αγορά της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου είναι ακόμα μικρή και έχει πολλές ευκαιρίες άνθισης, ενώ οι ΗΠΑ φαίνεται ότι είναι πολύ μπροστά στο θέμα αυτό, συγκριτικά με την Ε.Ε. Επιπροσθέτως, διαπιστώνουν σημαντικές ελλείψεις όσον αφορά την διαθέσιμη βιβλιογραφία και αρθρογραφία που να εστιάζει στο θέμα των κινδύνων του κυβερνοχώρου, καθώς και της ασφάλισης έναντι αυτών, επισημαίνοντας το ότι πρόκειται για ένα ιδιαίτερα δυναμικό θέμα, για το οποίο ακόμα και η βιβλιογραφία πέντε χρόνια πριν μπορεί να θεωρηθεί ξεπερασμένη.

Μια ακόμα ενδιαφέρουσα εργασία στην οποία επισκοπείται το θέμα της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου ήρθε πρόσφατα από τους Marotta et al. (2017)[45]. Σύμφωνα με τα όσα αναφέρουν οι αρθρογράφοι, η ασφάλιση έναντι των κινδύνων του κυβερνοχώρου είναι ένας ταχέως αναπτυσσόμενος χώρος, ο οποίος προσελκύει όλο και περισσότερη προσοχή από τους επαγγελματίες και τους ερευνητές. Ωστόσο, επισημαίνουν ότι αγορά αυτή είναι ακόμα αρκετά «ανώριμη» και αντιμετωπίζει ορισμένες μοναδικές προκλήσεις στο δρόμο της ανάπτυξής της. Για τον σκοπό της εργασίας του συνόψισαν τη βασική βιβλιογραφία, σχετικά με την ασφάλιση έναντι των κινδύνων του κυβερνοχώρου, που είναι διαθέσιμη μέχρι τώρα, συμπεριλαμβάνοντας τόσο τις θέσεις της ίδιας της αγοράς όσο και τις επιστημονικές προτάσεις. Για τον λόγο αυτό προσπάθησαν να παρουσιάσουν, με απλοποιημένους όρους, τα κυριότερα ζητήματα που άπτονται του θέματος και σχολίασαν τις πτυχές που καθιστούν αυτό το είδος ασφάλισης μοναδικό, επισημαίνοντας το ότι πολλές και διαφορετικές τεχνολογίες επηρεάζονται άμεσα από την ασφάλιση έναντι των κινδύνων αυτών. Ολοκληρώνοντας, παρουσιάζουν τις προτάσεις τους για περαιτέρω έρευνα όσον αφορά την ασφάλιση έναντι των κινδύνων του κυβερνοχώρου.

---

[44] Eling, M. and Schnell, W. (2016), "What do we know about cyber risk and cyber risk insurance?", *The Journal of Risk Finance,* 17 (5), pp. 474-491

[45] Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017), "Cyber-insurance survey", *Computer Science Review,* Vol. 24, pp. 35-61

Με την εμπειρική διερεύνηση της έκτασης των εργασιών και των προκλήσεων της ασφαλιστικής αγοράς έναντι των κινδύνων του κυβερνοχώρου στην Σουηδία ασχολήθηκε στην εργασία του ο Franke (2017)[46]. Για τον λόγο αυτό προχώρησε στην διενέργεια προσωπικών συνεντεύξεων με 15 ασφαλιστικές εταιρίες που δραστηριοποιούνται στον χώρο αυτό. Βάσει των ευρημάτων του, οι ασφαλιστικές εταιρείες επιβάλλουν στους πελάτες τους απαιτήσεις θωράκισης των πληροφοριακών τους συστημάτων και τείνουν να μην ασφαλίζουν πελάτες που δεν είναι πολύ δεκτικοί προς αυτή την κατεύθυνση ή παρουσιάζουν πολύ χαμηλά επίπεδα ασφάλειας των διαδικτυακών τους υποδομών. Κατά συνέπεια, η ασφάλιση έναντι των κινδύνων του κυβερνοχώρου, στην πράξη, δεν αποτελεί απλώς μέσο μεταφοράς του κινδύνου, αλλά περιλαμβάνει επίσης πτυχές αποφυγής και μετριασμού αυτού.

Με την παρουσίαση ενός μοντέλου για την επιλογή της βέλτιστης λύσης από ένα σύνολο πολιτικών που σχετίζονται με την ασφάλιση έναντι των κινδύνων στον κυβερνοχώρο από μια επιχείρηση, δεδομένου ότι ένας πεπερασμένος αριθμός πολιτικών προσφέρονται από μία ή περισσότερες ασφαλιστικές εταιρείες, ασχολήθηκαν στην εργασία τους οι Bodin et al. (2018)[47]. Ως βέλτιστη λύση ορίζεται η επιλογή της πολιτικής εκείνης που ελαχιστοποιεί τα ασφαλιστικά κόστη (δηλαδή τα ασφάλιστρα) για την εταιρία-ασφαλιζόμενο, καθώς και τις προσδοκώμενες ζημίες που δεν θα καλυφθούν, πιθανότατα, από την ασφαλιστική εταιρία. Μέσα από την επισκόπηση των σημαντικότερων πτυχών του μοντέλου τους, καταλήγουν στο ότι (κατόπιν πολλών επαναλήψεων) η συνηθέστερη έξοδος εμφανίζει τρεις, κυρίως, περιπτώσεις όπου η ασφαλιστική εταιρία δύναται να μην καλύψει τις ενδεχόμενες ζημίες από επιθέσεις στον κυβερνοχώρο μιας επιχείρησης. Κατά συνέπεια, οι συγγραφείς εφιστούν την προσοχή των εταιριών προς την ενδυνάμωση των αντίστοιχων δομών τους που είναι οι πιο ευπαθείς έναντι των κινδύνων αυτών και που, πολύ πιθανόν, οι ασφαλιστικές εταιρίες να μην δεχθούν να καλύψουν. Επιπροσθέτως, προτείνουν την διασπορά του εγγενούς ρίσκου μεταξύ διαφόρων ασφαλιστικών εταιριών, προκειμένου να μειωθεί ο συνολικός κίνδυνος κάλυψης και αποπληρωμής των ζημιών, ενώ επισημαίνουν τη σημαντικότητα της αποτελεσματικής χάραξης εταιρικής πολιτικής διαχείρισης των κινδύνων του κυβερνοχώρου, ως βασικό θεμέλιο λίθο προστασίας έναντι αυτών.

[46] Franke, U. (2017), "The cyber insurance market in Sweden", *Computers & Security*, Vol. 68, pp. 130-144

[47] Bodin, L., D., Gordon, L., A., Loeb, M., P. and Wang, A. (2018), "Cybersecurity insurance and risk-sharing", *Journal of Accounting and Public Policy*, 37 (6), pp. 527-544

ΚΕΦΑΛΑΙΟ 3

ΚΙΝΔΥΝΟΙ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ΚΑΙ ΤΡΟΠΟΙ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥΣ

3.1 Εισαγωγή

Στο τρίτο κεφάλαιο της εργασίας θα ασχοληθούμε την διεξοδικότερη ανάλυση της θεματολογίας περί των κινδύνων του κυβερνοχώρου. Συγκεκριμένα, ξεκινάμε με την παράθεση των ποικίλων ορισμών αυτής της μορφής των κινδύνων και συνεχίζουμε προσπαθώντας να τους στοιχειοθετήσουμε, τόσο ως προς τις μορφές τους, όσο και προς το κόστος που συνεπάγονται για τους οργανισμούς και τις επιχειρήσεις. Το κυρίως μέρος του παρόντος κεφαλαίου ασχολείται με την διαχείριση των κινδύνων του κυβερνοχώρου, σε μια προσπάθεια να παρουσιαστούν τα μέτρα και οι διαδικασίες που προτείνονται από την παγκόσμια βιβλιογραφία επί του θέματος.

3.2 Ορισμός του Κινδύνου

Τόσο τα μεμονωμένα άτομα, όσο και οι επιχειρήσεις, προσπαθούν να οργανώσουν τα μελλοντικά τους σχέδια, βασισμένοι σε ένα πλήθος παραγόντων, εναλλακτικών καταστάσεων και αβεβαιότητας. Ο παράγοντας που μπορεί να προκαλέσει σε δεδομένη μελλοντική περίοδο την εμφάνιση εναλλακτικών καταστάσεων και να επιφέρει αβεβαιότητα (uncertainty) καλείται κίνδυνος (risk). Σύμφωνα με τον Ελευθεριάδη (2018)[48], ο κίνδυνος είναι μια από τις παραμέτρους της καθημερινής μας ζωής και επηρεάζει σχεδόν το σύνολο των δραστηριοτήτων των οικονομικών μονάδων, ενώ παράλληλα υπάρχει σε όλες εκείνες τις περιπτώσεις στις οποίες δεν είναι δυνατό να προβλέψουμε με βεβαιότητα το αποτέλεσμα μιας δραστηριότητας. Η κάθε επιχειρηματική δραστηριότητα θα πρέπει να προσδιορίζει ποιος είναι ο κίνδυνος που συνδέεται με την υλοποίησή της και ποια είναι τα μέτρα που πρέπει να ληφθούν για την αποτελεσματική διαχείρισή του.

48 Ελευθεριάδης, Ι. (2018). *Διοίκηση Εταιρικών Κινδύνων*. Πανεπιστημιακές Σημειώσεις

Συνεχίζοντας, αναφέρει ότι ο κίνδυνος μπορεί να χρησιμοποιηθεί για να περιγράψει την αβεβαιότητα που συνδέεται με διαδικασίες και τα αποτελέσματά τους, που μπορεί να έχουν σημαντικές επιπτώσεις, είτε θετικές είτε αρνητικές στην: α) Λειτουργική απόδοση, β) Την επίτευξη των σκοπών και των στόχων και γ) Την εκπλήρωση των προσδοκιών των μετόχων. Ο κίνδυνος επίσης μπορεί να ορισθεί ως ο συνδυασμός της πιθανότητας ενός γεγονότος και των συνεπειών του (ISO-IEC Guide 73). Σε όλους τους τύπους των δραστηριοτήτων, υπάρχει το ενδεχόμενο για γεγονότα και συνέπειες που συνιστούν ευκαιρίες προς όφελος (upside) ή απειλές της επιτυχίας (downside). Συνεπώς, ο κίνδυνος είναι η αβεβαιότητα της μελλοντικής έκβασης ενός γεγονότος. Είναι κάτι που συμβαίνει στο μέλλον αλλά δεν μπορεί να προβλεφθεί ακριβώς σήμερα επειδή υπάρχει αβεβαιότητα. Κίνδυνος υφίσταται όταν ένα τυχαίο γεγονός θα επιδράσει αρνητικά στην πιθανότητα της πραγματοποίησης ενός εφικτού στόχου. Μαθηματικά ο κίνδυνος μπορεί να εκφρασθεί σαν το προϊόν της πιθανότητας των περιστατικών και των συνεπειών της απώλειας που προκλήθηκε από τον κίνδυνο. Οι καταστάσεις αβεβαιότητας προκύπτουν, όταν υπάρχει μια άγνωστη, απροσδιόριστη κατανομή πιθανότητας στο σύνολο των πιθανών εκβάσεων.

Η αβεβαιότητα σε αυτό το πλαίσιο έχει δύο διαστάσεις:

- Το εύρος των πιθανών εκβάσεων ενός γεγονότος ή μιας δράσης το οποίο μπορεί να είναι στενό, περιορισμένο ή άγνωστο.
- Την πιθανότητα εμφάνισης μιας έκβασης. Σε μερικές περιπτώσεις αυτό είναι σχετικά εύκολο να καθοριστεί. Σε πολλές άλλες περιπτώσεις μπορεί να μην είναι δυνατό να υπολογιστεί μια πιθανότητα ακριβώς. Η ακόμη και να μην είναι δυνατό να υπολογιστεί μια πιθανότητα καθόλου.

3.2.1 Κίνδυνοι του Κυβερνοχώρου

Σύμφωνα με τον Ελευθεριάδη (2018)[49], οι σημερινοί ταχύτατοι ρυθμοί σχεδιασμού, παραγωγής και διάθεσης προϊόντων και υπηρεσιών καθώς και η τεράστια εξάρτηση κάθε δραστηριότητας από περίπλοκα συστήματα υψηλής τεχνολογίας, δημιούργησαν νέους κινδύνους, οι οποίοι είναι δύσκολο να αντιμετωπισθούν. Οι κίνδυνοι που είναι πιθανό να προκύψουν από τη διαχείριση δεδομένων εξαρτώνται από τομείς όπως οι τηλεπικοινωνίες, η ενέργεια, ο κακός

49 Ελευθεριάδης, Ι. (2018). *Διοίκηση Εταιρικών Κινδύνων*. Πανεπιστημιακές Σημειώσεις

χειρισμός του λογισμικού και οι φυσικές καταστροφές. Η ασφάλεια των πληροφοριακών συστημάτων αναφέρεται στην προστασία δεδομένων που αποθηκεύονται, έχουν υποστεί επεξεργασία ή μεταφερθεί σε μηχανογραφικά κέντρα ή προσωπικούς υπολογιστές. Οι κίνδυνοι των πληροφοριακών συστημάτων μπορούν να συνοψισθούν σε τέσσερα σημεία:

- Ο κίνδυνος ζημιάς στο τεχνικό μέρος των συστημάτων και στον χώρο εγκατάστασης των συστημάτων, από φυσική καταστροφή, πυρκαγιά, κλιματολογικές συνθήκες, τρομοκρατικές ενέργειες κ.α.
- Ο κίνδυνος από τις διαδικασίες επεξεργασίας δεδομένων.
- Ο κίνδυνος απώλειας δεδομένων ή εμφάνισης των δεδομένων σε μη εξουσιοδοτημένα άτομα.
- Ο κίνδυνος ακούσιας αλλοίωσης των δεδομένων λόγω ενός τεχνικού προβλήματος.
- Ο κίνδυνος εκούσιας αλλοίωσης δεδομένων από μη εξουσιοδοτημένα άτομα.

Κατά καιρούς, έχουν δοθεί ποικίλοι ορισμοί για τους κινδύνους του κυβερνοχώρου. Άλλοι εξ αυτών προσπαθούν να τους αποδώσουν μέσα σε ένα πιο περιορισμένο εννοιολογικό εύρος, ενώ άλλοι επιχειρούν να εκφράσουν μέσα από τον ορισμό το πιο γενικευμένο φάσμα των διαδικασιών και των τεχνικών ζητημάτων που συνδέονται με αυτής της μορφής των κινδύνων. Ένα κοινό στοιχείο των περισσότερων ορισμών που δίδονται για τον προσδιορισμό των κινδύνων του κυβερνοχώρου, είναι ότι τους συγκαταλέγουν στην κατηγορία των λειτουργικών κινδύνων (operational risks).

Σύμφωνα με τα όσα αναφέρουν οι Eling και Wirfs (2016)[50], ο κυβερνοχώρος νοείται ως ο διαδραστικός τομέας που αποτελείται από όλα τα ψηφιακά δίκτυα που χρησιμοποιούνται για την αποθήκευση, την τροποποίηση και την επικοινωνία των πληροφοριών και περιλαμβάνει όλα τα πληροφοριακά συστήματα που χρησιμοποιούνται για την υποστήριξη των επιχειρήσεων, των υποδομών και των υπηρεσιών που παρέχονται μέσω αυτών. Συνεχίζοντας, ορίζουν τους κινδύνους του κυβερνοχώρου, ως λειτουργικούς κινδύνους που σχετίζονται με τα περιουσιακά στοιχεία πληροφορικής και τεχνολογίας που έχουν συνέπειες που επηρεάζουν την εμπιστευτικότητα, τη

[50] Eling, M. and Wirfs, J., H, (2016), "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", Institute of Insurance Economics, [online], Διαθέσιμο στο: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf, (Ημερομηνία Πρόσβασης: 29/11/2018)

διαθεσιμότητα ή την ακεραιότητα των πληροφοριών και των πληροφοριακών συστημάτων ενός μεμονωμένου χρήστη ή οργανισμού.

Οι Mukhopadhyay et al. (2005[51], 2013[52]), ορίζουν τους κινδύνους του κυβερνοχώρου ως τον κίνδυνο που σχετίζεται με κακόβουλες ηλεκτρονικές πράξεις που προκαλούν διαταραχές στις επιχειρήσεις, καθώς και οικονομικές απώλειες. Οι Böhme και Kataria (2006)[53], αναφέρουν ότι είναι οι υπαίτιοι για τα προβλήματα στα πληροφοριακά συστήματα – προσδιορίζοντάς τους έτσι μέσω των συνεπειών που των αποτελεσμάτων που επιφέρουν. Τέλος, οι Ögüt et al. (2011)[54], τους ορίζουν, επιγραμματικά, ως τους κινδύνους των πληροφοριακών συστημάτων.

3.3 Ταξινόμηση των Κινδύνων του Κυβερνοχώρου

Σύμφωνα με τους Eling και Schnell (2016)[55], οι κίνδυνοι του κυβερνοχώρου μπορούν να ταξινομηθούν ανάλογα με τη δραστηριότητα (π.χ. εγκληματική και μη εγκληματική), τον τύπο της επίθεσης (π.χ. κακόβουλα προγράμματα, ανεπιθύμητη αλληλογραφία κλπ.) και την πηγή (π.χ. τρομοκράτες, εγκληματίες). Υπογραμμίζουν δε ότι οι κίνδυνοι αυτοί συνίστανται, κυρίως, σε εκδηλώσεις εγκληματικής δραστηριότητας. Σε μια προσπάθεια να ταξινομήσουν τους κινδύνους του κυβερνοχώρου, βάσει της προέλευσής τους, οι Eling και Wirfs (2016)[56] τους διαχωρίζουν με

[51] Mukhopadhyay, A., Saha, D., Chakrabarti, B., B., Mahanti, A. and Podder, A. (2005), "Insurance for Cyber-risk: A Utility Model", *Decision*, 32 (1), pp. 1-19

[52] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2013), "Cyber-Risk Decision Models: To Insure IT or Not?", *Decision Support Systems*, 56 (1), pp. 11–26

[53] Böhme, R. and Kataria, G. (2006), "Models and measures for correlation in cyber-insurance", Workshop on Economics of Information Security (WEIS), [online], Διαθέσιμο στο: https://www.econinfosec.org/archive/weis2006/docs/16.pdf, (Ημερομηνία Πρόσβασης: 29/11/2018)

[54] Ögüt, H., Raghunathan, S., and Menon, N. (2011), "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection", *Risk Analysis*, 31 (3), pp. 497–512

[55] Eling, M. and Schnell, W. (2016), "What do we know about cyber risk and cyber risk insurance?", *The Journal of Risk Finance*, 17 (5), pp. 474-491

[56] Eling, M. and Wirfs, J., H, (2016), "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", Institute of Insurance Economics, [online], Διαθέσιμο στο:

κριτήριο την εγκληματική δραστηριότητα. Σύμφωνα με τους αρθρογράφους, οι κίνδυνοι του κυβερνοχώρου που δεν βασίζονται σε εγκληματικά κίνητρα, μπορεί να σχετίζονται με φυσικές καταστροφές (όπως π.χ. πλημμύρες, πυρκαγιές, σεισμούς, κλπ.), με αστοχίες του τεχνολογικού εξοπλισμού (π.χ. διαγραφή δεδομένων από τα φυσικά μέσα αποθήκευσης – «σκληροί δίσκοι» - μετά από κάποια επανεκκίνηση του πληροφοριακού συστήματος) και με περιπτώσεις ακούσιων ανθρωπίνων σφαλμάτων. Από την άλλη πλευρά, οι κίνδυνοι του κυβερνοχώρου που σχετίζονται με εγκληματικές πράξεις, μπορούν να εκδηλωθούν μέσω φυσικών επιθέσεων (όπως π.χ. η κλοπή δεδομένων από τον φυσικό εξοπλισμό του αποθηκευτικού χώρου του πληροφοριακού συστήματος), μέσω επιθέσεων χάκερ (π.χ. κατασκοπεία δεδομένων πελατών ή δολιοφθορά επιχειρήσεων) και μέσω κρουσμάτων εκβιασμού (π.χ. κλοπή ευαίσθητων δεδομένων και εκβιασμός για καταβολή χρηματικού ποσού – λύτρων – για την μη δημοσιοποίησή τους).

Ο RSA (2016)[57], κατατάσσει τους κινδύνους του κυβερνοχώρου, βάσει της πηγής προέλευσής τους και του σκοπού τους, σε εσωτερικούς και εξωτερικούς. Σύμφωνα με την κατηγοριοποίηση αυτή, εντοπίζονται οι εξής τέσσερις μορφές κινδύνων:

- Εσωτερικοί Κακόβουλοι (Internal Malicious): Σχετίζονται με εσκεμμένες πράξεις σαμποτάζ, κλοπής ή άλλων κακόβουλων δράσεων που διαπράττονται από υπαλλήλους του οργανισμού ή/και άλλα έμπιστα συνδεδεμένα μέρη αυτού. Παράδειγμα τέτοιας πράξης μπορεί να αποτελέσει ένας δυσαρεστημένος υπάλληλος ο οποίος διαγράφει βασικές πληροφορίες και δεδομένα προτού εγκαταλείψει τον οργανισμό.
- Εσωτερικοί Ακούσιοι (Internal Unintentional): Αφορούν πράξεις που οδηγούν σε ζημιές ή απώλειες δεδομένων από τα πληροφοριακά συστήματα του οργανισμού, που οφείλονται σε ανθρώπινο λάθος των εργαζομένων, καθώς και άλλων έμπιστων συνεργατών.
- Εξωτερικοί Κακόβουλοι (External Malicious): Σύμφωνα με τον RSA, πρόκειται για την πιο δημοφιλή μορφή κινδύνων στον κυβερνοχώρο. Σχετίζονται με οργανωμένες επιθέσεις από τρίτα - μη συνδεδεμένα μέρη – του οργανισμού, συμπεριλαμβανομένων των εγκληματικών οργανώσεων, των χάκερ και της οργανωμένης εθνικής κατασκοπείας.

---

https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf, (Ημερομηνία Πρόσβασης: 29/11/2018)

[57] https://www.rsa.com

- Εξωτερικοί Ακούσιοι (External Unintentional): Είναι κίνδυνοι παρόμοιοι με τους εσωτερικούς ακούσιους και προκαλούν απώλεια ή βλάβη στην επιχείρηση, αλλά όχι σκόπιμα.

Σε μια, σχετικά, παρόμοια ταξινόμηση των κινδύνων του κυβερνοχώρου, προχωράνε στην εργασία τους και οι Brockett et al. (2012)[58], οι οποίοι τους χωρίζουν (και τους αναλύουν περαιτέρω) σε εσωτερικούς και εξωτερικούς. Σχετικά με τους εσωτερικούς κινδύνους αναφέρουν ότι πληθώρα καταγεγραμμένων περιστατικών παραβιάσεων των εταιρικών κυβερνοχώρων προέρχεται από το εσωτερικό των οργανώσεων. Παρά το γεγονός ότι ένας υπάλληλος μπορεί να προσδίδει σημαντική (ίσως και αναντικατάστατη σε ορισμένες περιπτώσεις) προστιθέμενη αξία σε μια επιχείρηση, δεν αποκλείεται να εκτίθεται συνεχώς σε τεράστιες ποσότητες εμπιστευτικών πληροφοριών, γεγονός που δύναται, σε ορισμένες περιπτώσεις, να αυξήσει τον πειρασμό για δημιουργία ατομικού κέρδους από την εκμετάλλευσή τους.

Στο πλαίσιο αυτό, αναγνωρίζουν τις εξής δύο βασικές περιπτώσεις κινδύνων του κυβερνοχώρου που προέρχονται από το εσωτερικό μιας επιχείρησης (ορισμένοι εξ αυτών αφορούν και τους κινδύνους που προέρχονται από το εξωτερικό του οργανισμού):

- Κλοπή δεδομένων (Data theft): Η κλοπή δεδομένων είναι ο όρος που χρησιμοποιείται όταν οι πληροφορίες αντιγράφονται παράνομα ή υποκλέβονται από μια επιχείρηση ή ένα άλλο άτομο. Η κλοπή δεδομένων από το εσωτερικό του οργανισμού, μπορεί να θέσει σε κίνδυνο την επιχείρηση εξίσου εύκολα όσο μια αντίστοιχη εξωτερική επίθεση. Λόγω της προνομιακής θέσης τους, οι εργαζόμενοι έχουν μεγαλύτερη ικανότητα να ενεργήσουν ως δράστες, αφού ήδη έχουν τις άδειες εισόδου στα πληροφοριακά εταιρικά συστήματα. Οι συγγραφείς επισημαίνουν ωστόσο, το ότι η κλοπή των δεδομένων δεν είναι απαραίτητο να έχει πάντα ως στόχο τις πληροφοριακές δομές μιας επιχείρησης ή τα στοιχεία των πελατών της, αλλά δύναται να εστιάζει και στην υποκλοπή των στοιχείων που αφορούν τους υπαλλήλους του οργανισμού.
- Κλοπή ευαίσθητων προσωπικών δεδομένων (Identification theft): Σύμφωνα με τους ερευνητές, η κλοπή ευαίσθητων προσωπικών δεδομένων, είναι μια ακόμα γνωστή ευπάθεια των επιχειρήσεων στον κυβερνοχώρο, τόσο από εσωτερικές όσο και από εξωτερικές πηγές. Οι εργαζόμενοι μπορούν να αποκτήσουν πρόσβαση σε προσωπικά στοιχεία των πελατών, όπως

[58] Brockett, L., P., Golden, L., L. and Wolman, W. (2012), "Enterprise Cyber Risk Management, Risk Management for the Future - Theory and Cases", [online], Διαθέσιμο στο: http://www.intechopen.com/books/risk-management- for-the-future-theory-andcases/enterprise-cyber-risk-management, (Ημερομηνία Πρόσβασης: 29/11/2018)

ονόματα, αριθμούς τηλεφώνων, διευθύνσεις, ονόματα χρηστών, κωδικούς πρόσβασης και PIN, αριθμούς πιστωτικών καρτών και άλλων λογαριασμών, καθώς και αριθμούς κοινωνικής ασφάλισης, αλλά και όποια άλλη σχετική πληροφορία μπορεί να υπάρχει διαθέσιμη. Οι πληροφορίες αυτές μπορούν στη συνέχεια να πωληθούν στο διαδίκτυο ή να χρησιμοποιηθούν από τον ίδιο τον εισβολέα για σκοπούς εκβιασμού μέσω της απειλής έκθεσης των δεδομένων.

Τέλος, η Grant Thornton (2018)[59], αναφέρει στην σχετική της έκθεση περί των κινδύνων του κυβερνοχώρου ότι, σε σχέση με άλλες μορφές επιχειρηματικών κινδύνων, οι κίνδυνοι αυτοί παρουσιάζουν αρκετές προκλήσεις. Μια εξ αυτών σχετίζεται με το ότι οι κίνδυνοι στον κυβερνοχώρο αποτελούν μια συνεχόμενη και αδιάκοπη απειλή, ενώ είναι δύσκολο να προσδιοριστούν και να ποσοτικοποιηθούν. Σε αντίθεση με τους πιστωτικούς, τους επενδυτικούς και άλλους κινδύνους, οι κίνδυνοι στον κυβερνοχώρο εκθέτουν τον οργανισμό και τους ενδιαφερόμενους με τρόπους που είναι δύσκολο να οριοθετηθούν.

3.4 Κόστος και Συνέπειες των Κινδύνων του Κυβερνοχώρου

Η εκτίμηση του κόστους που συνεπάγονται οι κίνδυνοι του κυβερνοχώρου είναι δύσκολη, καθώς περικλείονται από μεγάλη αβεβαιότητα και δεν υπάρχει κάποια διαθέσιμη και κοινώς αποδεκτή πηγή πληροφοριών αναφορικά με το ορθώς υπολογισμένο κόστος αυτής της μορφής των κινδύνων. Σύμφωνα με τους Eling και Schnell (2016), ορισμένοι τύποι παραβάσεων στον κυβερνοχώρο δεν συνεπάγονται κάποιο άμεσο κόστος ή δεν μπορούν να ποσοτικοποιηθούν (π.χ. εξάπλωση ρατσισμού, εμπόριο παράνομων ναρκωτικών ουσιών κλπ.). Σύμφωνα με τα όσα αναφέρουν, το συνολικό κόστος των κινδύνων του κυβερνοχώρου εκτιμάται, γενικά, ότι ξεπερνά τα 100 δισ. δολάρια, γεγονός που υπογραμμίζει την οικονομική σημασία και το βαρύ αντίκτυπό τους για την παγκόσμια οικονομία. Αναγνωρίζουν ωστόσο, ότι αν και υπάρχουν πολλές σχετικές δημοσιεύσεις που επισκοπούν το κόστος των κινδύνων αυτών, τα ευρήματά τους ποικίλουν, ως αποτέλεσμα τόσο των στοιχείων που χρησιμοποιούνται, όσο και των μεθόδων αξιολόγησής τους.

[59] Grant Thornton. (2018), "*Taking AIM at cyber risk*".

Σύμφωνα με τον Ulsch (2014)[60], το κόστος που σχετίζεται με τους κινδύνους τους κυβερνοχώρου μπορεί να μετρηθεί και να αξιολογηθεί από διάφορες οπτικές. Καταρχάς, υπάρχει η πραγματική απώλεια που συνδέεται με μια παραβίαση, όπως για παράδειγμα μια χρηματική κλοπή. Πέραν των άμεσων φυσικών συνεπειών, εντοπίζονται τα κόστη διαχείρισης και αποκατάστασης των παραβιάσεων και των συνεπειών τους. Επιπλέον, δεν θα πρέπει να λησμονείται και το κόστος που σχετίζεται με τα διαφυγόντα/χαμένα έσοδα από την ενδεχόμενη μείωση της πελατειακής βάσης, μετά από κάποιο περιστατικό παραβίασης του εταιρικού κυβερνοχώρου. Μια ακόμα εξίσου σημαντική πτυχή κόστους είναι και η απώλεια της εμπιστοσύνης των άμεσων συνεργατών της επιχείρησης, η οποία μπορεί να συνοδεύεται και από την άμεση αποχώρησή τους ή τον δισταγμό τους για μελλοντικές συνεργασίες. Όπως χαρακτηριστικά αναφέρει, όλες οι ανωτέρω απώλειες και το κόστος που αυτές συνεπάγονται, δημιουργούν έντονη αβεβαιότητα για το μέλλον, ενώ επίσης καθιστούν δύσκολο τον υπολογισμό του βραχυπρόθεσμου κόστους για τον οργανισμό.

Στην έκθεση της Allianz (2015)[61], αναφέρονται πολλά και ενδιαφέροντα στατιστικά στοιχεία σχετικά με τον οικονομικό αντίκτυπο των καταγεγραμμένων επιθέσεων εναντίον των πληροφοριακών συστημάτων των οργανισμών και επιχειρήσεων σε παγκόσμια κλίμακα. Σύμφωνα με αυτά (και για το έτος 2015), το εκτιμώμενο κόστος για την παγκόσμια οικονομία από τα εγκλήματα στον κυβερνοχώρο, ανέρχεται στα 445 δις. δολάρια, ενώ το κόστος που αφορά τέσσερις από τις μεγαλύτερες οικονομίες του κόσμου (ΗΠΑ, Κίνα, Γερμανία και Ιαπωνία) ξεπερνάει τα 200 δις. δολάρια. Ενδιαφέρον παρουσιάζει επίσης ότι οι δέκα μεγαλύτερες οικονομίες, παγκοσμίως, συγκεντρώνουν περισσότερο από το 50% των εγκληματικών πράξεων στον κυβερνοχώρο. Τέλος, δύο ακόμα στατιστικά στοιχεία επί του θέματος μαρτυράνε την σοβαρότητα αυτής της μορφής των κινδύνων. Το πρώτο σχετίζεται με την δραματική αύξηση των καταγεγραμμένων κρουσμάτων κατά των πληροφοριακών συστημάτων, παγκοσμίως, σε περίπου 43 εκατομμύρια, αριθμός που συνεπάγεται την εκδήλωση, περίπου, 117.000 κρουσμάτων ημερησίως (τουλάχιστον για το 2015). Το δεύτερο στατιστικό στοιχείο αφορά την αλματώδη μετάβαση των κινδύνων του κυβερνοχώρου, στη λίστα των πιο σοβαρών μορφών κινδύνων παγκοσμίως, από την 15η θέση το 2013, στην 5η

[60] Ulsch, M. (2014), "*Cyber Threat! How to manage the growing risk of cyber attacks*", Published by John Wiley & Sons, Ltd.

[61] Allianz Global Corporate Specialty. (2015), "A Guide to Cyber Risk"

θέση το 2015. Κατά καιρούς, διάφορες έρευνες που δημοσιεύθηκαν από ασφαλιστικές εταιρείες και συναφείς οργανισμούς παροχής συμβουλευτικής καθοδήγησης, έχουν προσπαθήσει να εκτιμήσουν το παγκόσμιο κόστος των κινδύνων του κυβερνοχώρου. Η Symantec (2017)[62] υπολογίζει ότι το κόστος που επωμίστηκαν τα θύματα των επιθέσεων στον κυβερνοχώρο, ανέρχεται (για το 2017) στα 172 δις. δολάρια. Από την άλλη πλευρά, η McAfee (2017)[63], αναφέρει ότι το κόστος αυτό ανέρχεται στα 600 δις. δολάρια. Τέλος, παραθέτοντας μια σχετική δημοσίευση στο Forbes, από τον αρθρογράφο Eubanks (2018)[64], το κόστος των επιθέσεων στον κυβερνοχώρο αναμένεται να ξεπεράσει τα 6 τρις. δολάρια μετά το 2021.

Συνοψίζοντας το θέμα του κόστους που προκαλείται από τις επιθέσεις στον κυβερνοχώρο, παραθέτουμε τα όσα αναφέρει ο Ulsch (2014), σχετικά με ορισμένους παράγοντες που σχετίζονται με το κόστος των κινδύνων στον κυβερνοχώρο.

- Η μη έγκαιρη αναγνώριση των επιθέσεων. Είναι λογικό ότι όσο νωρίτερα ανιχνευτεί μια επικείμενη επίθεση κατά του εταιρικού πληροφοριακού συστήματος, τόσο περισσότερες είναι οι πιθανότητες να αποφευχθούν τα χειρότερα, υπό την έννοια της πρόκλησης περισσότερων και μεγαλύτερων ζημιών (οικονομικών και μη, τόσο άμεσων όσο και έμμεσων).
- Οι δείκτες και τα σημάδια που μαρτυράνε απόπειρες επιθέσεων δεν ερμηνεύονται σωστά και κατά συνέπεια δεν δημιουργείται αίσθηση επείγουσας ανάγκης ή αμεσότητας, κάτι που με την σειρά του οδηγεί στην ανωτέρω παρατήρηση, δηλαδή της μη έγκαιρης αναγνώρισης της επίθεσης και της απώλειας πολύτιμου χρόνου για την αποτελεσματικότερη αντιμετώπισή της.
- Μια από τις πρώτες αντιδράσεις είναι, συνήθως, η διαχείριση της επίθεσης εσωτερικά, χρησιμοποιώντας μόνο ίδιους πόρους, οι οποίοι συχνά αποτελούν ανεπαρκή προσέγγιση, με αποτέλεσμα την απώλεια πολύτιμου χρόνου διερεύνησης και την προσθήκη κόστους.

---

[62] Symantec. (2017), "*Norton Cyber Security Insights Report Global Results*", [online], Διαθέσιμο στο: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf, (Ημερομηνία Πρόσβασης: 30/11/2018)

[63] McAfee. (2017), "The Economic Impact of Cybercrime—No Slowing Down", [online], Διαθέσιμο στο: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf, (Ημερομηνία Πρόσβασης: 30/11/2018)

[64] Eubanks, N. (2018), "The True Cost Of Cybercrime For Businesses", [online], Διαθέσιμο στο: https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/, (Ημερομηνία Πρόσβασης: 30/11/2018)

- Η ανεπάρκεια συστηματικής προσέγγισης διαχείρισης των εταιρικών κινδύνων, η οποία ξεκινάει από τα ανώτερα διοικητικά στρώματα των οργανισμών, οδηγεί στον ελλιπή σεβασμό απέναντι σε αυτούς τους κινδύνους και κατά συνέπεια, στην υποδεέστερη οργάνωση έναντι αυτών.
- Τέλος, η έλλειψη επαρκούς εκπαίδευσης και προσομοίωσης των αντιδράσεων των κυρίων εμπλεκομένων μερών σε σενάρια εκδήλωσης τέτοιων γεγονότων είναι ένα ακόμα στοιχείο που δύναται να αυξήσει τον οικονομικό (και όχι μόνο) αντίκτυπο αυτής της μορφής των κινδύνων.

Σε αυτό το σημείο, θα πρέπει να τονίσουμε, για μία ακόμα φορά, ότι πολλοί επιστήμονες και ερευνητές είναι διστακτικοί ως προς την εγκυρότητα και την ακρίβεια των δημοσιευμένων στοιχείων περί του παγκόσμιου κόστους που προκαλείται από τις επιθέσεις έναντι των πληροφοριακών συστημάτων. Η έλλειψη έγκυρων στοιχείων σχετικά με τις οικονομικές επιπτώσεις αυτής της μορφής των κινδύνων οδηγεί, σε πολλές περιπτώσεις, στην διενέργεια επισφαλών εκτιμήσεων και στον συνυπολογισμό διαφόρων μορφών κόστους (όπως π.χ. το κόστος απώλειας της καλής φήμης, αλλά και άλλων μορφών άυλων στοιχείων), ο οποίος μπορεί και να απέχει πολύ από την πραγματικότητα της κατάστασης.

3.5 Διαχείριση των Κινδύνων του Κυβερνοχώρου

Σε αυτή την υποενότητα θα προχωρήσουμε στην παρουσίαση ορισμένων επιστημονικών, ερευνητικών και επαγγελματικών θέσεων που σχετίζονται με την διαχείριση των κινδύνων του κυβερνοχώρου. Αν και στο διαδίκτυο υπάρχει πληθώρα σχετικών δημοσιεύσεων, οι οποίες σε μεγάλο βαθμό αναπαράγουν τις ίδιες κεντρικές ιδέες, εντούτοις τα στοιχεία που θα παραθέσουμε επιλέχθηκαν εξαιτίας της απλότητας και της επεξηγηματικότητάς τους.

Στην έκθεση της Deloitte (2016)[65], σχετικά με την ορθή εκτίμηση και την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου, παρουσιάζονται δέκα καίριες ερωτήσεις, τις οποίες καλούνται να απαντήσουν οι διοικούντες των οργανισμών προκειμένου να αξιολογήσουν τον βαθμό της ετοιμότητας της επιχείρησής τους (αλλά και των ιδίων, καθώς και των υπαλλήλων) απέναντι στους κινδύνους του κυβερνοχώρου. Κεντρικός στόχος είναι εκτιμηθεί το κατά πόσον η επιχείρηση: α) είναι ασφαλής, β) βρίσκεται σε συνεχή επαγρύπνηση και γ) διαθέτει ανθεκτικές δομές έναντι αυτής της μορφής των κινδύνων.

1. Επιδεικνύεται η δέουσα επιμέλεια ως προς την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου;
2. Η ηγεσία της επιχείρησης διαθέτει τις απαιτούμενες γνώσεις και την αντίστοιχη διορατικότητα προκειμένου να διαχειριστεί σωστά αυτούς τους κινδύνους;
3. Έχει δημιουργηθεί ένα κατάλληλο πλαίσιο προσδιορισμού των κινδύνων του κυβερνοχώρου, καθώς και ταξινόμησής τους αναλόγως του αντικτύπου τους για τον οργανισμό, που να περιλαμβάνει την όρεξη για ανάληψη κινδύνου, αλλά και τα κατώτατα όρια αναφοράς;
4. Επικεντρωνόμαστε και επενδύουμε στα σωστά πράγματα; Και αν ναι, πώς αξιολογούμε και μετράμε τα αποτελέσματα των αποφάσεών μας;
5. Ευθυγραμμίζεται το εταιρικό πρόγραμμα διαχείρισης των κινδύνων του κυβερνοχώρου, καθώς και οι επιμέρους δυνατότητές μας με τα πρότυπα του κλάδου, αλλά και τις αντίστοιχες επιχειρήσεις του ίδιου κλάδου;
6. Η κουλτούρα του οργανισμού είναι προσανατολισμένη προς την αναγνώριση και την ευαισθητοποίηση έναντι των κινδύνων του κυβερνοχώρου;

[65] Deloitte. (2016), "*Assessing Cyber Risk. Critical questions for the board and the C-suite*"

7. Τι έχουμε πράξει έτσι ώστε να προστατέψουμε τον οργανισμό από τους κινδύνους του κυβερνοχώρου;
8. Μπορούμε να μετριάσουμε σύντομα τις ζημίες και να κινητοποιήσουμε άμεσα πόρους απόκρισης όταν συμβαίνει μια επίθεση κατά των πληροφοριακών μας συστημάτων;
9. Πώς αξιολογούμε την αποτελεσματικότητα του προγράμματος εταιρικής διαχείρισης των κινδύνων του κυβερνοχώρου;
10. Είμαστε ένας ισχυρός και ασφαλής κρίκος των εξαιρετικά συνδεδεμένων οικοσυστημάτων στα οποία λειτουργούμε;

Επισκοπώντας βιβλιογραφικά το θέμα της διαχείρισης των κινδύνων του κυβερνοχώρου, οι Eling και Schnell (2016), αναφέρουν ότι μια σημαντική πτυχή του ζητήματος αυτού είναι ότι ο κυβερνοχώρος δεν αποτελεί αποκλειστική ευθύνη του τμήματος πληροφορικής της επιχείρησης, αλλά απαιτεί έναν γενικό διάλογο μεταξύ των διαφόρων τμημάτων, αλλά κυρίως την άμεση ευαισθητοποίηση και εμπλοκή της ανώτατης διοίκησης και του διοικητικού συμβουλίου. Κατόπιν, συγκεντρώνουν την διαδικασία οργάνωσης και διαχείρισης των κινδύνων του κυβερνοχώρου, μέσα από τα εξής βήματα:

- Το πρώτο βήμα στην κλασική διαδικασία διαχείρισης των κινδύνων του κυβερνοχώρου είναι ο καθορισμός της αρχικής κατάστασης και των στόχων που η επιχείρηση επιθυμεί να επιτύχει μέσα από την αποτελεσματική διαχείριση των κινδύνων αυτών.
- Έπειτα, για την εκτίμηση του κινδύνου πρέπει να προσδιορίζονται τα σχετικά περιουσιακά στοιχεία που απειλούνται (άμεσα ή έμμεσα), καθώς και οι αντίστοιχες επιχειρηματικές διαδικασίες που σχετίζονται (ή εξαρτώνται) με αυτά. Στη συνέχεια, πρέπει να προσδιοριστούν οι πιθανές απειλές και οι πηγές τους.
- Το επόμενο βήμα εμπεριέχει τον, όσο το δυνατόν πιο έγκυρο, προσδιορισμό του εκτιμώμενου κόστους και των συνεπειών που δύναται να προκληθούν στον οργανισμό από την ανεπιτυχή αντιμετώπιση μιας επίθεσης στον κυβερνοχώρου του.
- Το τέταρτο βήμα, είναι αυτό της συνεχούς παρακολούθησης των κινδύνων του κυβερνοχώρου. Καθώς ο κυβερνοχώρος είναι εξαιρετικά δυναμικός και εξελίσσεται συνεχώς η αδιάκοπη παρακολούθηση των κινδύνων που εγκυμονεί είναι ένα ακόμα κλειδί στην αποτελεσματική διαχείρισή τους. Δεδομένου ότι οι στρατηγικές επίθεσης αλλάζουν διαρκώς, η διαχείριση του κινδύνου πρέπει να βελτιώνεται συνεχώς.

- Το τελευταίο βήμα είναι αυτό της εφαρμογής των διαφόρων μεθόδων διαχείρισης των κινδύνων του κυβερνοχώρου. Σύμφωνα με τους συγγραφείς, εντοπίζονται τέσσερις βασικές μέθοδοι, οι οποίοι είναι η αποφυγή του ρίσκου, ο μετριασμός των κινδύνων, η μεταφορά του ρίσκου (ή μέρους αυτού) και η διατήρηση/ανάληψη των κινδύνων και του ρίσκου που αυτοί συνεπάγονται.

Σχολιάζοντας περαιτέρω την τελευταία παράγραφο, οι συγγραφείς επεξηγούν ότι η αποφυγή/αποτροπή των κινδύνων του κυβερνοχώρου συνεπάγεται την μη λειτουργία εταιρικών πληροφοριακών συστημάτων, πράγμα αρκετά δύσκολο, ειδικά βάσει των απαιτήσεων της σημερινής εποχής. Από την άλλη πλευρά, η ανάληψη των κινδύνων απαιτεί την πολύ προσεκτική εκτίμηση του ρίσκου που αυτοί εγκυμονούν, καθώς και την ενδελεχή προετοιμασία για το ενδεχόμενο του να βρεθεί η επιχείρηση άμεσα αντιμέτωπη με κρούσματα επιθέσεων κατά των πληροφοριακών της συστημάτων. Όσον αφορά την μεταφορά του ρίσκου, αναγνωρίζουν τα γενναία βήματα που έχουν πραγματοποιηθεί, ειδικά τη τελευταία δεκαετία, προς την άνθιση της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου. Τέλος, σχετικά με το θέμα του μετριασμού των κινδύνων, επισημαίνουν ότι πρόκειται για τον πιο δημοφιλή τρόπο διαχείρισής τους, καθώς μπορεί να στοχεύσει παράλληλα στον μετριασμό τόσο της πιθανότητας εμφάνισης κρουσμάτων επιθέσεων έναντι των εταιρικών πληροφοριακών συστημάτων (π.χ. μέσα από την εκτεταμένη χρήση προγραμμάτων προστασίας του εταιρικού κυβερνοχώρου), όσο και των πιθανών απωλειών που μπορεί να προκύψουν από τα κρούσματα αυτά.

Επί του θέματος του μετριασμού/περιορισμού της πιθανότητας εμφάνισης των κινδύνων του κυβερνοχώρου, η Allianz (2015) αναφέρει στην σχετική της έκθεση πέντε βασικά βήματα για την αποτελεσματικότερη οργάνωση προς αυτή την κατεύθυνση.

1) Προσδιορισμός των βασικών στοιχείων του ενεργητικού που βρίσκονται σε κίνδυνο, καθώς και των οργανικών αδυναμιών όπως ο ανθρώπινος παράγοντας ή η υπερβολική εξάρτηση από τρίτα (συνδεδεμένα) μέρη.
2) Δημιουργία (ή ενδυνάμωση) μιας εταιρικής κουλτούρας που σέβεται και αναγνωρίζει την σημαντικότητα των κινδύνων του κυβερνοχώρου. Αυτό θα πρέπει να συνοδεύεται και από την επαρκή εκπαίδευση των εργαζομένων και των ενδιαφερομένων μερών της επιχείρησης.

3) Εφαρμογή ενός σχεδίου διαχείρισης κρίσεων και αντιμετώπισης παραβιάσεων, το οποίο θα πρέπει να δοκιμαστεί και να αξιολογηθεί προκειμένου να εντοπιστούν τυχόν αστοχίες ή/και παραλείψεις.
4) Ενδελεχής εξέταση του πώς οι εταιρικές δραστηριότητες που σχετίζονται με τα τρίτα (συνεργαζόμενα) μέρη, ενδέχεται να επηρεαστούν από κάποια πιθανή επίθεση στον κυβερνοχώρο. Επιπροσθέτως, θα πρέπει να προσδιοριστούν και τα περισσότερα πιθανά σενάρια παραβιάσεων που δύναται να κληθεί να αντιμετωπίσει η επιχείρηση.
5) Θα πρέπει να ληφθούν αποφάσεις σχετικά με τους κινδύνους που η επιχείρηση θα πρέπει να αποφύγει, να αναλάβει, να μετριάσει ή και να μεταφέρει.

Τέλος, παραθέτουμε τις προτάσεις των Siegel et al. (2002)[66], οι οποίες αν και προέρχονται από μια χρονικά «παλαιότερη» δημοσίευση (τουλάχιστον για το πολύ δυναμικό περιβάλλον των σύγχρονων πληροφοριακών συστημάτων), εντούτοις περιγράφουν πολύ περιεκτικά τα αναγκαία βήματα για την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου. Σύμφωνα με τα όσα αναφέρουν, η διαχείριση των κινδύνων του κυβερνοχώρου απεικονίζεται μέσα από μια κυκλική διαδικασία, η οποία περιλαμβάνει πέντε βασικά στάδια. Αυτά έχουν ως εξής:

Εκτίμηση (Assessment)

- Αξιολόγηση των ασφαλιστικών δικλίδων του οργανισμού, διενέργεια δοκιμαστικών προσομοιώσεων αντοχών και συνεντεύξεων με το προσωπικό που εμπλέκεται πιο άμεσα με την διαχείριση και την λειτουργία των εταιρικών πληροφοριακών συστημάτων.
- Χρησιμοποίηση τυποποιημένων προτύπων και μεθοδολογιών (όπως για παράδειγμα τα σχετικά πρότυπα ISO) και διενέργεια αξιολόγησης επ' αυτών.

Περιορισμός (Mitigation)

- Δημιουργία και εφαρμογή πολιτικών και διαδικασιών που διασφαλίζουν υψηλά επίπεδα ασφάλειας εντός του οργανισμού.
- Εφαρμογή μηχανισμών μετριασμού και μεταφοράς του χρηματοοικονομικού κινδύνου.
- Συνεχόμενος έλεγχος της διατήρησης του επιθυμητού επιπέδου ασφαλείας.

[66] Siegel, C., A., Sagalow , T., R. and & Serritella, P. (2002), "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security, *Information Systems Security*, 11 (4), pp. 33-49

Ασφάλιση (Insurance)

- Επιλέξτε του βέλτιστου ασφαλιστικού φορέα με βάση την τεχνογνωσία, την οικονομική ισχύ και την παγκόσμια εμβέλειά του.
- Επιλογή της σωστής πολιτικής ασφάλισης, συμπεριλαμβανομένης της άμεσης κάλυψης της επιχείρησης αλλά και των πλησιέστερων ενδιαφερομένων μερών.
- Η διενέργεια ασφάλισης έναντι των κινδύνων του κυβερνοχώρου θα πρέπει να θεωρείται ως μια λύση μετατόπισης του κινδύνου και θα πρέπει να προκύπτει μέσα από μια λεπτομερή και τεκμηριωμένη αξιολόγηση των εταιρικών κινδύνων.
- Συνεργασία με τον ασφαλιστικό πάροχο για τον έγκυρο και τεκμηριωμένο προσδιορισμό πιθανών απωλειών, καθώς και των επιχειρηματικών επιπτώσεων που μπορεί να συνεπάγεται μια παραβίαση του εταιρικού κυβερνοχώρου.

Ανίχνευση (Detection)

- Παρακολούθηση των περιουσιακών στοιχείων για την ανακάλυψη τυχόν ασυνήθιστων δραστηριοτήτων.
- Εφαρμογή ενός συστήματος εικοσιτετράωρης παρακολούθησης που θα περιλαμβάνει ανίχνευση εισβολών, καθώς και αδιάλειπτη λειτουργία λογισμικού τείχους προστασία, για τον έγκαιρο εντοπισμό και αποτροπή οποιασδήποτε πιθανής εισβολής.
- Ανάλυση των αρχείων καταγραφής για τον προσδιορισμό τυχόν παρελθόντων συμβάντων που δεν εντοπίστηκαν την στιγμή που έπρεπε.

Αποκατάσταση (Remediation)

- Κατανόηση των οργανικών προβλημάτων και των αναγκών για βελτίωση των πιο ευπαθών και τρωτών σημείων του πληροφοριακού συστήματος.
- Προσδιορισμός των πιο ευάλωτων περιοχών που χρήζουν άμεσης προσοχής.
- Διενέργεια όλων των απαραίτητων βημάτων και διαδικασιών για την αντιμετώπιση και θωράκιση των ευπαθών αυτών σημείων.
- Ανάκτηση χαμένων δεδομένων από τα συστήματα δημιουργίας αντιγράφων ασφαλείας.
- Εξασφάλιση της συνεχιζόμενης δραστηριότητας της επιχείρησης μέχρι την αποκατάσταση των όποιων τυχόν ζημιών έχουν σημειωθεί από κάποιο περιστατικό παραβίασης του κυβερνοχώρου.

3.6 ISO 31000:2009 και Αρχές του COBIT 5 GEIT

Ο Διεθνής Οργανισμός Τυποποίησης (ISO)[67] αποτελεί σημείο αναφοράς, δεδομένου ότι τα πρότυπά του προτείνονται από πολλούς μεγάλους φορείς και εφαρμόζονται από σημαντικό πλήθος επιχειρήσεων ανά τον κόσμο. Στο πλαίσιο αυτό, ο οργανισμός διαχείρισης κινδύνων (RIMS)[68], προτρέπει την εφαρμογή του Διεθνούς Προτύπου Τυποποίησης 31000:2009 (το οποίο και αναθεωρήθηκε πρόσφατα το 2018), ως ένα ισχυρό και αποτελεσματικό εργαλείο για την αντιμετώπιση και διαχείριση των κινδύνων του κυβερνοχώρου. Για τις ανάγκες της παρουσίασης του προτύπου, ο Antonucci (2017)[69], επικεντρώνεται στις πέντε βασικές αρχές του «COBIT 5 GEIT Principles», τις οποίες και συσχετίζει με τις βασικές θέσεις του ISO 31000:2009. Η αποτελεσματική εταιρική διακυβέρνηση και η διαχείριση των πληροφοριών και της σχετικής τεχνολογίας (GEIT) αποτελεί πρωτίστως ευθύνη του διοικητικού συμβουλίου. Το COBIT 5 είναι ένα διεθνώς αποδεκτό επιχειρηματικό πλαίσιο GEIT από την ISACA[70], το οποίο αναπτύχθηκε από και για τους επαγγελματίες και περιλαμβάνει πληροφορίες σχετικά με την πληροφοριακή τεχνολογία και τη βιβλιογραφία περί της αποτελεσματικότερης διοίκησης.

Σύμφωνα με τα όσα αναφέρει ο συγγραφέας, μπορούμε να εξάγουμε τον κάτωθι συσχετισμό μεταξύ των κατευθυντήριων γραμμών του ISO 31000:2009 και των θέσεων του COBIT 5 GEIT, ο οποίος και παρουσιάζεται στον ακόλουθο πίνακα. Στο σημείο αυτό θα πρέπει να υπογραμμιστεί ότι το Πρότυπο ISO 31000:2009 δεν αφορά συγκεκριμένα την διαχείριση των κινδύνων του κυβερνοχώρου, αλλά επισκοπεί και προτείνει ένα γενικότερο πλαίσιο διαδικασιών διαχείρισης των εταιρικών κινδύνων. Σκοπός του συγγραφέα είναι να προσπαθήσει να συσχετίσει ορισμένα κομμάτια του πλαισίου αυτού, με τις αρχές του COBIT 5, προκειμένου να παρουσιάσει μια ολοκληρωμένη πρόταση περί της αποτελεσματικής διαχείρισης των κινδύνων του κυβερνοχώρου.

---

[67] https://www.iso.org/home.html

[68] https://www.rims.org/Pages/Default.aspx

[69] Antonucci, D. (2017), "*The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities*", Published by John Wiley & Sons, Inc. Hoboken, New Jersey

[70] https://www.isaca.org/pages/default.aspx

Πίνακας 1

	COBIT 5 GEIT PRINCIPLES				
	Ικανοποίηση των αναγκών των Ενδιαφερομένων Μερών	**Συνολική κάλυψη του Οργανισμού**	**Εφαρμογή ενός ενιαίου πλαισίου**	**Εφαρμογή μιας ολιστικής προσέγγισης**	**Διαχωρισμός διακυβέρνησης από το μάνατζμεντ**
ISO 31000:2009 RISK MANAGEMENT PRINCIPLES	Η διαχείριση των κινδύνων πρέπει να είναι διαφανής και περιεκτική.	Η διαχείριση κινδύνων δημιουργεί και προστατεύει την αξία.	Η διαχείριση κινδύνων είναι συστηματική, δομημένη και έγκαιρη.	Η διαχείριση κινδύνων αποτελεί αναπόσπαστο μέρος των διαδικασιών της οργάνωσης.	Η διαχείριση κινδύνων διευκολύνει τη συνεχή βελτίωση του οργανισμού.
	Η διαχείριση των κινδύνων είναι δυναμική, αδιάλειπτη και ανταποκρίνεται στην αλλαγή.	Η διαχείριση κινδύνων είναι προσαρμοσμένη στις ανάγκες του οργανισμού.		Η διαχείριση του κινδύνου λαμβάνει υπόψη τους ανθρώπινους και πολιτισμικούς παράγοντες.	
		Η διαχείριση κινδύνων αντιμετωπίζει ρητά την αβεβαιότητα.		Η διαχείριση κινδύνων αποτελεί μέρος της διαδικασίας λήψης αποφάσεων.	
				Η διαχείριση των κινδύνων βασίζεται στις καλύτερες διαθέσιμες πληροφορίες.	

Ικανοποίηση των αναγκών των Ενδιαφερομένων Μερών

Η πρώτη αρχή του COBIT 5, επικαλείται την ανάγκη εναρμόνισης των στόχων και των προτεραιοτήτων των μεμονωμένων ατόμων και των τμημάτων του οργανισμού, με τις ανάγκες της επιχείρησης και των ενδιαφερομένων μερών. Επιπροσθέτως, η αρχή αναγνωρίζει ότι οι ανάγκες των ενδιαφερομένων μερών και οι επιχειρησιακοί στόχοι δύναται να αλλάζουν με την πάροδο του χρόνου. Στο πλαίσιο αυτό, το IS0 31000:2009 αναγνωρίζει δύο βασικές συνδρομές της εταιρικής διαχείρισης των κινδύνων του κυβερνοχώρου.

Η διαχείριση των κινδύνων πρέπει να είναι διαφανής και περιεκτική

Σύμφωνα με την θέση του Προτύπου ISO, η κατάλληλη και έγκαιρη συμμετοχή των ενδιαφερομένων και, ιδίως, των υπευθύνων για τη λήψη αποφάσεων σε όλα τα επίπεδα της οργάνωσης διασφαλίζει ότι η διαχείριση των κινδύνων του κυβερνοχώρου παραμένει σχετική και συμπλέει με τις τρέχουσες εξελίξεις. Παραδείγματα ενδιαφερόμενων μερών στις διαδικασίες αξιολόγησης των κινδύνων του κυβερνοχώρου μπορεί να περιλαμβάνουν: α) Πελάτες, μετόχους, εργαζομένους, συνεργάτες της εφοδιαστικής αλυσίδας κλπ., β) Κυβερνητικές και ρυθμιστικές αρχές, γ) Μη-κυβερνητικές οργανώσεις, δ) Κοινωνικές ομάδες και ε) Διάφορα άλλα μέρη του κοινωνικού συνόλου (π.χ. τα μέσα επικοινωνίας).

Η σημασία αυτής της αρχής επιδεικνύεται όταν ο οργανισμός μπορεί να απαντήσει σε ερωτήσεις όπως:

- Τι προσδοκά το κάθε ενδιαφερόμενο μέρος από τον οργανισμό σχετικά με την διαχείριση των κινδύνων του κυβερνοχώρου;
- Ποιοι είναι οι (θεσμικοί) κανονισμοί που ισχύουν για τα ψηφιακά και ευαίσθητα δεδομένα που χρησιμοποιούνται, αποθηκεύονται και διαβιβάζονται από τον οργανισμό;
- Ποιες είναι οι εθελοντικές ή συμβατικές υποχρεώσεις που έχει αναλάβει ο οργανισμός σε σχέση με το δίκτυο, τα συστήματα και τη διαθεσιμότητα των δεδομένων, την αξιοπιστία, την ασφάλεια και τον σεβασμό της ιδιωτικότητας;

Η διαχείριση των κινδύνων είναι δυναμική, αδιάλειπτη και ανταποκρίνεται στην αλλαγή

Με το που απαντηθούν οι ανωτέρω ερωτήσεις, το επόμενο βήμα είναι αυτό της ικανοποίησης των απαιτήσεων και των αναγκών των ενδιαφερομένων μερών του οργανισμού. Αυτή η αρχή αναφέρει ότι η διαχείριση των κινδύνων του κυβερνοχώρου θα πρέπει να βρίσκεται σε συνεχή επαγρύπνηση έτσι ώστε να ανταποκρίνεται στις αλλαγές του δυναμικού περιβάλλοντος. Τα μεταβαλλόμενα γεγονότα στο εσωτερικό και στο εξωτερικό περιβάλλον του οργανισμού και η νέα γνώση στο πεδίο της πληροφοριακής τεχνολογίας, θα πρέπει να παρακολουθούνται στενά και καθότι οι αλλαγές αυτές δύναται να φέρουν στο προσκήνιο νέους κινδύνους, να επιφέρουν αλλαγές σε υφιστάμενους ή ακόμα και να παραμερίσουν ορισμένους (π.χ. απαρχαιωμένα πληροφοριακά συστήματα που απειλούνταν από ορισμένες μορφές κινδύνων του κυβερνοχώρου δεν αποτελούν, ενδεχομένως, στόχο μετά την απαξίωσή τους).

Σκοπός αυτής της αρχής είναι να διασταυρώσει τις ανάγκες των ενδιαφερομένων μερών της επιχείρησης με τα νέα και δυναμικά δεδομένα των σύγχρονων απαιτήσεων των πληροφοριακών συστημάτων, έτσι ώστε μέσα από αυτή τη διαδικασία να ικανοποιηθούν τόσοι οι απαιτήσεις τους, όσο και να εντοπιστούν, έγκαιρα και έγκυρα, τυχόν ευκαιρίες και απειλές του περιβάλλοντος της επιχείρησης. Η ανανέωση της τεχνολογίας, οι αλλαγές επιχειρησιακών διαδικασιών, οι νέες εφαρμογές / λύσεις λογισμικού και οι αλλαγές στον τρόπο με τον οποίο κάθε ενδιαφερόμενος έχει πρόσβαση και χρησιμοποιεί το εταιρικό δίκτυο, τα συστήματα και τα δεδομένα του οργανισμού, αποτελούν ορισμένα μόνο από τα πολλά παραδείγματα που θα πρέπει να επισκοπηθούν αναλυτικά. Αυτή η αρχή ικανοποιείται όταν οι αβεβαιότητες και οι αλλαγέςπου μεταβάλλουν τα στοιχεία της πληροφοριακής τεχνολογίας της επιχείρησης, τους στόχους του οργανισμού ή τις ανάγκες των ενδιαφερομένων μερών, ενσωματώνονται στις διαδικασίες επίσημης και άτυπης διαχείρισης της αλλαγής του οργανισμού, ανεξάρτητα από το πότε δύναται να επέλθουν οι αλλαγές αυτές.

Συνολική κάλυψη του Οργανισμού

Η δεύτερη αρχή του COBIT 5 αναγνωρίζει ότι η διαχείριση της πληροφοριακής τεχνολογίας ως περιουσιακού στοιχείου της επιχείρησης, αποτελεί ουσιαστικό στοιχείο της δημιουργίας επιχειρηματικής αξίας που καλύπτει όλες τις λειτουργίες και τις διαδικασίες εντός της οργάνωσης για να της επιτρέψει να επιτύχει αποτελεσματικότερα το στόχο της ικανοποίησης των αναγκών των ενδιαφερομένων μερών. Η λογοδοσία για τη διαχείριση των στοιχείων της πληροφοριακής τεχνολογίας ανήκει στα ανώτερα διαχειριστικά στελέχη του οργανισμού και όχι στους υπαλλήλους και τους υπευθύνους λειτουργίας των συστημάτων αυτών.

Η διαχείριση κινδύνων δημιουργεί και προστατεύει την αξία

Η αρχή αυτή επικεντρώνεται στην ιδέα ότι η διαχείριση των κινδύνων του κυβερνοχώρου συμβάλλει στην αποδεδειγμένη επίτευξη των στόχων και τη βελτίωση της συνολικής απόδοσης του οργανισμού. Ικανοποιείται όταν η διαδικασία για την εξέταση των αβεβαιοτήτων και των αποφάσεων που σχετίζονται με τα πληροφοριακά συστήματα του οργανισμού, περιλαμβάνει την αναγνώριση της οργανωτικής αξίας που πρέπει να αποκτηθεί ή της αξίας που προστατεύεται.

Η διαχείριση κινδύνων είναι προσαρμοσμένη στις ανάγκες του οργανισμού

Η αρχή αυτή υπογραμμίζει ότι η διαχείριση των κινδύνων του κυβερνοχώρου είναι ευθυγραμμισμένη με το εξωτερικό και εσωτερικό πλαίσιο του οργανισμού, καθώς και το προφίλ κινδύνου του. Βάσει της αρχής αυτής αναγνωρίζεται η ύπαρξη πιθανών διαφορών μεταξύ των λειτουργιών της οντότητας, των προσδοκιών των ενδιαφερομένων μερών και του ευρύτερου επιχειρηματικού περιβάλλοντος, ωστόσο όμως προσδοκάτε ότι αυτές οι διαφορές λαμβάνονται υπόψη κατά τον σχεδιασμό του προγράμματος διαχείρισης των κινδύνων του κυβερνοχώρου. Αυτή η αρχή ικανοποιείται όταν οι μεθοδολογίες αξιολόγησης, οι αποφάσεις και οι συνακόλουθες ενέργειες προσαρμόζονται ανάλογα με τις περιστάσεις και το σύνολο των υπό εξέταση κινδύνων.

Η διαχείριση κινδύνων αντιμετωπίζει ρητά την αβεβαιότητα

Βάσει της ανωτέρω δήλωσης το Πρότυπο ISO 31000:2009 αναφέρεται σε συμπεριφορές στις οποίες οι άνθρωποι αναγνωρίζουν ότι το μέλλον μπορεί να είναι διαφορετικό από το παρελθόν. Αυτή η αρχή ενθαρρύνει τη διαχείριση κινδύνων που λαμβάνει ρητά υπόψη την αβεβαιότητα, τη φύση αυτής της αβεβαιότητας και τον τρόπο με τον οποίο αυτή μπορεί να αντιμετωπιστεί. Η αρχή αναγνωρίζει ότι δεν μπορούν όλες οι πιθανές εκβάσεις του περιβάλλοντος να είναι γνωστές εκ των προτέρων, ότι οι συνθήκες αλλάζουν και ότι η ασάφεια απαιτεί προγραμματισμό, σε ένα απρόβλεπτο, κατά τα άλλα, επιχειρηματικό, κοινωνικό και οικονομικό περιβάλλον. Αυτή η αρχή επιβεβαιώνεται με τη χρήση μεθοδολογιών αξιολόγησης που εξετάζουν πιθανούς παράγοντες και αναδυόμενα θέματα που θα μπορούσαν να επηρεάσουν τα επιθυμητά αποτελέσματα, να ανιχνεύσουν αλλαγές στο περιβάλλον του οργανισμού, να εξετάσουν διάφορα σενάρια και να σχεδιάσουν δράσεις αντιμετώπισης των κινδύνων του κυβερνοχώρου.

Εφαρμογή ενός ενιαίου πλαισίου

Βάσει της τρίτης αρχής του COBIT 5, προβλέπεται η χρήση ενός γενικού πλαισίου που ενσωματώνει τα σχετικά πρότυπα και τις ρυθμιστικές διαδικασίες που σχετίζονται με το γενικότερο πρόγραμμα διαχείρισης των εταιρικών κινδύνων, έτσι ώστε να εφαρμόζεται ένα συνεκτικό και ολοκληρωμένο πρόγραμμα με αποτελεσματικό τρόπο για την αντιμετώπιση των κινδύνων του κυβερνοχώρου.

Η διαχείριση κινδύνων είναι συστηματική, δομημένη και έγκαιρη

Η αρχή αυτή υποδηλώνει ότι η συστηματική, έγκαιρη και διαρθρωμένη προσέγγιση της διαχείρισης των κινδύνων του κυβερνοχώρου συμβάλλει στην αποτελεσματικότητα και στα συνεπή, συγκρίσιμα και αξιόπιστα αποτελέσματα. Προκειμένου να επιτευχθεί συνοχή και αποτελεσματικότητα σε όλη την επιχείρηση, τα κριτήρια, οι μετρήσεις και οι διαδικασίες για την εξέταση του κινδύνου θα πρέπει να ευθυγραμμιστούν με τις αντίστοιχες διαδικασίες που εφαρμόζονται για την παρακολούθηση των λοιπών εταιρικών κινδύνων (όχι μόνο δηλαδή των κινδύνων του εταιρικού κυβερνοχώρου).

Εφαρμογή μιας ολιστικής προσέγγισης

Η τέταρτη αρχή του COBIT 5 υπογραμμίζει ότι η αποτελεσματική και αποδοτική εφαρμογή της διακυβέρνησης απαιτεί μια ολιστική προσέγγιση που λαμβάνει υπόψη διάφορες αλληλεπιδρούσες συνιστώσες ή μηχανισμούς. Τέσσερις από αυτές - διαδικασίες, κουλτούρα, πληροφορίες και άνθρωποι, δεξιότητες και ικανότητες) σχετίζονται άμεσα με τέσσερις αρχές του ISO 31000.

Η διαχείριση κινδύνων αποτελεί αναπόσπαστο μέρος των διαδικασιών της οργάνωσης

Αυτή η αρχή του ISO 31000:2009, εξηγεί ότι η διαχείριση των κινδύνων του κυβερνοχώρου δεν είναι μια αυτόνομη δραστηριότητα που είναι ξεχωριστή από τις κύριες δραστηριότητες και τις διαδικασίες της οργάνωσης. Η διαχείριση κινδύνων αποτελεί μέρος των αρμοδιοτήτων της διοίκησης και αποτελεί αναπόσπαστο μέρος όλων των διαδικασιών οργάνωσης, συμπεριλαμβανομένου του στρατηγικού σχεδιασμού και όλων των διαδικασιών διαχείρισης έργων και αλλαγών.

Η διαχείριση του κινδύνου λαμβάνει υπόψη τους ανθρώπινους και πολιτισμικούς παράγοντες

Βάσει αυτής της αρχής, η διαχείριση των κινδύνων του κυβερνοχώρου οφείλει να αναγνωρίζει τις δυνατότητες, τις αντιλήψεις και τις προθέσεις των εξωτερικών και εσωτερικών συνεργατών και εργαζομένων της επιχείρησης που μπορούν να ενδυναμώσεις ή να παρεμποδίσουν την επίτευξη των στόχων της. Σχετικά με το εξωτερικό περιβάλλον, η αρχή υποδηλώνει ότι η αξιολόγηση αυτών των δυνατοτήτων, αντιλήψεων και προθέσεων μπορεί να δώσει πληροφορίες σχετικά με αβεβαιότητες που αφορούν για παράδειγμα, καταναλωτικές προτιμήσεις, τη συμπεριφορά της βιομηχανίας σε αντίστοιχα θέματα που προβληματίζουν τον οργανισμό, καθώς και τη στάση των συμμετεχόντων στην αλυσίδα εφοδιασμού απέναντι σε ζητήματα διαχείρισης αντίστοιχης μορφής κινδύνων. Όσον αφορά τις αβεβαιότητες που σχετίζονται με το εσωτερικό περιβάλλον, όπως η επίτευξη νέων καινοτομιών, η διατήρηση ηθικής συμπεριφοράς και τα προσωπικά κίνητρα των εργαζομένων, μπορούν να αξιολογηθούν για λόγους συνέπειας με τις προσδοκίες που θέτει η διοίκηση και να ανταμείβονται μέσω της απόδοσης.

Η διαχείριση κινδύνων αποτελεί μέρος της διαδικασίας λήψης αποφάσεων

Αυτή η αρχή υπογραμμίζει ότι η διαχείριση των κινδύνων του κυβερνοχώρου βοηθά τους υπεύθυνους λήψης αποφάσεων να προβαίνουν σε ενέργειες βασισμένοι σε απτά στοιχεία και πληροφορίες, να δίνουν προτεραιότητα σε συγκεκριμένες δράσεις που χρήζουν άμεσης προσοχής και να είναι σε θέση να διακρίνουν μεταξύ των εναλλακτικών τρόπων δράσης, προβαίνοντας στις βέλτιστες αποφάσεις (που είτε μεγιστοποιούν τα οφέλη, είτε ελαχιστοποιούν το ρίσκο ή/και το κόστος). Όλα τα άτομα σε μια επιχείρηση καλούνται να λάβουν καθημερινά αποφάσεις κατά την άσκηση των καθηκόντων τους. Οι περισσότερες από αυτές γίνονται, σχεδόν, αυτοματοποιημένα και πραγματοποιούνται επί τόπου, χωρίς να απαιτείται κάποια πολύπλοκη αξιολόγηση των υφιστάμενων κινδύνων. Τέτοιου είδους αποφάσεις σχετίζονται με τη συντριπτική πλειοψηφία των απλών και τυπικών καθημερινών εργασιών. Από την άλλη πλευρά, οι άνθρωποι που λαμβάνουν αποφάσεις που έχουν μεγάλη σημασία ή είναι πολύπλοκες, όπως εκείνοι που εμπλέκονται σε ένα έργο ή μια πρωτοβουλία, επωφελούνται από τη χρήση τεχνικών διαχείρισης του κινδύνου για την εκτίμηση και την αξιολόγηση των αβεβαιοτήτων που σχετίζονται με κάθε μία από τις διαθέσιμες επιλογές και τον εντοπισμό των πιθανών συνεπειών που συνεπάγονται οι τυχόν αστοχίες. Όσοι παίρνουν αποφάσεις που έχουν στρατηγική σημασία και είναι πολύπλοκες ωφελούνται από τη χρήση πιο επίσημων διαδικασιών λήψης αποφάσεων και διαχείρισης κινδύνων, εφαρμόζοντας πολλαπλές τεχνικές διαχείρισης κινδύνων.

Η διαχείριση των κινδύνων βασίζεται στις καλύτερες διαθέσιμες πληροφορίες

Βάσει αυτής της αρχής οι εισροές στη διαδικασία διαχείρισης των κινδύνων του κυβερνοχώρου θα πρέπει να βασίζονται σε έγκυρες πηγές πληροφοριών, όπως ιστορικά δεδομένα, πρωτύτερη εμπειρία στελεχών, στοιχεία από τα ενδιαφερόμενη μέρη της επιχείρησης, επιτόπια παρατήρηση, τεκμηριωμένες προβλέψεις, καθώς και τη γνώμη εμπειρογνωμόνων. Αυτή η αρχή ενθαρρύνει μια προσέγγιση με βάση τα γεγονότα, αναγνωρίζοντας ταυτόχρονα τους περιορισμούς των δεδομένων, τη μοντελοποίηση και την πιθανή απόκλιση απόψεων. Η σημασία της συμφωνίας ως προς την εγκυρότητα των υποκείμενων πληροφοριών που πρέπει να χρησιμοποιηθούν είναι καθοριστική.

Διαχωρισμός διακυβέρνησης από το μάνατζμεντ

Η πέμπτη και τελευταία αρχής του COBIT 5 αρχή προχωράει στη διάκριση μεταξύ διακυβέρνησης (governance) και διαχείρισης (management). Η αρχή διαχωρίζει τις δραστηριότητες εταιρικής διακυβέρνησης όπως η αξιολόγηση, η καθοδήγηση και η παρακολούθηση (κυρίως των επιχειρησιακών αναγκών και στο σύνολο του οργανισμού) από τις δραστηριότητες διαχείρισης, όπως ο σχεδιασμός, η υλοποίηση, και η παρακολούθηση των διαδικασιών. Η αρχή αυτή προβλέπει ένα επαναλαμβανόμενο σύστημα κλειστού βρόχου στο οποίο παρέχεται η απαιτούμενη ανατροφοδότηση από τα διαχειριστικά στελέχη για να εξασφαλιστεί η εναρμόνιση με την κατεύθυνση που έθεσαν τα διοικητικά όργανα και κατά συνέπεια, να επιτευχθούν οι επιχειρηματικοί στόχοι.

Η διαχείριση κινδύνων διευκολύνει τη συνεχή βελτίωση του οργανισμού

Η αρχή αυτή προβλέπει ότι οι οργανισμοί πρέπει να αναπτύξουν και να εφαρμόσουν στρατηγικές για τη βελτίωση της ωριμότητάς τους όσον αφορά τη διαχείριση των κινδύνων του κυβερνοχώρου, παράλληλα με όλες τις άλλες πτυχές των οργανωτικών διαδικασιών. Αυτή η αρχή θεωρεί τη συνεχή βελτίωση ως καθοδηγούμενη από μια στρατηγική ωριμότητας προς την αντιμετώπιση του κινδύνου που ευθυγραμμίζεται φυσικά με τις δραστηριότητες και τις διαδικασίες που εντοπίζονται στο διαχωρισμό της διακυβέρνησης από τη διαχείριση. Καθώς οι άνθρωποι χρησιμοποιούν διαδικασίες και τεχνικές διαχείρισης του κινδύνου, αποκτούν γνώσεις σχετικά με τις αβεβαιότητες που επηρεάζουν τους στόχους, σταθμίζουν εναλλακτικές λύσεις και λαμβάνουν αποφάσεις που έχουν ως αποτέλεσμα ευεργετικές δράσεις. Καθώς οι δυνατότητές τους αναφορικά με την διαχείριση των κινδύνων του κυβερνοχώρου βελτιώνονται και ωριμάζουν με την πάροδο του χρόνου, εφαρμόζουν φυσικά και με συνέπεια τις παραπάνω αρχές για να καθορίσουν εάν οι αποφάσεις και οι προκύπτουσες ενέργειες είναι χρήσιμες ή επιβλαβείς.

ΚΕΦΑΛΑΙΟ 4

ΑΣΦΑΛΙΣΗ ΕΝΑΝΤΙ ΤΩΝ ΚΙΝΔΥΝΩΝ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

4.1 Εισαγωγή

Στο παρόν κεφάλαιο επισκοπούμε το θέμα της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου. Αναλυτικότερα, η εισαγωγή του κεφαλαίου ασχολείται με μια σύντομη αναδρομή αναφορικά με την αναγνώριση της ανάγκης για ασφάλιση έναντι αυτής της μορφής των κινδύνων. Ακολούθως, παρατίθενται στοιχεία σχετικά με την κατάσταση της αγοράς της ασφαλιστικής κάλυψης έναντι των κινδύνων του κυβερνοχώρου, ενώ αναλύονται οι σχετικές με το θέμα πληροφορίες που αφορούν τόσο τις ασφαλιστικές εταιρίες, όσο και τους ασφαλισμένους. Το κεφάλαιο ολοκληρώνεται με την παρουσίαση μιας πρότασης-σχεδίου για την αποτελεσματικότερη εκτίμηση και οργάνωση των δράσεων για την ασφάλιση έναντι των κινδύνων του κυβερνοχώρου από την σκοπιά του ασφαλισμένου.

4.2 Σύντομη Ιστορική Ανασκόπηση

Σύμφωνα με τα όσα έχουμε δει από την μέχρι τώρα επισκόπηση της παγκόσμιας βιβλιογραφίας, η ασφάλιση έναντι των κινδύνων του κυβερνοχώρου είναι μια έννοια που προσελκύει, με αυξανόμενο ρυθμό, την προσοχή και το ενδιαφέρον των επιχειρήσεων τα τελευταία χρόνια. Δεδομένης της ραγδαίας ανάπτυξης της τεχνολογίας και της εκθετικά αυξανόμενης πολυπλοκότητας των σύγχρονων πληροφοριακών συστημάτων, ο φόβος για τις ολέθριες επιπτώσεις που δύναται να έχουν οι κίνδυνοι του κυβερνοχώρου – ακόμα και για την ίδια την βιωσιμότητα των επιχειρήσεων – έχει οδηγήσει πλήθος εταιριών και ανώτερων διοικητικών στελεχών στην αναγνώριση της σπουδαιότητας της διασποράς – και τελικά της μείωσης - του κινδύνου, αυτού (risk dispersion and risk mitigation).

Σύμφωνα με τους Refsdal et al. (2015)[71], η τελική επιλογή διαχείρισης και αντιμετώπισης των κινδύνων του κυβερνοχώρου είναι η στροφή προς την ασφάλιση έναντι των κινδύνων αυτών. Η ασφάλιση έναντι αυτής της μορφής των κινδύνων δείχνει σημαντικά σημάδια μιας ανερχόμενης αγοράς – η οποία έχει αναπτυχθεί περισσότερο στις ΗΠΑ απ' ότι στην Ε.Ε. (προς το παρόν), σύμφωνα με τους συγγραφείς. Ορίζουν την ασφάλιση έναντι των κινδύνων του κυβερνοχώρου ως τη μεταφορά του χρηματοοικονομικού κινδύνου που σχετίζεται με συμβάντα που δύναται να προκαλέσουν ζημίες στο πληροφοριακό σύστημα μιας εταιρίας ή ενός μεμονωμένου χρήστη, προς ένα τρίτο μέρος. Τέλος, αναφέρουν, συνοπτικά, τις προκλήσεις που σχετίζονται με την τιμολόγηση των υπηρεσιών ασφάλισης για τους κινδύνους αυτούς, ενώ αναγνωρίζουν την σπουδαιότητα της ύπαρξης μιας τέτοιας υπηρεσίας, δεδομένου ότι μπορεί να μετριάσει τις επιπτώσεις μιας εταιρίας από την έκθεσή της στους κινδύνους του κυβερνοχώρου και να την βοηθήσει να διαμορφώσει μια πιο αποτελεσματική πολιτική διαχείρισης των κινδύνων αυτών.

Η στάση των επιχειρήσεων ωστόσο, άργησε σημαντικά να διαμορφωθεί προς αυτή τη κατεύθυνση. Σύμφωνα με τα ευρήματα των, λίγο παλαιότερων, εργασιών των Westby (2010)[72] και Costanzo (2011)[73], παρά το σημαντικό κόστος των κρουσμάτων από τις επιθέσεις στον κυβερνοχώρο, πολλές επιχειρήσεις δεν κατάφεραν να διαχειριστούν την έκθεσή τους στους κινδύνους του κυβερνοχώρου (αναφέρονται στην περίοδο περί το 2010, όπου και γράφτηκαν οι σχετικές εργασίες), ενώ πάρα πολλές εξ αυτών δεν είχαν συνειδητοποιήσει την ύπαρξη αυτής της μορφής κινδύνου. Ο Schackelford (2012)[74] παραθέτει στο άρθρο του, τα ευρήματα μιας, σχετικής με το θέμα αυτό, έρευνας (Carnegie Mellon's CyLab, 2010), τα οποία συνοψίζονται στο ότι όλες οι υπό εξέταση επιχειρήσεις με ετήσια έσοδα που κυμαίνονταν μεταξύ 1 δισεκατομμυρίου δολαρίων και 10 δισεκατομμυρίων δολαρίων αντίστοιχα, δεν συνειδητοποιούσαν ότι οι κίνδυνοι του κυβερνοχώρου συγκαταλέγονται μεταξύ των λειτουργικών εταιρικών κινδύνων και κατά

[71] Refsdal, A., Solhaug, B. and Stolen, K. (2015), "Cyber Risk Management", *Springer Briefs in Computer Science*, Springer International Publishing

[72] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", *Pittsburgh, PA: Carnegie Mellon*

[73] Costanzo, C. (2011), "Is your company prepared for cyber risk?", [online], Διαθέσιμο στο: http://www.boardmember.com/MagazineArticle_Details.aspx?id=5943&page=1, (Ημερομηνία Πρόσβασης: 04/12/2018)

[74] Shackelford, S., J. (2012), "Should your firm invest in cyber risk insurance?", *Business Horizons*, 55 (4), pp. 349-356

συνέπεια, η βελτίωση των υποδομών προστασίας και θωράκισης έναντι των κινδύνων αυτών, δεν ήταν μεταξύ των βασικών τους προτεραιοτήτων. Οι μισές εξ αυτών θεωρούσαν ότι η διαχείριση των εταιρικών κινδύνων ήταν ένας τομέας στο οποίο έπρεπε να επενδύσουν με ταχείς ρυθμούς, ωστόσο εκλάμβαναν τα συμβάντα των διαδικτυακών επιθέσεων ως μεμονωμένα και υποδεέστερα των σημαντικότερων (τουλάχιστον για την οπτική των διοικούντων και των διοικητικών συμβουλίων) προβλημάτων που έπρεπε να επιλυθούν.

Σύμφωνα με τους Majuca et al. (2006)[75], αν και η εξειδικευμένη κάλυψη κατά των επιθέσεων που είχαν ως στόχο τα πληροφοριακά συστήματα των μεμονωμένων χρηστών και των επιχειρήσεων παρουσιάστηκε για πρώτη φορά στα τέλη της δεκαετίας του 1970, οι πολιτικές αυτές αποτελούσαν επέκταση της παραδοσιακής ασφάλισης των παραβιάσεων που αφορούσαν την ηλεκτρονική τραπεζική και αποσκοπούσαν κυρίως στην κάλυψη έναντι ενός δράστη που αποκτούσε φυσική πρόσβαση στα συστήματα πληροφορικής του ασφαλισμένου. Δεν ήταν μέχρι τα τέλη της δεκαετίας του 1990 όπου και εμφανίστηκαν για πρώτη φορά οι ασφάλειες – ως πιο οργανωμένα πλέον προϊόντα – που αφορούσαν την κάλυψη των ζημιών κατά των πληροφοριακών συστημάτων του ασφαλισμένου. Βάσει των όσων αναφέρουν, τα πρώτα γνωστά ασφαλιστήρια συμβόλαια που κάλυπταν τους κινδύνους του κυβερνοχώρου, εισήχθησαν για πρώτη φορά το 1998 από εταιρείες τεχνολογίας που συνεργάζονταν με ασφαλιστικές εταιρίες για να προσφέρουν στους πελάτες τους ένα πακέτο τεχνολογικών και ασφαλιστικών υπηρεσιών είτε για να υποστηρίξουν την επιδιόρθωση των όποιων τεχνικών προβλημάτων προκύπταν από την κακόβουλη επίθεση εναντίον του πληροφοριακού συστήματος του πελάτη, είτε για να παρέχουν μια ολοκληρωμένη λύση διαχείρισης των εταιρικών κινδύνων προς τους ασφαλισμένους. Σε ορισμένες περιπτώσεις προωθούνταν μάλιστα και υβριδικά πακέτα τα οποία περιλάμβαναν μια μίξη των δύο κυρίως ανωτέρω υπηρεσιών. Όπως μπορεί να γίνει εύκολα αντιληπτό, δεδομένου του «άγουρου» της ηλικίας αυτής της νέας προϊοντικής αγοράς, τα ασφαλιστήρια συμβόλαια ήταν λιγοστά και πολύ μικρότερων ποσών (τόσο ως προς το ασφαλιστικό κόμιστρο, όσο και ως προς το ποσό της ασφαλιστικής κάλυψης), από ότι οι αντίστοιχες σημερινές επιλογές ασφαλιστικών πακέτων. Τα συμβόλαια αυτά κάλυπταν τις δυνητικές ζημίες μόνο του άμεσα ασφαλισμένου, δίχως να αναγνωρίζουν την κάλυψη πιθανών ενδιαφερομένων μερών.

[75] Majuca, R., P., Yurcik, W. and Kesan, J., P. (2006), "The evolution of cyberinsurance", [online], Διαθέσιμο στο: https://arxiv.org/abs/cs/0601020, (Ημερομηνία Πρόσβασης: 04/12/2018)

Όπως αναφέρουν οι Marotta et al. (2017)[76], ένας από τους κύριους παράγοντες αύξησης της αγοράς για την παροχή ασφαλιστικής κάλυψης έναντι των κινδύνων του κυβερνοχώρου είναι τα σοβαρά κρούσματα επιθέσεων κατά των εταιρικών πληροφοριακών συστημάτων που συγκλόνισαν, κατά καιρούς, την παγκόσμια επιχειρηματική κοινότητα και προκάλεσαν μεγάλες απώλειες και σωρεία προβλημάτων. Ήδη από τις απαρχές του 2000 τέτοια ηχηρά περιστατικά έφεραν ακόμα περισσότερο στο προσκήνιο την ανάγκη για την αναζήτηση κάποιας μορφής κάλυψης έναντι αυτής της μορφής των κινδύνων. Οι εταιρίες που βρέθηκαν αντιμέτωπες με τις σοβαρότερες συνέπειες αυτών των επιθέσεων αναζήτησαν πιο ένθερμα την ασφαλιστική κάλυψη έναντι των κινδύνων του κυβερνοχώρου προκειμένου να επιτύχουν την άμβλυνση των μελλοντικών ζημιών και κατά συνέπεια, πολλές ασφαλιστικές εταιρίες ανέπτυξαν τα αντίστοιχα προϊόντα για να ικανοποιήσουν αυτή την ανάγκη (Filkins, 2016)[77].

Οι Marotta et al. (2017) συνεχίζουν αναφέροντας ότι με την πάροδο των ετών, οι πρακτικές ασφάλισης έναντι των κινδύνων του κυβερνοχώρου έχουν γίνει ολοένα και πιο εξελιγμένες ώστε να συμβαδίζουν με τη συνεχή εξέλιξη των επιθέσεων στον κυβερνοχώρο και την πολυπλοκότητα των πληροφοριακών συστημάτων. Επισημαίνουν επίσης το γεγονός ότι οι (δια)κρατικοί κανονισμοί για την προστασία των δεδομένων είναι ένας άλλος ισχυρός μοχλός για την εξέλιξη της ασφαλιστικής αγοράς για τους κινδύνους του κυβερνοχώρου. Επί αυτού του θέματος αναφέρουν την ραγδαία άνθιση των προϊόντων ασφάλισης έναντι των κινδύνων του κυβερνοχώρου κατά το 2003 όπου και η τότε κυβέρνηση των Η.Π.Α. ενέκρινε έναν σχετικό νόμο περί της προστασίας των πληροφοριακών συστημάτων και των επιθέσεων με στόχο αυτά. Μεταξύ άλλων, ο νόμος απαιτούσε από τις επιχειρήσεις να γνωστοποιούν το εάν και σε ποιο βαθμό έχουν πέσει θύματα παραβίασης του κυβερνοχώρου τους. Στο ίδιο μήκος κύματος, παραθέτουν και το παράδειγματης Ε.Ε. όπου μετά την ανακοίνωση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), παρατηρήθηκε μια αντίστοιχη αύξηση στην ζήτηση ασφαλιστικών υπηρεσιών για την κάλυψη έναντι των κινδύνων του κυβερνοχώρου.

---

[76] Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017), "Cyber-insurance survey", *Computer Science Review,* Vol. 24, pp. 35-61

[77] Filkins, B. (2016), "Quantifying risk: Closing the chasm between cybersecurity and cyber insurance", *SANS Institute*, [online], Διαθέσιμο στο: https://www.sans.org/reading-room/whitepapers/leadership/quantifying-risk-closing chasm-cybersecurity-cyber-insurance-36770, (Ημερομηνία Πρόσβασης: 05/12/2018)

4.3 Η Αγορά της Ασφάλισης Έναντι των Κινδύνων του Κυβερνοχώρου

Ενώ οι μεμονωμένες επιχειρήσεις ενδιαφέρονται για τα κρούσματα επιθέσεων στα πληροφοριακά τους συστήματα και κατ' επέκταση στην καλύτερη διαχείριση των κινδύνων του κυβερνοχώρου τους, οι ασφαλιστικές εταιρίες ανησυχούν για την συσχέτιση του κινδύνου σε ολόκληρο το χαρτοφυλάκιό τους, καθότι πρέπει να συμπεριλάβουν ποικίλους παράγοντες κατά τον προσδιορισμό του ασφαλίστρου που θα απαιτήσουν από τους ιδιώτες και τους οργανισμούς. Πολλές από τις εργασίες που επισκοπήθηκαν για την συγγραφή της παρούσας διατριβής, χρησιμοποίησαν ως κύρια πηγή σχολιασμού και ανάλυσης της αγοράς ασφάλισης έναντι των κινδύνων του κυβερνοχώρου, το μοντέλο του Berliner (1985)[78]. Ορμώμενοι από αυτό, θα χρησιμοποιήσουμε τις εννέα βασικές πτυχές του συγγραφέα, προκειμένου επεξηγήσουμε τους βασικές παράγοντες που καθορίζουν την προσφορά των ασφαλιστικών υπηρεσιών για την κάλυψη των κινδύνων του κυβερνοχώρου των επιχειρήσεων.

Το μοντέλο του Berliner (1985), περιλαμβάνει εννέα κριτήρια βάσει των οποίων ένας κίνδυνος καθίσταται ελκυστικός για να ασφαλιστεί από μια ασφαλιστική εταιρία. Τα πρώτα πέντε κριτήρια αφορούν το αναλογιστικό-μαθηματικό μοντέλο, το έκτο και το έβδομο των συνθηκών της αγοράς και τα δύο τελευταία το γενικότερο περιβάλλον (οικονομικό, κοινωνικό, τεχνολογικό κλπ). Σύμφωνα με τα ανωτέρω, τα κριτήρια αυτά έχουν ως εξής:

1. Τα τυχαία περιστατικά συμβάντων απώλειας (randomness of loss occurrence) πρέπει να συμβαίνουν ανεξάρτητα (δηλαδή να μην εμφανίζεται καμία συσχέτιση μεταξύ τους).
2. Η μέγιστη δυνατή απώλεια ανά περιστατικό (maximum possible loss per incident) πρέπει να είναι διαχειρίσιμη για τον ασφαλιστή.
3. Η μέση απώλεια ανά περιστατικό (average loss per incident) πρέπει να είναι μετρίου βαθμού.
4. Η έκθεση σε απώλειες (loss exposure) πρέπει να είναι αρκετά μεγάλη.
5. Η ασυμμετρία της πληροφόρησης (information asymmetry) δεν πρέπει να είναι υπερβολικά υψηλή.
6. Το ασφάλιστρο (insurance premium) θα πρέπει να είναι προσιτό για τους ασφαλισμένους.

[78] Berliner, B. (1985), "Large Risks and Limits of Insurability", *The Geneva Papers on Risk and Insurance - Issues and Practice*, 10 (4), pp. 313-329

7. Τα όρια κάλυψης (cover limits) πρέπει να είναι κατάλληλα για τους ασφαλισμένους.
8. Πρέπει να τηρείται η δημόσια πολιτική (public limits).
9. Οι νομικοί περιορισμοί (legal restrictions) δεν πρέπει να παραβιάζονται.

Στο σημείο αυτό θα πρέπει να επισημάνουμε ένα εξίσου σημαντικό μοντέλο που περιγράφει το κατά πόσο είναι συμφέρουσα η ανάληψη ασφαλιστικών υπηρεσιών, το οποίο έρχεται από τους Mehr και Cammack (1961)[79] και είναι αρκετά παλαιότερο από αυτό το Berliner. Αν και γίνεται μνεία σε αυτό το μοντέλο σε αρκετές εργασίες που επισκοπήσαμε, εντούτοις το μοντέλο του Berliner είναι αρκετά πιο δημοφιλές. Το μοντέλο των Mehr και Cammack προβλέπει επτά συνθήκες προκειμένου να ασφαλιστεί μια μορφή κινδύνου. Αυτές έχουν ως εξής:

- Τυχαία απώλεια (Incidental loss): Το περιστατικό πρέπει να είναι τυχαίο και όχι υπό τον έλεγχο του ασφαλισμένου.
- Περιορισμένος κίνδυνος καταστροφικών μεγάλων απωλειών (Limited risk of catastrophically large losses): Καταστροφικά μεγάλες απώλειες πρέπει να συμβούν με πολύ χαμηλή συχνότητα.
- Υπολογιζόμενη απώλεια (Calculable loss): Πρέπει να είναι δυνατή η εκτίμηση ή ο υπολογισμός πιθανών απωλειών, καθώς και η πιθανότητα εκδήλωσης ενός συμβάντος.
- Μεγάλος αριθμός παρόμοιων μονάδων έκθεσης στον αντίστοιχο κίνδυνο (Large number of similar exposure units): Για τη διευκόλυνση του προσδιορισμού της πιθανότητας πρέπει να υπάρχει ένας μεγάλος αριθμός ομοιογενών μονάδων έκθεσης στον ίδιο ή σε παρεμφερής μορφές αντίστοιχων κινδύνων.
- Προσιτό ασφάλιστρο (Affordable premium): Το ασφάλιστρο πρέπει να είναι λογικό και ελκυστικό για τον ασφαλισμένο.
- Σίγουρη απώλεια (Definite loss): Η απώλεια πρέπει να είναι δύσκολο να χειραγωγηθεί. Ο χρόνος, ο τόπος και η αιτία του συμβάντος που γεννάει την αξίωση για ασφαλιστική κάλυψη πρέπει να είναι εύκολο να προσδιοριστούν.
- Μεγάλη απώλεια (Large loss): Οι απώλειες πρέπει να είναι αρκετά μεγάλες ώστε να μην υπάρχουν υποψίες χειραγώγησης των κινήτρων για λήψη της ασφαλιστικής κάλυψης από τον ασφαλισμένο.

[79] Mehr, R. and Cammack, E. (1961), "*Principles of Insurance*", third ed., Richard D. Irwin, Inc.

Βάσει του μοντέλου του Berliner προχωράμε στην αναλυτικότερη παρουσίαση των παραγόντων που επηρεάζουν την παροχή των ασφαλιστικών υπηρεσιών έναντι των κινδύνων του κυβερνοχώρου.

4.3.1 Τυχαία Περιστατικά Συμβάντων Απώλειας

Ένα βασικό κριτήριο για την παροχή ασφαλιστικών υπηρεσιών έναντι συγκεκριμένων κινδύνων είναι η ανεξαρτησία των κινδύνων αυτών (Bohme, 2005)[80]. Σύμφωνα με το νόμο των μεγάλων αριθμών, όσο μεγαλύτερος είναι ο αριθμός των αμοιβαίως ανεξάρτητων κινδύνων στο χαρτοφυλάκιο μιας ασφαλιστικής εταιρίας, τόσο πιθανότερο είναι ότι οι μέσες συνολικές απώλειες αντιστοιχούν στις αναμενόμενες απώλειες, επιτρέποντας έτσι τη μείωση των κεφαλαίων ασφαλείας (Biener, 2013)[81].

Επομένως, η ανεξαρτησία των κινδύνων αποτελεί σημαντική προϋπόθεση για την ασφάλιση κάθε μορφής κινδύνου. Στην περίπτωση των κινδύνων του κυβερνοχώρου, αρκετοί συγγραφείς θεωρούν ότι παραβιάζεται αυτή η βασική προϋπόθεση. Οι Baer και Parkinson (2007)[82] υποστηρίζουν ότι τα υπάρχοντα πληροφοριακά συστήματα σχεδιάζονται με παρόμοιο τρόπο και κατά συνέπεια είναι ευάλωτα στα ίδια περιστατικά, πράγμα που δικαιολογεί την υπόθεση ότι τα περιστατικά μπορεί να συσχετιστούν σε μεγάλο βαθμό μεταξύ των επιχειρήσεων. Ορισμένοι άλλοι ερευνητές αναγνωρίζουν επίσης τη συσχετισμένη φύση των κινδύνων στον κυβερνοχώρο και συντάσσονται με την παραπάνω άποψη[8384]. Ωστόσο, δεν είναι λίγοι οι ερευνητές που υποστηρίζουν την αντίθετη άποψη, ότι δηλαδή οι κίνδυνοι είναι όντως ανεξάρτητοι και κατά

[80] Böhme, R. (2005), "Cyber-Insurance Revisited," *Workshop on the Economics of Information Security (WEIS)*, Harvard University, Cambridge, MA

[81] Biener, C. (2013), "Pricing in Microinsurance Markets", *World Development*, 41 (1), pp. 132–144

[82] Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," *IEEE Security and Privacy*, 5 (3), pp. 50–56

[83] Bolot, J. and Lelarge, M. (2009), "Cyber Insurance as an Incentive for Internet Security", In: M. E. Johnson (ed.), *Managing Information Risk and the Economics of Security*, New York: Springer, pp. 269-290

[84] Ögüt, H., Raghunathan, S., and Menon, N. (2011), "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection", Risk Analysis, 31 (3), pp. 497–512

συνέπεια δεν παραβιάζεται η βασική αυτή αρχή της ανάληψης οποιασδήποτε ασφαλιστικής δράσης (Biener et al. 2015)[85]. Σύμφωνα με τα όσα αναφέρει ωστόσο ο Payne (2016)[86], στην εργασία του η ποσοτικοποίηση των κινδύνων του κυβερνοχώρου είναι ένας από τους πιο προβληματικούς και περίπλοκους τομείς που καλούνται να αντιμετωπίσουν οι πάροχοι των ασφαλιστικών υπηρεσιών. Το σύνολο των αναλαμβανόμενων κινδύνων πρέπει να είναι όσο το δυνατόν πιο ασυσχέτιστο, έτσι ώστε ένα συμβάν ζημίας να μην προκαλέσει την κατάρρευση του χαρτοφυλακίου της ασφαλιστικής εταιρίας και κατά συνέπεια να την οδηγήσει σε αδυναμία αποπληρωμής των απαιτήσεων των πελατών της.

Παρόλα αυτά, οι Biener et al. (2015), επισημαίνουν το ότι η συγκέντρωση αυτής της μορφής κινδύνου (μέσω της ανάληψης ασφαλιστικών υποχρεώσεων προς τους πελάτες) θα μπορούσε να παρεμποδιστεί από το γεγονός ότι τα ασφαλιστικά χαρτοφυλάκια που αφορούν την κάλυψη των κινδύνων του κυβερνοχώρου δεν είναι αρκετά μεγάλα ακόμα, δηλαδή, υπάρχουν πολύ λίγες συμβάσεις, με αποτέλεσμα να μην υπάρχει η βέλτιστη διαφοροποίηση. Σύμφωνα με τους Herath και Herath (2011)[87], ένα ακόμα καίριο προκύπτει κατά την τιμολόγηση των ασφαλιστικών υπηρεσιών που καλύπτουν τους κινδύνους του κυβερνοχώρου είναι η έλλειψη μεγάλου όγκου δεδομένων (κυρίως ιστορικών στοιχείων). Ανεξάρτητα από το πόσο ακριβής και εξελιγμένη είναι η προσομοίωση των κινδύνων του κυβερνοχώρου, αν δεν υπάρχουν δεδομένα για τη δοκιμή των μοντέλων, η χρησιμότητά τους τίθεται σοβαρά υπό αμφισβήτηση (Betterley, 2010)[88]. Επί του θέματος αυτού, οι Bandyopadhyay et al. (2009)[89] αναφέρουν ότι οι ασφαλιστές θεωρούνται ότι έχουν ελάχιστα ή καθόλου πλεονεκτήματα πληροφόρησης σε σχέση με τις μεμονωμένες επιχειρήσεις που καλούνται να εξυπηρετήσουν. Ιδιαίτερα εύστοχη είναι η παρατήρηση του

[85] Biener, C., Eling, M. and Wirfs, J., H. (2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40 (1), pp. 131-158

[86] Payne, M. (2016), "*An Overview of the Cyber Insurance Industry: Challenges for Insurers and Insureds in Quantifying and Mitigating Cyber Risk*", Royal Holloway, University of London

[87] Herath, H. and Herath, T. (2011), "Copula Based Actuarial Model for Pricing Cyber Insurance Policies", *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2 (1), pp. 7–20

[88] Betterley, R. (2010), "Understanding the Cyber Risk Insurance and Remediation Services Marketplace: A Report on the Experiences and Opinions of Middle Market CFOs", [online], Διαθέσιμο στο: http://www.casact.org/community/affiliates/CANE/0412/Betterley2.pdf, (Ημερομηνία Πρόσβασης: 05/12/2018)

[89] Bandyopadhyay, T. M., Vijay, S. and Rao, R. C. (2009), "Why IT Managers Don't Go for Cyber-Insurance Products", Communications of the ACM, 52 (11), pp. 68–73

Chabrow (2012)[90], ο οποίος αναφέρει ότι δεδομένου ότι η παροχή ασφάλισης έναντι των κινδύνων του κυβερνοχώρου ενέχει πολύ υψηλό ρίσκο για τις ασφαλιστικές εταιρίες, μπορεί εύλογα να εννοηθεί ότι εξίσου μεγάλο ρίσκο αναλαμβάνει και όποιος επιδιώκει την απόκτηση των υπηρεσιών αυτών.

Ένα ακόμα πρόβλημα στην παροχή ασφάλισης έναντι των κινδύνων του κυβερνοχώρου είναι ότι ο κίνδυνος αλλάζει, μερικές φορές ξαφνικά και δραστικά, δηλαδή ο κίνδυνος είναι δυναμικός λόγω της τεχνολογικής προόδου και της χρήσης νέων και πιο εξελιγμένων πληροφοριακών συστημάτων και τεχνολογικών συσκευών. Επομένως, σύμφωνα με τους Gatzlaff και McCullough (2012)[91], μια ανάλυση των ιστορικών δεδομένων που σχετίζονται με αυτή τη μορφή κινδύνου θα μπορούσε να είναι παραπλανητική εάν η φύση του υποκείμενου κινδύνου έχει υποστεί ουσιαστικές αλλαγές. Ένα ακόμα ζήτημα που καλούνται να αντιμετωπίσουν οι ασφαλιστικές εταιρίες είναι αυτό των ρυθμιστικών παρεμβάσεων που μεταβάλλουν τους κανόνες που εφαρμόζονται για την ασφάλιση έναντι αυτών των ζημιών.

4.3.2 Μέγιστη Δυνατή Απώλεια ανά Περιστατικό

Βάσει των όσων αναφέρουν οι Biener et al. (2015)[92], το δεύτερο κριτήριο του μοντέλου ικανοποιείται εάν η μέγιστη δυνατή απώλεια ανά συμβάν είναι διαχειρίσιμη από την άποψη της φερεγγυότητας του ασφαλιστή. Οι μέγιστες ιστορικές απώλειες από κρούσματα επιθέσεων στον κυβερνοχώρο των επιχειρήσεων είναι σημαντικά χαμηλότερες από αυτές των γενικών λειτουργικών κινδύνων. Επιπλέον, οι ασφαλιστικές εταιρίες προστατεύονται από τα αντίστοιχα όρια κάλυψης έναντι των κινδύνων αυτών. Κατά συνέπεια, καταλήγουν στο ότι οι μέγιστες πιθανές απώλειες από τους κινδύνους του κυβερνοχώρου φαίνεται να είναι διαχειρίσιμες.

---

[90] Chabrow, E. (2012), "10 Concerns When Buying Cyber Insurance", [online], Διαθέσιμο στο: http://www.bankinfosecurity.com/10-concerns-when-buying-cyber-insurance-a-4859/op-1, (Ημερομηνία Πρόσβασης: 05/12/2018)

[91] Gatzlaff, K. and McCullough, K. A. (2012), "Implications of Privacy Breaches for Insurers", *Journal of Insurance Regulation*, Vol. 31, pp. 195–214

[92] Biener, C., Eling, M. and Wirfs, J., H. (2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40 (1), pp. 131-158

4.3.3 Μέση Απώλεια ανά Περιστατικό

Στόχος της κάθε ασφαλιστικής εταιρίας θα πρέπει να είναι η μείωση της μέσης απώλειας από τα περιστατικά παραβίασης του κυβερνοχώρου των πελατών της. Ο Shackelford (2012), αναφέρει ότι οι επιχειρήσεις που απασχολούν έναν υπεύθυνο ασφάλειας των πληροφοριακών τους συστημάτων (συνήθως έχει κάποια αντίστοιχη διευθυντική θέση), εμφανίζουν χαμηλότερα μέσα κόστη ανά περιστατικό παραβίασης του κυβερνοχώρου τους, σε σχέση με τις επιχειρήσεις που δεν απασχολούν προσωπικό σε αντίστοιχες θέσεις. Οι Biener et al. (2015)[93] διατείνονται ότι η στροφή των επιχειρήσεων, ειδικά τα τελευταία χρόνια, προς την διάθεση αυξημένων κονδυλίων για την βελτίωση της θωράκισής τους έναντι των κινδύνων του κυβερνοχώρου, έχει οδηγήσει σε σημαντική μείωση το μέσο κόστος ανά συμβάν παραβίασης των πληροφοριακών τους συστημάτων, καθιστώντας το κόστος αυτό σημαντικά χαμηλότερο απ' ότι τα μέσα κόστη των απωλειών που σχετίζονται με τις λοιπές λειτουργικές δραστηριότητες των επιχειρήσεων.

4.3.4 Έκθεση σε Απώλειες

Μεγάλο μέρος των ερευνών που έχουν παρατεθεί ανωτέρω (καθώς και σε προηγούμενα κεφάλαια της παρούσας εργασίας) συμφωνούν ότι οι περισσότεροι κίνδυνοι του κυβερνοχώρου των επιχειρήσεων είναι ενδογενείς στη φύση τους, ενώ ο ανθρώπινος παράγοντας είναι αυτός που βρίσκεται στο επίκεντρο των ευθυνών (είτε πρόκειται για ενδογενείς, είτε για εξωγενείς απειλές). Γεγονότα όπως για παράδειγμα, φυσικές καταστροφές κ.λπ., δεν φαίνεται να επιδρούν σημαντικά στον προσδιορισμό του βαθμού της σοβαρότητας του κινδύνου του κυβερνοχώρου. Σύμφωνα με τον Shackelford (2012)[94], η έκθεση σε ζημίες εξαρτάται από τη βιομηχανία (οι χρηματοπιστωτικές επιχειρήσεις έχουν υψηλότερη έκθεση) και το μέγεθος (οι μεγαλύτερες επιχειρήσεις έχουν υψηλότερη έκθεση).

[93] Biener, C., Eling, M. and Wirfs, J., H. (2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40 (1), pp. 131-158

[94] Shackelford, S., J. (2012), "Should your firm invest in cyber risk insurance?", *Business Horizons*, 55 (4), pp. 349-356

4.3.5 Ασυμμετρία της Πληροφόρησης

Η δυσμενής επιλογή και ο ηθικός κίνδυνος θεωρούνται συχνά ως τα κύρια εμπόδια στην ανάπτυξη της ασφαλιστικής αγοράς. Οι Majuca et al. (2006)[95], αναλύουν διεξοδικά και με παραδείγματα τις δύο αυτές παραμέτρους-προβλήματα που καλούνται να αντιμετωπίσουν οι ασφαλιστικές εταιρίες κατά την ανάπτυξη των προϊόντων ασφάλισης για την κάλυψη των κινδύνων του κυβερνοχώρου.

Δυσμενής Επιλογή (Adverse Selection): Σύμφωνα με τους συγγραφείς, σε έναν ιδανικό κόσμο, τα συμβαλλόμενα μέρη μιας συναλλαγής έχουν άριστες πληροφορίες σχετικά με την απόφαση που καλούνται να πάρουν. Ωστόσο, σε πολλές περιπτώσεις, ένα αντισυμβαλλόμενο μέρος μπορεί να έχει λιγότερες πληροφορίες σχετικά με τη φύση του προϊόντος που καλείται να διαπραγματευτεί. Στην ασφαλιστική αγορά, τα προβλήματα αυτά προκύπτουν όταν οι ασφαλιστές δεν γνωρίζουν αν ένας αιτών είναι πελάτης υψηλού ή χαμηλού κινδύνου. Δεδομένου ότι ο αιτών γνωρίζει εάν είναι υψηλού ή χαμηλού κινδύνου (ενώ ο ασφαλιστής όχι), υπάρχει μια ασυμμετρία πληροφόρησης μεταξύ των δύο αυτών μερών, που οδηγεί σε αυτό που είναι γνωστό στην οικονομική βιβλιογραφία ως το πρόβλημα της δυσμενούς επιλογής. Όταν προκύψει αυτή η κατάσταση, η θεωρία υποδεικνύει ότι οι ασφαλιστές θα προσφέρουν δύο τύπους συμβάσεων: ένα ασφαλιστήριο συμβόλαιο με χαμηλό ασφάλιστρο, δηλαδή μια σύμβαση χαμηλής κάλυψης που προορίζεται να καλύψει τις εταιρίες χαμηλού κινδύνου και μια σύμβαση υψηλού ασφαλίστρου και υψηλού επιπέδου κάλυψης για να καλύψουν τις εταιρίες υψηλού κινδύνου. Προκειμένου να αντιμετωπιστεί το πρόβλημα της δυσμενούς επιλογής, οι ασφαλιστικές εταιρίες που προσφέρουν κάλυψη έναντι των κινδύνων του κυβερνοχώρου απαιτούν από τους πελάτες τους να υποβάλλονται σε διεξοδικές, λεπτομερείς και εκτεταμένες αξιολογήσεις κινδύνου. Ως προϋπόθεση για την προσφορά της απαιτούμενης κάλυψης, οι ασφαλιστές πρέπει να αξιολογούν την ασφάλεια των υποδομών των πληροφοριακών συστημάτων του αιτούντος μέσω μιας πληθώρας δραστηριοτήτων, τόσο εκτός του φυσικού χώρου της επιχείρησής τους, όσο και εντός αυτής, με στόχο την επανεξέταση των πιθανών τρωτών σημείων του αιτούντος, που δύναται να προκαλέσουν με αυξημένες πιθανότητες κάποια παραβίαση του κυβερνοχώρου του.

[95] Majuca, R., P., Yurcik, W. and Kesan, J., P. (2006), "The evolution of cyberinsurance", [online], Διαθέσιμο στο: https://arxiv.org/abs/cs/0601020, (Ημερομηνία Πρόσβασης: 04/12/2018)

Ηθικός Κίνδυνος (Moral Hazard): Το δεύτερο μείζον πρόβλημα που καλείται να αντιμετωπίσει ο ασφαλιστικός φορέας, όσον αφορά την προσφορά προϊόντων για την κάλυψη της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου είναι αυτό του ηθικού κινδύνου. Το πρόβλημα έγκειται στο ότι όταν οι επιχειρήσεις που καλύπτονται από κάποιας μορφής ασφάλισης μπορεί είτε να προκαλέσουν σκόπιμα την απώλεια (που θα τους αποφέρει την είσπραξη της κάλυψης από τον ασφαλιστή) είτε να λάβουν λιγότερα μέτρα προστασίας έναντι των κινδύνων για τους οποίους έχουν συνάψει κάποιο ασφαλιστήριο (είτε εξαιτίας της οικονομικής τους στενότητας για να επενδύσουν προς αυτό το σκοπό, είτε επειδή έχουν μειωμένα κίνητρα διατήρησης ενός ικανοποιητικού επιπέδου ασφαλείας των πληροφοριακών τους συστημάτων). Η διαφορά μεταξύ του προβλήματος του ηθικού κινδύνου και της δυσμενούς επιλογής είναι πρώτον το κόστος και δεύτερον η δομή κινήτρων που οδηγούν στην εμφάνισή τους. Η αντιμετώπιση της δυσμενούς επιλογής απαιτεί μια αρχική επενδυτική δαπάνη από την ασφαλιστική εταιρία προκειμένου να ενισχύσει τα συστήματα λήψης αποφάσεων του δυναμικού τους έτσι ώστε να μπορεί να ταξινομήσει πιο αξιόπιστα τους πιθανούς πελάτες της. Επιπλέον, η όποια αναθεώρηση των προφίλ των πελατών της ενδεχομένως να μην απαιτείται να γίνεται πολύ συχνά. Αντίθετα, το πρόβλημα του ηθικού κινδύνου απαιτεί επενδύσεις σε υποδομές για την παρακολούθηση των πελατών, που ενδεχομένως χρειάζεται να αναθεωρούνται συνεχώς. Από την άλλη πλευρά, ενώ το πρόβλημα της δυσμενούς επιλογής ασχολείται με το κίνητρο του (υψηλού κινδύνου) ασφαλισμένου να αποκρύψει πληροφορίες σχετικά με το επίπεδο του κινδύνου που αυτός ενέχει, στον ασφαλιστή, το πρόβλημα του ηθικού κινδύνου ασχολείται με κίνητρο του ασφαλισμένου να χαλαρώσει τη δράση του όσον αφορά την ενίσχυση των υποδομών προστασίας του οργανισμού του. Ο πιο συνηθισμένος τρόπος για την αντιμετώπιση του προβλήματος του ηθικού κινδύνου είναι για τους ασφαλιστές να παρακολουθούν συνεχώς το επίπεδο φροντίδας που λαμβάνει ο ασφαλισμένος για να αποτρέψει την απώλεια και να συνδέσει το ύψος του ασφάλιστρου αναλόγως της δράσης του πελάτη προς αυτή την κατεύθυνση. Με αυτόν τον τρόπο, η ύπαρξη της ασφάλισης μπορεί στην πραγματικότητα να αυξήσει το επίπεδο αυτοπροστασίας που λαμβάνει ο ασφαλισμένος παρά να το μειώσει.

4.3.6 Ύψος του Ασφαλίστρου

Το ασφάλιστρο θα πρέπει να καθοριστεί σε επίπεδο τέτοιο έτσι ώστε να είναι ελκυστικό και προσιτό για τον ασφαλισμένο αλλά και ταυτόχρονα επαρκές για την κάλυψη των αναμενόμενων απαιτήσεων από πλευράς του ασφαλιστή. Οι Mukhopadhyay et al. (2005[96], 2006[97], 2013[98]) επισκοπούν το εν λόγω θέμα στις πολύ ενδιαφέρουσες εργασίες τους, εφαρμόζοντας το μοντέλο συλλογικού κινδύνου (collective risk model) σε συνδυασμό με την θεωρία της αναμενόμενης χρησιμότητας για να κρίνουν τη θεωρητική αξία της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου σε επιχειρήσεις με διαφορετικά επίπεδα αποστροφής έναντι του κινδύνου. Διαπιστώνουν ότι με την αυξανόμενη αποστροφή έναντι του κινδύνου, οι επιχειρήσεις θα δέχονται μια πολύ πιο δίκαιη (με την έννοια του χαμηλότερου ασφαλίστρου) τιμολόγηση έναντι των ασφαλιστικών υπηρεσιών που ζητάνε για την κάλυψη των κινδύνων του κυβερνοχώρου.

Επισημαίνουν ωστόσο το γεγονός ότι οι ασφαλιστικές υπηρεσίες για την κάλυψη των κινδύνων του κυβερνοχώρου είναι ακόμα αρκετά κοστοβόρες και δεν τιμολογούνται όσο χαμηλά θα έπρεπε. Διακρίνουν τέσσερις βασικούς λόγους που οδηγούν στην ανωτέρω διαπίστωση: α) την καινοτομία (εννοώντας το νεαρό της «ηλικίας» του) του προϊόντος και συνεπώς το μικρό μέγεθος των ομάδων κινδύνου που μπορούν να συγκεντρωθούν, β) τον μικρό αριθμό των συμμετεχόντων στην αγορά (περιορισμένη διαθεσιμότητα), γ) τον περιορισμένο όγκο των διαθέσιμων δεδομένων σε σχέση με αυτόν τον κίνδυνο, καθιστώντας αναγκαίες τις μεγάλες αναλήψεις κινδύνου από τις ασφαλιστικές εταιρίες και δ) σημαντικές ασυμμετρίες πληροφόρησης που απαιτούν δαπανηρές επαληθεύσεις της κατάστασης του προφίλ κινδύνου των πελατών, καθώς και της εκ των προτέρων πολύπλοκης αξιολόγησης του συνολικού κινδύνου τους.

---

[96] Mukhopadhyay, A., Saha, D., Chakrabarti, B., B., Mahanti, A. and Podder, A. (2005), "Insurance for Cyber-risk: A Utility Model", *Decision*, 32 (1), pp. 1-19

[97] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2006), "*e-Risk Management with Insurance: A Framework Using Copula Aided Bayesian Belief Networks*", Hawaii International Conference on System Sciences, Hawaii

[98] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2013), "Cyber-Risk Decision Models: To Insure IT or Not?", *Decision Support Systems*, 56 (1), pp. 11–26

Σύμφωνα με την πολύ ενδιαφέρουσα προσέγγιση του Betterley (2013)[99], τα ασφάλιστρα που αφορούν την υπηρεσίες για την κάλυψη των κινδύνων του κυβερνοχώρου μπορεί να κυμαίνονται ακόμα, τουλάχιστον, σε υψηλά επίπεδα, ειδικά για τις μικρομεσαίες επιχειρήσεις, αλλά μπορούν να θεωρηθούν ότι βρίσκονται σε σχετικά μέτρια επίπεδα τιμών, λαμβάνοντας υπόψη τις μεγάλες αβεβαιότητες που συνεπάγεται η ανάληψη της ασφαλιστικής ευθύνης αυτής της μορφής των κινδύνων. Παρόλα αυτά, η επιστημονική κοινότητα προσδοκάει ότι το επίπεδο των τιμών των ασφαλίστρων θα μειωθεί ακόμα περισσότερο μέσα στα επόμενα χρόνια, δεδομένου ότι θα συλλεχθούν ακόμα περισσότερες πληροφορίες που σχετίζονται με τα ιστορικά στοιχεία των κρουσμάτων παραβίασης των πληροφοριακών συστημάτων των επιχειρήσεων και οι ίδιες οι ασφαλιστικές εταιρίες θα έχουν περισσότερη εμπειρία ως προς την αξιολόγηση και την διαχείριση των πελατών τους και των αντίστοιχων χαρτοφυλακίων τους.

4.3.7 Ασφαλιστικά Όρια Κάλυψης

Τα ασφαλιστήρια συμβόλαια έναντι των κινδύνων του κυβερνοχώρου καλύπτουν συνήθως μια μέγιστη απώλεια, αλλά τα πραγματικά όρια κάλυψης ποικίλλουν. Η αύξηση των ορίων αυτών είναι μεν διαπραγματεύσιμη, αλλά οδηγεί, συνήθως, σε υψηλότερα ασφάλιστρα. Σύμφωνα με τους Gatzlaff and McCullough (2012)[100], τα ασφαλιστήρια αυτά περιέχουν συνήθως αρκετές εξαιρέσεις, π.χ. για τις αυτοπροκαλούμενες ζημίες, για κρούσματα παραβίασης του εταιρικού κυβερνοχώρου που μπορεί να προκύψουν από την πρόσβαση σε μη ασφαλείς ιστότοπους, για περιπτώσεις κατασκοπείας ή/και τρομοκρατίας. Επιπλέον, ενδέχεται να υπάρχουν και άλλες έμμεσες επιπτώσεις από τις απώλειες στον κυβερνοχώρο που δεν μπορούν να μετρηθούν και συνεπώς δεν καλύπτονται. Υπάρχει ένας μεγάλος αριθμός εξαιρέσεων και η φύση του κυβερνοχώρου είναι πολύ δυναμική, έτσι ώστε τόσο η ασφαλιστική εταιρία όσο και ο πελάτης, διατηρούν υψηλά επίπεδα αβεβαιότητας για το τι πραγματικά καλύπτει το ασφαλιστήριο συμβόλαιο.

---

[99] Betterley, R. (2013), "Cyber/Privacy Insurance Market Survey 2013: Carriers Deepen Their Risk Management Services Benefits—Insureds Grow Increasingly Concerned with Coverage Limitations", [online], Διαθέσιμο στο: http://betterley.com/samples/cpims13_nt.pdf, (Ημερομηνία Πρόσβασης: 07/12/2018)

[100] Gatzlaff, K. and McCullough, K. A. (2012), "Implications of Privacy Breaches for Insurers", *Journal of Insurance Regulation*, Vol. 31, pp. 195–214

4.3.8 Δημόσια Πολιτική

Σύμφωνα με τους Biener et al. (2015)[101], η διαθεσιμότητα της ασφάλισης κατά των κινδύνων στον κυβερνοχώρο, εγείρει μια εύλογη ανησυχία για το γεγονός ότι τα εμπόδια στη διάπραξη των εγκλημάτων στον κυβερνοχώρο θα μειωθούν, καθιστώντας έτσι για τους δράστες πιο ελκυστική την διάπραξή τους. Επιπλέον, η ασφαλιστική απάτη μπορεί να ενθαρρυνθεί, καθώς διελευκανθούν. Επίσης, οι επιχειρήσεις ενδέχεται να έχουν λιγότερα κίνητρα για αυτοπροστασία. Η μείωση της αυτοπροστασίας δύναται να αυξήσει τη συνολική έκθεση στον κίνδυνο, ακόμα και ολόκληρων κλάδων επιχειρήσεων, κάτι που με την σειρά του δύναται να οδηγήσει σε μεγάλες απώλειες στην κοινωνική πρόνοια. Οι συγγραφείς παραθέτουν πλήθος αντικρουόμενων απόψεων και ερευνητικών προσεγγίσεων επί αυτού του θέματος. Ωστόσο συντάσσονται περισσότερο με την άποψη ότι η αναζήτηση ασφαλιστικής κάλυψης έναντι των κινδύνων του κυβερνοχώρου μπορεί στο τέλος να αυξήσει την εντροπία των επιχειρήσεων και να τις οδηγήσει στην βελτίωση των δομών προστασίας των πληροφοριακών τους συστημάτων – τόσο μέσω του άμεσου κινήτρου της μείωσης του ασφαλίστρου, όσο και μέσω της συνειδητοποίησης ότι η στάση αυτή θα βελτιώσει τις υποδομές και την συνολικότερη αντοχή του οργανισμού έναντι αυτής της μορφής των κινδύνων.

4.3.9 Νομικοί Περιορισμοί

Σύμφωνα με τον Antonucci (2017)[102], οι ποικίλοι νομικοί περιορισμοί ενδέχεται να αποτρέψουν την κάλυψη της ασφάλισης έναντι των κινδύνων στον κυβερνοχώρο, γεγονός που μπορεί να οδηγήσει σε πρόσθετους κινδύνους ή περιορισμούς. Ως εκ τούτου, ο κίνδυνος αλλαγής των κανονισμών και των νόμων αποτελεί σημαντικό ζήτημα για τους ασφαλιστές. Επίσης, οι πολιτικές των ασφαλιστικών εταιριών πρέπει να προσαρμόζονται αναλόγως όταν τίθενται σε ισχύ νέοι κανονισμοί που αφορούν την προστασία του κυβερνοχώρου, π.χ. ο GDPR. Από την άλλη πλευρά όμως, νέοι νόμοι και κανονισμοί μπορούν να οδηγήσουν σε αυξημένη ζήτηση για ασφάλιση, γεγονός που δύναται να τονώσει την αγορά αυτή.

---

[101] Biener, C., Eling, M. and Wirfs, J., H. (2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40 (1), pp. 131-158

[102] Antonucci, D. (2017), "*The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities*", Published by John Wiley & Sons, Inc. Hoboken, New Jersey

4.4 Εταιρικός Σχεδιασμός για την Ασφάλιση έναντι των Κινδύνων του Κυβερνοχώρου

Οι επιχειρήσεις πρέπει να εξετάζουν διαρκώς τις εξελισσόμενες συνθήκες και τις νέες απειλές στον κυβερνοχώρο προκειμένου να βρίσκονται σε συνεχή επαγρύπνηση και ετοιμότητα απέναντι σε κάθε δυνητική απειλή. Τα στελέχη που ασχολούνται με την διαχείριση των εταιρικών κινδύνων (ή οι εξωτερικοί συνεργάτες που έχουν επιφορτιστεί με την ασχολία αυτή) θα πρέπει να συνεργάζονται με τους υπευθύνους των διαφόρων επιχειρησιακών τμημάτων κατά τον συντονισμό των σχεδίων πρόληψης, μετριασμού και αντιμετώπισης των κινδύνων του κυβερνοχώρου, καθώς και να εξασφαλίζουν ότι οι εκτελούμενες δράσεις βρίσκονται σε πλήρη εναρμόνιση με την κατεύθυνση που έχει ορίσει η ανώτατη διοίκηση του οργανισμού. Σύμφωνα με τον Antonucci (2017)[103], ένα σχέδιο ασφάλισης έναντι των κινδύνων του κυβερνοχώρου θα πρέπει να λαμβάνει υπόψη τον προγραμματισμό και την επιθυμητή ανταπόκριση ενός οργανισμού. Υπάρχουν τέσσερα βασικά στάδια προς αυτή την κατεύθυνση:

1. **Εκπαίδευση και Προγραμματισμός πριν το συμβάν της επίθεσης**. Ο κατάλληλος προγραμματισμός πριν από κάποιο περιστατικό παραβίασης του κυβερνοχώρου της επιχείρησης είναι πρωταρχικής σημασίας πριν την απόφαση για την αναζήτηση της οποιασδήποτε λύσης για ασφαλιστική κάλυψη έναντι των κινδύνων του κυβερνοχώρου. Ο σωστός σχεδιασμός μειώνει την πιθανότητα εμφάνισης των κρουσμάτων παραβίασης του εταιρικού κυβερνοχώρου και επηρεάζει θετικά την ικανότητα ενός οργανισμού να ανταποκρίνεται σε ένα τέτοιο περιστατικό. Ένα βασικό στοιχείο του σχεδιασμού είναι η εκπαίδευση στο σύνολο της οργάνωσης, δηλαδή η παροχή των κατάλληλων γνωστικών εφοδίων σε όλες τις βαθμίδες της επιχείρησης – από το διοικητικό συμβούλιο μέχρι και τα κατώτερα διοικητικά και εκτελεστικά στελέχη και τους εργαζομένους. Οι επιχειρήσεις θα πρέπει να συνειδητοποιήσουν ότι η συνεχής επιμόρφωση για θέματα σχετικά με τους κινδύνους του κυβερνοχώρου δεν είναι μια εξειδίκευση που αφορά μόνο του προσωπικό της πληροφοριακής τεχνολογίας, αλλά αγκαλιάζει το σύνολο του οργανισμού.

---

103 Antonucci, D. (2017), "*The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities*", Published by John Wiley & Sons, Inc. Hoboken, New Jersey

2. **Ανάπτυξη σχεδίου αντιμετώπισης περιστατικών παραβίασης του εταιρικού κυβερνοχώρου και προγράμματος διαχείρισης κρίσεων**. Κάθε μεμονωμένο κρούσμα απόπειρας παραβίασης του εταιρικού κυβερνοχώρου δεν θα πρέπει να συγχέεται και να εκλαμβάνεται ως ένα καταστροφικό συμβάν. Για τον λόγο αυτό, θα πρέπει να υπάρχει ένα σχέδιο αντιμετώπισης των μικρότερων, σε σημαντικότητα, περιστατικών, το οποίο όμως θα πρέπει να προβλέπει τις αντιδράσεις των αρμοδίων στελεχών σε περίπτωση κλιμάκωσης του προβλήματος. Ένα σχέδιο διαχείρισης κρίσεων περιγράφει τις ευθύνες, τις διαδικασίες και τους υπευθύνους λήψης αποφάσεων σε κεντρικό επίπεδο, σε περίπτωση που προκύψει κάποιο περιστατικό το οποίο δεν θα συγκαταλέγεται μεταξύ των υποδεέστερων απειλών. Σύμφωνα με τον συγγραφέα, είναι εξίσου σημαντικό τα σχέδια αυτά να επανεξετάζονται ανά τακτά χρονικά διαστήματα, καθότι τόσο η πληροφοριακή τεχνολογία όσο και οι μορφές των κινδύνων του κυβερνοχώρου εξελίσσονται συνεχώς. Τέλος, τα σχέδια αυτά θα πρέπει να εξετάζουν ζητήματα που αφορούν ολιστικά τις αντιδράσεις της οργάνωσης (δηλαδή σε όλα τα διοικητικά και εκτελεστικά επίπεδα) και όχι μόνο του αρμοδίου τμήματος πληροφορικής του οργανισμού.
3. **Δημιουργία ενός σχεδίου συνέχισης της επιχειρηματικής δραστηριότητας**. Ο οργανισμός θα πρέπει να είναι ικανός να ανακάμψει όσο το δυνατόν συντομότερα από το οποιοδήποτε περιστατικό παραβίασης του κυβερνοχώρου του. Για το λόγο αυτό, θα πρέπει να έχει οργανώσει εκ των προτέρων τα κατάλληλα σχέδια για την συνέχιση της επιχειρηματικής του δραστηριότητας, όπως θα έκανε και στην αντίστοιχη περίπτωση των υλικών προβλημάτων ή των ποικίλων αστοχιών (που προέρχονται είτε από εσωτερικούς είτε από εξωτερικούς παράγοντες).
4. **Αναζήτηση ασφάλισης έναντι των κινδύνων του κυβερνοχώρου**. Το τέταρτο και τελευταίο βήμα σύμφωνα με τον Antonucci είναι η αξιολόγηση των τρεχουσών ασφαλιστικών συμβολαίων, αλλά και ο καθορισμός της δυνητικής ανάγκης συμπληρωματικής κάλυψης σε περίπτωση που δεν καθίσταται δυνατή η αντιμετώπιση του πλήρους (ή τουλάχιστον σημαντικότερου) όγκου των συνεπειών που μπορεί να συνεπάγεται μια δυνητικά σημαντική παραβίαση του κυβερνοχώρου της επιχείρησης. Μέσω της διαδικασίας αυτής ενθαρρύνεται ο εντοπισμός των όποιων κενών στις ασφαλιστικές δικλείδες της επιχείρησης, τονώνεται η κάλυψή τους, ενώ αξιολογούνται με έγκυρο τρόπο οι οργανωτικές αδυναμίες και σχεδιάζονται τα βέλτιστα μέτρα προστασίας, τα οποία προσαρμόζονται στις επιμέρους ανάγκες του οργανισμού.

Κατόπιν, ο συγγραφέας παρέχει κατευθυντήριες οδηγίες προς τα στελέχη διαχείρισης των εταιρικών κινδύνων, για τον αποτελεσματικότερο σχεδιασμό των βημάτων που πρέπει να υλοποιηθούν προκειμένου η αναζήτηση ασφαλιστικής κάλυψης έναντι των κινδύνων του κυβερνοχώρου να αποδώσει τα βέλτιστα για τον οργανισμό και με τον πιο αποδοτικό τρόπο. Για τον λόγο αυτό, προτείνει τα εξής επτά βήματα:

- Πρώτον, ο υπεύθυνος διαχείρισης των εταιρικών κινδύνων θα πρέπει να συντονίσει και τα τέσσερα στάδια που συνοψίστηκαν παραπάνω.
- Δεύτερον, οι υπηρεσίες ασφαλιστικής κάλυψης έναντι των κινδύνων του κυβερνοχώρου θα πρέπει να τεθούν ως ένα υποσύνολο των δυνατοτήτων του συστήματος ERM του οργανισμού. Μόλις προσδιοριστούν οι κίνδυνοι στον κυβερνοχώρο του οργανισμού, προσδιοριστούν ποσοτικά και ταξινομηθούν βάσει της προτεραιότητας αντιμετώπισής τους, τα ειδικά προσαρμοσμένα πρωτόκολλα των ενδιαφερομένων μερών του ERM θα πρέπει να περιλαμβάνουν: α) Εξασφάλιση ότι η ηγεσία του οργανισμού διαθέτει μια κατάλληλη δομή διακυβέρνησης και ότι είναι συνεχώς ενήμερη, ειδικά για τις κόκκινες ζώνες του εταιρικού κυβερνοχώρου που δεν περιλαμβάνονται στο ασφαλιστήριο συμβόλαιο, β) Εξασφάλιση ότι η οργάνωση διαθέτει κατάλληλη κατάρτιση μέσω του ανθρώπινου δυναμικού για να μετριάσει τις παραβιάσεις και τα όποια κρούσματα επιθέσεων έναντι του κυβερνοχώρου της, γ) Κατανόηση συγκεκριμένων αδυναμιών του κυβερνοχώρου που σχετίζονται με την λειτουργική οργάνωση του οργανισμού και δ) Κατανόηση των νομικών υποχρεώσεων και της χρηματοοικονομικής έκθεσης εξαιτίας των πληροφοριακών συστημάτων και των συναφών συμβάσεων με τους πελάτες και τους προμηθευτές της επιχείρησης.
- Τρίτον, θα πρέπει να επανεξεταστούν οι προμηθευτές της επιχείρησης και η αλυσίδα εφοδιασμού προκειμένου να αξιολογηθεί η οποιαδήποτε πιθανή ασφαλιστική κάλυψη, καθώς και οι τυχόν συμβατικές αποζημιώσεις που συνεπάγονται οι δυνητικές ζημίες στον κυβερνοχώρο της ασφαλισμένης επιχείρησης, εξαιτίας αστοχιών, παραλήψεων ή προβλημάτων στις δομές των ανωτέρω ενδιαφερομένων μερών της οργάνωσης.
- Τέταρτον, θα πρέπει να αναζητήσει τυχόν κενά στα υπάρχοντα ασφαλιστικά συμβόλαια, μέσω της εξέτασης της συμφωνημένης κάλυψης που παρέχει ο εκάστοτε πάροχος των ασφαλιστικών υπηρεσιών. Η αξιοποίηση εξωτερικών εμπειρογνωμόνων συνίσταται κατά την εκπόνηση αυτής της διαδικασίας, καθότι η εμπειρία τους στον χώρο μπορεί να αποβεί καίρια για την διεκδίκηση δυνητικών καλύψεων που διαφορετικά δεν θα ήταν εφικτή.

- Πέμπτον, θα πρέπει να προετοιμάσει τους μηχανισμούς για την κατάθεση της δήλωσης προς την ασφαλιστική εταιρία, σχετικά με τις δυνητικές παραβιάσεις του κυβερνοχώρου της επιχείρησης, πριν εκδηλωθεί κάποιο αντίστοιχο συμβάν. Αυτοί οι μηχανισμοί θα πρέπει να συμφωνηθούν εκ των προτέρων με τον ασφαλιστή και να συμπεριληφθούν στο ασφαλιστήριο συμβόλαιο. Ωστόσο, είναι βασικής σημασίας η επιχείρηση να είναι σε θέση να καλύψει με ίδια κεφάλαια τις όποιες αρνητικές επιπτώσεις-ζημίες μπορεί να επιφέρει μια κακόβουλη επίθεση στον κυβερνοχώρο της, δίχως να στηρίζεται βραχυπρόθεσμα στην όποια κάλυψη της παράσχει η εκάστοτε ασφαλιστική εταιρία (η οποία εν τέλει μπορεί να μην αποφέρει την προσδοκώμενη οικονομική κάλυψη για διάφορους λόγους).
- Έκτον, θα πρέπει να βρίσκεται σε συνεχή επικοινωνία και επαφή με εξωτερικούς συμβούλους και ειδήμονες στον χώρο της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου προκειμένου να εξασφαλίσει την απρόσκοπτη υποστήριξή τους σε πάσης φύσεως θέματα, αλλά κυρίως σε νομικά ζητήματα που, αδιαμφισβήτητα, θα προκύψουν σε περιπτώσεις σοβαρών γεγονότων παραβίασης του εταιρικού κυβερνοχώρου.
- Έβδομον, οφείλει να παρακολουθεί συνεχώς τις εξελίξεις γύρω από τον χώρο των κινδύνων του κυβερνοχώρου και της εξέλιξης των πληροφοριακών συστημάτων, μιας και πρόκειται για ένα ιδιαίτερα ευμετάβλητο περιβάλλον που εξελίσσεται διαρκώς. Δεν θα πρέπει επίσης να παραβλέπονται και οι όποιες εξελίξεις στην ασφαλιστική αγορά έναντι των κινδύνων του κυβερνοχώρου, καθότι ακόμα βρίσκεται σε ένα σχετικά πρώιμο στάδιο και αναμένεται να αυξηθεί ραγδαία κατά τα επόμενα χρόνια, φέρνοντας σπουδαίες εξελίξεις στο χώρο.

4.5 Παράγοντες που Επηρεάζουν την Παροχή των Ασφαλιστικών Προϊόντων για την Κάλυψη των Κινδύνων του Κυβερνοχώρου

Σύμφωνα με τους Mukhopadhyay et al. (2005)[104], μια ασφαλιστική εταιρία δύναται να αναλάβει την κάλυψη των κινδύνων του κυβερνοχώρου εφόσον πληρούνται έξι βασικές προϋποθέσεις. Πρώτον, η πιθανότητα να συμβεί το γεγονός ή τα γεγονότα που οδηγούν σε απώλεια θα πρέπει να είναι σχετικά μικρή. Δεύτερον, θα πρέπει να υπάρχει ένας μεγάλος αριθμός παρόμοιων κινδύνων για τη συγκέντρωση των απαραίτητων πληροφοριών και τη μείωση της διακύμανσης. Αυτό είναι εφικτό καθώς ένας μεγάλος αριθμός οργανισμών παγκοσμίως εξαρτώνται από τις ηλεκτρονικές συναλλαγές. Τρίτον, καθώς οι απώλειες που προκύπτουν από τις επιθέσεις εναντίον των πληροφοριακών συστημάτων των επιχειρήσεων είναι οικονομικά μεγάλες, οι οργανώσεις αυξάνουν το ενδιαφέρον τους προς την αναζήτηση τρόπων μείωσης των δυνητικών αυτών συνεπειών. Κατά συνέπεια, υπάρχουν οι προϋποθέσεις για την εξασφάλιση μιας απρόσκοπτης ροής των απαραίτητων ασφαλίστρων. Τέταρτον, η ανάληψη της ασφαλιστικής δράσης έναντι αυτής της μορφής των κινδύνων μπορεί να είναι συμφέρουσα εφόσον τα κρούσματα επιθέσεων είναι ανεξάρτητα μεταξύ τους. Πέμπτον, ο ασφαλιστής μπορεί να δεχθεί έναν τέτοιο κίνδυνο, δεδομένου ότι είναι ποσοτικοποιήσιμος και μπορεί να καθοριστεί ένα ανώτατο όριο πιθανής ευθύνης από πλευράς του. Έκτον ο ασφαλιστής μπορεί να υποθέσει ότι ο ηθικός κίνδυνος θα μπορεί να αποφευχθεί.

Για τον λόγο αυτό, οι συγγραφείς προτείνουν την διεξοδική επισκόπηση τεσσάρων βασικών παραγόντων που σχετίζονται με την ασφάλιση αυτής της μορφής των κινδύνων. Αρχικά θα πρέπει να προσδιοριστούν, αυστηρά, τα εκτιμώμενα οφέλη καθώς και η πλειοψηφία των δυνητικών κινδύνων από την ανάληψη της ασφαλιστικής αυτής δραστηριότητας. Το επόμενο βήμα είναι ο προσδιορισμός του βαθμού της έκθεσης στον κίνδυνο του ασφαλισμένου. Αυτό με τη σειρά του θα αποτελέσει και τον βασικό παράγοντα προσδιορισμού του ύψους του ασφαλίστρου που θα πρέπει να ζητηθεί για την παροχή της ασφαλιστικής κάλυψης. Τρίτον, θα πρέπει να αναλυθούν πιθανά σενάρια απαιτήσεων ασφαλιστικής κάλυψης και να εκτιμηθούν οι τρόποι διασταύρωσης της ειλικρίνειας των ασφαλισμένων, καθώς και το πιθανό εύρος της καταβολής

[104] Mukhopadhyay, A., Saha, D., Chakrabarti, B., B., Mahanti, A. and Podder, A. (2005), "Insurance for Cyber-risk: A Utility Model", *Decision*, 32 (1), pp. 1-19

αποζημιώσεων. Ο τέταρτος παράγοντας είναι αυτός του αποτελεσματικού προσδιορισμού και της αξιολόγησης των κινδύνων του κυβερνοχώρου.

Σύμφωνα με τα όσα αναφέρει ο Antonucci (2017), η ασφαλιστική αγορά έναντι των κινδύνων του κυβερνοχώρου αντιμετωπίζει ορισμένους ουσιώδεις περιορισμούς, οι οποίοι επηρεάζουν δραστικά τις παρεχόμενες υπηρεσίες. Ως προς τους ρυθμιστικούς περιορισμούς που δύναται να υπάρχουν (ή να εμφανιστούν μελλοντικά) αναφέρει την περίπτωση του Γενικού Κανονισμού Προστασίας Δεδομένων και τις απαιτήσεις που αυτός συνεπάγεται για την αναφορά και την αντιμετώπιση των κρουσμάτων παραβίασης των εταιρικών πληροφοριακών συστημάτων. Ένας δεύτερος περιορισμός είναι αυτός των οργανωτικών κενών που εντοπίζονται μεταξύ των τρόπων δράσης των ασφαλιστικών εταιριών, ανά χώρα δραστηριοποίησης. Ο περιορισμός αυτός ενισχύεται ακόμα περισσότερο από το μικρό, ακόμα τουλάχιστον, μέγεθος της αγοράς που κινείται προς την αναζήτηση και την απόκτηση υπηρεσιών για την ασφάλιση των κινδύνων του κυβερνοχώρου. Ο τρίτος περιορισμός άπτεται των μεταβλητών που αξιολογεί η κάθε ασφαλιστική εταιρία προκειμένου να προχωρήσει στην παροχή των αντίστοιχων υπηρεσιών. Δεδομένης της έλλειψης ενός ενιαίου ρυθμιστικού πλαισίου, τα προβλήματα επικοινωνίας και διακύμανσης μεταξύ των προσφερόμενων υπηρεσιών, καθώς και των επιμέρους όρων των ασφαλιστηρίων συμβολαίων, μπορούν να γίνουν εύκολα αντιληπτά.

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ, ΠΕΡΙΟΡΙΣΜΟΙ ΤΗΣ ΕΡΓΑΣΙΑΣ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ

5.1 Συμπεράσματα

Σκοπός της παρούσας διπλωματικής εργασίας ήταν η θεωρητική επισκόπηση τριών βασικών ζητημάτων: α) του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), β) των Κινδύνων του Κυβερνοχώρου (Cyber Risks) και γ) της Ασφάλισης έναντι των Κινδύνων του Κυβερνοχώρου (Cyber Risk Insurance). Μέσα από την παρουσίαση των πιο σημαντικών εννοιών σχετικών με τα ανωτέρω θέματα, προσπαθούμε να προσφέρουμε στον αναγνώστη μια, όσο το δυνατόν, πιο πλήρη εικόνα, τόσο ως προς την τρέχουσα κατάσταση της αγοράς, όσο και προς τις προκλήσεις που καλούνται να αντιμετωπίσουν οι επιχειρήσεις.

Όσον αφορά το Γενικό Κανονισμό Προστασίας Δεδομένων, διαφαίνεται ότι, σε γενικές γραμμές, η επιστημονική κοινότητα συντάσσεται με την άποψη ότι πρόκειται περί ενός γόνιμου μέτρου και μιας προσπάθειας της Ευρωπαϊκής Ένωσης, προς την θετική κατεύθυνση, για την αποτελεσματικότερη και πιο αυστηρή προστασία της αξίας των προσωπικών δεδομένων των Ευρωπαίων χρηστών του διαδικτύου. Παρόλα αυτά, η υποχρεωτική εφαρμογή του Κανονισμού, αρχής γενομένης τον Μάιο του 2018, φανέρωσε τα οργανικά προβλήματα και την έλλειψη της απαραίτητης οργάνωσης ορισμένων επιχειρήσεων, πολλές εκ των οποίων είτε δεν αντιλήφθηκαν εγκαίρως τη βαρύτητά του, είτε θεώρησαν ότι πρόκειται για ακόμα μια πηγή επιπρόσθετου κόστους (δίχως κάποιο επιπρόσθετο όφελος για τις ίδιες) και κατά συνέπεια προσπάθησαν απλώς να τον αγνοήσουν (κάτι το οποίο φυσικά δεν καθίσταται εύκολο). Το μόνο βέβαιο είναι ότι απαιτείται επιπρόσθετος χρόνος και περισσότερα στοιχεία προκειμένου να αξιολογηθούν πληρέστερα οι επιπτώσεις του GDPR, καθώς και η ευεργετική του (ή μη) συνδρομή προς την προστασία των προσωπικών δεδομένων, ενώ είναι δεδομένο ότι στα επόμενα χρόνια, η επιστημονική έρευνα θα εστιάσει ακόμα πιο πολύ προς αυτή τη κατεύθυνση.

Σχετικά με τους κινδύνους του κυβερνοχώρου, θα μπορούσαμε να πούμε ότι η τρέχουσα εικόνα μαρτυράει μόνο δυσοίωνα στοιχεία για το μέλλον και τις επιπτώσεις τους. Πρόκειται για μια μορφή κινδύνων που έχει εξελιχθεί ραγδαία, κατά τη τελευταία 15ετία, σκαρφαλώνοντας πλέον στην κορυφή της λίστας μεταξύ των πιο σημαντικών κινδύνων που απειλούν, τόσο τις επιχειρήσεις, όσο και τους μεμονωμένους ιδιώτες, στο σύνολο της παγκόσμιας οικονομίας. Η ραγδαία ανάπτυξη της τεχνολογίας και των πολύπλοκων πληροφοριακών συστημάτων, έχει οδηγήσει σε μια παράλληλη αύξηση, όχι μόνο των κρουσμάτων επιθέσεων στον παγκόσμιο κυβερνοχώρο, αλλά και της σοβαρότητας των κινδύνων αυτών, καθώς και των δυνητικών ευπαθειών των πληροφοριακών συστημάτων απέναντι στους κινδύνους αυτούς. Σύμφωνα μάλιστα με ορισμένες πρόσφατες εκτιμήσεις, το κόστος που συνεπάγονται οι κίνδυνοι του κυβερνοχώρου ανέρχεται έως και τα 600 δις. δολάρια, παγκοσμίως. Ενδιαφέρον ωστόσο έχει η παρατήρηση ότι ενώ η πλειοψηφία των επιχειρήσεων, έως και πριν μια δεκαετία, δεν απέδιδε στους κινδύνους του κυβερνοχώρου την απαιτούμενη αναγνώριση, ως προς τις δυνητικές τους συνέπειες και τις επιπτώσεις τους, σήμερα η κατάσταση έχει αντιστραφεί σε πολύ μεγάλο βαθμό. Πλέον, οι προσπάθειες στρέφονται προς την πιο αποτελεσματική και επαγγελματική διαχείριση των κινδύνων αυτών, ενώ τα δεκάδες ηχηρά παραδείγματα παραβιάσεων εταιρικών πληροφοριακών συστημάτων έχουν ευαισθητοποιήσει την παγκόσμια επιχειρηματική κοινότητα προς την ανάληψη των ευθυνών της για την βελτίωση των εταιρικών δομών και τη θωράκισή τους έναντι αυτής της μορφής των κινδύνων.

Η ραγδαία αύξηση των κινδύνων του κυβερνοχώρου (τόσο σε απόλυτα μεγέθη, όσο και σε βαρύτητα των καταγεγραμμένων περιστατικών παραβιάσεων), έχει οδηγήσει στην άνθιση του επαγγέλματος της ασφάλισης έναντι των κινδύνων αυτών. Για τις επιχειρήσεις, αυτό αποτελεί μια επιπρόσθετη επιλογή για τον σχεδιασμό του βέλτιστου προγράμματος διαχείρισης των εταιρικών κινδύνων. Τα κύρια ζητήματα που αντιμετωπίζουν οι ασφαλιστικές εταιρίες επικεντρώνονται στην έλλειψη ιστορικών δεδομένων και στη δυσκολία μοντελοποίησης των υφιστάμενων δεδομένων λόγω της εξελισσόμενης φύσης των κινδύνων στον κυβερνοχώρο. Επιπρόσθετα ζητήματα όπως η ασυμμετρία της πληροφόρησης και ο ηθικός κίνδυνος που συνεπάγεται το κάθε ασφαλιστικό εγχείρημα, φαίνεται ότι δυσχεραίνουν ακόμα περισσότερο, την ήδη περίπλοκη εικόνα που παρουσιάζει αυτή η αγορά. Παρόλα αυτά, η εικόνα για το μέλλον της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου φαίνεται ιδιαίτερα ενθαρρυντική, δεδομένου ότι αποτελεί κοινή γνώμη ότι υπάρχει τεράστιο περιθώριο ανάπτυξης.

5.2 Περιορισμοί της Εργασίας

Καταρχάς, τα τρία θέματα που εξετάσθηκαν στην παρούσα εργασία, θα μπορούσαν να αποτελέσουν πηγή έμπνευσης και συγγραφής τριών αυτοτελών εργασιών. Επιπροσθέτως, όσα στοιχεία παραθέσαμε, αφορούν την επισκόπηση βιβλιογραφικών, αμιγώς, πηγών, γεγονός που δεν προσδίδει κάποια ιδιαίτερη ερευνητική αποδεικτική ισχύ στα λεγόμενά μας. Αυτό αποτελεί και έναν βασικό περιορισμό της παρούσας διατριβής, ότι δηλαδή δεν προχωρήσαμε στην διενέργεια κάποιας έρευνας αναφορικά με το θέμα που επιλέχθηκε προς εξέταση.

Όσον αφορά τον Γενικό Κανονισμό Προστασίας Δεδομένων, τα στοιχεία και οι ερευνητικές προσπάθειες που σχετίζονται με αυτόν είναι ακόμα περιορισμένα, εξαιτίας του πρώιμου του χρόνου κατά τον οποίο βρίσκεται σε ισχύ. Αν και είχε δημοσιευθεί πλήθος συζητήσεων και προβληματισμών πριν την ημερομηνία της επίσημης εφαρμογής του, εντούτοις στους μήνες που μεσολάβησαν έκτοτε, δεν καθίστατο δυνατό να διενεργηθούν μεγάλα ερευνητικά εγχειρήματα που να εξετάζουν ποικίλα θέματα που προέκυψαν από την εφαρμογή του.

Από την άλλη πλευρά, οι κίνδυνοι του κυβερνοχώρου, καθώς και η διαχείρισή τους σε εταιρικό επίπεδο, είναι ένα θέμα για το οποίο θα μπορούσαμε να προχωρήσουμε σε πολύ πιο εκτενής και τεχνικές αναλύσεις, κάτι όμως που, εν τέλει, δεν υλοποιήθηκε στην παρούσα διατριβή. Τα πληροφοριακά συστήματα, περικλείουν πλήθος πολύπλοκων και τεχνικών όρων, οι οποίοι αν και είναι ιδιαίτερα χρήσιμοι για την βαθύτερη ανάλυση του θέματος, εντούτοις δεν θα εξυπηρετούσαν την επισκόπησή του μέσα από την πιο θεωρητική οργανωσιακή οπτική που στοχεύσαμε να του προσδώσουμε.

Τέλος, η ασφάλιση έναντι των κινδύνων του κυβερνοχώρου, αποτελεί και αυτή ένα εξίσου σημαντικό θέμα, για το οποίο θα μπορούσαμε να έχουμε αναφερθεί εκτενέστερα, αναλύοντας περαιτέρω, τόσο τα ζητήματα που ανακύπτουν από πλευράς του ασφαλιστή, όσο και τις προκλήσεις που καλείται να αντιμετωπίσει ο ασφαλισμένος. Η μοντελοποίηση των στοιχείων που σχετίζονται με τους κινδύνους του κυβερνοχώρου, καθώς και του προσδιορισμού του ύψους του ασφαλίστρου, είναι ένα ακόμα θέμα που δεν επισκοπήθηκε, αλλά αποτελεί βασική πηγή προβληματισμού για πλήθος ερευνητών και επιστημόνων.

5.3 Προτάσεις για Περαιτέρω Έρευνα

Μια εκ των βασικών διαπιστώσεών μας κατά την επισκόπηση των πηγών που χρησιμοποιήθηκαν για την συγγραφή της παρούσας εργασίας ήταν ότι η υφιστάμενη έρευνα στον τομέα των κινδύνων του κυβερνοχώρου και της ασφάλισης έναντι αυτών επικεντρώνεται κυρίως στην πλευρά της προσφοράς, δηλαδή εξετάζει το θέμα δυσανάλογα περισσότερο από την οπτική των ασφαλιστικών εταιριών. Η πλευρά της ζήτησης – δηλαδή των επιχειρήσεων που καλούνται να αντιμετωπίσουν τους κινδύνους που απειλούν τα πληροφοριακά τους συστήματα, καθώς και να αποφασίσουν το εάν θα αναζητήσουν την συνδρομή της ασφαλιστικής κάλυψης έναντι των κινδύνων αυτών - ωστόσο, μπορεί να προσελκύσει εξίσου σημαντικό ερευνητικό ενδιαφέρον στο μέλλον.

Πιο συγκεκριμένα, προτείνουμε την εξέταση του αντιληπτού επιπέδου της σοβαρότητας των κινδύνων του κυβερνοχώρου. Μια τέτοια έρευνα θα μπορούσε να αναδείξει τα όποια προβλήματα και τις γνωστικές ελλείψεις του επιχειρηματικού κόσμου αναφορικά με την έκταση και την βαρύτητα των κινδύνων του κυβερνοχώρου, καθώς επίσης και να αναδείξει τη σημασία της ασφάλισης έναντι των κινδύνων αυτών.

Επιπρόσθετα ζητήματα όπως η διερεύνηση των συνθηκών που δημιουργούν ένα ευνοϊκότερο κλίμα προς την αναζήτηση των ασφαλιστικών υπηρεσιών για την κάλυψη των κινδύνων του κυβερνοχώρου, η εξέταση των πιθανών τρόπων και μέσων βελτίωσης της αυτοπροστασίας έναντι των κινδύνων αυτών, καθώς και η εύρεση της ισορροπίας μεταξύ των ποικίλων τεχνικών διαχείρισης των εταιρικών κινδύνων προκειμένου να προταθεί ένα βέλτιστο μίγμα πολιτικής, θα μπορούσαν να αποτελέσουν έμπνευση για μελλοντική έρευνα.

Η εξέταση των υπαρχόντων μεθόδων μοντελοποίησης του ρίσκου που εγκυμονεί η ανάληψη της ασφαλιστικής κάλυψης έναντι συγκεκριμένων κινδύνων του κυβερνοχώρου, καθώς και η διασύνδεσή τους με τις τελευταίες εξελίξεις της τεχνολογίας, είναι ένα ακόμα θέμα που μπορεί να διερευνηθεί μελλοντικά. Παραδείγματος χάριν, ποια θα μπορούσε να είναι η ευθύνη της ασφαλιστικής εταιρίας απέναντι σε κρούσματα παραβίασης των πληροφοριακών συστημάτων των νέων «έξυπνων αυτοκινήτων» τα οποία καθοδηγούνται από προγράμματα τεχνητής νοημοσύνης (Artificial Intelligence – AI).

ΚΑΤΑΛΟΓΟΣ ΑΝΑΦΟΡΩΝ

ΠΗΓΕΣ ΚΑΙ ΑΡΘΡΑ

- Allianz Global Corporate Specialty. (2015), "A Guide to Cyber Risk"
- Anderson, R. and Moore, T. (2006), "The Economics of Information Security", *Science*, 314 (5799), pp. 610-613
- Antonucci, D. (2017), "*The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities*", Published by John Wiley & Sons, Inc. Hoboken, New Jersey
- Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," *IEEE Security and Privacy*, 5 (3), pp. 50–56
- Bandyopadhyay, T. M., Vijay, S. and Rao, R. C. (2009), "Why IT Managers Don't Go for Cyber-Insurance Products", Communications of the ACM, 52 (11), pp. 68–73
- Berliner, B. (1985), "Large Risks and Limits of Insurability", *The Geneva Papers on Risk and Insurance - Issues and Practice*, 10 (4), pp. 313-329
- Biener, C. (2013), "Pricing in Microinsurance Markets", *World Development*, 41 (1), pp. 132–144
- Biener, C., Eling, M. and Wirfs, J., H. (2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40 (1), pp. 131-158
- Bodin, L., D., Gordon, L., A., Loeb, M., P. and Wang, A. (2018), "Cybersecurity insurance and risk-sharing", *Journal of Accounting and Public Policy*, 37 (6), pp. 527-544
- Böhme, R. (2005), "Cyber-Insurance Revisited," *Workshop on the Economics of Information Security (WEIS)*, Harvard University, Cambridge, MA
- Bolot, J. and Lelarge, M. (2009), "Cyber Insurance as an Incentive for Internet Security", In: M. E. Johnson (ed.), *Managing Information Risk and the Economics of Security*, New York: Springer, pp. 269-290
- Caldwell, T. (2015), "Securing small businesses – the weakest link in a supply chain?", *Computer & Fraud Security*, 2015 (9), pp. 5-10

- Datoo, A. (2018), "Data in the post-GDPR world", *Computer Fraud & Security*, 2018 (9), pp. 17-18
- De Hert, P. and Papakonstantinou, V. (2016), "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", *Computer Law & Security Review*, 32 (2), pp. 179-194
- Deloitte. (2016), "*Assessing Cyber Risk. Critical questions for the board and the C-suite*"
- Edwards, B., Hofmeyr, S. and Forrest, S. (2016), "Hype and heavy tails: a closer look at data breaches", *Journal of Cybersecurity*, 2 (1), pp. 3-14
- Eling, M. and Schnell, W. (2016), "What do we know about cyber risk and cyber risk insurance?", *The Journal of Risk Finance*, 17 (5), pp. 474-491
- Eling, M. and Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, Vol. 272, pp. 1109-1119
- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F. (2016), "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol. 86, pp. 13-23
- Franke, U. (2017), "The cyber insurance market in Sweden", *Computers & Security*, Vol. 68, pp. 130-144
- Garber, J. (2018), "GDPR – compliance nightmare or business opportunity?", *Computer Fraud & Security*, 2018 (6), pp. 14-15
- Garg, A., Curtis, J. and Halper, H. (2003), "Quantifying the financial impact of IT security breaches", *Information Management and Computer Security*, 11 (2), pp. 74-83
- Gatzlaff, K. and McCullough, K. A. (2012), "Implications of Privacy Breaches for Insurers", *Journal of Insurance Regulation*, Vol. 31, pp. 195–214
- Geer, D., E. (2010), "Cybersecurity and National Policy," *Cybersecurity National Policy*, Vol. 1, pp: 203–215
- Gellert, R. (2018), "Understanding the notion of risk in the General Data Protection Regulation", *Computer Law & Security Review*, 34 (2), pp. 279-288
- Gordon, L., Loeb, M. and Sohail, T. (2003), "A Framework for Using Insurance for Cyber Risk Management", *Communications of the Association of Computing Machinery*, 46 (3), pp. 81-85
- Goucher, W. (2011), "Do SMEs have the right attitude to security?", *Computer & Fraud Security*, 2011 (7), pp. 18-20
- Grant Thornton. (2018), "*Taking AIM at cyber risk*".

- Herath, H. and Herath, T. (2011), "Copula Based Actuarial Model for Pricing Cyber Insurance Policies", *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2 (1), pp. 7–20
- Hofmann, A. and Ramaj, H. (2011), "Interdependent Risk Networks: The Threat of Cyber Attack", *International Journal of Management and Decision Making*, 11 (5/6), pp. 312–323
- James, L. (2018), "Making cyber-security a strategic business priority", *Network Security*, 2018 (5), pp. 6-8
- Krystlik, J. (2017), "With GDPR, preparation is everything", *Computer Fraud & Security*, 2017 (6), pp. 5-8
- Kurpjuhn, T. (2015), "The SME security challenge", *Computer Fraud & Security*, 2015 (3), pp. 5-7
- Maillart, T. and Sornette, D. (2010), "Heavy-tailed distribution of cyber-risks", *European Physical Journal B*, 75 (3), pp. 357–364
- Mark, H. (2016), "Why people are key to cyber-security", *Network Security*, 2016 (6), pp. 9-10
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017), "Cyber-insurance survey", *Computer Science Review*, Vol. 24, pp. 35-61
- Marsh. (2014), "Cyber gap insurance," *Global Energy Practice*
- McCall, B. (2018), "What does the GDPR mean for the medical community?", *The Lancet*, 391 (20127), pp. 1249-1250
- McKenna, B. (2018), "Measuring Cyber-Risk", *Network Security*, 2018 (4), pp. 12-14
- Mehr, R. and Cammack, E. (1961), "*Principles of Insurance*", third ed., Richard D. Irwin, Inc.
- Miglicco, G. (2018), "GDPR is here and it is time to get serious", *Computer Fraud and Security*, 2018 (9), pp. 9-11
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2006), "*e-Risk Management with Insurance: A Framework Using Copula Aided Bayesian Belief Networks*", Hawaii International Conference on System Sciences, Hawaii
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2013), "Cyber-Risk Decision Models: To Insure IT or Not?", *Decision Support Systems*, 56 (1), pp. 11–26
- Mukhopadhyay, A., Saha, D., Chakrabarti, B., B., Mahanti, A. and Podder, A. (2005), "Insurance for Cyber-risk: A Utility Model", *Decision*, 32 (1), pp. 1-19

- Ögüt, H., Raghunathan, S., and Menon, N. (2011), "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection", Risk Analysis, 31 (3), pp. 497–512
- Pandit, H., J., O' Sullivan, D. and Lewis, D. (2018), "Queryable Provenance Metadata For GDPR Compliance", *SEMANTiCS 2018 – 14th International Conference on Semantic Systems*, Procedia Computer Science
- Paul, S. (2017), "Reinforcing your SME against cyberthreats", *Computer Fraud & Security*, 2017 (10), pp. 13-15
- Payne, M. (2016), "*An Overview of the Cyber Insurance Industry: Challenges for Insurers and Insureds in Quantifying and Mitigating Cyber Risk*", Royal Holloway, University of London
- Politou, E., Michota, A., Alepis, E., Pocs, M. and Patsakis, K. (2018), "Backups and the right to be forgotten in the GDPR: An uneasy relationship", *Computer Law & Security Review*, 34 (6), pp. 1247-1257
- Refsdal, A., Solhaug, B. and Stolen, K. (2015), "Cyber Risk Management", *Springer Briefs in Computer Science*, Springer International Publishing
- Roldan-Molina, G., Almache-Cueva, M., Silva-Rabadao, C., Yevseyeva, I. and Basto-Fernandez, V. (2017), "A Comparison of Cybersecurity Risk Analysis Tools", *Procedia Computer Science*, Vol. 121, pp. 568-575
- Ryz, L. and Crest, L. (2016), "A new era in data protection", *Computer Fraud & Security*, 2016 (3), pp. 18-20
- Shackelford, S., J. (2012), "Should your firm invest in cyber risk insurance?", *Business Horizons*, 55 (4), pp. 349-356
- Shetty, N., Schwartz, G., Felegyhazi, M. and Walrand, J. (2010), "Competitive Cyber-Insurance and Internet Security", *Economics of Information Security and Privacy*, Springer, Boston, MA, pp. 229-247
- Siegel, C., A., Sagalow , T., R. and & Serritella, P. (2002), "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security, *Information Systems Security*, 11 (4), pp. 33-49

- Sinanaj, G. and Muntermann, J. (2013), "Assessing corporate reputational damage of data breaches: an empirical analysis", *Proceedings of the 26th International Bled eConference*, pp. 78–89
- Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review*, 34 (1), pp. 134-153
- Ulsch, M. (2014), "*Cyber Threat! How to manage the growing risk of cyber attacks*", Published by John Wiley & Sons, Ltd.
- Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR*", Computer Law & Security Review*, 34 (3), pp. 436-449
- Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", *Pittsburgh, PA: Carnegie Mellon*
- Zerlang, J. (2017), "GDPR: a milestone in convergence for cybersecurity and compliance", *Network Security*, 17 (6), pp. 8-11
- Ελευθεριάδης, I. (2018). *Διοίκηση Εταιρικών Κινδύνων*. Πανεπιστημιακές Σημειώσεις

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

- A&L Goodbody. (2016), "THE GDPR: A guide for businesses", [online], Διαθέσιμο στο: https://www.algoodbody.com/media/The_GDPR-AGuideforBusinesses1.pdf., [Ημερομηνία Πρόσβασης: 15/11/2018]
- Bendiek, A. and Römer, M. (2018), "Externalizing Europe: the global effects of European data protection", Digital Policy, Regulation and Governance, [online], Διαθέσιμο στο: https://doi.org/10.1108/DPRG-07-2018-0038, (Ημερομηνία Πρόσβασης, 18/11/2018)
- Betterley, R. (2010), "Understanding the Cyber Risk Insurance and Remediation Services Marketplace: A Report on the Experiences and Opinions of Middle Market CFOs", [online], Διαθέσιμο στο: http://www.casact.org/community/affiliates/CANE/0412/Betterley2.pdf, (Ημερομηνία Πρόσβασης: 05/12/2018)
- Betterley, R. (2013), "Cyber/Privacy Insurance Market Survey 2013: Carriers Deepen Their Risk Management Services Benefits—Insureds Grow Increasingly Concerned with Coverage

Limitations", [online], Διαθέσιμο στο: http://betterley.com/samples/cpims13_nt.pdf, (Ημερομηνία Πρόσβασης: 07/12/2018)

- Bird & Bird. (2017), "Guide to the General Data Protection Regulation", [online], Διαθέσιμο στο: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird–bird–guide-to-the-general-data-protection-regulation.pdf?la=en., [Ημερομηνία Πρόσβασης: 15/11/2018]
- Bitkom. (2016), "What to know about the General Data Protection Regulation (GDPR)?", [online], Διαθέσιμο στο: https://www.privacy-conference.com/sites/default/files/160916_EU-DS-GVO_FAQ_EN_02.pdf. [Ημερομηνία Πρόσβασης: 15/11/2018]
- Böhme, R. and Kataria, G. (2006), "Models and measures for correlation in cyber-insurance", *Workshop on Economics of Information Security (WEIS)*, [online], Διαθέσιμο στο: https://www.econinfosec.org/archive/weis2006/docs/16.pdf, (Ημερομηνία Πρόσβασης: 27/11/2018)
- Brockett, L., P., Golden, L., L. and Wolman, W. (2012), "Enterprise Cyber Risk Management, Risk Management for the Future - Theory and Cases", [online], Διαθέσιμο στο: http://www.intechopen.com/books/risk-management-for-the-future-theory-andcases/enterprise-cyber-risk-management, (Ημερομηνία Πρόσβασης: 24/11/2018)
- Chabrow, E. (2012), "10 Concerns When Buying Cyber Insurance", [online], Διαθέσιμο στο: http://www.bankinfosecurity.com/10-concerns-when-buying-cyber-insurance-a-4859/op-1, (Ημερομηνία Πρόσβασης: 05/12/2018)
- Costanzo, C. (2011), "Is your company prepared for cyber risk?", [online], Διαθέσιμο στο: http://www.boardmember.com/MagazineArticle_Details.aspx?id=5943&page=1, (Ημερομηνία Πρόσβασης: 04/12/2018)
- Eling, M. and Wirfs, J., H, (2016), "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", Institute of Insurance Economics, [online], Διαθέσιμο στο: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf, (Ημερομηνία Πρόσβασης: 29/11/2018)
- Eubanks, N. (2018), "The True Cost Of Cybercrime For Businesses",[online], Διαθέσιμο στο: https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/, (Ημερομηνία Πρόσβασης: 30/11/2018)
- Filkins, B. (2016), "Quantifying risk: Closing the chasm between cybersecurity and cyber insurance", *SANS Institute*, [online], Διαθέσιμο στο: https://www.sans.org/reading-

room/whitepapers/leadership/quantifying-risk-closing-chasm-cybersecurity-cyber-insurance-36770, (Ημερομηνία Πρόσβασης: 05/12/2018)

- Hallam-Baker, P. (2008), "Famous for Fifteen Minutes: A History of Hacking Culture, In: CSO Online-Security and Risk", [online], Διαθέσιμο στο: http://www.csoonline.com/article/217058/famous-for-fifteen-minutes-a-historyofhacking-culture, (Ημερομηνία Πρόσβασης: 24/11/2018)
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el
- https://www.isaca.org/pages/default.aspx
- https://www.iso.org/home.html
- https://www.rims.org/Pages/Default.aspx
- https://www.rsa.com
- Linklaters. (2016), "The General Data Protection Regulation: a survival guide", [online], Διαθέσιμο στο: http://www.linklaters.com/Insights/Pages/General-Data-Protection-Regulation-survival-guide.aspx, [Ημερομηνία Πρόσβασης: 15/11/2018]
- Majuca, R., P., Yurcik, W. and Kesan, J., P. (2006), "The evolution of cyberinsurance", [online], Διαθέσιμο στο: https://arxiv.org/abs/cs/0601020, (Ημερομηνία Πρόσβασης: 04/12/2018)
- McAfee. (2017), "The Economic Impact of Cybercrime—No Slowing Down", [online], Διαθέσιμο στο: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf, (Ημερομηνία Πρόσβασης: 30/11/2018)
- Rhemann, M. (2011). "Cyber Trends", *Trends Digest*, [online], Διαθέσιμο στο: http://trendsdigeststore.com/CyberTrends.aspx, (Ημερομηνία Πρόσβασης: 24/11/2018)
- Schwartz, G., Shetty, N. and Walrand, J. (2010), "Cyber-Insurance: Missing Market Driven by User Heterogeneity", *Submission to Workshop on the Economics of Information Security (WEIS)*, [online], Διαθέσιμο στο: https://pdfs.semanticscholar.org/d1db/6af4b7c93315e48c8ab407f1f75187a88687.pdf, (Ημερομηνία Πρόσβασης: 27/11/2018)
- Symantec. (2017), "*Norton Cyber Security Insights Report Global Results*", [online], Διαθέσιμο στο: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf, (Ημερομηνία Πρόσβασης: 30/11/2018)