Πανεπιστήμιο Πειραιά

Τμήμα
Ψηφιακών Συστημάτων

ΠΜΣ
Τεχνοοικονομική
Διοίκηση Ψηφιακών
Συστημάτων

Διαχείριση Επικινδυνότητας στις Τηλεπικοινωνίες

Risk Management in Telecoms

Ονομ/νο: Σπυρόπουλος Δημήτριος Α.Μ.: M.T.E1032

Επιβλέπων Καθηγητής: Μαρίνος Θεμιστοκλέους

Η εργασία αυτή αφιερώνεται στη "Sophita" και τα παιδιά με τα desmo, για την μεγάλη επιτυχία του WDW2012…

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1ο

Εισαγωγή

1.1 Διακυβέρνηση Ασφάλειας Πληροφοριών.

Οι πληροφορίες μπορούν να οριστούν ως «Δεδομένα με νόημα και σκοπό» και διαδραματίζουν όλο και πιο σημαντικό ρόλο σε όλες τις πτυχές της ζωής μας. Η πληροφορία αποτελεί ένα απαραίτητο στοιχείο των διεργασιών για σχεδόν όλους τους οργανισμούς. Σε έναν αυξανόμενο αριθμό εταιρειών μάλιστα, οι πληροφορίες είναι η ίδια η επιχείρηση. Αυτό περιλαμβάνει σημαντικούς παράγοντες της αναδυόμενης κοινωνίας της γνώσης, όπως η Google, το e-Bay, η Microsoft και αμέτρητες άλλες, μεγάλες και μικρές επιχειρήσεις.

Παραδοσιακοί οργανισμοί έχουν υποστεί ριζικές μετατροπές στην «εποχή της πληροφορίας». Οι γραφικές τέχνες και η βιομηχανία των εκτυπώσεων για παράδειγμα, ασχολούνται σχεδόν αποκλειστικά με πληροφορίες σε ψηφιακή μορφή.

Θα ήταν δύσκολο να βρεθεί μια επιχείρηση που δεν έχει αγγιχτεί από την τεχνολογία των πληροφοριών και δεν εξαρτάται από τις πληροφορίες τις οποίες επεξεργάζεται.

Σύμφωνα δε με το Ίδρυμα Brookings, οι πληροφορίες ενός οργανισμού και τα υπόλοιπα άυλα περιουσιακά στοιχεία του, αντιπροσωπεύουν περισσότερο από το 80% της αξίας του στην αγορά. Ως αποτέλεσμα, τα προβλήματα που επηρεάζουν την ακεραιότητα των πληροφοριών μπορεί να είναι καταστροφικά για μια επιχείρηση και τα ανώτερα στελέχη της.

Η αυξανόμενη εξάρτηση από τις πληροφορίες ήταν εμφανής περισσότερο από μια δεκαετία πριν, όταν ο Peter Drucker δήλωσε, «Η διάδοση της τεχνολογίας και την εμπορευματοποίηση των πληροφοριών μετασχηματίζει τον ρόλο των πληροφοριών σε ένα πόρο ίδιας σημασίας με τους παραδοσιακά σημαντικούς πόρους της γης» (Management Challenges for the 21st Century).

Πάνω από μια δεκαετία αργότερα, η τάση της κλιμάκωσης της αξίας και της εξάρτησης της πληροφορίας έχει αυξηθεί εκθετικά. Υπάρχουν ενδείξεις ότι η άνοδος της θα συνεχιστεί αμείωτη στο προσεχές μέλλον. Ο Gartner υπολόγισε πρόσφατα ότι, σε λιγότερο από μια δεκαετία, οι επιχειρήσεις θα λειτουργούν με 30 φορές περισσότερες πληροφορίες από ότι σήμερα. Ωστόσο, τα συνεχώς αυξανόμενα τρωτά σημεία που παρατηρούνται στην πλειονότητα των επιχειρήσεων πληροφορικής και τηλεπικοινωνιών, δεν αποτελούν σε καμία περίπτωση καθησυχαστικό παράγοντα.

Κατά την ίδια περίοδο, η εγκληματικότητα και ο βανδαλισμός της ηλεκτρονικής πληροφορίας έχει πολλαπλασιαστεί ανεξέλεγκτα. Περίπου το 80% των εθνικών υποδομών ζωτικής σημασίας στον ανεπτυγμένο κόσμο ελέγχονται από τον ιδιωτικό τομέα. Σε

συνδυασμό με την συχνά αναποτελεσματική γραφειοκρατία και τις αμέτρητες αλληλοσυγκρουόμενες δικαιοδοσίες, τα ιδρύματα δεν μπορούν να προσαρμοστούν στην αντιμετώπιση της παγκόσμιας έκρηξης της εγκληματικότητας αυτού του είδους.

Για την επαρκέστερη προστασία των πηγών πληροφόρησης, το θέμα πρέπει να τεθεί σε ένα επίπεδο παρόμοιο των άλλων κρίσιμων λειτουργιών διαχείρισης.

Η πολυπλοκότητα, η σημασία και η κρισιμότητα της ασφάλειας των πληροφοριών και της διακυβέρνησης της πρέπει να αντιμετωπιστούν και με την κατάλληλη στήριξη σε ανώτατο οργανωτικό επίπεδο.

Σταδιακά, αυτοί που καταλαβαίνουν την έκταση και το βάθος των κινδύνων των πληροφοριών παίρνουν θέση ότι, ως κρίσιμος πόρος, οι πληροφορίες πρέπει να αντιμετωπίζονται με την ίδια φροντίδα, προσοχή και σύνεση όπως οποιοδήποτε άλλο περιουσιακό στοιχείο ουσιαστικής σημασίας για την επιβίωση του οργανισμού.

Μέχρι πρόσφατα, η εστίαση της προστασίας ήταν στα συστήματα IT, που επεξεργάζονται και αποθηκεύουν την πλειοψηφία των πληροφοριών και όχι στην ίδια την πληροφορία. Αυτή η προσέγγιση όμως, δεν είναι αρκετή για να επιτευχθεί το επιθυμητό επίπεδο ολοκλήρωσης και η συνολική ασφάλεια που απαιτείται σήμερα. Η ασφάλεια των πληροφοριών επιβάλει ότι το περιεχόμενο, οι πληροφορίες και οι γνώσεις που βασίζονται σε αυτές, πρέπει να προστατεύονται επαρκώς, ανεξάρτητα από το πώς έχει γίνει η επεξεργασία, η, μεταφορά και η αποθήκευση των δεδομένων.

Το IT security, αφορά την διασφάλιση της τεχνολογίας και συνήθως καθοδηγείται από το εκάστοτε ανώτερο στέλεχος πληροφορικής (CIO). Η ασφάλεια των πληροφοριών αντιμετωπίζει το σύνολο των κινδύνων και πρέπει να καθοδηγείται από το executive management και να υποστηρίζεται από το διοικητικό συμβούλιο.

Η αδιάκοπη πρόοδος της τεχνολογίας των πληροφοριών και η απαράμιλλη ικανότητα πρόσβασης, χειρισμού και χρήσης πληροφοριών έχει φέρει τεράστια οφέλη και ευκαιρίες στην παγκόσμια οικονομία. Έφερε επίσης νέους κινδύνους και ένα συνονθύλευμα των υπαρχόντων και επερχόμενων νόμων και οδηγιών.

Το executive management, έρχεται όλο και περισσότερο αντιμέτωπο με την ανάγκη να παραμείνει ανταγωνιστικό στην παγκόσμια οικονομία και πρέπει να λάβει σοβαρά υπόψη του την υπόσχεση για μεγαλύτερα κέρδη από την ανάπτυξη περισσότερων πηγών πληροφόρησης. Αλλά, καθώς οι επιχειρήσεις θα καρπώνονται αυτά τα κέρδη, η αυξανόμενη εξάρτηση από τις πληροφορίες και τα συστήματα που τις υποστηρίζουν αναγκάζουν την διοίκηση να λάβει δύσκολες αποφάσεις για το πώς να αντιμετωπίσει αποτελεσματικά την ασφάλεια των πληροφοριών.

Επιπλέον, δεκάδες νέες και υπάρχουσες νομοθετικές και κανονιστικές διατάξεις απαιτούν όλο και περισσότερο τη τήρηση τους από τα υψηλότερα επίπεδα ευθύνης.

Η διακυβέρνηση της ασφάλειας των πληροφοριών αποτελεί ευθύνη του διοικητικού συμβουλίου και του executive management. Πρέπει να είναι αναπόσπαστο και διαφανές τμήμα της διακυβέρνησης των επιχειρήσεων. Αποτελείται από την ηγεσία, τις οργανωτικές δομές και τις διαδικασίες που διασφαλίζουν την ασφαλή πληροφόρηση.

1.2 Σύνοψη

Στην παρούσα λοιπόν διπλωματική μελετάμε – ανά κεφάλαιο – τα εξής:

Δεύτερο κεφάλαιο διπλωματικής εργασίας

Στο κεφάλαιο αυτό εξηγούμε λεπτομερειακά την διακυβέρνηση της ασφάλειας πληροφοριών περιγράφοντας τα χαρακτηριστικά της, τα περιεχόμενα που πρέπει να έχει και παρουσιάζοντας τα εμπλεκόμενα σε αυτή μέρη.

Στην πορεία του κεφαλαίου αυτού, γίνεται σαφές ότι η πολιτική ασφάλειας είναι ταυτισμένη με την έννοια της συμμόρφωσης και των μετρήσεων

Η πολιτική ασφάλειας είναι ένα σημαντικό κείμενο, όχι μόνο επειδή θέτει τα όρια, αλλά και επειδή είναι ενδεικτική της γενικότερης φιλοσοφίας και κουλτούρας ενός οργανισμού που διαθέτει τηλεπικοινωνιακό δίκτυο. Και μπορεί η ασφάλεια πληροφοριών να χρειάζεται σε όλους όσους έχουν πληροφοριακό δίκτυο, το περιεχόμενό της όμως διαφοροποιείται και προσαρμόζεται στην κάθε περίπτωση.

Η ασφάλεια είναι μια πολύ-παραγοντική διαδικασία που αφορά τους πάντες στο Internet: τον πάροχο δικτύου, τον οργανισμό, τους μόνιμους χρήστες, τους επισκέπτες.

Τρίτο κεφάλαιο διπλωματικής εργασίας

Στο τρίτο κεφάλαιο της εργασίας αυτής αναπτύσσουμε την έννοια της Διαχείρισης Επικινδυνότητας. Η Διαχείριση Επικινδυνότητας είναι το απόλυτο εργαλείο όλων των δραστηριοτήτων της ασφάλειας πληροφοριών και όλων των προσπαθειών διασφάλισης του εκάστοτε οργανισμού.

Κάθε επιτυχημένο πρόγραμμα Διαχείρισης Επικινδυνότητας μπορεί να οριστεί ως ένα πρόγραμμα που ανταποκρίνεται στις προσδοκίες και επιτυγχάνει συγκεκριμένους στόχους του οργανισμού αποδοτικά, αποτελεσματικά και με συνέπεια.

Αναλύονται λοιπόν η Στρατηγική, τα εμπλεκόμενα μέρη, η υλοποίηση και οι μεθοδολογίες κατά την διεξαγωγή της ανάλυσης των κινδύνων στους εκάστοτε οργανισμούς.

Τέταρτο κεφάλαιο διπλωματικής εργασίας

Στο κεφάλαιο τέσσερα αναλύεται η μεθοδολογία που χρησιμοποιήθηκε κατά την διεξαγωγή της διαχείρισης επικινδυνότητας σε οργανισμό – επιχείρηση παροχής υπηρεσιών κινητής τηλεφωνίας.

Καταγράφονται οι κίνδυνοι – ευπάθειες - τρωτά σημεία που διαπιστώθηκαν στις φάσεις **έναρξης, ανάπτυξης ή απόκτησης, υλοποίησης, λειτουργίας ή συντήρησης και διάθεσης** ενός νέου συστήματος για την εξυπηρέτηση υπηρεσιών προπληρωμένης κινητής τηλεφωνίας.

Στην συνέχεια παρουσιάζονται στο κεφάλαιο αυτό τα Φύλλα Κινδύνου με τους παραπάνω κινδύνους καταγεγραμμένους και ομαδοποιημένους ανάλογα με τους τομείς που εμφανίζονται κα επηρεάζουν.

Πέμπτο και Έκτο κεφάλαιο διπλωματικής εργασίας

Στα κεφάλαια αυτά αναλύονται οι μελλοντικές επεκτάσεις ενός προγράμματος ασφαλείας σε έναν πάροχο κινητών επικοινωνιών και καταγράφεται ο επίλογος της εργασίας αυτής.

Όπως εύκολα αντιλαμβάνεται κανείς, βγαίνει ένα γενικό συμπέρασμα από την παρούσα διπλωματική εργασία και γίνονται κάποιες προτάσεις σε κάποιον που θα θελήσει να επεκτείνει την εργασία αυτή που παρουσιάζεται στην συνέχεια.

Κεφάλαιο 2ο

Ασφάλεια Πληροφοριών

2.1 Η σημασία της διακυβέρνησης της ασφάλειας πληροφοριών

Στις σύγχρονες επιχειρήσεις, η διακυβέρνηση της ασφάλειας πληροφοριών, είναι όλο και πιο κρίσιμη καθώς η εξάρτηση από τις πληροφορίες μεγαλώνει.

Οι πληροφορίες είναι η ουσία της γνώσης. Και η γνώση, είναι με την σειρά της αποθηκευμένη και οργανωμένη πληροφορία. Για τους περισσότερους οργανισμούς, οι πληροφορίες και η γνώση που βασίζεται σε αυτές, αποτελούν όλο και περισσότερο, τα σημαντικότερα περιουσιακά τους στοιχεία.

Τα συστήματα και οι διαδικασίες που χειρίζονται τις πληροφορίες αυτές έχουν γίνει πραγματικά απαραίτητα σε όλες τις επιχειρήσεις και τους κυβερνητικούς οργανισμούς σε παγκόσμιο επίπεδο. Αυτή η αυξανόμενη εξάρτηση των επιχειρήσεων από την πληροφορία και τα συστήματα που την διαχειρίζονται, σε συνδυασμό με τους κινδύνους αλλά και τα οφέλη και τις ευκαιρίες αυτών των πόρων σήμερα έχουν καταστήσει την διακυβέρνηση της ασφάλειας πληροφοριών μια όλο και πιο σημαντική πτυχή της συνολικής διακυβέρνησης των οργανισμών. Έτσι, η συνετή διαχείριση παρέχει σημαντικά οφέλη:

- Διασφάλιση της τήρησης των πολιτικών των οργανισμών.
- Αύξηση της δυνατότητας πρόγνωσης και μείωση της αβεβαιότητας των επιχειρηματικών δραστηριοτήτων μειώνοντας τους κινδύνους σε αποδεκτά επίπεδα
- Παρέχει την δομή και το πλαίσιο για τη βελτιστοποίηση της κατανομής των περιορισμένων πόρων ασφάλειας.
- Διασφαλίζει ότι οι σημαντικές αποφάσεις δεν βασίζονται σε εσφαλμένες πληροφορίες.
- Παρέχει μια σταθερή βάση για την αποδοτική και αποτελεσματική διαχείριση των κινδύνων, τη βελτίωση της διαδικασίας και την ταχεία αντιμετώπιση τέτοιου είδους περιστατικών.
- Παρέχει μεγαλύτερη εμπιστοσύνης στις αλληλεπιδράσεις με τους εμπορικούς εταίρους
- Βελτιώνει την εμπιστοσύνη στους πελάτες της επιχείρησης.
- Διαφυλάττει την φήμη του οργανισμού
- Προωθεί νέους, καλύτερους τρόπους διαχείρισης των ηλεκτρονικών συναλλαγών.
- Έχει την ευθύνη διαφύλαξης των πληροφοριών κατά τις σοβαρές επιχειρησιακές δραστηριότητες, όπως είναι οι συγχωνεύσεις και οι εξαγορές.

2.2 Συμπεράσματα από την διακυβέρνηση της ασφάλειας πληροφοριών

Η ασφάλεια πληροφοριών περιλαμβάνει όλα εκείνα τα στοιχεία που απαιτούνται για την διασφάλιση της διοίκησης ότι οι κατευθύνσεις και οι προθέσεις της αντανακλούνται στην κατάσταση ασφάλειας του οργανισμού, αξιοποιώντας μια δομημένη προσέγγιση για την υλοποίηση ενός προγράμματος ασφαλείας.

Ο σκοπός της ασφάλειας πληροφοριών είναι η ανάπτυξη, η υλοποίηση και η διαχείριση ενός προγράμματος ασφαλείας το οποίο θα ικανοποιεί τις ακόλουθες 6 πτυχές της:

1. **Strategic alignment** (Στρατηγική ευθυγράμμιση). Η συμπόρευση της ασφάλειας πληροφοριών με την επιχειρηματική στρατηγική για την επίτευξη των ακόλουθων στόχων του οργανισμού:
    - Security requirements. Πρέπει να καθοδηγούνται από τις επιχειρηματικές απαιτήσεις οι οποίες αναπτύσσονται στον εκάστοτε οργανισμό.
    - Security Solutions. Κατάλληλες λύσεις ασφαλείας, για τις διαδικασίες των επιχειρήσεων, που λαμβάνουν υπόψη την κουλτούρα, τον τρόπο διαχείρισης, την τεχνολογία και της δομή της οργάνωσης.
    - Επενδύσεις στην ασφάλεια των πληροφοριών. Ευθυγραμμισμένη με τη στρατηγική της επιχείρησης, η ασφάλεια πληροφοριών πρέπει να αναγνωρίζει τις απειλές, τα τρωτά σημεία και το εκάστοτε ρίσκο.

2. **Risk Management** (Διαχείριση επικινδυνότητας). Η λήψη των κατάλληλων μέτρων για την μείωση των κινδύνων και των πιθανών επιπτώσεων στις πηγές πληροφορίας σε ένα αποδεκτό επίπεδο.
    - Κατανόηση των απειλών και των τρωτών σημείων του οργανισμού.
    - Κατανόηση της έκθεσης του σε κινδύνους και τις πιθανές συνέπειες ενός συμβιβασμού.
    - Συνειδητοποίηση των προτεραιοτήτων διαχείρισης των κινδύνων με βάση τις πιθανές συνέπειες.
    - Επαρκής μείωση του κινδύνου για την επίτευξη αποδεκτών συνεπειών από τους υπολειπόμενους κινδύνους.
    - αποδοχή του κινδύνου με βάση την κατανόηση των πιθανών συνεπειών του υπολειπόμενου κινδύνου.

3. **Value delivery** (Παροχή αξίας). Βελτιστοποίηση των επενδύσεών της ασφάλειας για την υποστήριξη των επιχειρηματικών στόχων, όπως:
    - Ένα τυποποιημένο σύνολο από πρακτικές ασφαλείας, δηλαδή βασικές απαιτήσεις ασφάλειας ύστερα από κατάλληλες πρακτικές, ανάλογες των κίνδυνων.
    - Σωστά κατανεμημένες προσπάθειες στις περιοχές με την μεγαλύτερη επίδραση και όφελος των επιχειρήσεων.

- Θεσμοθετημένες και εμπορευματοποιημένες, βασισμένες σε πρότυπα, λύσεις.
- Ολοκληρωμένες λύσεις, που καλύπτουν την οργάνωση , τις διαδικασίες καθώς και την τεχνολογία, με βάση την κατανόηση της οργάνωσης όλης της επιχείρησης.
- Η συνεχής βελτίωση της κουλτούρας του οργανισμού, που βασίζεται στην αντίληψη ότι η ασφάλεια είναι μια διαδικασία και όχι ένα γεγονός.

4. **Resource management** (Διαχείριση πόρων). Η αποτελεσματική και αποδοτική χρήση των γνώσεων της ασφάλειας πληροφοριών για τα ακόλουθα:
    - Διασφάλιση παροχής και διάθεσης των γνώσεων σε όλα τα επίπεδα του οργανισμού.
    - Διαδικασίες ασφάλειας εγγράφων και πρακτικών.
    - Ανάπτυξη αρχιτεκτονικών ασφάλειας για αποτελεσματικό καθορισμό και αξιοποίηση των πόρων των υποδομών.

5. **Performance Measurement** (Μέτρηση απόδοσης). Η παρακολούθηση και η υποβολή αναφορών σχετικά με τις διαδικασίες της ασφάλειας πληροφοριών για να εξασφαλιστεί ότι οι στόχοι έχουν επιτευχθεί περιλαμβάνει:
    - Ένα σύνολο μετρήσεων καθορισμένο, συμφωνημένο και με ουσία, ευθυγραμμισμένο με τους στρατηγικούς στόχους.
    - Την διαδικασία μέτρησης, η οποία βοηθά στον εντοπισμό των ελλείψεων και παρέχει πληροφορίες (και ανατροφοδότηση) σχετικά με την πρόοδο στην επίλυση ζητημάτων.
    - Ανεξάρτητη ασφάλεια με εξωτερικές αξιολογήσεις και ελέγχους.

6. **Integration** (Ολοκλήρωση). Ενσωμάτωση όλων των σχετικών παραγόντων για την εξασφάλιση ότι οι διαδικασίες λειτουργούν όπως προβλέπεται σε όλο τον οργανισμό:
    - Καθορισμός όλων των οργανωτικών λειτουργιών ασφαλείας.
    - Δημιουργία δεσμών με όλες τις λειτουργίες ασφάλειας.
    - Συντονισμός όλων των λειτουργιών ασφαλείας για πληρέστερη ασφάλεια.
    - Διασφάλιση επικάλυψης μεταξύ ρόλων και ευθυνών στις λειτουργίες ασφαλείας.

2.3 Στόχοι και σκοποί των επιχειρήσεων.

Η εταιρική διακυβέρνηση είναι το σύνολο των αρμοδιοτήτων και των πρακτικών εκείνων που ασκούνται από το διοικητικό συμβούλιο και την ανώτερη διοίκηση με σκοπό την παροχή στρατηγικών κατευθύνσεων, διασφαλίζοντας την επίτευξη των στόχων, την μείωση των κινδύνων και τον έλεγχο των πόρων της επιχείρησης με υπευθυνότητα.

Η στρατηγική κατεύθυνση της επιχείρησης καθορίζεται από τους επιχειρηματικούς σκοπούς και στόχους.

Η ασφάλεια των πληροφοριών πρέπει να υποστηρίζει τις επιχειρηματικές δραστηριότητες για να έχουν αξία για τον οργανισμό.

Η διακυβέρνηση της ασφάλειας πληροφοριών είναι ένα υποσύνολο της εταιρικής διακυβέρνησης. Παρέχει όλες εκείνες τις στρατηγικές κατευθύνσεις σε δραστηριότητες που σχετίζονται με την ασφάλεια κα διασφαλίζει την επίτευξη των στόχων. Εξασφαλίζει ότι οι κίνδυνοι της ασφάλειας πληροφοριών διευθετούνται κατάλληλα και οι πληροφορίες των επιχειρήσεων χρησιμοποιούνται υπεύθυνα.

Για την επίτευξη αποτελεσματικής διαχείρισης της ασφάλειας πληροφοριών, η διοίκηση, πρέπει να καθιερώσει και να διατηρήσει ένα πλαίσιο που θα καθορίζει την ανάπτυξη και την διαχείριση ενός ολοκληρωμένου προγράμματος για την ασφάλεια πληροφοριών που θα υποστηρίζει τους επιχειρηματικούς στόχους.

Το πλαίσιο αυτό θα πρέπει γενικά να αποτελείται από:

1. Μια ολοκληρωμένη στρατηγική για την ασφάλεια, άμεσα συνδεδεμένη με τους επιχειρηματικούς στόχους.

2. Πολιτικές ασφάλειας που θα καλύπτουν κάθε πτυχή της στρατηγικής, των ελεγκτικών μηχανισμών και κανονισμών.

3. Ένα πλήρες σύνολο προτύπων, για να εξασφαλιστεί ότι οι διαδικασίες και οι κατευθυντήριες γραμμές συμμορφώνονται με τις πολιτικές του οργανισμού.

4. Μια αποτελεσματική οργανωτική δομή της ασφάλειας, που να καλύπτει τις συγκρούσεις συμφερόντων, με κύρος και πόρους.

5. Θεσμοθετημένες μετρήσεις και διαδικασίες παρακολούθησης που να διασφαλίζουν την εταιρική συμμόρφωση, να παρέχουν πληροφορίες για την αποτελεσματικότητα του οργανισμού και να αποτελούν την βάση για την λήψη των κατάλληλων αποφάσεων της διοίκησης.

Το πλαίσιο αυτό, με τη σειρά του, αποτελεί τη βάση για την ανάπτυξη ενός οικονομικά αποτελεσματικού προγράμματος ασφάλειας πληροφοριών, που να υποστηρίζει τους επιχειρηματικούς στόχους του οργανισμού.

2.4 Ρόλοι και αρμοδιότητες της ανώτατης διοίκησης.

2.4.1 Ανώτερη διοίκηση (Board of Directors/Senior Management)

Η διαχείριση της ασφάλειας πληροφοριών απαιτεί ώθηση και στρατηγική κατεύθυνση, δέσμευση, πόρους και ανάθεση των ευθυνών καθώς και ένα τρόπο, το διοικητικό συμβούλιο, να καθορίσει ότι ο σκοπός έχει επιτευχθεί. Η αποτελεσματική διαχείριση της ασφάλειας πληροφοριών μπορεί να επιτευχθεί μόνο με τη συμμετοχή της ανώτερης διοίκησης, την κατάλληλη παρακολούθηση και τις μετρήσεις, σε συνδυασμό με την υποβολή εκθέσεων και την ανάλυση των τάσεων.

Τα μέλη του διοικητικού συμβουλίου πρέπει να έχουν επίγνωση των περιουσιακών στοιχείων του οργανισμού και της κρισιμότητάς τους στις τρέχουσες επιχειρηματικές δραστηριότητες. Αυτό μπορεί να επιτευχθεί με την παροχή υψηλού επιπέδου αποτελεσμάτων, εκτενών αξιολογήσεων κινδύνου και την ανάλυση των επιχειρηματικών επιπτώσεων (business impact analysis -BIA) ανά τακτά χρονικά διαστήματα.

Μπορεί επίσης να επιτευχθεί με την αξιολόγηση της εξάρτησης των επιχειρήσεων από τις πηγές πληροφόρησης. Το αποτέλεσμα αυτών θα πρέπει να περιλαμβάνει την επικύρωση των προστατευόμενων κεφαλαίων από τα μέλη του διοικητικού συμβουλίου και το γεγονός ότι οι προτεραιότητες και τα επίπεδα προστασίας συμμορφώνονται με τα πρότυπα ασφαλείας του οργανισμού.

Η διοίκηση θα πρέπει να συμβάλλει στην αποτελεσματική διαχείριση της ασφάλειας. Είναι παράλογο να απαιτείται από το προσωπικό των χαμηλότερων επιπέδων, συμμόρφωση με τα μέτρα ασφαλείας εάν η ίδια η ανώτερη διοίκηση δεν τα εφαρμόζει. Η έγκριση των απαιτήσεων ασφαλείας από την εκτελεστική διεύθυνση αποτελεί την βάση για την διασφάλιση ότι η ασφάλεια εφαρμόζεται σε όλα τα επίπεδα του εκάστοτε οργανισμού. Κυρώσεις για την μη συμμόρφωση θα πρέπει να καθορίζονται, να κοινοποιούνται και να εκτελούνται από το διοικητικό συμβούλιο και σε όλα τα υπόλοιπα επίπεδα.

2.4.2 Εκτελεστική Διεύθυνση (Executive management)

Η εφαρμογή αποτελεσματικής διακυβέρνησης της ασφάλειας και ο καθορισμός των στρατηγικών στόχων της ασφάλειας ενός οργανισμού μπορεί να είναι ένα σύνθετο και επίπονο έργο. Όπως και με κάθε άλλη σημαντική πρωτοβουλία, για να επιτύχει πρέπει να έχει διαρκή υποστήριξη από την εκτελεστική διεύθυνση εντός του οργανισμού.

Η ανάπτυξη μιας αποτελεσματικής στρατηγικής για την ασφάλεια των πληροφοριών απαιτεί την ενσωμάτωση και συνεργασία με τους χρήστες των επιχειρηματικών διαδικασιών. Το αποτέλεσμα θα είναι η ευθυγράμμιση της ασφάλειας πληροφοριών με τους επιχειρηματικούς

στόχους. Ο βαθμός στον οποίο αυτό επιτυγχάνεται καθορίζει την αποδοτικότητα του προγράμματος της ασφάλειας πληροφοριών στην επίτευξη του επιδιωκόμενου στόχου, παρέχοντας ένα επίπεδο διασφάλισης των επιχειρηματικών διαδικασιών και ένα αποδεκτό επίπεδο επιπτώσεων από τις ανεπιθύμητες ενέργειες.

2.4.3 Οργανωτική Επιτροπή (Steering Committee)

Έως κάποιο βαθμό, η ασφάλεια επηρεάζει όλες τις πτυχές ενός οργανισμού και για να είναι αποτελεσματική πρέπει να είναι διάχυτη σε όλη την επιχείρηση. Για να εξασφαλιστεί η συμμετοχή όλων των παραγόντων που επηρεάζονται, πολλοί οργανισμοί χρησιμοποιούν μια οργανωτική επιτροπή η οποία αποτελείται από υψηλόβαθμους εκπροσώπους των επηρεαζόμενων ομάδων.

2.4.4 Γενικός Διευθυντής Ασφάλειας Πληροφοριών (Chief Information Security Officer – CISO)

Όλοι οι οργανισμοί έχουν ένα υπεύθυνο ασφάλειας πληροφοριών (ClSO), είτε κάποιος κατέχει αυτόν τον τίτλο είτε όχι. Μπορεί να είναι ο Διευθυντής συστημάτων πληροφορικής (Chief Information Officer – CIO), ο επικεφαλής αξιωματικός ασφαλείας (Chief Security Officer - CSO), ο Οικονομικός Διευθυντής (Chief Financial Officer - CFO) ή, σε ορισμένες περιπτώσεις, ο διευθύνων σύμβουλος (Chief Enterprise Officer - CEO). Το πεδίο εφαρμογής και το εύρος της ασφάλειας πληροφοριών σήμερα είναι τέτοια που η εξουσία που απαιτείται και οι ευθύνες που αναπόφευκτα πρέπει να αποδοθούν απαιτούν ένα στέλεχος επιπέδου εκτελεστικού διευθυντή. Οι νομικές ευθύνες επεκτείνουν την δομή της διοίκησης και τελικά αποδίδονται στα ανώτερα διοικητικά στελέχη και το διοικητικό συμβούλιο.

Ενδεχόμενη αποτυχία στην εφαρμογή των προηγουμένων αλλά και των κατάλληλων δομών διαχείρισης μπορεί να οδηγήσει σε ανώτερα διοικητικά στελέχη που αγνοούν αυτή την ευθύνη και των υποχρεώσεων που απορρέουν. Επίσης, έχει συνήθως ως αποτέλεσμα την έλλειψη αποτελεσματικής ευθυγράμμισης των δραστηριοτήτων ασφαλείας με τους οργανωτικούς στόχους.

Η συνετή διαχείριση προάγει την θέση ενός υπεύθυνου ασφάλειας πληροφοριών σε διευθυντικό στέλεχος όσο οι οργανισμοί αρχίζουν να κατανοούν την εξάρτησή τους από τις πληροφορίες και τις αυξανόμενες απειλές σε αυτές. Επιπρόσθετα, η διασφάλιση της θέσης σε συνδυασμό με τις ευθύνες και τους πόρους που απαιτούνται αποδεικνύει την ευαισθητοποίηση της εκάστοτε διοίκησης και την προσήλωση στην σωστή διαχείριση της ασφάλειας πληροφοριών.

Οι αρμοδιότητες και οι εξουσίες των διαχειριστών της ασφάλειας πληροφοριών ποικίλλουν σημαντικά μεταξύ των οργανισμών, παρά το γεγονός ότι βρίσκονται σε άνοδο σε παγκόσμιο επίπεδο. Αυτό μπορεί να αποδοθεί στην αυξανόμενη συνειδητοποίηση της σημασίας της, καθώς προκύπτουν σε καθημερινή βάση σημαντικές αποτυχίες ασφάλειας και αυξανόμενες απώλειες. Οι ευθύνες αυτές σήμερα κυμαίνονται από τον υπεύθυνο ασφάλειας πληροφοριών (CISO) ή τον αντιπρόεδρο για την ασφάλεια, που αναφέρεται στον διευθύνοντα σύμβουλο, (CEO) μέχρι το επίπεδο των διαχειριστών συστημάτων, οι οποίοι έχουν μερική ευθύνη για τη διαχείριση της ασφάλειας και μπορούν να υποβάλουν εκθέσεις στον IT manager ή τον Διευθυντής συστημάτων πληροφορικής (CIO).

2.5 Διάγραμμα αρμοδιοτήτων

Η σχέση μεταξύ των συμπερασμάτων της αποτελεσματικής διαχείρισης της ασφάλειας και των ευθυνών της διοίκησης φαίνεται στον ***πίνακα 2.1***. Αυτά δεν αποσκοπούν σε μια εκτενή παρουσίαση, απλώς υποδεικνύουν ορισμένα επίπεδα της διοίκησης και τα καθήκοντα για τα οποία είναι υπεύθυνη.

Πίνακας 2.1—Συσχέτιση των αποτελεσμάτων της Διαχείρισης της Ασφάλειας Πληροφοριών με τις ευθύνες της Διοίκησης.

Επίπεδο Διοίκησης	Στρατηγική Ευθυγράμμιση	Διαχείριση Επικινδυνότητας	Παροχή Αξίας	Μέτρηση Απόδοσης	Διαχείριση Πόρων	Διασφάλιση Διαδικασιών
Διοικητικό Συμβούλιο	Απαιτεί ευθυγράμμιση με αποδείξεις.	Καθιέρωση ανοχής κινδύνου Ελέγχει την πολιτική Διαχείρισης Επικινδυνότητας Διασφαλίζει την κανονιστική συμμόρφωση	Απαιτεί αναφορά του κόστους των δραστηριοτήτων ασφαλείας.	Απαιτεί αναφορά της αποτελεσματικότητας της ασφάλειας.	Επιβλέπει την πολιτική διαχείρισης γνώσης και αξιοποίησης των πόρων.	Επιβλέπει την πολιτική διασφάλισης της διαδικασίας Ολοκλήρωσης.
Εκτελεστική Διεύθυνση	Θεσπίζει τις διαδικασίες για την ενσωμάτωση της ασφάλειας στους επιχειρηματικούς στόχους	Διασφαλίζει ότι οι ρόλοι και οι αρμοδιότητες τους εμπεριέχουν την Διαχείριση Επικινδυνότητας σε κάθε δραστηριότητά τους. Παρακολουθεί την κανονιστική συμμόρφωση.	Απαιτεί μελέτες περιπτώσεων επιχειρήσεων για πρωτοβουλίες σχετικές με την ασφάλεια.	Απαιτεί παρακολούθηση και μετρήσεις για τις δραστηριότητες ασφαλείας.	Διασφάλιση των διαδικασιών λήψης γνώσεων και αποδοτικών μετρήσεων.	Έχει την εποπτεία όλων των λειτουργιών διασφάλισης και τα σχέδια ολοκλήρωσης.
Οργανωτική Επιτροπή	Επανεξετάζει και βοηθά την στρατηγική ασφαλείας και τις προσπάθειες Ολοκλήρωσης. Διασφαλίζει ότι οι ιδιοκτήτες των επιχειρήσεων υποστηρίζουν την Ολοκλήρωση.	Αναγνωρίζει ενδεχόμενους κινδύνους, Προωθεί πρακτικές ασφαλείας στις επιχειρηματικές μονάδες και εντοπίζει ζητήματα συμμόρφωσης.	Επανεξετάζει και παρέχει συμβουλές σχετικά με την επάρκεια των πρωτοβουλιών της ασφάλειας για την εξυπηρέτηση των επιχειρηματικών λειτουργιών	Επανεξετάζει και συμβουλεύει εάν οι πρωτοβουλίες ασφαλείας πληρούν τους επιχειρηματικούς στόχους.	Επανεξετάζει τις διαδικασίες λήψης γνώσεων και διάδοσής της.	Προσδιορίζει τις κρίσιμες επιχειρηματικές διαδικασίες και τους παρόχους ασφαλείας. Άμεση διασφάλιση των προσπαθειών ολοκλήρωσης.
CISO/ Διεύθυνση Ασφάλειας Πληροφοριών	Ανάπτυξη της στρατηγικής ασφαλείας, επίβλεψη του προγράμματος ασφαλείας και των πρωτοβουλιών και επαφή με τους ιδιοκτήτες των επιχειρήσεων για συνεχή ευθυγράμμιση.	Διασφάλιση διεξαγωγής αξιολογήσεων κινδύνων και επιχειρηματικών επιδράσεων. Ανάπτυξη στρατηγικών μείωσης του κινδύνου Ενίσχυση της πολιτικής και κανονιστικής	Παρακολούθηση της αξιοποίησης και της αποτελεσματικότητας των πόρων ασφάλειας	Ανάπτυξη και εφαρμογή παρακολούθησης και μετρήσεων καθώς και παρακολούθηση των δραστηριοτήτων ασφαλείας.	Ανάπτυξη μεθόδων για την λήψη γνώσεων και για την διάδοσή της. Ανάπτυξη μετρήσεων αποτελεσματικότητας και αποδοτικότητας.	Βρίσκεται σε επαφή με άλλους παρόχους ασφαλείας Διασφάλιση ότι τα κενά και οι αλληλεπικαλύψεις εντοπίζονται και αντιμετωπίζονται
Στελέχη Εσωτερικού Ελέγχου	Αξιολόγηση και αναφορές για το βαθμό ευθυγράμμισης	Αξιολόγηση και αναφορές στις πρακτικές και τα αποτελέσματα της Διαχείρισης Επικινδυνότητας	Αξιολόγηση των αναφορών αποδοτικότητας.	Αξιολόγηση και αναφορές σχετικά με την αποτελεσματικότητα και τη διαχείριση των πόρων.	Αξιολόγηση και αναφορές αποδοτικότητας και διαχείρισης πόρων	Αξιολόγηση και αναφορές αποτελεσματικότητας των διαδικασιών διασφάλισης που εκτελούνται από διαφορετικές περιοχές της διαχείρισης.

Source: UGI, Information Security Governance: Guidance tor Information Security Managers, 2008.

2.6 Το αντικείμενο της Ασφάλειας Πληροφοριών

Η ασφάλεια πληροφοριών αναφέρεται σε όλες τις πτυχές της πληροφορίας είτε πρόκειται για ομιλία, κείμενα, έντυπα, κείμενα ηλεκτρονικής μορφής είτε οποιαδήποτε άλλο μέσο, ανεξάρτητα από το αν έχει δημιουργηθεί, προβληθεί, μεταφερθεί, αποθηκευτεί ή καταστραφεί. Αυτό έρχεται σε αντίθεση με την ασφάλεια των IT συστημάτων, η οποία ασχολείται με την ασφάλεια των πληροφοριών εντός των ορίων του τομέα της τεχνολογίας.

Συνήθως, οι εμπιστευτικές πληροφορίες που αποκαλύπτονται από μία συζήτηση ή στέλνονται μέσω mail θα έπρεπε να είναι εκτός από το πεδίο της ασφάλειας πληροφοριών. Ωστόσο, από την άποψη της ασφάλειας πληροφοριών, η φύση και το είδος του συμβιβασμού δεν είναι σημαντικός παράγοντας. Το γεγονός ότι η ασφάλεια έχει παραβιαστεί είναι ο πλέον σημαντικός παράγοντας.

Στο πλαίσιο της διαχείρισης της ασφάλειας πληροφοριών, είναι σημαντικό ότι το πεδίο εφαρμογής και οι ευθύνες της ασφάλειας πληροφοριών είναι σαφώς ορισμένες στη στρατηγική της ασφάλειας πληροφοριών.

Η ομάδα *"Corporate Governance Task Force"* της *"National Security Partnership"*, μιας ομάδας συνεργασίας των εταιρικών και κυβερνητικών ηγετών, έχει προσδιορίσει ένα βασικό σύνολο από αρχές για να βοηθήσει την εφαρμογής της αποτελεσματικής διακυβέρνησης της ασφάλειας των πληροφοριών:

- Οι διευθύνοντες σύμβουλοι (CEOs) θα πρέπει να προβαίνουν σε ετήσια αξιολόγηση της ασφάλειας πληροφοριών, την επανεξέταση των αποτελεσμάτων με το κατάλληλο προσωπικό και να υποβάλλουν εκθέσεις σχετικά με τις επιδόσεις στο διοικητικό συμβούλιο.
- Οι οργανισμοί θα πρέπει να διεξάγουν περιοδικές αξιολογήσεις των κινδύνων των πληροφοριών από τα περιουσιακά στοιχεία, ως μέρος ενός προγράμματος διαχείρισης επικινδυνότητας.
- Οι οργανισμοί θα πρέπει να εφαρμόζουν πολιτικές και διαδικασίες που να βασίζονται στην εκτίμηση της επικινδυνότητας, για τη διασφάλιση των πληροφοριών των περιουσιακών στοιχείων.
- Οι οργανισμοί θα πρέπει να θεσπίσουν μια δομή διαχείρισης της ασφάλειας η οποία να αναθέσει ρητά τους επιμέρους ρόλους, αρμοδιότητες, εξουσίες και την υποχρέωση λογοδοσίας.
- Οι οργανισμοί πρέπει να αναπτύξουν σχέδια και να αναλάβουν δράση για την παροχή επαρκούς ασφάλειας των πληροφοριών για τις εγκαταστάσεις δικτύων, των συστημάτων και των πληροφοριών.
- Οι οργανισμοί θα πρέπει να αντιμετωπίζουν την ασφάλεια των πληροφοριών ως αναπόσπαστο μέρος του κύκλου ζωής των συστημάτων.
- Οι οργανισμοί πρέπει να παρέχουν τις απαραίτητες πληροφορίες για την ενημέρωση σε θέματα ασφαλείας, την κατάρτιση και την εκπαίδευση του προσωπικού.
- Οι οργανισμοί θα πρέπει να διεξάγουν περιοδικές δοκιμές και αξιολογήσεις της αποτελεσματικότητας των πολιτικών της ασφάλειας πληροφοριών και των διαδικασιών.

- Οι οργανισμοί πρέπει να δημιουργήσουν και να εκτελέσουν ένα σχέδιο για την επανορθωτική δράση και την αντιμετώπιση τυχόν αδυναμιών της ασφάλειας πληροφοριών.
- Οι οργανισμοί πρέπει να αναπτύξουν και να εφαρμόσουν διαδικασίες αντιμετώπισης περιστατικών.
- Οι οργανισμοί πρέπει να καταρτίσουν σχέδια, διαδικασίες και δοκιμές για να εξασφαλιστεί η συνέχεια των λειτουργιών τους.
- Οι οργανισμοί θα πρέπει να χρησιμοποιούν τις καλύτερες πρακτικές ασφαλείας όπως είναι το ISO 17799, για τη μέτρηση της απόδοσης της ασφάλειας πληροφοριών.

2.7 Μετρήσεις διαχείρισης ασφάλειας πληροφοριών.

Οι μετρήσεις (metrics) είναι ένας όρος που χρησιμοποιείται για να υποδηλώσει μέτρα που βασίζονται σε αναφορές και στηρίζονται σε τουλάχιστον 2 σημεία: την μέτρηση και την αναφορά.

Στην βασική της έννοια, η ασφάλεια, είναι η προστασία από τους κινδύνους ή την έλλειψή τους. Κυριολεκτώντας, οι μετρήσεις ασφαλείας πρέπει να υποδηλώνουν την κατάσταση ή τον βαθμό ασφαλείας σε σχέση με ένα σημείο αναφοράς. Οι σύγχρονές μετρήσεις ασφαλείας, σε γενικές γραμμές, αποτυγχάνουν να το κάνουν αυτό.

Πιθανόν να είναι χρήσιμο να διευκρινιστεί η διάκριση μεταξύ της διαχείρισης της ασφάλειας των μηχανημάτων του IT σε επιχειρησιακό επίπεδο και της συνολικής διαχείρισης ενός προγράμματος ασφάλειας πληροφοριών. Οι τεχνικές μετρήσεις προφανώς και είναι χρήσιμες για την τακτική επιχειρησιακή διαχείριση της τεχνικής υποδομής ασφαλείας (servers, βάσεις δεδομένων, firewalls, κτλ.) Μπορούν να δείχνουν ότι η υποδομή λειτουργεί με ορθό τρόπο και ότι οι τεχνικές αδυναμίες εντοπίζονται και αντιμετωπίζονται. Ωστόσο, αυτές οι μετρήσεις έχουν μικρή αξία από την στρατηγική σκοπιά της διαχείρισης. Δηλαδή, δεν λένε τίποτα για τη στρατηγική ευθυγράμμιση με τους στόχους του οργανισμού ή το πόσο καλά διαχειρίζονται οι κίνδυνοι, δεν παρέχουν καμία πληροφορία σχετικά με το εάν το πρόγραμμα της ασφάλειας πληροφοριών είναι προς τη σωστή κατεύθυνση και την επίτευξη των επιθυμητών αποτελεσμάτων.

Από την άποψη της διαχείρισης, ενώ έχουν υπάρξει βελτιώσεις στην τεχνική των μετρήσεων, δεν είναι σε θέση να δοθούν απαντήσεις σε ερωτήματα όπως:

- Πόσο ασφαλής είναι ο οργανισμός;
- Πώς ξέρουμε πότε έχουμε επιτύχει την επιθυμητή ασφάλεια;
- Ποιες είναι οι πιο αποδοτικές λύσεις;
- Πώς μπορούμε να καθορίσουμε το βαθμό κινδύνου;
- Πόσο καλά μπορούν να προβλεφθούν οι κίνδυνοι;
- Οδεύουμε προς τη σωστή κατεύθυνση;

- Τι αντίκτυπο έχει η έλλειψη ασφάλειας στην παραγωγικότητα;
- Τι αντίκτυπο θα έχει μια καταστροφική παραβίαση της ασφάλειας;
- Τι αντίκτυπο έχουν οι λύσεις ασφάλειας στην παραγωγικότητα;

2.7.1 Αποτελεσματικές Μετρήσεις Ασφαλείας

Είναι γενικά δύσκολο ή αδύνατο να διαχειριστεί οποιαδήποτε δραστηριότητα, η οποία δεν μπορεί να μετρηθεί. Ο θεμελιώδης σκοπός των μετρήσεων είναι η υποστήριξη στη λήψη αποφάσεων. Οι μετρήσεις για να είναι χρήσιμες, θα πρέπει οι πληροφορίες που παρέχουν να είναι σχετικές με τους ρόλους και τις ευθύνες του αποδέκτη, έτσι ώστε να μπορούν να ληφθούν αποφάσεις στηριγμένες στις πληροφορίες αυτές.

Τα πρότυπα μετρήσεων ασφαλείας περιλαμβάνουν παράγοντες όπως ο χρόνος διακοπής (downtime), ο αριθμός εισβολών στα συστήματα, τις επιπτώσεις και τις απώλειες, τους χρόνους αποκατάστασης των συστημάτων, τον αριθμό των τρωτών σημείων που βρέθηκαν μετά από σάρωση του δικτύου, το ποσοστό των διακομιστών που έγιναν διορθώσεις.

Ενώ τα μέτρα αυτά μπορούν να είναι ενδεικτικά των πτυχών της ασφάλειας, κανένα δεν παρέχει καμία πραγματική πληροφορία σχετικά με το πόσο ασφαλής είναι ο οργανισμός.

Ο λειτουργικός κίνδυνος δεν μπορεί εύκολα να μετρηθεί. Διάφορες προσεγγίσεις που μπορεί να είναι χρήσιμες περιλαμβάνουν το κόστος κινδύνου (Value at Risk - VAR), την απόδοση των επενδύσεων της ασφάλειας (return on security investment - ROSI) και το προσδόκιμο ετήσιας απώλειας (annual loss expectancy - ALE). Το VAR χρησιμοποιείται για τον υπολογισμό της μέγιστης πιθανής απώλειας σε μια ορισμένη χρονική περίοδο (ημέρα, εβδομάδα, έτος) με ποσοστό αξιοπιστίας 95% ή 99%. Το ROSI χρησιμοποιείται για τον υπολογισμό της απόδοσης της επένδυσης με βάση τη μείωση των απωλειών που προκύπτει από τον έλεγχο ασφαλείας. Η ALE παρέχει την πιθανή ετησιοποιημένη απώλεια, βασισμένη στην συχνότητα και το μέγεθος των συμβιβασμών για την ασφάλεια. Αυτοί, οι συχνά αριθμοί, μπορούν να χρησιμοποιηθούν ως βάση για την κατανομή και την αιτιολόγηση των πόρων για τις δραστηριότητες ασφαλείας.

Ορισμένες οργανώσεις προσπαθούν να καθορίσουν το μέγιστο δυνατό αντίκτυπο των πιθανών ανεπιθύμητων ενεργειών, ως μέτρο ασφαλείας. Η μέτρηση της ασφάλειας από τις συνέπειες και τις επιπτώσεις είναι παρόμοια με την εκτίμηση του ύψους ενός δέντρου από το θόρυβο που κάνει όταν πέφτει. Με άλλα λόγια, πρέπει να συμβούν οι ανεπιθύμητες ενέργειες για να διαπιστωθεί εάν η ασφάλεια λειτουργεί ενώ ταυτόχρονα η απουσία των ανεπιθύμητων ενεργειών δεν παρέχει πληροφορίες για την κατάσταση της ασφάλειας ενός οργανισμού. Φυσικά, η προσομοίωση επιθέσεων με δοκιμές εισβολής στα συστήματα μπορεί να παρέχει κάποια μέτρηση της αποτελεσματικότητας της άμυνας τους εναντίον αυτών των επιθέσεων. Ωστόσο, αν και μόνο ένα σχετικό ποσοστό όλων των πιθανών επιθέσεων που

πραγματοποιούναι, καμία πρόβλεψη δεν μπορεί να γίνει για την κατάσταση της ασφάλειας και την ικανότητα του οργανισμού να αντισταθεί στην επίθεση.

Το μόνο που μπορούμε να πούμε με βεβαιότητα για την ασφάλεια είναι ότι:

1. Ορισμένες επιχειρήσεις δέχονται πιο συχνά επιθέσεις και έχουν μεγαλύτερες απώλειες από τις υπόλοιπες και
2. Υπάρχει ισχυρή συσχέτιση μεταξύ καλής διαχείρισης και πρακτικών ασφαλείας, που αντιστοιχούν σε λιγότερα γεγονότα και ζημίες.

Η καλή διαχείριση είναι, αναμφισβήτητα, ένα από τα αποτελέσματα της καλής διοίκησης. Η μέτρηση της αποτελεσματικής διακυβέρνησης της ασφάλειας πληροφοριών και της διαχείρισης με ακρίβεια μπορεί να είναι πιο δύσκολη διαδικασία από τη μέτρηση της ίδιας της ασφάλειας. Οι μετρήσεις, στις περισσότερες εκτιμήσεις βασίζονται στο κόστος και στα αποτελέσματα ενός προγράμματος ασφαλείας.

Γενικότερα, καλά οργανωμένο πρόγραμμα για την ασφάλεια μπορεί να χαρακτηριστεί ένα πρόγραμμα το οποίο ανταποκρίνεται στις προσδοκίες και επιτυγχάνει συγκεκριμένους στόχους αποδοτικά, αποτελεσματικά και με συνέπεια. Αυτό είναι ωστόσο μεγάλη βοήθεια για τους περισσότερους οργανισμούς, δεδομένου ότι είναι ασαφές ποιες είναι οι προσδοκίες και οι στόχοι της ασφάλειας σε συγκεκριμένη έννοια.

Εμπορικές προσπάθειες για τη μέτρηση της σωστής διακυβέρνησης της ασφάλειας που έγιναν από οργανώσεις όπως η Institutional Shareholder Services (ISS) και η Governance Metrics International (EEE) δεν μπορούν να ελέγξουν ενδελεχώς σύμφωνα με πρόσφατη έκθεση του Yale με τίτλο “Good Governance and the Misleading Myths of Bad Metrics” (Sonnenfeld, Jeffrey; Associate Dean for Executive Programs at Yale, Academy of Management Executive, 2004, vol. 18, no. 1).

Επειδή η διακυβέρνηση και συγκεκριμένα η διακυβέρνηση ασφαλείας, είναι δύσκολο να καταμετρηθεί από ένα σύνολο αντικειμενικών μετρήσεων, υπάρχει η τάση για την χρησιμοποίηση μετρήσεων που είναι διαθέσιμες, ανεξάρτητα από τις συσχετίσεις που τις αποδεικνύουν. Ένα τυπικό παράδειγμα εμφανές σε πολλούς οργανισμούς είναι η σάρωση των τρωτών σημείων σαν ένδειξη της συνολικής ασφάλειας. Εύλογα, εάν ήταν δυνατόν να εξαλειφτούν όλα τα τρωτά σημεία, οι περισσότεροι κίνδυνοι θα είχαν αποφευχθεί. Η πλάνη είναι η υπόθεση ότι οι απειλές και οι κίνδυνοι μπορούν να καταμετρηθούν με τις τεχνικές αδυναμίες.

Ενώ δεν υπάρχει καθολική αντικειμενική κλίμακα ασφαλείας ή διακυβέρνησης ασφαλείας για τους οργανισμούς που έχουν αναπτύξει στόχους για την ασφάλεια πληροφοριών, για την ανάπτυξη και την διαχείριση ενός τέτοιου προγράμματος μπορούν να σχεδιαστούν και να υλοποιηθούν μετρήσεις. Πρέπει επίσης να γίνει κατανοητό ότι διαφορετικές μετρήσεις χρειάζονται για την παροχή πληροφοριών σε στρατηγικό ή λειτουργικό επίπεδο. Οι

μετρήσεις στρατηγικού επιπέδου θα είναι προσανατολισμένες προς υψηλού επιπέδου στόχους του προγράμματος της ασφάλειας πληροφοριών.

2.7.2 Διακυβέρνηση υλοποίησης μετρήσεων.

Η υλοποίηση της διακυβέρνηση της ασφάλειας πληροφοριών και η δομή της απαιτούν σημαντικό φόρτο. Οι δείκτες Key Goal Indicators (KGIs) και Key Performance Indicators (KPIs) μπορεί να είναι πολύ χρήσιμοι στην επίτευξη των διαδικασιών και στους στόχους των υπηρεσιών, ενώ παράλληλα καθορίζουν εάν τα βήματα του οργανισμού και οι στόχοι του υλοποιούνται.

2.7.3 Στρατηγική Ευθυγράμμιση (Strategic alignment)

Η στρατηγική ευθυγράμμιση της ασφάλειας πληροφοριών για την υποστήριξη των στόχων μιας επιχείρησης - οργανισμού είναι ένας ιδιαίτερα επιθυμητός στόχος, όμως είναι συχνά δύσκολο να επιτευχθεί. Πρέπει να διευκρινισθεί ότι ακόμη και η οικονομική αποτελεσματικότητα του προγράμματος για την ασφάλεια είναι αναπόφευκτα συνδεδεμένη με το πόσο καλά θα υποστηρίζει τους στόχους της οργάνωσης και με ποιο κόστος. Χωρίς στόχους ως σημείο αναφοράς κάθε άλλος δείκτης μέτρησης μπορεί να είναι υπερβολικός, ανεπαρκής ή σε λανθασμένη κατεύθυνση. Από την πλευρά της επιχείρησης, κατάλληλες και επαρκείς πρακτικές, ανάλογες με τις απαιτήσεις, είναι πιθανό να είναι περισσότερο δαπανηρές και από τις βέλτιστες πρακτικές.

Ο καλύτερος συνολικά δείκτης, ότι οι δραστηριότητες ασφάλειας είναι σε ευθυγράμμιση με τους επιχειρησιακούς στόχους, είναι η ανάπτυξη μιας στρατηγικής ασφάλειας που να καθορίζει τους στόχους της ασφάλειας, όσον αφορά τις επιχειρήσεις, και να εξασφαλίζει ότι οι στόχοι είναι άμεσα ξεκάθαροι από το σχεδιασμό έως την υλοποίηση των πολιτικών, των προτύπων, των διαδικασιών και της εκάστοτε τεχνολογίας. Οι δοκιμές, είναι η αντίστροφη διαδικασία αξιολόγησης ενός συγκεκριμένου ελέγχου που καθοδηγείται από συγκεκριμένες απαιτήσεις των επιχειρήσεων. Κάθε έλεγχος ο οποίος δεν μπορεί να επαληθεύσει άμεσα τις απαιτήσεις των επιχειρήσεων είναι ύποπτος και θα πρέπει να αναλυθεί για πιθανή διακοπή.

Οι δείκτες της ευθυγράμμισης μπορεί να περιλαμβάνουν:

- Ένα πρόγραμμα ασφαλείας που ενεργοποιεί αποδεδειγμένα συγκεκριμένες επιχειρηματικές δραστηριότητες.
- Έναν οργανισμό ασφαλείας που να ανταποκρίνεται στις προκαθορισμένες απαιτήσεις των επιχειρήσεων.

- Επιχειρησιακούς στόχους και στόχους ασφαλείας καθορισμένους και πλήρως κατανοητούς από όλους τους εμπλεκομένους στην ασφάλεια και τις σχετικές διαδικασίες διασφάλισης.
- Προγράμματα ασφαλείας σε απόλυτη αντιστοίχιση με τους στόχους των επιχειρήσεων και επικυρωμένα από την ανώτερη διοίκηση.
- Συντονιστική επιτροπή ασφαλείας που να αποτελείται από στελέχη με σκοπό την διασφάλιση της ευθυγράμμισης των δραστηριοτήτων της ασφάλειας και της επιχειρηματικής στρατηγικής.

2.7.4 Διαχείριση Επικινδυνότητας (Risk Management)

Η Διαχείριση Επικινδυνότητας είναι το απόλυτο εργαλείο όλων των δραστηριοτήτων της ασφάλειας πληροφοριών και όλων των προσπαθειών διασφάλισης του εκάστοτε οργανισμού. Ενώ η αποτελεσματικότητα της Διαχείριση Επικινδυνότητας δεν υπόκειται σε άμεση μέτρηση, υπάρχουν δείκτες που συσχετίζονται με μια επιτυχή προσέγγιση. Ένα επιτυχημένο πρόγραμμα Διαχείρισης Επικινδυνότητας μπορεί να οριστεί ως ένα πρόγραμμα που ανταποκρίνεται στις προσδοκίες και επιτυγχάνει συγκεκριμένους στόχους του οργανισμού αποδοτικά, αποτελεσματικά και με συνέπεια.

Για άλλη μια φορά, είναι απαίτηση και της Διαχείρισης Επικινδυνότητας ότι οι προσδοκίες και οι στόχοι της διαχείρισης πρέπει να είναι ορισμένες ευκρινώς, διαφορετικά δεν υπάρχει καμία βάση που να καθορίζει εάν το πρόγραμμα είναι επιτυχημένο ή / και κινείται προς τη σωστή κατεύθυνση και αν η κατανομή των πόρων είναι κατάλληλη.

Οι δείκτες της κατάλληλης διαχείρισης επικινδυνότητας περιλαμβάνουν:

- Μια καθορισμένη οργανωτική διάθεση ανάληψης κινδύνου ή ανοχή του κινδύνου.
- Ανάληψη ευθυνών και ανοχή κινδύνων σύμφωνα με τους όρους του οργανισμού.
- Μια συνολική στρατηγική για την ασφάλεια και πρόγραμμα για την επίτευξη αποδεκτών επιπέδων κινδύνου.
- Μείωση των αναγνωρισμένων σοβαρών κινδύνων.
- Διαδικασίες για διαχείριση και μείωση των αρνητικών επιπτώσεων.
- Συστηματικές, συνεχείς διαδικασίες διαχείρισης κινδύνων.
- Περιοδική αξιολόγηση επικινδυνότητας που υποδεικνύει την πρόοδο προς την κατεύθυνση των καθορισμένων στόχων.
- Δοκιμασμένο πλάνο επιχειρησιακής συνέχειας / σχέδιο ανάκαμψης από καταστροφή.
- Σωστή αποτίμηση του κεφαλαίου.
- Business Impact Assessments (BIAs) όλων των κρίσιμων ή ευαίσθητων συστημάτων.

Ο κύριος στόχος της ασφάλειας πληροφοριών είναι η μείωση των αρνητικών επιπτώσεων για τον οργανισμό σε αποδεκτά επίπεδα. Ως εκ τούτου, μία βασική μέτρηση είναι οι αρνητικές επιπτώσεις των περιστατικών ασφάλειας των πληροφοριών σε ένα οργανισμό. Ένα αποτελεσματικό πρόγραμμα ασφάλειας θα δείξει μια τάση όσον αφορά τη μείωση των επιπτώσεων. Τα ποσοτικά μέτρα μπορούν να περιλαμβάνουν την ανάλυση των τάσεων των επιπτώσεων κατά την πάροδο του χρόνου.

2.7.5 Παροχή αξίας (Value delivery)

Value Delivery υπάρχει όταν οι επενδύσεις στην ασφάλεια βελτιστοποιούνται για την υποστήριξη των στόχων της επιχείρησης. Αποτελεί συνάρτηση της στρατηγικής ευθυγράμμισης της στρατηγικής ασφάλειας και των επιχειρηματικών στόχων. Τα βέλτιστα επίπεδα επενδύσεων παρουσιάζονται όταν οι στρατηγικοί στόχοι για την ασφάλεια επιτυγχάνονται με αποδεκτά επίπεδα κίνδυνου και το χαμηλότερο δυνατό κόστος.

Οι δείκτες KGIs και KPIs περιλαμβάνουν:

- Δραστηριότητες ασφαλείας που έχουν σχεδιαστεί για την επίτευξη συγκεκριμένων στρατηγικών στόχων.
- Το κόστος της ασφάλειας (ανάλογο με την αξία των περιουσιακών στοιχείων).
- Ασφάλεια πόρων που θα διατεθούν ανάλογα με το βαθμό του κινδύνου και πιθανές επιπτώσεις.
- Το κόστος προστασίας συνολικά σε συνάρτηση με τα έσοδα ή τα περιουσιακά στοιχεία.
- Έλεγχοι, καλά σχεδιασμένοι με βάση προκαθορισμένους ελέγχους και πλήρως αξιοποιήσιμους.
- Έναν επαρκή και κατάλληλο αριθμός ελέγχων για την επίτευξη αποδεκτών επίπεδων κινδύνων και επιπτώσεων.
- Έλεγχος της αποτελεσματικότητας μέσα από περιοδικούς ελέγχους.
- Πολιτικές που απαιτούν όλοι οι έλεγχοι να υπόκεινται σε περιοδική επαναξιολόγηση κόστους, συμμόρφωσης και αποτελεσματικότητας.
- Η αξιοποίηση των ελέγχων. Έλεγχοι που χρησιμοποιούνται σπάνια δεν είναι οικονομικά αποδοτικοί.
- Ο αριθμός των ελέγχων για την επίτευξη αποδεκτών επίπεδων κινδύνου και επιπτώσεων. Ένας μικρός αριθμός αποτελεσματικών έλεγχων αναμένεται να είναι περισσότερο δαπανηρος από ότι ένας μεγαλύτερος αριθμός λιγότερο αποτελεσματικών ελέγχων.
- Η αποτελεσματικότητα των ελέγχων, όπως καθορίζεται από τις δοκιμές.

2.7.6 Διαχείριση Πόρων (Resource Management)

Η διαχείριση των πόρων της ασφάλειας πληροφοριών αποτελεί τον όρο που χρησιμοποιείται για να περιγράψει τις διαδικασίες για το σχεδιασμό, την κατανομή και τον έλεγχο των πόρων της ασφάλειας πληροφοριών, συμπεριλαμβανομένων των ανθρώπων, των διαδικασιών και των τεχνολογικών επιλογών για τη βελτίωση της αποδοτικότητας και της αποτελεσματικότητας των επιχειρηματικών λύσεων.

Όπως και με τα άλλα στοιχεία του ενεργητικού και των πόρων του οργανισμού, πρέπει και αυτό να διαχειρίζεται σωστά. Η γνώση λοιπόν πρέπει να αποκτάται, να διαδίδεται και να είναι διαθέσιμη όταν ο οργανισμός την χρειαστεί. Παρέχοντας πολλαπλές λύσεις στο ίδιο πρόβλημα είναι, προφανώς, αναποτελεσματικό και υποδεικνύει έλλειψη διαχείρισης πόρων. Επιπλέον, οι έλεγχοι και οι διαδικασίες πρέπει να είναι τυποποιημένες, όσο αυτό είναι δυνατόν, έτσι ώστε να μειώνουν τις διαχειριστικές δαπάνες και τα κόστη των εκπαιδεύσεων. Τα εκάστοτε προβλήματα που πιθανόν να προκύψουν και οι λύσεις τους πρέπει να είναι καλά καταγεγραμμένα, αρχειοθετημένα και άμεσα διαθέσιμα όταν αυτό χρειαστεί.

Οι δείκτες της αποτελεσματικής διαχείρισης των πόρων περιλαμβάνουν:

- Αποτελεσματική διαχείριση της γνώσης και μετάδοσης αυτής.
- Τυποποιημένες διαδικασίες.
- Ξεκάθαρα καθορισμένους ρόλους και αρμοδιότητες για τις λειτουργίες της ασφάλειας πληροφοριών.
- Λειτουργίες της ασφάλειας πληροφοριών.
- Πληροφορίες των περιουσιακών στοιχείων και τις σχετικές απειλές αυτών, οι οποίες καλύπτονται από την ασφάλεια.
- Την κατάλληλη τοποθεσία του οργανισμού, τα επίπεδα εξουσίας και τον αριθμό του προσωπικού για τη λειτουργία της ασφάλειας πληροφοριών.

2.7.7 Μέτρηση απόδοσης (Performance Measurement)

Η μέτρηση, η παρακολούθηση και η υποβολή εκθέσεων σχετικά με τις διαδικασίες της ασφάλειας πληροφοριών είναι απαραίτητες για να εξασφαλιστεί η επίτευξη των οργανωτικών στόχων. Είναι αρκετά σαφές ότι "δεν μπορείτε να διαχειριστείτε ό,τι δεν μπορείτε να μετρήσετε."

Πρέπει να αναπτυχθούν μέθοδοι παρακολούθησης των δραστηριοτήτων που σχετίζονται με την ασφάλεια σε όλα τα επίπεδα του οργανισμού. Είναι πολύ σημαντικός ο σχεδιασμός μετρήσεων που να παρέχουν ενδείξεις των επιδόσεων των μηχανισμών ασφάλειας και από την οπτική της διαχείρισης, οι πληροφορίες που απαιτούνται για τις αποφάσεις για τον συντονισμό των δραστηριοτήτων ασφαλείας του οργανισμού. Όταν το κατάλληλο πλαίσιο

ασφάλειας δεν έχει ακόμη υλοποιηθεί, τα περισσότερα μέτρα είναι έμμεσοι δείκτες της κατάστασης της ασφάλειας και της απόδοσης του προγράμματος ασφαλείας.

Οι δείκτες αποτελεσματικής μέτρησης της απόδοσης περιλαμβάνουν:

- Τον χρόνος που χρειάζεται για τον εντοπισμό και την αναφορά περιστατικών σχετικά με την ασφάλεια
- Τον αριθμός και την συχνότητα των μετέπειτα περιστατικών που δεν αναφέρθηκαν.
- Την συγκριτική αξιολόγηση του κόστους και της αποτελεσματικότητας ανάλογων επιχειρήσεων.
- την ικανότητα προσδιορισμού αποτελεσματικότητας / αποδοτικότητας των ελέγχων.
- Σαφείς ενδείξεις ότι είναι στόχοι ασφάλειας επιτυγχάνονται.
- Την απουσία απρόσμενων γεγονότων ασφάλειας.
- Την γνώση των επικείμενων απειλών.
- Μεθόδους παρακολούθησης εξελισσόμενων κινδύνων.
- Συνάφεια των πρακτικών ελέγχου των logs.
- Τα αποτελέσματα του σχεδιασμού επιχειρηματικής συνέχειας (business continuity planning BCP) / δοκιμές αποκατάστασης μετά από καταστροφή (disaster recovery DR)

2.7.8 Διασφάλιση, Ολοκλήρωση Διεργασιών - Σύγκλιση (Convergence)

Όπως αναφέρθηκε νωρίτερα, μια αναδυόμενη περιοχή ενδιαφέροντος, που σχετίζεται με τα αποτελέσματα της διακυβέρνησης της ασφάλειας πληροφοριών, είναι η διασφάλιση επιχειρησιακών διαδικασιών ή διασφάλιση ολοκλήρωσης.

Για οργανισμούς που εξετάζουν το ενδεχόμενο μιας προσέγγισης για τη διακυβέρνηση της ασφαλείας πληροφοριών που να περιλαμβάνει προσπάθεια ολοκλήρωσης μιας πλειάδας μηχανισμών ασφαλείας και διασφαλίζει ότι οι διαδικασίες λειτουργούν σε όλα τα επίπεδα του οργανισμού, ελαχιστοποιώντας τους κινδύνους μπορούν να περιλαμβάνουν:

- Την προστασία των πληροφοριών των περιουσιακών στοιχείων χωρίς κενά.
- Την εξάλειψη των περιττών επικαλύψεων σε θέματα ασφαλείας
- Την ομαλή ενσωμάτωση των δραστηριοτήτων διασφάλισης.
- Καλά-καθορισμένους ρόλους και αρμοδιότητες.
- Όλες τις λειτουργίες διασφάλισης αναγνωρίζονται και είναι μέρος της στρατηγικής.

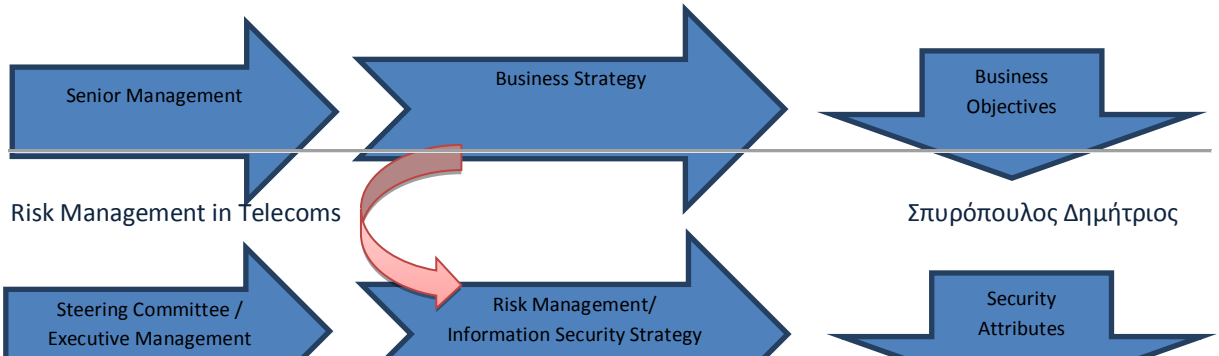
2.8 Επισκόπηση Ασφάλειας Πληροφοριών

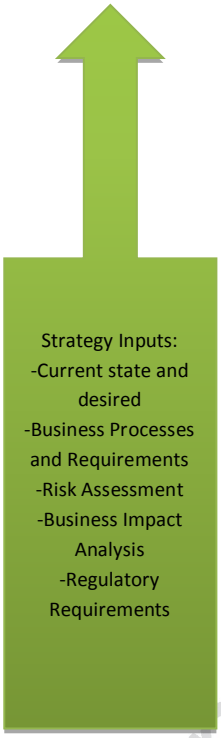
Υπάρχουν πολλοί ορισμοί της στρατηγικής. Ενώ όλοι σε γενικές γραμμές κινούνται προς την ίδια κατεύθυνση, διαφέρουν σε μεγάλο βαθμό στο πεδίο εφαρμογής, την έμφαση και τη λεπτομέρεια. Στο *"The Concept of Corporate Strategy"* , 2η Έκδοση, ο Kenneth Andrews περιγράφει την εταιρική στρατηγική, η οποία ισχύει εξίσου για την ανάπτυξη και τους σκοπούς της στρατηγικής για την ασφάλεια πληροφοριών:

Η Εταιρική στρατηγική είναι το υπόδειγμα των αποφάσεων σε μια εταιρεία το οποίο καθορίζει και αναδεικνύει το αντικείμενο αυτής, τους σκοπούς ή τους στόχους της, παράγει τις κυριότερες πολιτικές και τα σχέδια για την επίτευξη των στόχων αυτών και ορίζει το εύρος των επιχειρηματικών δραστηριοτήτων της εταιρείας, το είδος της οικονομικής οργάνωσης, το ανθρώπινο δυναμικό και τη φύση της οικονομικής και μη οικονομικής συνεισφοράς που προτίθεται να κάνει προς τους μετόχους, τους εργαζόμενους, τους πελάτες και τις αγορές.

Το ακόλουθο ***σχήμα 2.2*** αποτυπώνει τους συμμετέχοντες στην ανάπτυξη στρατηγικής για την ασφάλεια, τις σχέσεις τους και την ευθυγράμμιση τους με τους επιχειρηματικούς στόχους. Το βέλος με την ένδειξη "Στρατηγική των Επιχειρήσεων" παρέχει έναν οδηγό για την επίτευξη των στόχων των επιχειρήσεων. Επιπλέον, παρέχει έναν από τους κύριους συντελεστές στα πλάνα της "Διαχείρισης Επικινδυνότητας" και της "Στρατηγικής της Ασφάλειας Πληροφοριών." Το παρακάτω σχεδιάγραμμα συμβάλλει στην ευθυγράμμιση της ασφάλειας πληροφοριών με τους επιχειρηματικούς στόχους. Η ισορροπία μεταξύ των συντελεστών προέρχεται από τον προσδιορισμό της επιθυμητής κατάστασης της ασφάλειας σε σύγκριση με την υπάρχουσα, την τρέχουσα, κατάσταση. Οι Επιχειρηματικές διαδικασίες πρέπει επίσης να αποτελούν αποτελέσματα της αξιολόγησης κινδύνων και η ανάλυση των επιπτώσεων να προσδιορίζει τα επίπεδα προστασίας και τις προτεραιότητες. Τέλος, οι ρυθμιστικές απαιτήσεις θα πρέπει επίσης να ληφθούν υπόψη στη διαμόρφωση της στρατηγικής ασφάλειας.

Σχήμα 2.2 — Οι συμμετέχοντες στην ανάπτυξη στρατηγικής για την ασφάλεια πληροφοριών.





Ο σκοπός της στρατηγικής ασφαλείας είναι η επιθυμητή κατάσταση που ορίζεται από τα χαρακτηριστικά της επιχείρησης και της ασφαλείας. Η στρατηγική αποτελεί τη βάση για ένα σχέδιο δράσης που αποτελείται από ένα ή περισσότερα προγράμματα ασφαλείας το οποίο καθώς υλοποιείται, επιτυγχάνει τους στόχους της ασφάλειας.

Η στρατηγική και τα πλάνα δράσης πρέπει να περιέχουν διατάξεις για την παρακολούθηση, ως μέτρηση για τον προσδιορισμό του επιπέδου της επιτυχίας. Αυτό παρέχει υλικό ανατροφοδότησης για τον CISO και την οργανωτική επιτροπή να καταστεί δυνατή η διόρθωση midcourse και η διασφάλιση ότι οι πρωτοβουλίες της ασφάλειας είναι σε καλό δρόμο για την επίτευξη καθορισμένων στόχων.

2.9 Αντικείμενο Στρατηγικής της Ασφάλειας Πληροφοριών

Οι στόχοι για την ανάπτυξη μιας στρατηγικής για την ασφάλεια των πληροφοριών πρέπει να καθορίζονται και να αναπτυχθούν μετρήσεις για να καθορίσουν εάν οι εν λόγω στόχοι επιτυγχάνονται.

Συνήθως, υψηλού επιπέδου καθοδήγηση παρέχουν έξι αποτελέσματα της διακυβέρνησης ασφάλειας:

- Στρατηγική ευθυγράμμιση.
- Αποτελεσματική διαχείριση επικινδυνότητας.
- Value Delivery.
- Διαχείριση πόρων.
- Μέτρηση των επιδόσεων.
- ολοκλήρωση της διαδικασίας ασφαλείας.

Η στρατηγική πρέπει να εξετάσει τι σημαίνει στην επιχείρηση κάθε μία από τις επιλεγμένες περιοχές και πώς μπορεί να επιτευχθούν επιτυχώς.

Επιπλέον, δεν είναι δυνατό να αναπτυχθεί μια αποδοτική και αποτελεσματική στρατηγική για την ασφάλεια που θα είναι ευθυγραμμισμένη με τις απαιτήσεις των επιχειρήσεων πριν από:

- Καθορισμό των στόχων της ασφάλειας των πληροφοριών
- Εντοπισμό και αναγνώριση περιουσιακών στοιχείων και πόρων.
- Αποτίμηση των περιουσιακών στοιχείων και των πόρων
- Ταξινόμηση περιουσιακών στοιχείων ως προς την κρισιμότητας και την ευαισθησία.

2.9.1 Η επιθυμητή κατάσταση

Ο όρος "επιθυμητή κατάσταση" χρησιμοποιείται για να υποδηλώσει μια πλήρη εικόνα όλων των σχετικών συνθηκών σε ένα συγκεκριμένο σημείο στο μέλλον. Για να ολοκληρωθεί αυτή η εικόνα, θα πρέπει να συμπεριληφθούν οι άνθρωποι, οι διαδικασίες και οι τεχνολογίες.

Ο ορισμός μιας «κατάστασης ασφάλειας» με καθαρά ποσοτική άποψη, δεν είναι εφικτός. Κατά συνέπεια, η "επιθυμητή κατάσταση της ασφάλειας" πρέπει να οριστεί με βάση τα ποιοτικά χαρακτηριστικά και τα αποτελέσματα. Σύμφωνα με το COBIT, μπορεί να περιλαμβάνει υψηλού επιπέδου στόχους, όπως: "Η προστασία των συμφερόντων εκείνων που στηρίζονται σε πληροφορίες και διαδικασίες, τα συστήματα και οι επικοινωνίες που διαχειρίζονται, αποθηκεύουν και μεταφέρουν τις πληροφορίες, τη ζημιά που προκύπτει από τις αποτυχίες της διαθεσιμότητας, της εμπιστευτικότητας και της ακεραιότητας." Αυτή η δήλωση, ενώ είναι χρήσιμη για την έκφραση των προθέσεων και των σκοπών, προβλέπει ελάχιστη σαφήνεια στον καθορισμό των διαδικασιών ή των στόχων.

Τα ποιοτικά στοιχεία, όπως είναι τα επιθυμητά αποτελέσματα, θα πρέπει να ορίζονται όσο το δυνατόν ακριβέστερα για την παροχή καθοδήγησης για την ανάπτυξη της στρατηγικής. Για παράδειγμα, εάν μια συγκεκριμένη κανονιστική συμμόρφωση αποτελεί ένα επιθυμητό αποτέλεσμα, είναι εμφανής ένας σημαντικός αριθμός τεχνικών και διαδικαστικών απαιτήσεων.

Μια σειρά από χρήσιμες προσεγγίσεις είναι διαθέσιμες για να παρέχουν ένα πλαίσιο για να επιτευχθεί μια καλά καθορισμένη "επιθυμητή κατάσταση" για την ασφάλεια. Αυτά, και ίσως και άλλα, πρέπει να αξιολογηθούν ώστε να καθορισθεί ποια παρέχουν την καλύτερη μορφή, εφαρμογή και λειτουργία της επιχείρησης. Μπορεί να είναι χρήσιμο να συνδυαστούν πολλά διαφορετικά πρότυπα και πλαίσια για την παροχή μια πολυδιάστατη άποψη στην επιθυμητή κατάσταση. Βλέπε ακόλουθο σχήμα 2.3:

Σχήμα 2.3: Επικρατέστερα Πρότυπα και Πλαίσια

Αρκετές από τις πιο αποδεκτές μεθόδους περιγράφονται παρακάτω.

COBIT

Η μέθοδος “Control Objectives for Information and related Technology – COBIT” επικεντρώνεται στις σχετικές IT διαδικασίες της διακυβέρνησης του IT, της διαχείρισης και του ελέγχου. Η COBIT αποτελεί ένα πλαίσιο διακυβέρνησης του IT και ένα σύνολο εργαλείων υποστήριξης που επιτρέπει στους διαχειριστές να γεφυρώσουν το χάσμα μεταξύ των απαιτήσεων ελέγχου, τεχνικών θεμάτων και επιχειρηματικών κινδύνων. Η COBIT επιτρέπει σαφή χάραξη πολιτικής και καλών πρακτικών για τον έλεγχο του IT σε ολόκληρο τον οργανισμό. Η COBIT θα πρέπει να θεωρείται ένα ισχυρό, καλά αναπτυγμένο πλαίσιο που μπορεί να προσφέρει σημαντικό όφελος για την αντιμετώπιση των στόχων της ασφάλειας πληροφοριών.

Οι «Έλεγχοι» ορίζονται ως «οι πολιτικές, οι διαδικασίες, οι πρακτικές και οι οργανωτικές δομές που σχεδιάστηκαν για να παρέχουν την απαραίτητη διαβεβαίωση ότι οι στόχοι των επιχειρήσεων θα επιτευχθούν και ότι οι ανεπιθύμητες ενέργειες θα προληφθούν ή θα εντοπιστούν.»

Οι «Στόχοι των ελέγχων» ορίζονται ως «η δήλωση του επιθυμητού αποτελέσματος ή του σκοπού που πρέπει να επιτευχθεί με την εφαρμογή διαδικασιών ελέγχου σε μια συγκεκριμένη διαδικασία."

Η COBIT καθορίζει την επιχειρηματική διακυβέρνηση ως «ένα σύνολο αρμοδιοτήτων και πρακτικών που ασκείται από το διοικητικό συμβούλιο και τα στελέχη διαχείρισης με στόχο την παροχή στρατηγικής κατεύθυνσης, εξασφαλίζοντας ότι οι στόχοι επιτυγχάνονται, διασφαλίζοντας ότι οι κίνδυνοι διαχειρίζονται σωστά και οι πόροι της επιχείρησης χρησιμοποιούνται υπεύθυνα».

Το πλαίσιο COBIT καθορίζει 34 διαδικασίες για τη διαχείριση και τον έλεγχο των πληροφοριών και τις τεχνολογίες που υποστηρίζει. Οι διαδικασίες χωρίζονται σε τέσσερις τομείς:

- Σχεδιασμός και Οργάνωση - Ο τομέας αυτός καλύπτει τη στρατηγική και τις τακτικές και αφορά τον προσδιορισμό του τρόπου με τον οποίο το IT μπορεί καλύτερα να συμβάλει στην επίτευξη των επιχειρηματικών στόχων. Επιπλέον, η υλοποίηση του στρατηγικού οράματος πρέπει να σχεδιαστεί, να κοινοποιηθεί και να διαχειριστεί από διαφορετικές οπτικές γωνίες. Τέλος, πρέπει να τεθεί σε εφαρμογή η σωστή οργάνωση καθώς και η τεχνολογική υποδομή.
- Απόκτηση και Εφαρμογή - Για την υλοποίηση της στρατηγικής IT, οι IT λύσεις πρέπει να προσδιοριστούν, να αναπτυχθούν ή να αποκτηθούν, καθώς και να εφαρμοστούν και να ενσωματωθούν στις επιχειρηματικές διαδικασίες. Επιπλέον, οι

αλλαγές και η συντήρηση των υπαρχόντων συστημάτων που καλύπτονται από αυτό το πεδίο να διασφαλίζουν ότι ο κύκλος της ζωής συνεχίζεται στα συστήματα αυτά.

- Παράδοση και Υποστήριξη - Αυτός ο τομέας ασχολείται με την πραγματική παράδοση των απαιτούμενων υπηρεσιών, οι οποίες κυμαίνονται από τις παραδοσιακές εργασίες για την ασφάλεια και τις πτυχές επιχειρησιακής συνέχισης μέχρι την κατάρτιση. Για την παροχή υπηρεσιών πρέπει να συσταθούν οι αναγκαίες διαδικασίες στήριξης. Αυτός ο τομέας περιλαμβάνει την πραγματική επεξεργασία των δεδομένων από τα συστήματα εφαρμογής που συχνά κατατάσσονται κάτω από τους ελέγχους εφαρμογών.
- Η Παρακολούθηση και Αξιολόγηση - Όλες οι διαδικασίες πληροφορικής πρέπει να αξιολογούνται τακτικά στην πάροδο του χρόνου για την ποιότητα και τη συμμόρφωσή τους με τις απαιτήσεις του ελέγχου. Έτσι, ο τομέας αυτός ασχολείται με την παρακολούθηση της διαχείρισης και την αξιολόγηση των απόδοσης του IT και την ενίσχυση των ελέγχων, διασφαλίζοντας την κανονιστική συμμόρφωση και την παροχής εποπτεία της διακυβέρνησης του IT.

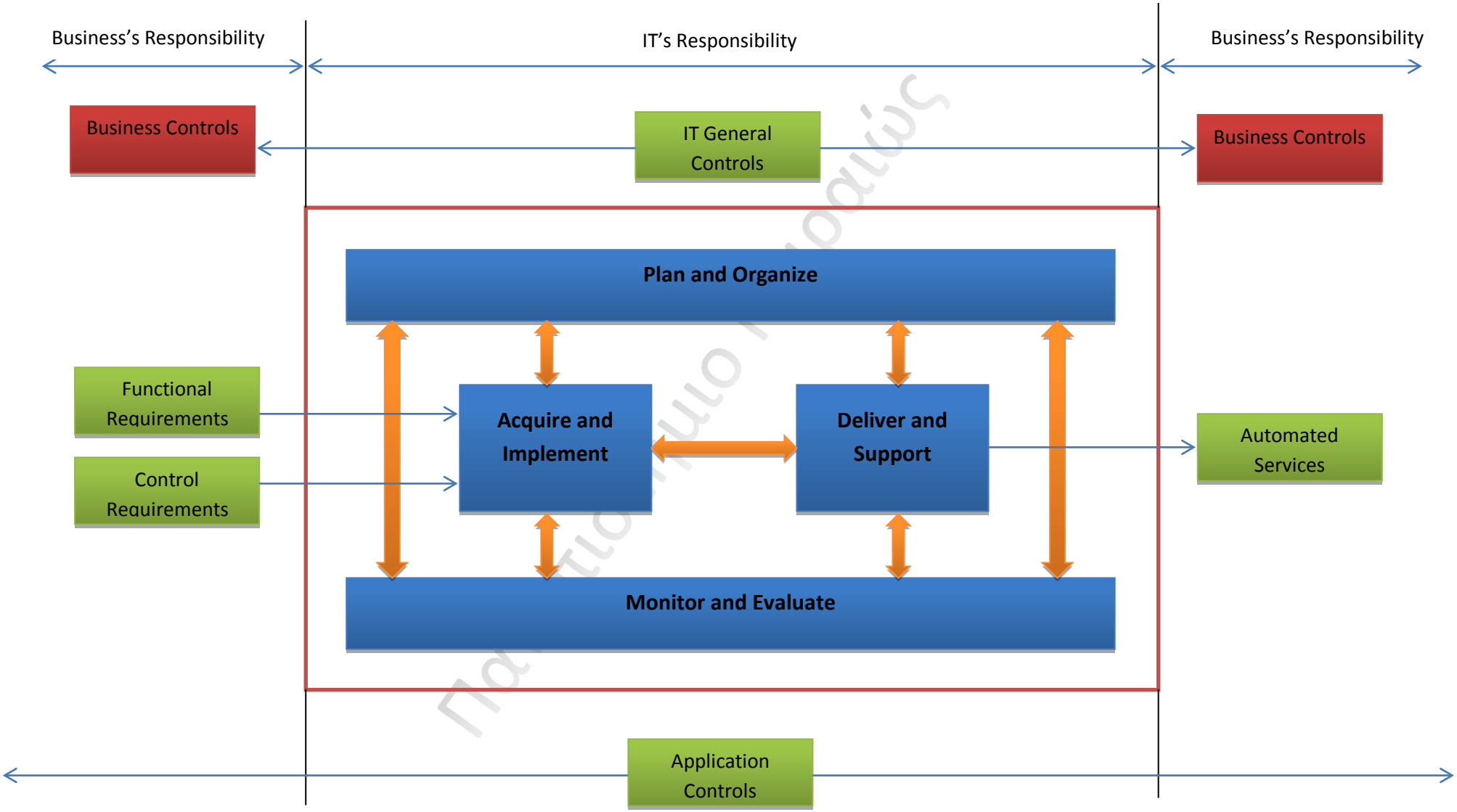
Το σχήμα 2.4 έχει μια γραφική παρουσίαση των ελέγχων και των συστατικών της διακυβέρνησης της ασφάλειας.

Capacity Maturity Model

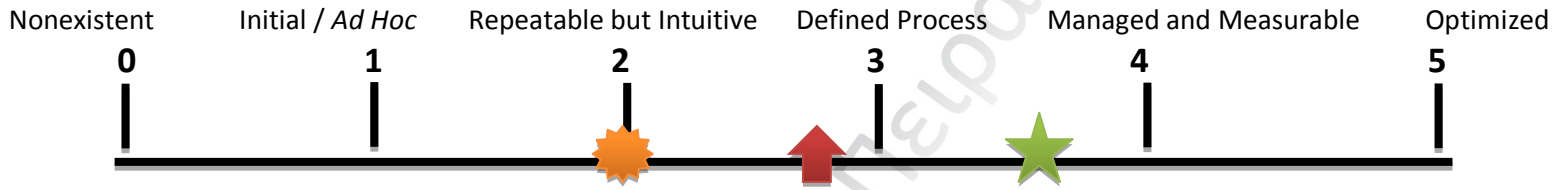
Η επιθυμητή κατάσταση ασφάλειας μπορεί επίσης να οριστεί ως επίτευξη ενός συγκεκριμένου επιπέδου στο Capacity Maturity Model (CMM), όπως παρουσιάζεται στο σχήμα 2.5. Αποτελείται από την ταξινόμηση σε κάθε τομέα ασφάλειας σε μια κλίμακα από το 0 έως το 5, με βάση την ωριμότητα των διαδικασιών. Τα επίπεδα ωριμότητας περιγράφονται ως:

- 0: Ανύπαρκτο – Δεν εντοπίζεται από την επιχείρηση η ανάγκη για ασφάλεια
- 1: Ad hoc – Οι κίνδυνοι λαμβάνονται υπόψη σε ad hoc βάση, χωρίς τυπικές διαδικασίες.
- 2: Επαναλαμβανόμενο αλλά διαισθητικά - Επείγουσα κατάσταση κινδύνου και ανάγκη για ασφάλεια
- 3: Καθορισμένων διαδικασιών - πολιτική διαχείρισης κινδύνων / ενημέρωση για θέματα ασφάλειας σε όλο τον οργανισμό.
- 4: Διαχειρίσιμο και μετρήσιμο - Διαδικασία αξιολόγησης Κινδύνου, ρόλοι και αρμοδιότητες, πολιτικές και πρότυπα.
- 5: Βελτιωμένο - Διαδικασίες εφαρμογής, παρακολούθησης και διαχείρισης σε όλα τα επίπεδα του οργανισμού.

Σχήμα 2.4: COBIT



Σχήμα 2.5: Capability Maturity Model



LEGEND FOR SYMBOLS USED

Enterprise current status

Industry average

Enterprise target

LEGEND FOR RANKINGS USED

0 – Management processes are not applied at all.

1 - Processes are ad - hoc and disorganized.

2 - Processes follow a regular pattern.

3 - Processes are documented and communicated.

4 -Processes are monitored and measured.

5 - Good practices are followed and automated.

Balanced Scorecard

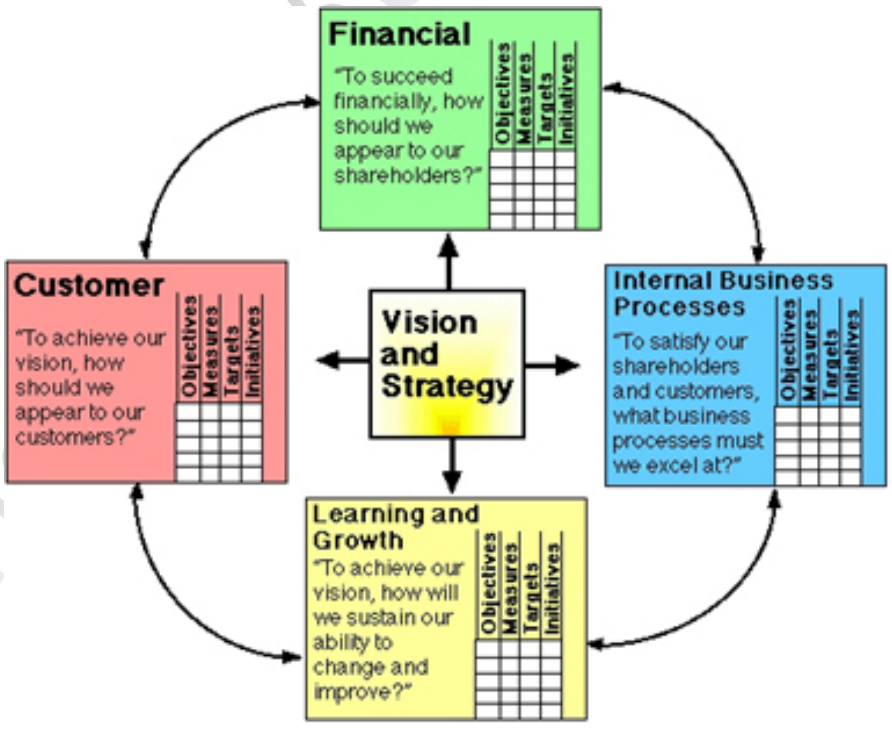
Σύμφωνα με την balance scorecard:

> *Η balance scorecard είναι ένα σύστημα διαχείρισης (όχι μόνο ένα σύστημα μέτρησης) που επιτρέπει στους οργανισμούς να αποσαφηνίσουν το όραμα και τη στρατηγική τους και να το μετατρέψουν σε δράση. Παρέχει ανατροφοδότηση γύρω από τις εσωτερικές επιχειρηματικές διαδικασίες και τα εξωτερικά αποτελέσματα ώστε να βελτιώνεται συνεχώς τα αποτελέσματα και η στρατηγική απόδοση. Όταν αναπτυχθεί πλήρως, το Balanced Scorecard μεταμορφώνει τον στρατηγικό σχεδιασμό από μια ακαδημαϊκή άσκηση σε νευραλγικό κέντρο της επιχείρησης.*

Το Balanced Scorecard, όπως φαίνεται στο σχήμα 2.6, χρησιμοποιεί τέσσερις οπτικές γωνίες, αναπτύσσει τις μετρήσεις, συλλέγει και αναλύει τα δεδομένα σε σχέση με κάθε μία από αυτές τις προοπτικές:

- Εκπαίδευση και ανάπτυξη.
- Επιχειρησιακές διαδικασίες.
- Πελάτες
- Χρηματοοικονομικά

Σχήμα 2.6: Balanced Scorecard



SABSA

Σύμφωνα με το SABSA (Sherwood Applied Business Security Architecture):

Το κλειδί για την επιτυχία της μεθοδολογίας SABSA ® είναι να είναι καθοδηγούμενη και εστιασμένη στις επιχειρήσεις. Η επιχειρηματική στρατηγική, οι στόχοι, οι σχέσεις, οι κίνδυνοι, οι περιορισμοί και οι προϋποθέσεις μπορούν να μας πουν πολλά για το τι είδος αρχιτεκτονική ασφάλειας η επιχείρηση έχει ανάγκη. Η ανάλυση και περιγραφή της ίδιας της επιχείρησης ονομάζεται «Συναφής αρχιτεκτονική ασφαλείας».

Η SABSA χρησιμοποιεί ένα πίνακα, όπως απεικονίζεται στο σχήμα 2.7, για να περιγράψει τους στόχους της ασφάλειας από αρχιτεκτονική άποψη. Η αρχιτεκτονική θα πρέπει να είναι μια έκφραση της στρατηγικής και, ως εκ τούτου, τα χαρακτηριστικά που ορίζονται στον πίνακα ισχύουν τόσο για τη στρατηγική όσο και την πολιτική. Η προσέγγιση αυτή υπογραμμίζει επίσης την ιχνηλασιμότητα, από την στρατηγική έως την εκτέλεση, καθώς και την επιχειρησιακή άποψη για την παροχή υπηρεσιών.

Σχήμα 2.7: SABSA

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

ISO/IEC 17799 / ISO 27002

Για να εξασφαλιστεί ότι όλα τα σχετικά στοιχεία ασφάλειας που απευθύνονται σε μια οργανωτική στρατηγική ασφαλείας, 11 περιοχές του ISO / IEC 27002 (μετονομάστηκε) μπορούν να προσφέρουν ένα χρήσιμο πλαίσιο για τη μέτρηση της πληρότητας. Με παρόμοιο τρόπο, οι πολιτικές και τα πρότυπα πρέπει να δημιουργηθούν, τα οποία μπορούν άμεσα να παρακολουθήσουν κάθε στοιχείο του προτύπου.

Οι 11 βασικές ενότητες του ISO / IEC 27002 είναι:

- Πολιτική Ασφάλειας
- Οργάνωση της ασφάλειας πληροφοριών
- Διαχείριση περιουσιακών στοιχείων
- Ασφάλεια Ανθρώπινων πόρων.
- Φυσική και περιβαλλοντική ασφάλεια
- Διαχείριση επικοινωνίας και λειτουργιών
- Έλεγχος πρόσβασης
- Ανάπτυξη, απόκτηση και συντήρηση ασφάλειας πληροφοριών
- Διαχείριση συμβάντων ασφάλειας πληροφοριών
- Διαχείριση επιχειρησιακής συνέχειας
- Συμμόρφωση

Κάθε ένα από τα 11 μεγάλα τμήματα χωρίζεται σε 10 ενότητες που πρέπει να αντιμετωπιστούν κατάλληλα σε μια συνολική στρατηγική για την ασφάλεια και την αρχιτεκτονική. Δεν είναι όλα τα τμήματα του προτύπου σχετικά με την κάθε επιχείρηση και το πρότυπο πρέπει να προσαρμόζεται όπου απαιτείται. Βλέπε σχήμα 2.8:

Σχήμα 2.8: ISO/IEC 17799 :2005

<table>
<tr><td colspan="4">Security Policy</td></tr>
<tr><td colspan="4">Information Security Organization</td></tr>
<tr><td colspan="4">Information Asset Management</td></tr>
<tr><td>Human Resource Security</td><td>Physical and Environmental Security</td><td>Communications and Operations Management</td><td rowspan="2">Information Systems Acquisition, Development and Maintenance</td></tr>
<tr><td colspan="3">Access Control</td></tr>
<tr><td colspan="4">Information Security Incident Management</td></tr>
<tr><td colspan="4">Business Continuity Management</td></tr>
<tr><td colspan="4">Compliance</td></tr>
</table>

Άλλες προσεγγίσεις

Άλλες προσεγγίσεις και μέθοδοι, οι οποίες ενδεχομένως να είναι χρήσιμες, όπως τα άλλα πρότυπα ISO σχετικά με την ποιότητα (ISO 9001:2000) είναι το Six Sigma, οι εκδόσεις από το NIST και το ISF και το US Federal Information Security Management Act - FISMA. Μερικές από αυτές επικεντρώνονται περισσότερο στην διαχείριση διαδικασιών και διαχείριση ποιότητας από ότι αφορά τους στρατηγικούς στόχους της ασφάλειας. Ωστόσο, ένα έγκυρο επιχείρημα θα μπορούσε να αναφέρει ότι, αν ο στόχος μιας στρατηγικής για την ασφάλεια ήταν να εφαρμόσει πλήρως τις σχετικές συνιστώσες του ISO 27001, οι περισσότερες ή όλες οι απαιτήσεις ασφαλείας είναι πιθανόν να πληρούνται. Αυτό θα μπορούσε πιθανότατα να είναι μια δαπανηρή προσέγγιση άσκοπα, και το ίδιο το πρότυπο προτείνει ότι πρέπει να προσαρμοστεί με προσοχή στις ειδικές απαιτήσεις του οργανισμού. Άλλες μέθοδοι είναι βέβαιο ότι θα προκύψουν στο μέλλον, που ενδεχομένως να αποδειχθούν πιο αποτελεσματικές από αυτές που αναφέρονται.

Μπορεί να είναι χρήσιμο να χρησιμοποιηθεί ένας συνδυασμός των μεθόδων για να περιγράψει την "επιθυμητή κατάσταση" και να βοηθήσει στην επικοινωνία με τους άλλους και ως ένας τρόπος για να γίνει διασταύρωση των στόχων και να επιβεβαιωθεί ότι όλα τα σχετικά στοιχεία λαμβάνονται υπόψη. Για παράδειγμα, ένας συνδυασμός των COBIT στόχων ελέγχου, CMM, Balanced Scorecard και SABSA κάνουν έναν ισχυρό συνδυασμό.

Ενώ μπορεί να φαίνεται υπερβολή, κάθε προσέγγιση παρουσιάζει μια διαφορετική άποψη η οποία, σε συνδυασμό, είναι πιθανό να καταστήσει βέβαιο ότι καμία σημαντική πτυχή δεν αγνοείται. Δεδομένου ότι είναι απίθανο ότι ένα αποτελεσματικό πρόγραμμα ασφάλειας θα απορρέει από μια ελαττωματική στρατηγική, αυτό μπορεί να είναι μια συνετή προσέγγιση.

GASSP / GAISP

Ένας άλλος χρήσιμος οδηγός κατά την ανάπτυξη μιας στρατηγικής για την ασφάλεια των πληροφοριών είναι η Generally Accepted Security System Principles - GASSP και / ή ο διάδοχός του, Generally Accepted Information Security Principles - GAISP. Παρέχουν μια σαφή διάρθρωση των βασικών χαρακτηριστικών ασφαλείας, διαβεβαιώσεις και πρακτικές. Οι αρχές που περιλαμβάνονται πρέπει να θεωρούνται ως ένας βασικός κατάλογος ελέγχου για τη στρατηγική και όλα τα σχέδια δράσης της ασφάλειας.

Οι εννέα αρχές είναι οι εξής:

1. Αρχή Υπευθυνότητας: Η ευθύνες για την Ασφάλεια των Πληροφοριών πρέπει να ορίζονται σαφώς.
2. Αρχή Ενημέρωσης: Όλα τα μέρη, που συμπεριλαμβάνουν αλλά δεν περιορίζονται στους ιδιοκτήτες πληροφοριών και τους ειδικούς για την ασφάλεια των πληροφοριών, λόγω της ανάγκης να γνωρίζουν, πρέπει να έχουν πρόσβαση σε διαθέσιμες ή εφαρμοσμένες αρχές, πρότυπα, συμβάσεις ή μηχανισμούς για την ασφάλεια των

πληροφοριών και των συστημάτων και πρέπει να ενημερώνονται για απειλές στην ασφάλεια των πληροφοριών.

3. Ηθικές αρχές: Οι πληροφορίας πρέπει να χρησιμοποιούνται, και ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να ενεργεί, με ηθικό τρόπο.
4. Διεπιστημονική αρχή: Οι αρχές, οι κανόνες, οι συμβάσεις και οι μηχανισμοί για την ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων ασφαλείας θα πρέπει να λαμβάνουν υπόψη τους τις σκέψεις και τις απόψεις όλων των ενδιαφερομένων μερών.
5. Αρχή της αναλογικότητας: Οι έλεγχοι της ασφαλείας πληροφοριών πρέπει να είναι ανάλογοι των κινδύνων των τροποποιήσεων, της άρνηση χρήσης ή της δημοσιοποίησης των πληροφοριών.
6. Αρχή Ολοκλήρωσης: Οι αρχές, οι κανόνες, οι συμβάσεις και οι μηχανισμοί για την ασφάλεια των πληροφοριών πρέπει να συντονίζονται μεταξύ τους καθώς και με τις πολιτικές και τις διαδικασίες του οργανισμού, για τη δημιουργία και τη διατήρηση της ασφάλειας σε όλο το πληροφοριακό σύστημα.
7. Αρχή Επικαιρότητας: Όλα τα μέρη θα πρέπει να ενεργούν έγκαιρα και συντονισμένα για την πρόληψη ή την αντιμετώπιση παραβάσεων και απειλών για την ασφάλεια των πληροφοριών και των συστημάτων.
8. Αρχή Αξιολόγησης: Οι κίνδυνοι για την αξιολόγηση των πληροφοριών και τα συστήματα πληροφοριών θα πρέπει να αξιολογούνται περιοδικά ή όταν γίνονται σημαντικές αλλαγές στα συστήματα, το περιβάλλον ή την τεχνολογία.
9. Αρχή δικαιοσύνης: Η ασφάλεια πληροφοριών πρέπει να αντικατοπτρίζει αμερόληπτα τα δικαιώματα, τις ανάγκες και τις υποχρεώσεις όλων των μερών που επηρεάζονται ή που ευθύνονται για τις πληροφορίες.

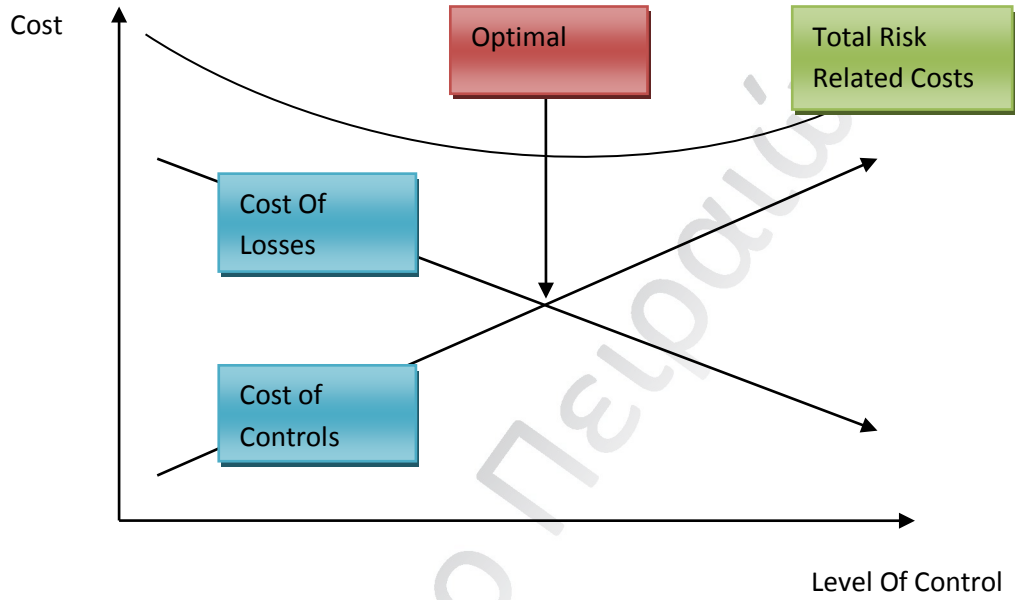
2.9.2 Στόχοι Επικινδυνότητας (Risk Objectives)

Σημαντική συνεισφορά στο καθορισμό της επιθυμητής κατάστασης είναι η προσέγγιση του οργανισμού στον κίνδυνο, που είναι τι η διοίκηση εκλαμβάνει ως αποδεκτό κίνδυνο. Αυτό είναι ένα ακόμη κρίσιμο βήμα καθώς ο καθορισμένος αποδεκτός κίνδυνος εμπεριέχεται στους στόχους του ελέγχου ή των άλλων μέτρων μείωσης του κινδύνου που χρησιμοποιούνται. Ο στόχος των ελέγχων είναι καθοριστικής σημασίας για τον καθορισμό του τύπου, της φύσης και της έκτασης των ελέγχων και των αντίμετρων που η οργάνωση χρησιμοποιεί για τη διαχείριση επικινδυνότητας. Το ακόλουθο σχήμα 2.9 παρουσιάζει τη σχέση μεταξύ των κινδύνων, των μέτρων ελέγχου και του κόστους αυτών.

Χωρίς αρκετά σαφή καθορισμό του αποδεκτού κινδύνου, είναι δύσκολο να καθοριστεί αν η ασφάλεια πληροφοριών επιτυγχάνει τους στόχους της και αν το κατάλληλο επίπεδο των πόρων που έχει αναπτυχθεί.

Πρέπει να υπενθυμίσουμε ότι ο κίνδυνος είναι ένα σύνθετο θέμα και είναι συχνά δύσκολο να εξακριβωθεί με ακρίβεια.

Σχήμα 2.9: Βελτιστοποίηση Κόστους Κινδύνων



Σύμφωνα με το SABSA:

Η λειτουργική διαχείριση επικινδυνότητας είναι ένας συμβιβασμός: αν υπάρχει ένας κίνδυνος που σχετίζεται με τη λήψη μια συγκεκριμένης πορείας δράσης, υπάρχει επίσης ο κίνδυνος να μην το κάνει. Επιπλέον, μεμονωμένοι κίνδυνοι που αλληλεπιδρούν με περίπλοκους τρόπους, και να μειωθούν κατά ένας σχεδόν σίγουρα θα αυξηθούν σε τουλάχιστον ένα άλλο κίνδυνο που πρέπει να αντιμετωπιστεί.

Ο κίνδυνος πάντα επιφέρει ένα κόστος άσχετα εάν είναι ελεγχόμενος ή όχι. Το κόστος του κινδύνου μπορεί να εκφράζεται ως Annual Loss Expectation (ALE), για παράδειγμα, το ποσό των πιθανών απωλειών καταμετρά την πιθανότητα εμφάνισης και δείχνει το βέλτιστο επίπεδο ελέγχου. Το διάγραμμα απεικονίζει την ισορροπία του κόστους των ελέγχων με το κόστος των ζημιών, δείχνοντας το βέλτιστο επίπεδο ελέγχου.

Ένας τρόπος για τον διαχειριστή της ασφάλειας πληροφοριών να προσεγγίσει το ζήτημα του αποδεκτού κινδύνου είναι η ανάπτυξη στόχων του χρόνου επαναφοράς (RTOs), ο οποίος αναλύεται λεπτομερώς στο επόμενο κεφάλαιο. Ωστόσο, μια εκτενή προσέγγιση μπορούν να παρέχει τα στοιχεία που απαιτούνται για την ανάπτυξη της στρατηγικής. Αυτό μπορεί να είναι ένας άτυπος προσδιορισμός από τους ιδιοκτήτες της επιχειρηματικής διαδικασίας του

χρόνου των κρίσιμων συστημάτων που μπορούν να είναι εκτός λειτουργίας, χωρίς σοβαρές οικονομικές συνέπειες. Αυτό, με τη σειρά του, παρέχει τη βάση για την προσέγγιση κόστους αποκατάστασης. Αν αυτό θεωρείται πολύ υψηλό, η επανάληψη της διαδικασίας μπορει καταλήξει σε αποδεκτό χρονικό διάστημα αποκατάστασης με αποδεκτό κόστος. Αυτός ενδεχομένως να θεωρηθεί αποδεκτός κίνδυνος.

Η ανάπτυξη των κατάλληλων στόχων της στρατηγικής, χρειάζεται συνήθως να είναι μια επαναληπτική προσέγγιση με βάση την ανάλυση του κόστους, για την επίτευξη της επιθυμητής κατάστασης και των αποδεκτών επίπεδων κινδύνου. Είναι πιθανό ότι η μείωση του επιπέδου του αποδεκτού κινδύνου θα είναι πιο δαπανηρή. Ωστόσο, η προσέγγιση για την επίτευξη της επιθυμητής κατάστασης έχει σημαντική επίπτωση στο κόστος.

Για παράδειγμα, ορισμένοι κίνδυνοι μπορεί να υπάρχουν εξαιτίας ορισμένων πρακτικών οι οποίες δεν είναι αναγκαίες ή χρήσιμες για τον οργανισμό ή έχουν αρνητικές συνέπειες στη λειτουργία του. Αυτό θα μπορούσε να περιλαμβάνει πρακτικές που θα μπορούσαν να θεωρηθούν αντίθετες με το νόμο και να δημιουργήσουν τον κίνδυνο μιας δίκης. Τέτοιες πρακτικές, όταν εξετάζονται, μπορεί να έχουν προκύψει από ξεπερασμένες νοοτροπίες και προσεγγίσεις που μπορεί να αλλάξουν αποτελεσματικά με χαμηλό κόστος, με αποτέλεσμα την εξάλειψη ή την μείωση του κινδύνου. Με άλλα λόγια, η προσέγγιση για την αντιμετώπιση ή την μείωση συγκεκριμένων κινδύνων έχει σημαντικό αντίκτυπο στο κόστος.

Ο διαχειριστής της ασφάλειας των πληροφοριών πρέπει να κατανοήσει ότι οι τεχνικοί έλεγχοι (π.χ. firewalls, συστήματα ανίχνευσης εισβολής [IDSs], κ.λπ.) είναι απλώς μια διάσταση που πρέπει να ληφθεί υπόψη. Στους περισσότερους οργανισμούς, οι κίνδυνοι των διαδικασιών αποτελούν το μεγαλύτερο κίνδυνο και εδώ οι τεχνικοί έλεγχοι είναι απίθανο να αντιμετωπίσουν επαρκώς την κακή διαχείριση.

Μόλις οι στόχοι καθοριστούν ευκρινώς, θα υπάρξει μια σειρά από αρχιτεκτονικές λύσεις που θα διαφέρουν σημαντικά σε κόστος και πολυπλοκότητα. Όποια διαδικασία χρησιμοποιηθεί, ο στόχος είναι να καθορίσει συγκεκριμένα την επιθυμητή συνολική κατάσταση της ασφάλειας σε κάποια στιγμή στο μέλλον.

Κεφάλαιο 3ο

Διαχείριση Επικινδυνότητας

Ορισμός
Η Διαχείριση Επικινδυνότητας είναι η συστηματική εφαρμογή των πολιτικών διαχείρισης, των διαδικασιών και των πρακτικών για τον εντοπισμό, την ανάλυση, την αξιολόγηση και την παρακολούθηση των σχετικών κινδύνων των πληροφοριών.

Σκοπός
Ο στόχος αυτής της περιοχής εργασίας είναι να εξασφαλιστεί ότι ο διευθυντής της ασφάλειας πληροφοριών κατανοεί τη σημασία της Διαχείρισης Επικινδυνότητας ως εργαλείο για την ικανοποίηση των αναγκών των επιχειρήσεων και την ανάπτυξη ενός προγράμματος διαχείρισης της ασφάλειας για την κάλυψη αυτών των αναγκών.

Ενώ η διακυβέρνηση της ασφάλειας των πληροφοριών καθορίζει τις σχέσεις μεταξύ των επιχειρηματικών στόχων και του προγράμματος ασφάλειας, το security Risk Management προσδιορίζει την έκταση της προστασίας βάσει των απαιτήσεων των επιχειρήσεων, τους στόχους και τις προτεραιότητες τους.

Ο σκοπός της Διαχείρισης Επικινδυνότητας είναι να εντοπίζει, να αναλύει, να ποσοτικοποιεί και να διαχειρίζεται τους κινδύνους που σχετίζονται με την ασφάλεια των πληροφοριών, για την επίτευξη των επιχειρηματικών στόχων μέσα από μια σειρά λειτουργιών, αξιοποιώντας τις γνώσεις του διευθυντή της ασφάλειας πληροφοριών πάνω στις βασικές τεχνικές διαχείρισης κινδύνου.

Δεδομένου ότι η ασφάλεια των πληροφοριών είναι ένα από τα στοιχεία της διαχείρισης του επιχειρηματικού κινδύνου, οι τεχνικές, οι μέθοδοι και οι μετρήσεις που χρησιμοποιούνται για τον καθορισμό των κινδύνων της ασφάλειας πληροφοριών μπορεί να χρειαστεί να εξεταστούν στο ευρύτερο πλαίσιο του επιχειρηματικού κινδύνου. Όπως αναφέρεται και στο προηγούμενο κεφάλαιο, η Διαχείριση Επικινδυνότητας της ασφάλειας πληροφοριών πρέπει επίσης να ενσωματώνει τους κινδύνους του ανθρώπινου δυναμικού, τους φυσικούς καθώς και τους περιβαλλοντικούς.

3.1 Σύνοψη

Η Διαχείριση Επικινδυνότητας είναι, σε γενικές γραμμές, μια διαδικασία με στόχο την επίτευξη της βέλτιστης ισορροπίας μεταξύ ευκαιριών για κέρδος και ελαχιστοποίησης των τρωτών σημείων και των απωλειών. Αυτό επιτυγχάνεται συνήθως με τη διασφάλιση ότι οι επιπτώσεις των απειλών που βασίζονται στην εκμετάλλευση των τρωτών σημείων είναι εντός των αποδεκτών ορίων με αποδεκτό κόστος.

Στην πράξη, η Διαχείριση Επικινδυνότητας σημαίνει ότι οι κίνδυνοι αντιμετωπίζονται έτσι ώστε να μην επηρεάσουν σημαντικά τις επιχειρηματικές διαδικασίες με δυσμενή τρόπο και ότι παρέχεται ένα αποδεκτό επίπεδο βεβαιότητας και προβλεψιμότητας των επιθυμητών αποτελεσμάτων σε κάθε σημαντική δραστηριότητα της επιχείρησης - οργανισμού. Ο κίνδυνος αυτός συνδέεται με όλες τις δραστηριότητες: Υπάρχει κίνδυνος να κάνουμε κάτι και κίνδυνος να μην το κάνουμε. Αλλά για τους περισσότερους οργανισμούς, η σημασία και η κρισιμότητα των πληροφοριών σήμερα δημιουργεί την ανάγκη για αποτελεσματική διαχείριση τους έτσι ώστε να εξασφαλιστεί ο οργανισμός.

Η βάση για την αποτελεσματική Διαχείριση Επικινδυνότητας είναι η ολοκληρωμένη εκτίμηση του κινδύνου (risk assessment) σε συνδυασμό με την ανάλυση των επιπτώσεων στις επιχειρήσεις (BIA - business impact analysis). Δεν είναι δυνατόν η θέσπιση ενός αντίστοιχου προγράμματος Διαχείρισης Επικινδυνότητας αν δεν υπάρχει κατανόηση της φύσης και της έκτασης των κινδύνων των πληροφοριών και των πιθανών επιπτώσεων στις δραστηριότητες της επιχείρησης.

Η Διαχείριση Επικινδυνότητας, η ανάπτυξη αξιολόγησης των επιπτώσεων των επιχειρήσεων και οι αναλύσεις αποτελούν θεμελιώδεις προϋποθέσεις για την ανάπτυξη μιας σημαντικής στρατηγικής για την ασφάλεια. Οργανισμοί που ανέπτυξαν ένα πρόγραμμα διακυβέρνησης της ασφάλειας των πληροφοριών, περιλαμβάνουν τη Διαχείριση Επικινδυνότητας ως αναπόσπαστο μέρος του συνολικού προγράμματος ασφάλειας τους. Ωστόσο, στην πλειονότητα των οργανισμών, η διακυβέρνηση της ασφάλειας των πληροφοριών μόλις αρχίζει να αναπτύσσεται και η διαχείριση του κινδύνου είναι απαραίτητη ανεξάρτητα από την κατάσταση της διακυβέρνησης. Σε υψηλότερο επίπεδο, η Διαχείριση Επικινδυνότητας επιτυγχάνεται εξισορροπώντας την έκθεση κίνδυνου με το κόστος και εφαρμόζοντας τα κατάλληλα αντιμέτρα καθώς και ελέγχους.

Μέρος του πλαισίου της Διαχείριση Επικινδυνότητας των πληροφοριών λοιπόν, αποτελούν οι Έλεγχοι. Το πλαίσιο της Διαχείριση Επικινδυνότητας των πληροφοριών αποτελείται από πολιτικές, διαδικασίες, πρακτικές και οργανωτικές δομές και είναι στην ουσία μια αρχιτεκτονική. Το πλαίσιο αυτό έχει σχεδιαστεί για να παρέχει την διαβεβαίωση ότι οι επιχειρηματικοί στόχοι επιτυγχάνονται και προλαμβάνονται ή να ανιχνεύονται ανεπιθύμητες καταστάσεις και εν τέλει αντιμετωπίζονται. Το πλαίσιο αυτό πρέπει να διευθύνει τους ανθρώπους, τις διαδικασίες και την τεχνολογία και να καλύπτει τις φυσικές, τεχνικές, και διαδικαστικές πτυχές του οργανισμού ή της επιχείρησης. Θα πρέπει επίσης για να είναι

αποτελεσματικό να λαμβάνει υπόψη του θέματα στρατηγικής, τακτικής καθώς και διοικητικά και λειτουργικά στοιχεία του οργανισμού.

Τα αντίμετρα περιλαμβάνουν κάθε διαδικασία που χρησιμεύει για τη μείωση συγκεκριμένων απειλών ή τρωτών σημείων και μπορούν να θεωρηθούν ***επικεντρωμένοι*** έλεγχοι. Τα αντίμετρα μπορεί να περιλαμβάνουν τροποποιημένες αρχιτεκτονικές ή ανασχεδιασμό των διαδικασιών για τη μείωση ή την εξάλειψη των εγγενών αδυναμιών, για τη δημιουργία προγράμματος ενημέρωσης όλων των εργαζόμενων σχετικά με το social engineering και την προώθηση της έγκαιρης αναγνώρισης και αναφοράς των περιστατικών ασφάλειας.

Η Διαχείριση Επικινδυνότητας αποτελεί τη βάση για σχεδόν για όλες τις αποφάσεις που θα ληφθούν σχετικά με τις δραστηριότητες και τα projects ασφάλειας. Σε ορισμένους οργανισμούς, η ασφάλεια των πληροφοριών της Διαχείρισης Επικινδυνότητας είναι ενσωματωμένη σε ένα ήδη υπάρχον πλαίσιο διαχείρισης κινδύνων. Σε άλλες περιπτώσεις, ο κίνδυνος διαχειρίζεται από έναν αριθμό διαφορετικών τμημάτων και επιχειρησιακών μονάδων, που απαιτούν προσπάθειες για να εξασφαλιστεί η συνέχεια και ολοκλήρωση των δραστηριοτήτων της Διαχείρισης Επικινδυνότητας.

Δεδομένου ότι οι αποφάσεις διαχείρισης του κινδύνου έχουν κατά κανόνα σημαντικές οικονομικές επιπτώσεις και ενδεχομένως να απαιτούν αλλαγές σε όλη την επιχείρηση, είναι επιτακτική ανάγκη η εκτελεστική διεύθυνση (executive management) να στηρίζει τη διαδικασία και να κατανοεί πλήρως και να συμφωνεί με τα αποτελέσματα του προγράμματος.

Ο διευθυντής της ασφάλειας πληροφοριών θα πρέπει να γνωρίζει ότι η Διαχείριση Επικινδυνότητας σημαίνει διαφορετικά πράγματα σε διαφορετικούς ανθρώπους στην επιχείρηση. Για παράδειγμα, ο επιχειρησιακός διευθυντής (Business Manager) ενδέχεται να θεωρεί ότι σπάνια συμβαίνουν απειλές και να μην είναι πεπεισμένος για την απόδοση της επένδυσης (ROI) όσον αφορά τα μέτρα ασφαλείας. Η άποψη ενός εσωτερικού ελεγκτή (auditor) μπορεί να εστιάζει στην πρόληψη της απώλειας, ενώ ένας διευθυντής ασφαλείας (insurance manager) μπορεί να την θεωρεί ως οικονομικά αποδοτική χρηματοδότηση κινδύνων.

Ο διαχειριστής της ασφάλειας των πληροφοριών θα πρέπει επίσης να κατανοεί ότι η Διαχείριση Επικινδυνότητας πρέπει να λειτουργεί σε πολλαπλά επίπεδα, συμπεριλαμβανομένων των στρατηγικών, των διαχειριστικών και επιχειρησιακών επίπεδων. Η σημασία της εμπειρίας των επιχειρήσεων και της λήψης επιχειρηματικών αποφάσεων σε οποιαδήποτε διαδικασία αξιολόγησης των κινδύνων (risk assessment) θα πρέπει να θεωρηθούν σημαντικοί παράγοντες για την επίτευξη ρεαλιστικών και επιτυχημένων αποτελεσμάτων από τη διαδικασία αυτή. Η πιθανότητα συσχέτισης μιας συγκεκριμένης απειλής ή κινδύνου αποτελεί συνήθως θέμα κρίσης και η εμπειρία στην περίπτωση αυτή είναι ευεργετική για την επίτευξη ρεαλιστικών αποτελεσμάτων.

Η αξιολόγηση του κινδύνου (Risk assessment) μπορεί να είναι **ποσοτική** (quantitative), **ποιοτική** (qualitative) ή, όπως συνήθως συμβαίνει, ένας συνδυασμός και των δύο, **ημι-ποσοτική** (semiquantitative). Είτε η αξιολόγηση είναι ποιοτική είτε ποσοτική, βασίζεται σε μια ποικιλία παραγόντων, συμπεριλαμβανομένων των ειδών του κινδύνου και των επιπτώσεων αυτών και στο εάν εύκολα μειώνονται στα αποδεκτά επίπεδα. Η κύρια διαφορά στην προσέγγιση τους είναι κατά πόσο ο κίνδυνος καθορίζεται είτε από υπολογιστικές μεθόδους, όπως είναι το προσδόκιμο ετήσιας απώλειας (annual loss expectancy - ALE) ή η εκτίμηση του κινδύνου (value at risk - VAR), για να καταλήξει σε συγκεκριμένες τιμές, είτε στην κρίση και εμπειρία που χρησιμοποιείται, για να τοποθετήσει τον κίνδυνο σε κάποια κατηγορία κλίμακας όπως είναι η χαμηλή (low), η μεσαία (medium) και η υψηλή (high). Πρέπει να γίνει κατανοητό ότι όλες οι αξιολογήσεις του κινδύνου (risk assessments) είναι σε μεγάλο βαθμό ποιοτικές, στηριζόμενες σε υποκειμενικές εκτιμήσεις, συσχετίσεις και αποτελέσματα.

Ποσοτική αξιολόγηση του κινδύνου (Quantitative Risk assessment). Ένα πλεονέκτημα της ποσοτικής ανάλυσης στην αξιολόγηση του κινδύνου είναι ότι μπορεί να δώσει μια κατά προσέγγιση εκτίμηση του μεγέθους των επιπτώσεων, χρησιμοποιώντας οικονομικούς όρους. Το μέτρο αυτό με τη σειρά του, μπορεί να χρησιμοποιηθεί για την ανάλυση κόστους-οφέλους (cost-benefit analysis) των συνιστώμενων ελέγχων. Μολονότι μπορεί να χρησιμοποιηθεί μια υπολογιστική προσέγγιση για να καταλήξουμε σε διάφορες πτυχές του κινδύνου, παρ 'όλα αυτά, η προσέγγιση αυτή είναι ποιοτική και υποκειμενική έως κάποιο βαθμό. Οι τιμές που χρησιμοποιούνται αποτελούν αναπόφευκτα αντικείμενο εικασιών και τα αποτελέσματα πρέπει να επιτρέπουν μεγάλα περιθώρια σφάλματος.

Ποιοτική αξιολόγηση του κινδύνου (Quantitative Risk assessment). Μια ποιοτική αξιολόγηση του κινδύνου μπορεί να είναι ευκολότερο να εκτελεστεί και να επιτρέψει την ιεράρχηση των κινδύνων καθώς και να βοηθήσει στον εντοπισμό των τρωτών σημείων που απαιτούν άμεση προσοχή. Η προσέγγιση αυτή περιλαμβάνει την κατάταξη του κίνδυνου σε μια βάση που να αντικατοπτρίζει τον σχετικό κίνδυνο από χαμηλό έως υψηλό. Αυτή η εκτίμηση της αξιολόγησης του κινδύνου χρησιμοποιεί διαφορετικά σενάρια των δυνατοτήτων του κινδύνου και κατατάσσει τη σοβαρότητα των απειλών καθώς και την κρισιμότητα και την ευαισθησία των περιουσιακών στοιχείων. Βασίζεται στην κρίση, τη διαίσθηση και την εμπειρία παρά σε αριθμούς και οικονομικές αξίες.

Ημι-ποσοτική αξιολόγηση του κινδύνου (Semi-quantitative Risk assessment). Μια τυπική αξιολόγηση κινδύνων χρησιμοποιεί συχνά έναν συνδυασμό και των δύο, ποιοτικών και ποσοτικών μεθόδων. Αυτό αποτελεί ένα δημοφιλές πρώτο βήμα προσέγγισης της εκτίμησης κινδύνου λόγω της ταχύτητας και της χαμηλής πολυπλοκότητας της μεθόδου.

Όποια προσέγγιση ή συνδυασμός των προσεγγίσεων χρησιμοποιηθεί, οι εκτιμήσεις θα πρέπει να επιτρέπουν κάποιο σχετικό εύρος πιθανών σφαλμάτων στην ίδια τη διαδικασία. Με άλλα λόγια, ενώ η αξιολόγηση του κινδύνου βασίζεται σε προβλέψεις μελλοντικών γεγονότων και στη συχνότητα και το μέγεθός τους, είναι φρόνιμο να εξετάζεται το εύρος των πιθανών

αποτελεσμάτων για να εξασφαλιστεί ότι το σενάριο της χειρότερης περίπτωσης δεν θα οδηγήσει σε καταστροφικά αποτελέσματα. Με αυτή την εξαίρεση, τα πιο πιθανά αποτελέσματα θα πρέπει να είναι το πρωταρχικό κριτήριο, ώστε να αποφευχθεί η υπερβολική αντίδραση σε γεγονότα εξαιρετικά απίθανα. Για παράδειγμα, κατά την εξέταση των περιβαλλοντικών κινδύνων, το χτύπημα από έναν κομήτη ενώ είναι πιθανό, είναι εξαιρετικά απίθανο να συμβεί στην πράξη και δεν αξίζουν οι όποιες σημαντικές προσπάθειες για επίγειες εγκαταστάσεις για αυτό το σενάριο. Επιπλέον, θα ήταν εξίσου δύσκολο να αποτραπεί ένας κίνδυνος σαν κι αυτόν και γι 'αυτό είναι συνήθως ένα απλά αποδεκτό αποτέλεσμα.

Ίσως είναι χρήσιμο να θεωρηθεί ότι η επιτυχία οποιασδήποτε διαδικασίας Διαχείρισης Επικινδυνότητας είναι σε κάποιο βαθμό εξαρτώμενη από την εφικτότητα της ίδιας της διαδικασίας. Ένας από τους σημαντικούς παράγοντες είναι το κόστος και η πολυπλοκότητα εκτέλεσης της διαδικασίας αυτής. Όπως και με άλλες πτυχές της ασφάλειας, είναι σημαντικό να βρεθεί η βέλτιστη σχέση κόστους-οφέλους μεταξύ της ακρίβειας της διαδικασίας, της πολυπλοκότητα και του κόστους.

Ανάλογα με τον τύπο του οργανισμού και την ωριμότητα του, όσον αφορά τη Διαχείριση Επικινδυνότητας, μια απλή διαδικασία διαχείρισης κινδύνου μπορεί να έχει μεγαλύτερες πιθανότητες επιτυχίας από μία αρκετά πολύπλοκη. Επιπλέον, μια απλή διαδικασία έχει το πλεονέκτημα του να καταδείξει τα οφέλη με χαμηλό κόστος.

3.1.1 Η Σημασία της Διαχείρισης Επικινδυνότητας

Η Διαχείριση Επικινδυνότητας αποτελεί βασική λειτουργία της ασφάλειας των πληροφοριών. Παρέχει το σκεπτικό και την αιτιολόγηση για σχεδόν όλες τις δραστηριότητες της ασφάλειας των πληροφοριών. Η ασφάλεια των πληροφοριών ως ελεγκτικός μηχανισμός υπάρχει για τη διαχείριση των κινδύνων, την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα. Η Διαχείριση Επικινδυνότητας είναι επίσης το κλειδί για τη διαχείριση των κανονιστικών απαιτήσεων. Αποτελεί καταλύτη των επιχειρήσεων. Λειτουργικά, επιτρέπει τις επιχειρηματικές δραστηριότητες μέσω της μείωσης ή της διαχείρισης των κινδύνων σε εύλογα προβλέψιμα επίπεδα, αποδεκτά και κατάλληλα στην αποστολή της επιχείρησης ή του οργανισμού. Χωρίς τον προσδιορισμό των κινδύνων, δεν είναι δυνατόν να προσδιοριστεί το ενδεχόμενο κόστος ή οι επιπτώσεις μιας συγκεκριμένης δραστηριότητας ή γεγονότος. Η αποτελεσματικότητα της Διαχείρισης Επικινδυνότητας εξαρτάται από το βαθμό στον οποίο αποτελεί μέρος της κουλτούρας του εκάστοτε οργανισμού.

Ο σχεδιασμός και η εφαρμογή της διαδικασίας Διαχείρισης Επικινδυνότητας ενός οργανισμού επηρεάζεται από:

- Την κουλτούρα του οργανισμού.

- Την αποστολή και τους στόχους του οργανισμού
- Την οργανωτική δομή του
- Τα προϊόντα και τις υπηρεσίες του
- Τη διαχείριση του και τις διαδικασίες λειτουργίας
- Συγκεκριμένες πρακτικές που χρησιμοποιούνται και
- Τις τοπικές φυσικές, περιβαλλοντικές και κανονιστικές συνθήκες που επικρατούν.

3.1.2 Αποτελέσματα της Διαχείρισης Επικινδυνότητας.

Η αποτελεσματική Διαχείριση Επικινδυνότητας χρησιμεύει στην μείωση της συχνότητας εμφάνισης των σημαντικών αρνητικών επιπτώσεων στη λειτουργία ενός οργανισμού είτε με την αντιμετώπιση των απειλών και την μείωση της έκθεσης σε αυτές είτε με τη μείωση της ευπάθειας ή των επιπτώσεων. Στο βαθμό που αυτό επιτυγχάνεται, η Διαχείριση Επικινδυνότητας παρέχει ένα βαθμό προβλεψιμότητας ο οποίος υποστηρίζει την ικανότητα του οργανισμού να λειτουργεί αποτελεσματικά και αποδοτικά.

Όπως αναφέρθηκε, ένα από τα αποτελέσματα της χρηστής διακυβέρνησης είναι η αποτελεσματική διαχείριση του κινδύνου, δηλαδή, η εκτέλεση κατάλληλων μέτρων για την μείωση των κινδύνων και τη μείωση των πιθανών επιπτώσεων των πληροφοριακών πόρων σε ένα αποδεκτό επίπεδο και παρέχει:

- Κατανόηση των απειλών της επιχείρησης , την ευπάθεια του και το προφίλ κινδύνου.
- Κατανόηση της έκθεσης σε πιθανούς κίνδυνους και τις πιθανές συνέπειες ενδεχόμενου συμβιβασμού.
- Συνειδητοποίηση των προτεραιοτήτων της Διαχείριση Επικινδυνότητας, βασισμένες στις πιθανές συνέπειες.
- Στρατηγική μείωσης του επιχειρηματικού κινδύνου, επαρκή για την επίτευξη αποδεκτών συνεπειών από τους υπολειπόμενους κίνδυνους
- Οργανωτική αποδοχή βασισμένη στην κατανόηση των πιθανών συνεπειών του υπολειπόμενου κινδύνου.

3.2 Στρατηγική Διαχείρισης Επικινδυνότητας

Μια στρατηγική Διαχείρισης Επικινδυνότητας για να είναι αποτελεσματική πρέπει να είναι μια ολοκληρωμένη επιχειρηματική διαδικασία με καθορισμένους στόχους που θα ενσωματώνουν: το σύνολο των διαδικασιών διαχείρισης κινδύνων, τις δραστηριότητες του οργανισμού, τις μεθοδολογίες και τις πολιτικές του. Η στρατηγική Διαχείρισης Επικινδυνότητας καθορίζει τις παραμέτρους και τα χαρτογραφεί την εξέλιξη του

προγράμματος Διαχείρισης Επικινδυνότητας του οργανισμού. Πρέπει να συνάδει και να ενσωματωθεί στη συνολική στρατηγική διακυβέρνησης της ασφάλειας, όπως αναφέρεται στο προηγούμενο κεφάλαιο. Η στρατηγική ασφάλειας με τη σειρά της περιέρχεται στους γενικούς στόχους του οργανισμού και την επιχειρηματική στρατηγική.

Οι στρατηγικές Διαχείρισης Επικινδυνότητας καθορίζονται από έναν αριθμό εσωτερικών και εξωτερικών παραγόντων. Οι εσωτερικοί παράγοντες περιλαμβάνουν την οργανωτική ωριμότητα, την ιστορία, τον πολιτισμό, τη δομή, και την ανοχή κινδύνου των ανώτερων διευθυντικών στελεχών. Οι διάφοροι εξωτερικοί παράγοντες όπως είναι ο τομέας της βιομηχανίας και οι νομικές και κανονιστικές απαιτήσεις έχουν συλλογικά μια σημαντική επίδραση στην ανάπτυξη μιας αποτελεσματικής στρατηγικής.

Όλες οι στρατηγικές Διαχείρισης Επικινδυνότητας περιλαμβάνουν τον καθορισμό της βέλτιστης προσέγγισης για την ευθυγράμμιση των διαδικασιών, της τεχνολογίας, της συμπεριφοράς και την αποδοχή ή απόρριψη των κινδύνων που βασίζονται στην ανοχή της διοίκησης για τους κίνδυνους και την ικανότητα της εταιρείας να τους διαχειριστεί. Συλλογικά, οι στρατηγικές Διαχείρισης Επικινδυνότητας θα πρέπει να οδηγούν σε απόρριψη των ανεξέλεγκτων κινδύνων, μείωση αντίκτυπου των αποδεκτών κινδύνων κατά την υλοποίηση, έλεγχο και πρόβλεψη τυχόν κινδύνων σε ολόκληρο τον οργανισμό.

3.2.1 Επικοινωνία, Ενημέρωση και Παροχή Συμβουλών για τους κινδύνους.

Για να γίνει η Διαχείριση Επικινδυνότητας μέρος της κουλτούρας του οργανισμού, είναι απαραίτητη η επικοινωνία και η ενημέρωση των θεμάτων της διαδικασίας αυτής, σε κάθε της βήμα, στην επιχείρηση.

Η επικοινωνία πρέπει να περιλαμβάνει όλους τους ενδιαφερόμενους με εστίαση στην ανάπτυξη μιας κοινής αντίληψης των στόχων και των απαιτήσεων του προγράμματος αυτού. Αυτό θα επιτρέψει διαφοροποιήσεις ως προς τις ανάγκες και τις αντιλήψεις που θα πρέπει να εντοπιστούν και να αντιμετωπιστούν πιο αποτελεσματικά.

3.3 Αποτελεσματική Διαχείριση Επικινδυνότητας Ασφάλειας Πληροφοριών

Οι αποτελεσματικές δραστηριότητες της Διαχείριση Επικινδυνότητας της Ασφάλειας πληροφοριών πρέπει να υποστηρίζονται σε συνεχή βάση από όλα τα μέλη της επιχείρησης. Η υποστήριξη των Εκτελεστικών (C-level/Executive) στελεχών προσδίδει αξιοπιστία και κίνητρα στις προσπάθειες της Διαχείρισης Επικινδυνότητας. Ακόμα και οι καλύτερα σχεδιασμένοι και υλοποιημένοι έλεγχοι δεν θα λειτουργήσουν όπως προβλέπεται εάν οι

λειτουργίες εκτελούνται από απρόσεκτο, αδιάφορο ή μη εκπαιδευμένο προσωπικό. Η κουλτούρα του εκάστοτε οργανισμού – επιχείρησης, η οποία περιλαμβάνει ορθές πρακτικές ασφάλειας πληροφοριών, σε συνδυασμό με την προσήλωση της ανώτερης διοίκησης για την αποτελεσματική Διαχείριση Επικινδυνότητας είναι αναγκαίες για την επίτευξη των στόχων του προγράμματος αυτού. Επιπλέον, το προσωπικό πρέπει να κατανοήσει τις ευθύνες του και να εκπαιδευτεί στην εφαρμογή των διαδικασιών ελέγχου. Η συμμόρφωση με τους ελέγχους ασφάλειας των πληροφοριών θα πρέπει να δοκιμαστούν και να εκτελούνται σε συνεχή βάση. Επιπρόσθετα, πρέπει να γίνονται προσπάθειες για την ενσωμάτωση όλων των λειτουργιών διαχείρισης κινδύνου, για να εξασφαλιστεί η συνέχεια και η πληρότητα των δραστηριοτήτων της Διαχείρισης Επικινδυνότητας σε ολόκληρη την επιχείρηση και η παροχή επαρκούς επίπεδου διασφάλισης των επιχειρηματικών διαδικασιών.

3.3.1 Ανάπτυξη προγράμματος Διαχείρισης Επικινδυνότητας

Τα αρχικά βήματα στην ανάπτυξη ενός προγράμματος Διαχείρισης Επικινδυνότητας περιλαμβάνουν τη θέσπιση:

- Περιεχομένου και σκοπού του προγράμματος
- Πεδίου εφαρμογής και χαρτογράφησης επιχείρησης
- Ομάδας υλοποίησης.

Θέσπιση πλαισίου και σκοπού του προγράμματος

Όλοι οι οργανισμοί αντιμετωπίζουν ποικίλους κινδύνους σε συνεχή βάση και πρέπει να τους αντιμετωπίσουν είτε με τους επίσημους κανονισμούς, είτε ad hoc, είτε σε ορισμένες περιπτώσεις, να τις αγνοήσει. Η Διαχείριση Επικινδυνότητας για την ασφάλεια των πληροφοριών είναι συνήθως ευθύνη του διαχειριστή της ασφάλειας των πληροφοριών.

Η πρωτογενής απαίτηση είναι να προσδιοριστεί ο σκοπός της δημιουργίας ενός προγράμματος Διαχείρισης Επικινδυνότητας στην επιχείρηση, τα επιθυμητά αποτελέσματα και να καθοριστούν οι στόχοι αυτού. Θα μπορούσε ενδεχομένως να είναι μια προσπάθεια για τη μείωση των επιπτώσεων που βασίζονται στις επιθέσεις μέσω Internet ή η διασφάλιση συμμόρφωσης με τις νομικές και κανονιστικές απαιτήσεις. Εάν η Διαχείριση Επικινδυνότητας δεν είναι τυπικά εγκατεστημένη, το πρόγραμμα μπορεί να είναι ευρύτερο και να περιλαμβάνει όλες τις πτυχές της οργανωτικής δραστηριότητας και τις κατανεμημένες αρμοδιότητες μεταξύ των διαφόρων τμημάτων.

Ο ορισμός του πλαισίου Διαχείρισης Επικινδυνότητας προϋποθέτει τον καθορισμό των διαδικασιών, των δραστηριοτήτων, των πεδίων εφαρμογής και τη θέσπιση των σκοπών και των στόχων της επιχείρησης.

Όπως αναφέρθηκε και προηγουμένως, για τη δημιουργία ενός αποτελεσματικού προγράμματος, αποτελεί βασικό στοιχείο ο προσδιορισμός της ανοχής των κινδύνων στην επιχείρηση ή αυτών που θεωρεί η διοίκηση αποδεκτό επίπεδο κινδύνου. Κάθε οργανισμός έχει διαφορετικό επίπεδο ανοχής κινδύνων για το σύνολο και τα είδη των κινδύνων που θεωρεί αποδεκτά και αυτό είναι πολύ πιθανό να διαφέρει ανάλογα ακόμα και με το τμήμα ή την οργανωτική μονάδα αυτών. Αυτό είναι αναπόφευκτα μια απόφαση της ίδιας της επιχείρησης που βασίζεται σε μια σειρά κριτηρίων, συμπεριλαμβανομένης της αποστολής και της κουλτούρας αυτής, και όχι σε συγκεκριμένες ποσοτικές μετρήσεις. Κατά κανόνα, τα διευθυντικά στελέχη με το διοικητικό συμβούλιο δίνουν το στίγμα για το πρόγραμμα Διαχείρισης Επικινδυνότητας. Αυτή η κλήση προς την κορυφή είναι ένα σημαντικό συστατικό της ευθύνης της διοίκησης για την εταιρική διακυβέρνηση. Όπως συμβαίνει με όλες τις άλλες πτυχές της ασφάλειας, μια top-down προσέγγιση είναι σημαντικά πιο αποτελεσματική από μια bottom-up προσέγγιση, στην οποία χαμηλότερου επίπεδου διαχειριστές προσπαθούν να επηρεάσουν τον οργανισμό. Οι εργαζόμενοι γενικά θεωρούν ότι τα ανώτερα διευθυντικά στελέχη προσδιορίζουν τα θέματα που χρίζουν υψηλότερης προτεραιότητας.

Καθορισμός πεδίου εφαρμογής και χαρτογράφηση επιχείρησης

Δεδομένου ότι όλα τα τμήματα και οι επιχειρησιακές μονάδες έχουν κάποιο βαθμό ευθύνης στη Διαχείρισης Επικινδυνότητας, είναι σημαντικό να προσδιοριστεί ξεκάθαρα το πεδίο εφαρμογής των ευθυνών και των αρμοδιοτήτων που αφορούν ειδικά τον διευθυντή της ασφάλειας των πληροφοριών και άλλους παράγοντες. Αυτό βοηθά στην αποφυγή κενών στη διαδικασία, βελτιώνει τη συνολική συνοχή των προσπαθειών της Διαχείρισης Επικινδυνότητας και μειώνει την περιττή επανάληψη τους.

Θα πρέπει να σημειωθεί ότι, δεδομένου ότι σχεδόν όλες οι δραστηριότητες της ασφάλειας των πληροφοριών κατά κάποιον τρόπο σχετίζονται με τη Διαχείριση Επικινδυνότητας, το εγχείρημα αυτό σχετίζεται άμεσα με τις ευθύνες του διευθυντή της ασφαλείας πληροφοριών. Ανεξάρτητα από το πεδίο εφαρμογής των ευθυνών του διευθυντή της ασφάλειας πληροφοριών, πρέπει να καθορίζεται το πεδίο εφαρμογής του προγράμματος της Διαχείρισης Επικινδυνότητας της επιχείρησης και να προσδιορίζονται οι γενικοί στόχοι του προγράμματος αυτού.

Μολονότι πολλά μέρη της επιχείρησης είναι υπεύθυνα για ορισμένες πτυχές της Διαχείρισης Επικινδυνότητας, οι βασικοί τομείς της ασφάλειας των πληροφοριών σχετίζονται συνήθως με τη διαχείριση της φυσικής ασφάλειας και το γενικό ή λειτουργικό κίνδυνο. Ένα απλό παράδειγμα μιας περιοχής στην οποία πρέπει να οριστεί ο υπεύθυνος είναι η διασφάλιση ότι οι ευαίσθητες πληροφορίες οι οποίες ενδεχομένως να βρεθούν σε εκτυπωτές με αποτέλεσμα την ακούσια αποκάλυψη εμπιστευτικών εγγράφων τα οποία και δεν τεμαχίστηκαν προτού

πεταχτούν στα σκουπίδια. Ενώ αυτό το παράδειγμα μπορεί να φαίνεται ασήμαντο, είναι σημαντικό από την άποψη της ασφάλειας των πληροφοριών.

Επιπλέον, σε κάθε επιχείρηση, υπάρχουν πολλά σημεία τομής της ασφάλειας πληροφοριών, της ασφάλειας του IT, της ασφάλειας των εγκαταστάσεων αλλά και της φυσικής ασφάλειας καθώς και τους φορείς διασφάλισης ποιότητας και είναι ιδιαίτερα σημαντικό οι περιοχές των αντίστοιχων αυτών αρμοδιοτήτων να ορίζονται σαφώς.

Είναι επίσης πολύ πιθανό ένα σημαντικό μέρος της Διαχείρισης Επικινδυνότητας της ασφάλειας πληροφοριών να ασχοληθεί με δραστηριότητες του IT και για το λόγο αυτό είναι επίσης αναγκαίο να καθοριστούν τα όρια των συστημάτων IT, για τα οποία ο διευθυντής της ασφάλειας των πληροφοριών θα είναι υπεύθυνος

Ομάδα ανάπτυξης προγράμματος

Το επόμενο βήμα είναι να ορίσει η ομάδα που θα είναι υπεύθυνη για την ανάπτυξη και την εφαρμογή του προγράμματος της Διαχείρισης Επικινδυνότητας της επιχείρησης. Ενώ η ομάδα αυτή είναι η κυρίως υπεύθυνη για το πλάνο της Διαχείρισης Επικινδυνότητας, ένα επιτυχημένο πρόγραμμα απαιτεί την ενσωμάτωση της σε όλα τα επίπεδα της επιχείρησης. Το προσωπικό και τα μέλη του διοικητικού συμβουλίου πρέπει να βοηθούν την επιτροπή της Διαχείρισης Επικινδυνότητας στον εντοπισμό των κινδύνων, τον καθορισμό των αποδεκτών επίπεδων κινδύνου και την ανάπτυξη κατάλληλων στρατηγικών για την απώλεια ελέγχου και τις σχετικές παρέμβασης.

Μείζονος σημασίας είναι η ανάγκη το πρόγραμμα Διαχείρισης Επικινδυνότητας να ευθυγραμμίζεται πλήρως με τη στρατηγική και τον προσανατολισμό της επιχείρησης. Για το λόγο αυτό, είναι ζωτικής σημασίας η συμμετοχή εκπροσώπων από όλες τις βασικές επιχειρηματικές μονάδες. Μπορεί επίσης να είναι σκόπιμο άλλες περιοχές κινδύνου να λαμβάνονται ιδιαιτέρως υπόψη, καθώς ενδεχομένως να επηρεάζουν την προστασία των πληροφοριών. Το πιο σημαντικό είναι ότι η διαδικασία διεξάγεται με γνώμονα την επιχείρηση και όχι με γνώμονα την εκάστοτε τεχνολογία.

3.3.2 Ρόλοι και Ευθύνες

Η Διαχείριση Επικινδυνότητας της ασφάλειας πληροφοριών αποτελεί αναπόσπαστο μέρος της διαχείρισης ασφάλειας και είναι η ευθύνη του διοικητικού συμβουλίου να εξασφαλίσουν ότι οι προσπάθειες αυτές του προγράμματος είναι αποτελεσματικές. Απαιτούνται περιοδικές εκθέσεις για τις προσπάθειες και την αποτελεσματικότητα των δραστηριοτήτων της Διαχείρισης Επικινδυνότητας καθώς παρέχουν την απαραίτητη ανατροφοδότηση ώστε να εξασφαλιστεί ότι οι προθέσεις και οι προσδοκίες της διοίκησης υλοποιούνται.

Η ανώτερη διοίκηση πρέπει να διασφαλίζει την ύπαρξη επαρκών πόρων και τη στήριξη των δραστηριοτήτων της Διαχείρισης Επικινδυνότητας και θα πρέπει να λαμβάνει αναφορές κατάστασης περιοδικά αλλά και σε κάθε περιστατικό. Οι αναφορές ανά περιστατικό χρειάζονται τη συμμετοχή της διοίκησης για τον καθορισμό της φύσης και της σοβαρότητας της αναφοράς. Η διοίκηση πρέπει επίσης να έχει συμμετοχή και να υπογράψει τα αποδεκτά επίπεδα κινδύνου καθώς και τους στόχους του προγράμματος της Διαχείρισης Επικινδυνότητας.

Το διοικητικό συμβούλιο, πρέπει να θέσει της προτεραιότητες της Διαχείρισης Επικινδυνότητας και να καθορίσει τους στόχους της όσον αφορά την υποστήριξη της επιχειρηματικής στρατηγικής. Το συμβούλιο πρέπει επίσης να επιφορτιστεί με την ανάπτυξη επιπέδων των αποδεκτών επιπέδων μείωσης του κινδύνου για διάφορες επιχειρηματικές διαδικασίες και να τα παρουσιαστεί στη διοίκηση για τη αποδοχή τους. Ο καθορισμός των επιπέδων του αποδεκτού κινδύνου και την υποστήριξη της ανώτερης διοίκησης αποτελεί απαραίτητη προϋπόθεση για την αποτελεσματική Διαχείριση Επικινδυνότητας.

Ο διευθυντής της ασφάλειας πληροφοριών είναι υπεύθυνος για την ανάπτυξη, τη συνεργασία και τη διαχείριση του προγράμματος της Διαχείρισης Επικινδυνότητας, με σκοπό την επίτευξη των καθορισμένων στόχων. Έχει επίσης την ευθύνη για τη διατήρηση συνδέσμων με τις άλλες ομάδες διαχείρισης κινδύνων και τις δραστηριότητες ασφαλείας της επιχείρησης με σκοπό την προώθηση της ενσωμάτωσης των δραστηριοτήτων και την ύπαρξη ενός αποτελεσματικού και συντονισμένου επίπεδου της διαδικασίας ασφαλείας της επιχείρησης.

Βασικοί Ρόλοι

Η Διαχείρισης Επικινδυνότητας είναι ευθύνη της Διοίκησης. Το αμερικανικό Εθνικό Ινστιτούτο Επιστήμης και Τεχνολογίας (NIST - National Institute of Science and Technology) στην δημοσίευση 800-30 περιγράφει τους βασικούς ρόλους του προσωπικού, οι οποίοι πρέπει να υποστηρίξουν και να συμμετάσχουν στη διαδικασία διαχείρισης των κινδύνων. Ενώ οι λεπτομέρειες ποικίλλουν μεταξύ των επιχειρήσεων, αυτή η άποψη πρέπει γενικά να καθοδηγεί τους περισσότερους οργανισμούς.

- **Διοικητικά συμβούλια** και **ανώτερη διοίκηση**. Η ανώτερη διοίκηση, σύμφωνα με τα πρότυπα επιμέλειας και απόλυτης ευθύνης στην εκπλήρωση της αποστολής, πρέπει να διασφαλίζει ότι οι αναγκαίοι πόροι εφαρμόζονται αποτελεσματικά για την ανάπτυξη των ικανοτήτων που απαιτούνται για την ολοκλήρωση της αποστολής. Πρέπει επίσης να αξιολογήσει και να ενσωματώσει τα αποτελέσματα της δραστηριότητας αξιολόγησης του κινδύνου στη διαδικασία λήψης αποφάσεων. Ένα αποτελεσματικό πρόγραμμα Διαχείρισης Επικινδυνότητας που αξιολογεί και μειώνει τους κινδύνων που σχετίζονται με το IT απαιτεί την υποστήριξη και τη συμμετοχή των ανώτερων στελεχών.

- **Διευθυντής Συστημάτων Πληροφορικής** (CIO - Chief Information Officer). Ο Διευθυντής Συστημάτων Πληροφορικής είναι υπεύθυνος για τον σχεδιασμό, την κατάρτιση του προϋπολογισμού καθώς και την απόδοση των συστημάτων IT. Οι αποφάσεις που λαμβάνονται σε αυτούς τους τομείς πρέπει να βασίζονται σε ένα αποτελεσματικό πρόγραμμα Διαχείρισης Επικινδυνότητας.
- **Διευθυντής Ασφάλειας Πληροφοριών** (Information Security Manager). Οι διευθυντές της ασφάλειας πληροφοριών είναι υπεύθυνοι για τα προγράμματα ασφάλειας των επιχειρήσεων τους, που συνήθως περιλαμβάνουν την Διαχείριση Επικινδυνότητας. Ως εκ τούτου, διαδραματίζουν ηγετικό ρόλο στην καθιέρωση μιας κατάλληλα δομημένης μεθοδολογίας, η οποία θα βοηθήσει στον εντοπισμό, την αξιολόγηση και την ελαχιστοποίηση των κινδύνων των πληροφοριακών συστημάτων. Οι διευθυντές της ασφάλειας πληροφοριών λειτουργούν επίσης ως σημαντικοί σύμβουλοι των ανώτερων διευθυντικών στελεχών για να διασφαλιστεί ότι η δραστηριότητα αυτή διεξάγεται σε συνεχή βάση.
- **Ιδιοκτήτες Συστημάτων και Πληροφοριών** (System and Information Owners). Είναι υπεύθυνοι για να εξασφαλίζουν ότι οι κατάλληλοι έλεγχοι είναι σε θέση να διαχειριστούν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των IT συστημάτων και των δεδομένων που αυτά κατέχουν. Συνήθως, οι ιδιοκτήτες είναι υπεύθυνοι για τις αλλαγές στα συστήματα πληροφορικής. Κατά συνέπεια, συνήθως πρέπει να εγκρίνουν και να υπογράψουν για τις αλλαγές στα συστήματα πληροφορικής (π.χ. βελτίωση του συστήματος και σημαντικές αλλαγές στο λογισμικό και hardware). Οι ιδιοκτήτες, ως εκ τούτου, πρέπει να καταλάβουν επακριβώς τον ρόλο τους στη διαδικασία Διαχείρισης Επικινδυνότητας και να την υποστηρίξουν πλήρως.
- **Διευθυντές Επιχειρήσεων και λειτουργιών** (Business and Functional Managers). Οι διευθυντές οι οποίοι είναι υπεύθυνοι για τις δραστηριότητες των επιχειρήσεων και τις IT διαδικασίες σύναψης των συμβάσεων πρέπει να έχουν ενεργό ρόλο στη διαδικασία της Διαχείρισης Επικινδυνότητας. Οι διευθυντές αυτοί είναι τα άτομα με την εξουσία και την ευθύνη για την πραγματοποίηση των αποφάσεων συμβιβασμών, οι οποίες είναι απαραίτητες για ολοκλήρωση της διαδικασίας. Η συμμετοχή τους στη διαδικασία της Διαχείριση Επικινδυνότητας επιτρέπει την επίτευξη της κατάλληλης ασφάλειας των συστημάτων πληροφορικής, τα οποία, με την σωστή διαχείριση, αναδεικνύουν την αποτελεσματικότητα του προγράμματος, με την ελάχιστη δαπάνη των πόρων.
- **Συμμετέχοντες στην ασφάλεια IT** (IT Security Practitioners). Οι συμμετέχοντες (π.χ. διαχειριστές βάσεων δεδομένων, δικτύων, συστημάτων, εφαρμογών, Ειδικοί υπολογιστών, Αναλυτές και Σύμβουλοι ασφαλείας) είναι υπεύθυνοι για την ορθή υλοποίηση των απαιτήσεων ασφαλείας στα συστήματα IT. Καθώς συμβαίνουν αλλαγές στο υπάρχον περιβάλλον του IT συστήματος (π.χ. επέκταση του δικτύου, αλλαγές στην υπάρχουσα υποδομή και τις οργανωτικές πολιτικές, εισαγωγή νέων τεχνολογιών), οι συμμετέχοντες στην ασφάλεια IT πρέπει να υποστηρίζουν ή να χρησιμοποιούν τη διαδικασία Διαχείρισης Επικινδυνότητας για τον εντοπισμό και την

αξιολόγηση νέων πιθανών κινδύνων και να εφαρμόζουν νέους ελέγχους ασφαλείας, όπου αυτό απαιτείται, για τη διασφάλιση των IT συστημάτων.

- **Εκπαιδευτές Ενημέρωσης Ασφάλειας** (Security Awareness Trainer). Το προσωπικό της επιχείρησης είναι οι χρήστες των IT συστημάτων. Η χρήση των πληροφοριακών συστημάτων και των δεδομένων σύμφωνα με τις πολιτικές, τις κατευθυντήριες γραμμές του οργανισμού και τους κανόνες συμπεριφοράς είναι κρίσιμης σημασίας για την εξάλειψη των κινδύνων και την προστασία του πόρων μιας επιχείρησης. Για να ελαχιστοποιηθεί ο κίνδυνος για τα συστήματα πληροφορικής, είναι σημαντικό ότι οι χρήστες των συστημάτων και των εφαρμογών τους έχουν εκπαιδευτεί σε θέματα ασφάλειας. Ως εκ τούτου, οι Εκπαιδευτές ασφάλειας πρέπει να κατανοήσουν τη διαδικασία Διαχείρισης Επικινδυνότητας, ώστε να μπορούν να αναπτύξουν το κατάλληλο διδακτικό υλικό και να ενσωματώσει την αξιολόγηση των κινδύνων στα προγράμματα κατάρτισης για την εκπαίδευση των τελικών χρηστών.

3.4 Θεωρητικές προσεγγίσεις της Διαχείρισης Επικινδυνότητας.

Η συνολική Διαχείριση Επικινδυνότητας στις περισσότερες επιχειρήσεις παρέχεται από ένα ή περισσότερα ξεχωριστά τμήματα. Η γνώση του θέματος όμως απαιτείται να είναι αποτελεσματική και, ως εκ τούτου, η διαχείριση των κινδύνων της ασφάλειας πληροφοριών επιβαρύνει συνήθως τον διευθυντή της ασφάλειας πληροφοριών. Για να είναι αποτελεσματικός, ο διευθυντής της ασφάλειας πληροφοριών απαιτείται μια ευρεία αντίληψη σε μια σειρά από θεμελιώδεις έννοιες για τη διαχείριση της ασφάλειας και των κινδύνων. Αυτό περιλαμβάνει τεχνικά, στρατηγικά, τακτικά, διοικητικά και λειτουργικά στοιχεία. Μερικές από τις βασικές αυτές έννοιες αναλύονται παρακάτω.

3.4.1 Έννοιες

Υπάρχουν ορισμένες βασικές έννοιες με τις οποίες ένας διαχειριστής ασφαλείας πρέπει να είναι εξοικειωμένος και είναι απαραίτητες για να κατανοήσουμε αυτό το κεφάλαιο και την χρήση τους στη Διαχείριση Επικινδυνότητας. Οι περισσότεροι διευθυντές της ασφάλειας πληροφοριών είναι εξοικειωμένοι με αυτές τις έννοιες, αλλά θα ήταν χρήσιμο να επανεξετάσουμε τους ορισμούς για να διασφαλιστεί η σαφής κατανόηση που απαιτείται για καλύτερα αποτελέσματα. Οι έννοιες αυτές περιλαμβάνουν τα ακόλουθα:

- Απειλές
- Αδυναμίες
- Χρηματοδοτικά ανοίγματα
- Κίνδυνοι
- Επιπτώσεις

- Έλεγχοι
- Αντίμετρα
- Αποτίμηση πόρων
- Πληροφορίες ταξινόμησης περιουσιακών στοιχείων
- Κρισιμότητα
- Ευαισθησία
- Χρόνος επαναφοράς (Recovery Time Objectives - RTOs)
- Σημείο επαναφοράς (Recovery Point Objectives - RPOs)
- Παράδοση Υπηρεσία (Service Delivery Objectives - SDOs)
- Παράθυρο Αποδεκτής Διακοπής (Acceptable Interruption Window - AIW)
- Εφεδρείες

Άλλες λειτουργίες Διαχείρισης Επικινδυνότητας, που σχετίζονται με την ασφάλεια των πληροφοριών και πρέπει να γίνει κατανοητές είναι οι ακόλουθες:

- Service Level Agreements (SLAs)
- Αξιοπιστία και Αντοχή Συστημάτων
- Συνέχιση επιχειρηματικής δραστηριότητας / ανάκτηση από καταστροφή (Business continuity/disaster recovery)
- Ανασχεδιασμός Επιχειρησιακών Διαδικασιών
- Χρονοδιαγράμματα και πολυπλοκότητα διαχείρισης έργου
- Επιχειρησιακή αρχιτεκτονική και αρχιτεκτονική ασφαλείας
- Διακυβέρνηση πληροφορικής (IT) και ασφάλειας πληροφοριών
- Διαχείρισης του κύκλου ζωής των συστημάτων.
- Πολιτικές, πρότυπα και διαδικασίες

3.4.2 Τεχνολογίες

Υπάρχει επίσης μια ποικιλία από τεχνολογίες ασφάλειας πληροφοριών και τεχνικές έννοιες οι οποίες είναι σημαντικό για το διαχειριστή της ασφάλειας πληροφοριών να έχουν μια πλήρη εννοιολογική κατανόηση καθώς σχετίζονται με τη Διαχείριση Επικινδυνότητας. Ορισμένες από αυτές είναι οι ακόλουθες:

- Εφαρμογή μέτρων ασφαλείας
- Μέτρα φυσικής ασφάλειας
- Περιβαλλοντικοί έλεγχοι
- Logical access controls
- Network access controls
- Routers, firewalls και άλλα στοιχεία του δικτύου (bridges, gateways)
- Ανίχνευση / πρόληψη εισβολών

- Ασύρματη ασφάλεια
- Platform security
- Κρυπτογράφηση και Υποδομή Δημοσίου Κλειδιού (public key infrastructure - PKI)
- Antivirus/malware
- Spyware/adware
- Antispam συσκευές
- voice-over IP (VoIP)

Επιπλέον, ενώ το προσωπικό και οι εγκαταστάσεις ασφαλείας δεν μπορεί να είναι μέρος της διαχείρισης της ασφάλειας πληροφοριών ή του προγράμματος Διαχείρισης Επικινδυνότητας, πρόκειται για περιοχές κινδύνου που πρέπει να θεωρούνται μέρος της Διαχείρισης Επικινδυνότητας. Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να γνωρίζει και θέματα προσωπικού και τους ελέγχους ασφαλείας αυτού καθώς και τους ελέγχους των εγκαταστάσεων ως μέρος της αξιολόγησης κινδύνου και της διαχείρισης των δραστηριοτήτων.

3.5 Υλοποίηση Διαχείρισης Επικινδυνότητας

Ως μέρος του σχεδιασμού ενός προγράμματος Διαχείρισης Επικινδυνότητας, ο διευθυντής της ασφάλειας πληροφοριών πρέπει να αναγνωρίζει όλες τις άλλες δραστηριότητες διαχείρισης κινδύνου της επιχείρησης και να επιδιώκει την ενσωμάτωση αυτών των λειτουργιών ή δραστηριοτήτων στο πλαίσιο του προγράμματος της ασφάλειας πληροφοριών. Οι μεγαλύτερες επιχειρήσεις έχουν συνήθως μια λειτουργία Διαχείρισης Επικινδυνότητας, που ασχολείται με δραστηριότητες που συνήθως σχετίζονται με τους φυσικούς κινδύνους. Στην περίπτωση των χρηματοπιστωτικών ιδρυμάτων, υπάρχει συνήθως ένα τμήμα που ασχολείται με τον πιστωτικό κίνδυνο. Άλλα τμήματα, όπως η διαχείριση των ανθρώπινων πόρων και ο εσωτερικός έλεγχος εμπλέκονται τυπικά στην διαχείριση κινδύνων στον εκάστοτε οργανισμό. Για να είναι αποτελεσματικοί οι μηχανισμοί αυτοί, είναι σημαντικό να τεθούν σε εφαρμογή έτσι ώστε να εξασφαλιστεί η καλή επικοινωνία με τις υπόλοιπες λειτουργίες της Διαχείρισης Επικινδυνότητας και ασφάλειας. Διαφορετικά, για να εξασφαλιστεί ότι η αποτελεσματική Διαχείριση Επικινδυνότητα της ασφάλειας πληροφοριών δεν παρακάμπτεται ή υπονομεύεται από την έλλειψη αποτελεσματικών διαδικασιών και σε άλλους τομείς. Επίσης, αποτρέπει την επανάληψη προσπαθειών και ελαχιστοποιεί τα κενά στις λειτουργίες ασφαλείας, τα οποία μπορούν να επηρεάσουν αρνητικά τις δραστηριότητες προστασίας των πληροφοριών καθώς και άλλες περιοχές των λειτουργικών και επιχειρησιακών κινδύνων.

3.5.1 Διαδικασία Διαχείρισης Επικινδυνότητας

Η Διαχείριση Επικινδυνότητας είναι οι διαδικασίες αξιολόγησης, ξεχωριστές από την εκτίμηση του κινδύνου, των εναλλακτικών πολιτικών σε συνεργασία με τα ενδιαφερόμενα μέρη, λαμβάνοντας υπόψη την εκτίμηση του κινδύνου και άλλους παράγοντες, και επιλέγοντας τα κατάλληλα μέσα πρόληψης και ελέγχου σε αποδεκτά επίπεδα κόστους.

Η Διαχείριση Επικινδυνότητας αποτελείται από τις ακόλουθες διαδικασίες:

- Θέσπιση πεδίου δράσης και ορίων
- Αξιολόγηση του κινδύνου
- Χειρισμός κινδύνου
- Αποδοχή του εναπομένοντος κινδύνου
- Κοινοποίηση κινδύνων και παρακολούθηση.

Οι διαδικασίες αυτές καθορίζονται ως εξής:

Θέσπιση πεδίου δράσης και ορίων: Διαδικασία για την καθιέρωση συνολικών παραμέτρων για τις επιδόσεις της Διαχείρισης Επικινδυνότητας εντός οργανισμού. Και οι εσωτερικοί και οι εξωτερικοί παράγοντες πρέπει να ληφθούν υπόψη.

Αξιολόγηση του κινδύνου (Risk Assessment): Μια μεθοδική διαδικασία που αποτελείται από τρία βήματα: τον προσδιορισμό, την ανάλυση και την αξιολόγηση των κινδύνων.

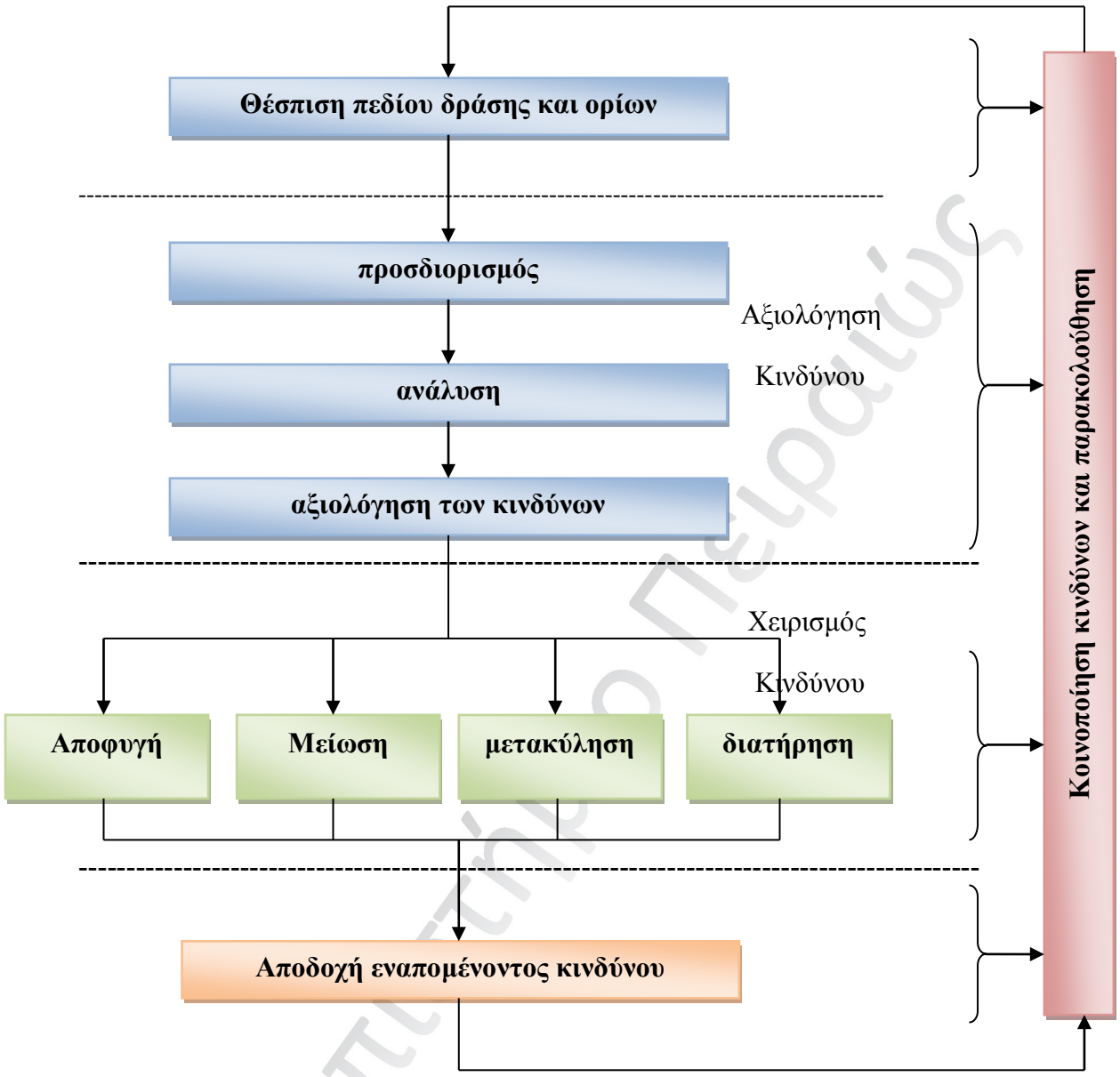
Χειρισμός κινδύνου (Risk treatment): Διαδικασία για την επιλογή των στρατηγικών για την αντιμετώπιση των κινδύνων, σύμφωνα με τον επιχειρησιακό κίνδυνο. Οι στρατηγικές αντιμετώπισης του κινδύνου είναι: *η αποφυγή*, με παύση των δραστηριοτήτων υψηλού κινδύνου, *η μείωση*, με την ανάπτυξη και την εφαρμογή ελέγχων, *η μετακύλιση των κινδύνων σε έναν τρίτο*, ο οποίος θα μπορούσε να είναι εντός ή εκτός του οργανισμού και *η διατήρηση* του κίνδυνου. Ο κίνδυνος συνήθως θα διατηρηθεί αν δεν υπάρχει οικονομικά αποδοτικός τρόπος για να μειωθεί, αν υπάρχει μικρή έκθεση ή πιθανές επιπτώσεις ή αν απλά δεν είναι εφικτό να αντιμετωπιστεί αποτελεσματικά.

Αποδοχή του εναπομένοντος κινδύνου (Acceptance of residual risk): Αποδοχή του κινδύνου μπορεί να οριστεί ως η λήψη απόφασης και έγκρισης από τη διοίκηση αποδοχής του συνεπαγόμενου κίνδυνου, αφού η διαδικασία αντιμετώπισης ολοκληρωθεί.

Κοινοποίηση κινδύνων και παρακολούθηση (Risk communication and monitoring): Μια διαδικασία για την ανταλλαγή και διακίνηση πληροφοριών που σχετίζονται με τον κίνδυνο καθώς και την ανασκόπηση της αποτελεσματικότητας όλης της διαδικασίας Διαχείρισης Επικινδυνότητας. Η κοινοποίηση των κινδύνων γίνεται συνήθως μεταξύ των υπευθύνων για την λήψη των αποφάσεων εντός και εκτός του οργανισμού. Μέσω της κοινοποίησης και παρακολούθησης είναι βέβαιο ότι το πεδίο εφαρμογής, τα όρια, οι κίνδυνοι και τα σχέδια δράσης παραμένουν επίκαιρα και ενημερώνονται συνεχώς.

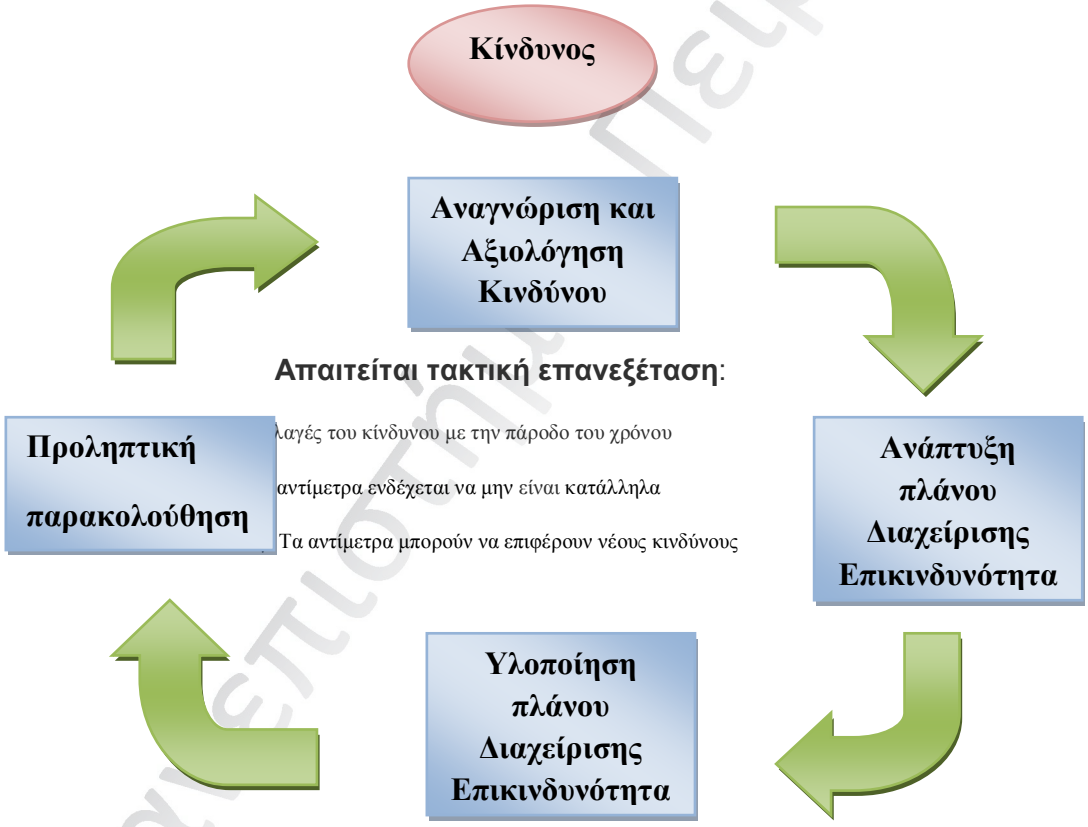
Η διαδικασία Διαχείρισης Επικινδυνότητας παρουσιάζεται στο επόμενο σχήμα 3.1

Σχήμα 3.1 Διαδικασία Διαχείρισης Επικινδυνότητας



Η ανάπτυξη μιας συστηματικής, αναλυτικής και συνεχούς διαδικασίας Διαχείρισης Επικινδυνότητας, όπως φαίνεται στο επόμενο σχήμα 3.2 είναι κρίσιμη για την επιτυχία κάθε προγράμματος για την ασφάλεια και πρέπει να εφαρμοστεί ως τυπική διαδικασία. Ο προσδιορισμός του σωστού ή κατάλληλου επίπεδου ασφάλειας εξαρτάται από τους πιθανούς κινδύνους που αντιμετωπίζει μια επιχείρηση και την ικανότητά της να τους αντιμετωπίσει. Οι κίνδυνοι αυτοί μπορεί να είναι μοναδικοί σε κάθε επιχείρηση και οι γενικεύσεις θα πρέπει να αποφεύγονται. Επιπλέον, ένα επαρκές πρόγραμμα ασφάλειας πληροφοριών γίνεται πιο ανταγωνιστικό με οργανωτικές, τεχνολογικές και επιχειρηματικές / λειτουργικές αλλαγές. Η Διαχείρισης Επικινδυνότητας πρέπει να είναι μια συνεχής και δυναμική διαδικασία για να εξασφαλιστεί ότι οι μεταβαλλόμενες απειλές και τα τρωτά σημεία θα αντιμετωπιστούν εγκαίρως.

Σχήμα 3.2 Συνεχόμενα στάδια Διαχείρισης Επικινδυνότητας



Επιπλέον, πρέπει να αναπτυχθούν διαδικασίες για την παρακολούθηση της κατάστασης των ελέγχων ασφαλείας και των αντίμετρων για να επιβεβαιωθεί η συνεχής αποτελεσματικότητά τους. Οι έλεγχοι συνήθως υποβαθμίζονται με την πάροδο του χρόνου και τείνουν στην

αποτυχία, επιβάλλοντας με τον τρόπο αυτό τη συνεχή παρακολούθηση και τον έλεγχο των περιοδικών ελέγχων.

Οι επιχειρήσεις κατά κανόνα χρησιμοποιούν την ακόλουθη διαδικασία για τον καθορισμό των αναγκαίων δραστηριοτήτων Διαχείρισης Επικινδυνότητας:

- Προσδιορισμός του προφίλ κινδύνου ενός οργανισμού
- Κατανόηση και τεκμηρίωση της φύσης και της έκτασης των κινδύνων
- Ο προσδιορισμός των προτεραιοτήτων της Διαχείρισης Επικινδυνότητας συνήθως επιτυγχάνεται μέσω:

  α. Προσδιορισμός της πιθανότητας των απειλών.

  β. Προσδιορισμός της ποσοτικής (χρηματική) και ποιοτικής (επίδραση) αξίας των κρίσιμων πληροφοριών / περιουσιακών στοιχείων, τα οποία το πρόγραμμα ασφαλείας είναι σε θέση να προστατεύσει

  γ. Προσδιορισμός των επιπτώσεων στην επιχείρηση εάν ένα τρωτό σημείο εκμεταλλευτεί επιτυχώς από την απειλή.

Ο διαχειριστής της ασφάλειας πληροφοριών θα πρέπει να καθιερώσει μια τακτική διαδικασία κατά την οποία οι εκτιμήσεις κινδύνου διενεργούνται στο επίπεδο συστημάτων και εφαρμογών του οργανισμού. Η διασφάλιση ότι υπάρχουν μετρήσεις για να εκτιμήσουν τον κίνδυνο και την αποτελεσματικότητα των μέτρων ασφαλείας είναι μέρος της ευθύνης του διαχειριστή της ασφάλειας πληροφοριών. Ο διαχειριστής της ασφάλειας πληροφοριών θα πρέπει επίσης να διερευνά και να συστήνει στους ιδιοκτήτες των περιουσιακών στοιχείων την χρήση αυτοματοποιημένων τεχνικών για την παρακολούθηση των κινδύνων του οργανισμού. Αυτή η διαδικασία αξιολόγησης των κινδύνων είναι ιδιαίτερα σημαντική, δεδομένου ότι είναι αναγκαίο να επικεντρωθούν οι δραστηριότητες της ασφάλειας του οργανισμού σε θέματα που έχουν τη μεγαλύτερη επίπτωση και σημασία.

3.5.2 Ορισμός πλαισίου Διαχείρισης Επικινδυνότητας.

Για να αναπτύξει μία επιχείρηση ένα συστηματικό πρόγραμμα Διαχείρισης Επικινδυνότητας θα πρέπει να χρησιμοποιηθεί ένα πλαίσιο ασφάλειας πληροφοριών ως μοντέλο αναφοράς και να προσαρμοστεί στις συνθήκες του οργανισμού. Αρκετές εξαιρετικές δημοσιεύσεις / πρότυπα είναι διαθέσιμα για την παροχή καθοδήγησης σχετικά με την τεχνολογία των πληροφοριών και τις προσεγγίσεις για τη Διαχείριση Επικινδυνότητας. Μερικά παραδείγματα περιλαμβάνουν:

- CobiT 4.1
- Draft ISO 3100 Risk Management - Guidelines on principles and implementation of risk management

- NIST's Risk Management Guide for Information Technology Systems, Special Publication 800-30
- AS/NZS 4360:2004 Risk Management Standard
- HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004
- Emerging ISO Standard 27005 Information Security Management

Τα πρότυπα που αναφέρονται παραπάνω έχουν παρόμοιες απαιτήσεις διαχείρισης κινδύνων, συμπεριλαμβανομένων:

Πολιτικές (Policies). Η ανάγκη των ανώτερων στελεχών ενός οργανισμού να προσδιορίσουν και να τεκμηριώσουν την πολιτική της επιχείρησης για τη Διαχείρισης Επικινδυνότητας, συμπεριλαμβανομένων των στόχων και των δεσμεύσεων της. Η πολιτική πρέπει να είναι συναφής με το στρατηγικό πλαίσιο, τους στόχους, τους σκοπούς και τη φύση των δραστηριοτήτων της επιχείρησης. Η διοίκηση πρέπει να διασφαλίσει ότι η πολιτική αυτή έχει γίνει αντιληπτή, εφαρμόζεται και διατηρείται σε όλα τα επίπεδα του οργανισμού.

Σχεδιασμός και διάθεση πόρων (planning and resourcing). Η επιχείρηση πρέπει να διασφαλίσει ότι το πρόγραμμα έχει καθιερωθεί και τηρείται. Η Απόδοση θα πρέπει να αναφέρεται στη διοίκηση και να χρησιμοποιείται ως βάση για βελτίωση. Η ευθύνη, η εξουσία και οι αλληλεξαρτήσεις του προσωπικού, που εκτελεί και ελέγχει τις εργασίες που αφορούν τη Διαχείριση Επικινδυνότητας, θα πρέπει να καθορίζονται και να τεκμηριώνονται. Ο οργανισμός πρέπει να αναγνωρίζει τους απαιτούμενους πόρους και να διευκολύνει την εφαρμογή των προγραμμάτων Διαχείρισης Επικινδυνότητας, μέσω της ανάθεσης στο εκπαιδευμένο προσωπικό, της συνεχόμενης διαχείρισης των δραστηριοτήτων και των δραστηριοτήτων ελέγχου, για εσωτερική επανεξέταση.

Πρόγραμμα υλοποίησης (Implementation Program). Η επιχείρηση θα πρέπει να καθορίσει τα βήματα που απαιτούνται για να εφαρμόσει – υλοποιήσει ένα αποτελεσματικό σύστημα Διαχείρισης Επικινδυνότητας.

Επανεξέταση από την διοίκηση (Management review). Η εκτελεστική διαχείριση θα πρέπει να εξασφαλίζει την επανεξέταση του συστήματος Διαχείρισης Επικινδυνότητας σε συγκεκριμένα χρονικά διαστήματα, ικανά για να εξασφαλίσουν τη διατήρηση της σταθερότητας και της αποτελεσματικότητας της στην ικανοποίηση των απαιτήσεων του προγράμματος. Οι εγγραφές αυτών των επανεξετάσεων πρέπει να διατηρούνται.

Διαδικασία Διαχείρισης Επικινδυνότητας (Risk management process). Η Διαχείριση Επικινδυνότητας μπορεί να εφαρμοστεί σε πολλά επίπεδα στην οργάνωση, τόσο σε στρατηγικό όσο και σε λειτουργικό επίπεδο. Μπορεί επίσης να εφαρμοστεί σε συγκεκριμένους τομείς, προϊόντα / υπηρεσίες, επιχειρήσεις / IT διαδικασίες, έργα, αποφάσεις, πλατφόρμες και εφαρμογές. Η επιχείρηση πρέπει να δώσει προτεραιότητα στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα ανάλογα με το προφίλ της και το κανονιστικό πλαίσιο.

Έγγραφα Διαχείρισης Επικινδυνότητας (Risk management documentation) Για κάθε στάδιο της διαδικασίας, θα πρέπει να τηρούνται τα κατάλληλα αρχεία που είναι επαρκή για κάθε ανεξάρτητο έλεγχο.

Με τη θέσπιση του πλαισίου για τη Διαχείριση Επικινδυνότητας, καθορίζονται οι βασικές παράμετροι εντός των οποίων οι κίνδυνοι πρέπει να διαχειριστούν και να αντιμετωπιστούν. Συνεπώς, το πεδίο εφαρμογής για το υπόλοιπο της διαδικασίας Διαχείρισης Επικινδυνότητας έχει καθοριστεί: Περιλαμβάνει τον προσδιορισμό των βασικών υπολογισμών των εξωτερικών και εσωτερικών συνθηκών του περιβάλλοντος του οργανισμού και τους γενικούς στόχους και δραστηριότητες της διαδικασίας Διαχείρισης Επικινδυνότητας. Αν και ο καθορισμός του πεδίου εφαρμογής και το πλαίσιο του προγράμματος είναι θεμελιώδη για την καθιέρωση της Διαχείρισης Επικινδυνότητας, είναι ανεξάρτητα από τη συγκεκριμένη δομή της διαχείρισης, τις μεθόδους και τα εργαλεία που θα χρησιμοποιηθούν για την υλοποίηση του.

Προκειμένου να καθοριστεί ένα αποτελεσματικό πλαίσιο, είναι σημαντικό να:

- Γίνει αντιληπτό το υπόβαθρο της επιχείρησης και των κινδύνων της (π.χ. βασικές διαδικασίες, πολύτιμα περιουσιακά στοιχεία, ανταγωνιστικές περιοχές, κλπ.)
- Γίνει αξιολόγηση των δραστηριοτήτων της Διαχείρισης Επικινδυνότητας που έχουν ανατεθεί μέχρι στιγμής.
- Ανάπτυξη δομής για τις πρωτοβουλίες και τους ελέγχους που θα ακολουθήσει η Διαχείριση Επικινδυνότητας (αντίμετρα, ελέγχους ασφαλείας κ.λπ.). Η προσέγγιση αυτή είναι χρήσιμη για:
    a. Την αποσαφήνιση και την κοινή κατανόηση των οργανωτικών στόχων.
    b. Τον Προσδιορισμό του περιβάλλοντος στο οποίο καθορίζονται οι στόχοι αυτοί
    c. Τον καθορισμός του κύριου πεδίου εφαρμογής και των στόχων της Διαχείρισης Επικινδυνότητας, των περιορισμών ή των ειδικών προϋποθέσεων και των αποτελεσμάτων που απαιτούνται.
    d. Την ανάπτυξη ενός συνόλου κριτηρίων, βάσει των οποίων οι κίνδυνοι θα πρέπει να υπολογίζονται
    e. Τον καθορισμό ενός συνόλου βασικών στοιχείων για τη διάρθρωση του εντοπισμού των κινδύνων και τη διαδικασία αξιολόγησης τους.

Ένας οργανισμός πρέπει να ενσωματώσει τη Διαχείριση Επικινδυνότητας στο πλαίσιο του συνολικού συστήματος διαχείρισης και να προσαρμόσει τα διάφορα στοιχεία όπως είναι οι πολιτικές, οι επιχειρησιακές διαδικασίες, οι ευθύνες, οι πόροι και οι μέθοδοι επικοινωνίας, με συγκεκριμένες ανάγκες τους.

Οι υπάρχουσες διαδικασίες και πρακτικές διαχείρισης των επιχειρήσεων περιλαμβάνουν στοιχεία της Διαχείρισης Επικινδυνότητας και πολλοί οργανισμοί έχουν ήδη υιοθετήσει μια επίσημη διαδικασία Διαχείρισης Επικινδυνότητας για συγκεκριμένα είδη κινδύνου ή περιστάσεις. Αυτά πρέπει να επανεξεταστούν και να αξιολογηθούν.

3.6.3 Ορισμός του εξωτερικού περιβάλλοντος

Ο ορισμός του εξωτερικού περιβάλλοντος περιλαμβάνει τον προσδιορισμό του περιβάλλοντος στο οποίο δραστηριοποιείται ο οργανισμός, καθώς και τον ορισμό της σχέσης μεταξύ του περιβάλλοντος και του ίδιου του οργανισμού.

Το εξωτερικό περιβάλλον περιλαμβάνει συνήθως:

- Την τοπική αγορά, την επιχείρηση, το ανταγωνιστικό, οικονομικό και πολιτικό περιβάλλον
- Τους νόμους και το ρυθμιστικό περιβάλλον
- Τις κοινωνικές και πολιτιστικές συνθήκες
- Τα εξωτερικά ενδιαφερόμενα μέρη

Είναι επίσης πολύ σημαντικό να αξιολογηθούν δεόντως και να ληφθούν υπόψη τόσο οι αντιλήψεις και οι αξίες των διαφόρων ενδιαφερομένων μερών όσο και οι έξωθεν απειλές ή ευκαιρίες που δημιουργούνται.

3.6.4 Ορισμός του εσωτερικού περιβάλλοντος

Όπως σε κάθε σημαντική επιχειρηματική διαδικασία, το προαπαιτούμενο είναι να κατανοήσουμε την ίδια την οργάνωση. Οι βασικοί τομείς που πρέπει να αξιολογηθούν προκειμένου να παρέχουν μια ολοκληρωμένη εικόνα του εσωτερικού περιβάλλοντος του οργανισμού περιλαμβάνουν:

- Τους βασικούς μοχλούς των επιχειρήσεων (π.χ. δείκτες της αγοράς, βελτίωση του ανταγωνισμού, ελκυστικότητα του προϊόντος, κλπ.)
- Τα αδύνατα και δυνατά σημεία του οργανισμού, τις ευκαιρίες και τις απειλές
- Τους εσωτερικούς παράγοντες
- Την οργανωτική δομή και νοοτροπία
- Τα περιουσιακά στοιχεία όσον αφορά τους πόρους (δηλ. τους ανθρώπους, τα συστήματα, τις διαδικασίες, το κεφάλαιο, κλπ.)
- Τους σκοπούς, τους στόχους και τις στρατηγικές που έχουν ήδη θεσπιστεί για την επίτευξή τους.

3.6.5 Δημιουργία περιεχομένου Διαχείρισης Επικινδυνότητας

Όσον αφορά τις επιχειρήσεις, η Διαχείριση Επικινδυνότητας ως διαδικασία θα πρέπει να παρέχει μια ισορροπία ανάμεσα στο κόστος, τα οφέλη και τις ευκαιρίες. Ως εκ τούτου, είναι

απαραίτητο να σκιαγραφηθεί το κατάλληλο πλαίσιο, και να ρυθμιστεί σωστά το πεδίο εφαρμογής και τα όρια της διαδικασίας αυτής.

Η θέσπιση του πλαισίου Διαχείρισης Επικινδυνότητας συνεπάγεται τον προσδιορισμό:

- της οργάνωσης, των διαδικασιών, της αποστολής ή της δραστηριότητας (τα οποία πρέπει να αξιολογηθούν) και της θέσπισης των σκοπών και των στόχων αυτής.
- της διάρκεια του έργου, της δραστηριότητας ή λειτουργίας
- του πλήρους πεδίου των δραστηριοτήτων της Διαχείρισης Επικινδυνότητας που πρέπει να πραγματοποιηθούν, διευκρινίζοντας τις ενδεχόμενες προσθήκες και εξαιρέσεις
- τους ρόλους και τις αρμοδιότητες των διαφόρων τμημάτων του οργανισμού που συμμετέχουν στη διαδικασία διαχείρισης
- τις εξαρτήσεις μεταξύ του έργου ή της δραστηριότητας με άλλα έργα ή τμήματα της επιχείρησης.

Τα κριτήρια με τα οποία αξιολογούνται οι κίνδυνοι πρέπει να αποφασιστούν και να συμφωνηθούν. Η απόφαση για το πότε απαιτείται η διαχείριση του κινδύνου συνήθως βασίζεται σε επιχειρησιακά, τεχνικά, οικονομικά, κανονιστικά, νομικά, κοινωνικά ή περιβαλλοντικά κριτήρια ή ακόμα και σε ενδεχόμενους συνδυασμούς τους. Τα κριτήρια θα πρέπει να ευθυγραμμίζονται με το πεδίο εφαρμογής και την ποιοτική ανάλυση των εσωτερικών πολιτικών και των διαδικασιών της επιχείρησης καθώς και να υποστηρίζουν τους σκοπούς και τους στόχους της.

Σημαντικά κριτήρια που πρέπει να εξεταστούν είναι:

- Επιπτώσεις και τα είδη των συνεπειών
- Τα κριτήρια των πιθανοτήτων
- Οι κανόνες που θα καθορίσουν κατά πόσο το επίπεδο του κινδύνου είναι τέτοιο ώστε να απαιτούνται περαιτέρω δραστηριότητες.

Είναι πολύ σύνηθες ότι τα κριτήρια που προσδιορίζονται κατά τη διάρκεια αυτών των βημάτων αναπτύσσονται ή ακόμα και τροποποιούνται περαιτέρω στις μεταγενέστερες φάσεις της διαδικασίας Διαχείρισης Επικινδυνότητας.

3.7 Εκτίμηση κινδύνου και ανάλυση μεθοδολογίας

Δεν υπάρχει σωστή ή λανθασμένη προσέγγιση για την επιλογή της μεθοδολογίας για τη διενέργεια αξιολόγησης του κινδύνου. Ωστόσο, τα αποτελέσματα πρέπει να συνάδουν με τους σκοπούς και τους στόχους του οργανισμού για τον εντοπισμό της σχετικής αξιολόγησης του κινδύνου των περιουσιακών στοιχείων που είναι ζωτικής σημασίας για την επιχείρηση. Η εκτίμηση κινδύνου είναι η διαδικασία ανάλυσης των απειλών και των τρωτών σημείων των

συστημάτων πληροφοριών που θέτουν σε κίνδυνο τα περιουσιακά στοιχεία πληροφόρησης του οργανισμού. Σε συνδυασμό είτε με την ανάλυση BIA είτε με πληροφορίες ταξινόμησης των περιουσιακών στοιχείων για τον προσδιορισμό της κρισιμότητας, η προκύπτουσα ανάλυση χρησιμοποιείται ως βάση για τον προσδιορισμό των κατάλληλων και οικονομικά αποτελεσματικών ελέγχων ή σαν αντίμετρο για τον μετριασμό των αναγνωρισμένων κινδύνων.

Οι διαφορές μεταξύ της "ανάλυσης", της "αξιολόγησης" και της "διαχείρισης" των δραστηριοτήτων σε σχέση με τα πληροφοριακά συστήματα είναι:

- Η ανάλυση κινδύνου είναι η εξέταση των πληροφοριών με σκοπό την αναγνώριση του κινδύνου ενός πληροφοριακού συστήματος.
- Η αξιολόγηση του κινδύνου είναι η επίσημη περιγραφή και η αξιολόγηση του κινδύνου ενός πληροφοριακού συστήματος
- Η διαχείριση του κινδύνου είναι η διαδικασία προσδιορισμού και εφαρμογής αντιμέτρων ανάλογα με την αξία των προστατευόμενων περιουσιακών στοιχείων βάσει της αξιολόγησης του κινδύνου.

Στο ακόλουθο σχήμα 3.3 παρουσιάζεται η σχέση μεταξύ της ανάλυσης, της αξιολόγησης και της διαχείρισης επικινδυνότητας.

Σχήμα 3.3 Ανάλυση, αξιολόγηση και της διαχείριση επικινδυνότητας

Περιοχές Κινδύνου	Αξιολόγηση κινδύνου	Διαχείριση Επικινδυνότητας
Η ανάλυση κινδύνου είναι η αναγνώριση και η εκτίμηση των κινδύνων.	Η αξιολόγηση του κινδύνου ορίζεται ως η διαδικασία για τον εντοπισμό και την ιεράρχηση των κίνδυνων στην επιχείρηση. Αναφέρεται κυρίως στη "φάση αξιολόγησης του κινδύνου" στο πλαίσιο του ευρύτερου τομέα της Διαχείριση Επικινδυνότητας. Η ανάλυση κινδύνου αποτελεί μέρος της αξιολόγησης κινδύνου.	Η διαχείριση επικινδυνότητας είναι η συνολική προσπάθεια για τη διαχείριση του κινδύνου σε αποδεκτά επίπεδα στην επιχείρηση. Αποτελείται από 4 βασικές φάσεις: **Εκτίμηση του κινδύνου**, την **υποστήριξης αποφάσεων**, την **εφαρμογή των ελέγχων** και τη **μέτρηση της αποτελεσματικότητας του προγράμματος.** Το ISO / IEC Guide 73:2002 την ορίζει ως: "συντονισμένες δραστηριότητες για την καθοδήγηση και τον έλεγχο ενός οργανισμού, όσον αφορά τον κίνδυνο." Στο AS / NZS 4360:1999 ορίζεται ως “η συστηματική εφαρμογή των πολιτικών διαχείρισης, διαδικασιών και πρακτικών για τη θέσπιση του πλαισίου, τον εντοπισμό, την ανάλυση, την

		αξιολόγηση, τη αντιμετώπιση, την παρακολούθηση και ενημέρωση του κινδύνου. “ Σημείωση: Η διαχείριση κινδύνων συνήθως περιλαμβάνει την αξιολόγηση του κινδύνου, την αντιμετώπιση του κινδύνου, την αποδοχή και την ενημέρωση.
Τυπικές ερωτήσεις για την ανάλυση του κινδύνου (κατανόηση της αιτίας του προβλήματος): • Τι προκάλεσε το πρόβλημα; • Τι επηρεάζει; • Ποιό είναι το κόστος; • Ποιος είναι ο υπεύθυνος για την αποκατάσταση; • Ποια λύση θα διορθώσει το πρόβλημα; • Αξίζει η επίλυση περαιτέρω διερεύνηση • Τα προβλήματα αυτά προκύπτουν από αναποτελεσματικές διαδικασίες των επιχειρήσεων, κακή διαχείριση ή ανεπαρκή ικανότητα των εργαζομένων;	Τυπικές ερωτήσεις για την αξιολόγηση του κινδύνου: • Ποιο είναι το πρόβλημα; • Πόσο σημαντικό είναι αυτό; • Τι θα συμβεί αν αγνοήσουμε το πρόβλημα;	

3.8 Αξιολόγηση Κινδύνου

Στο πλαίσιο για την αξιολόγηση κινδύνου που περιγράφεται στην COBIT, όπως απεικονίζεται στο επόμενο σχήμα 3.4, το πρώτο βήμα για την εκτέλεση της αξιολόγησης είναι ο **προσδιορισμός και η αποτίμηση** των περιουσιακών στοιχείων.

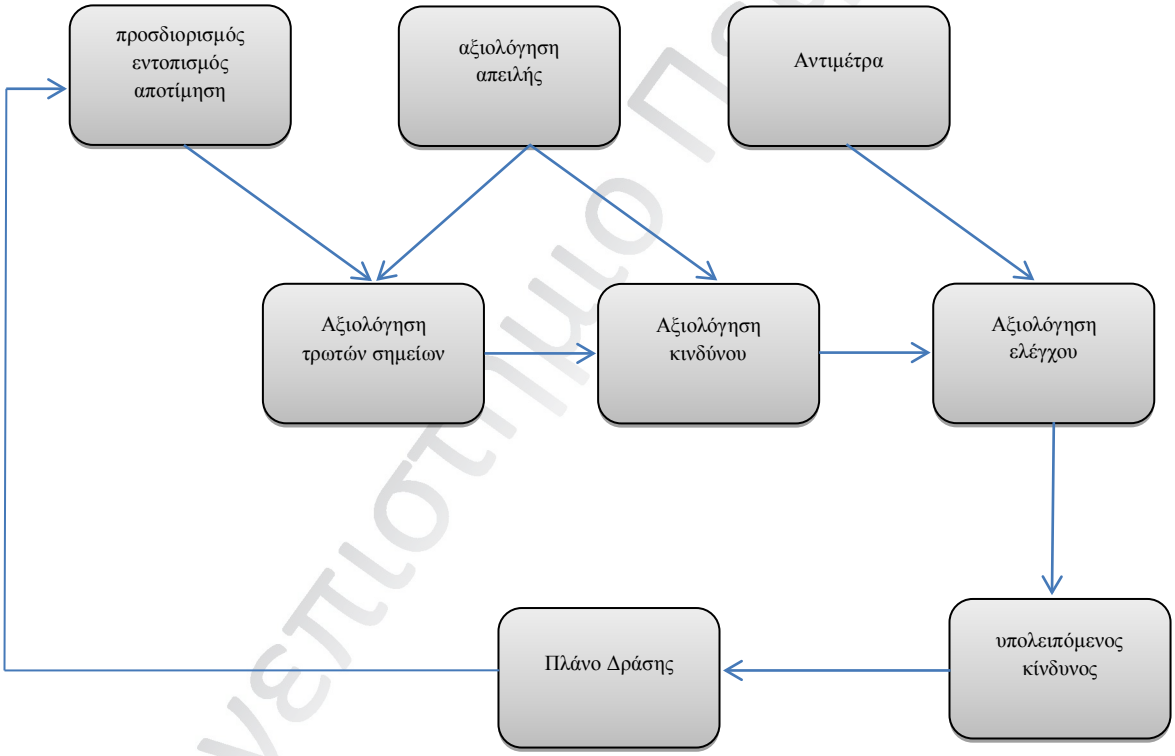
Προφανώς, αν η αξία τους είναι χαμηλή, ο κίνδυνος δεν θεωρείται σημαντικός και έλλειψη σχετικών ελέγχων ή αντίμετρων είναι δικαιολογημένη.

Υποθέτοντας ότι ένα περιουσιακό στοιχείο είναι μεγάλης αξίας, το επόμενο στοιχείο που πρέπει να εξεταστεί είναι ο **προσδιορισμός των τρωτών σημείων** που υφίστανται. Αν υπάρχουν τρωτά σημεία, πρέπει να γίνει **εκτίμηση των απειλών**.

Αν το περιουσιακό στοιχείο έχει αξία καθώς και τρωτά σημεία επιρρεπή σε απειλές, τότε υπάρχει κίνδυνος.

Είναι προφανές ότι τρωτά σημεία για τα οποία δεν υπάρχουν απειλές δεν ενέχουν κανένα κίνδυνο. Εναλλακτικά, όσο μεγαλύτερη είναι η αξία, ο αριθμός και ο βαθμός των τρωτών σημείων, σε συνδυασμό με την αύξηση του αριθμού των απειλών, τόσο μεγαλύτερος ο κίνδυνος.

Σχήμα 3.4: Πλαίσιο Ανάλυσης Κινδύνου



Υπάρχουν πολλά μοντέλα Διαχείριση Επικινδυνότητας και διαθέσιμες προσεγγίσεις αξιολόγησης στο διαχειριστή της ασφάλειας πληροφοριών. Η προσέγγιση που θα επιλεχθεί θα πρέπει να καθορίζεται από το καλύτερη εφαρμογή και λειτουργία στην επιχείρηση. Μερικές από τις προσεγγίσεις είναι: COBIT, OCTAVE, NIST 800-30, AS / NZS 4360-2005, ITIL, CRAMM. Υπάρχουν και άλλες προσεγγίσεις, όπως η factor analysis of information

risk (FAIR), risk factor analysis, value at risk (VAR) κλπ. οι οποίες ενδεχομένως να είναι περισσότερο κατάλληλες, ανάλογα με την επιχείρηση και τις ειδικές απαιτήσεις.

Σημείωση: οι διαχειριστές της ασφάλειας πληροφοριών θα πρέπει να έχουν ευρεία γνώση της ύπαρξης των διαφόρων μεθόδων για τον προσδιορισμό της κατάλληλης προσέγγισης ή συνδυασμού των προσεγγίσεων αυτών για την εκάστοτε επιχείρηση τους.

Η προσέγγιση της εκτίμησης κινδύνου που αναπτύχθηκε από το NIST αποτελεί μια καλά αναπτυγμένη και ολοκληρωμένη μεθοδολογία. Ενώ κατά κύριο λόγο είναι προσανατολισμένη στο IT, μπορεί να διευρυνθεί το πεδίο εφαρμογής της και να συμπεριλάβει και άλλα είδη κινδύνων.

3.8.1 Μεθοδολογία Αξιολόγησης Κινδύνου NIST

Η μεθοδολογία αξιολόγησης των κινδύνων περιλαμβάνει εννέα βήματα:

Βήμα 1 - Χαρακτηρισμός Συστήματος (ή τομέα)

Βήμα 2 – Αναγνώριση απειλής

Βήμα 3 - Αναγνώριση ευπάθειας

Βήμα 4 - Ανάλυση ελέγχων

Βήμα 5 - Προσδιορισμός Πιθανοτήτων

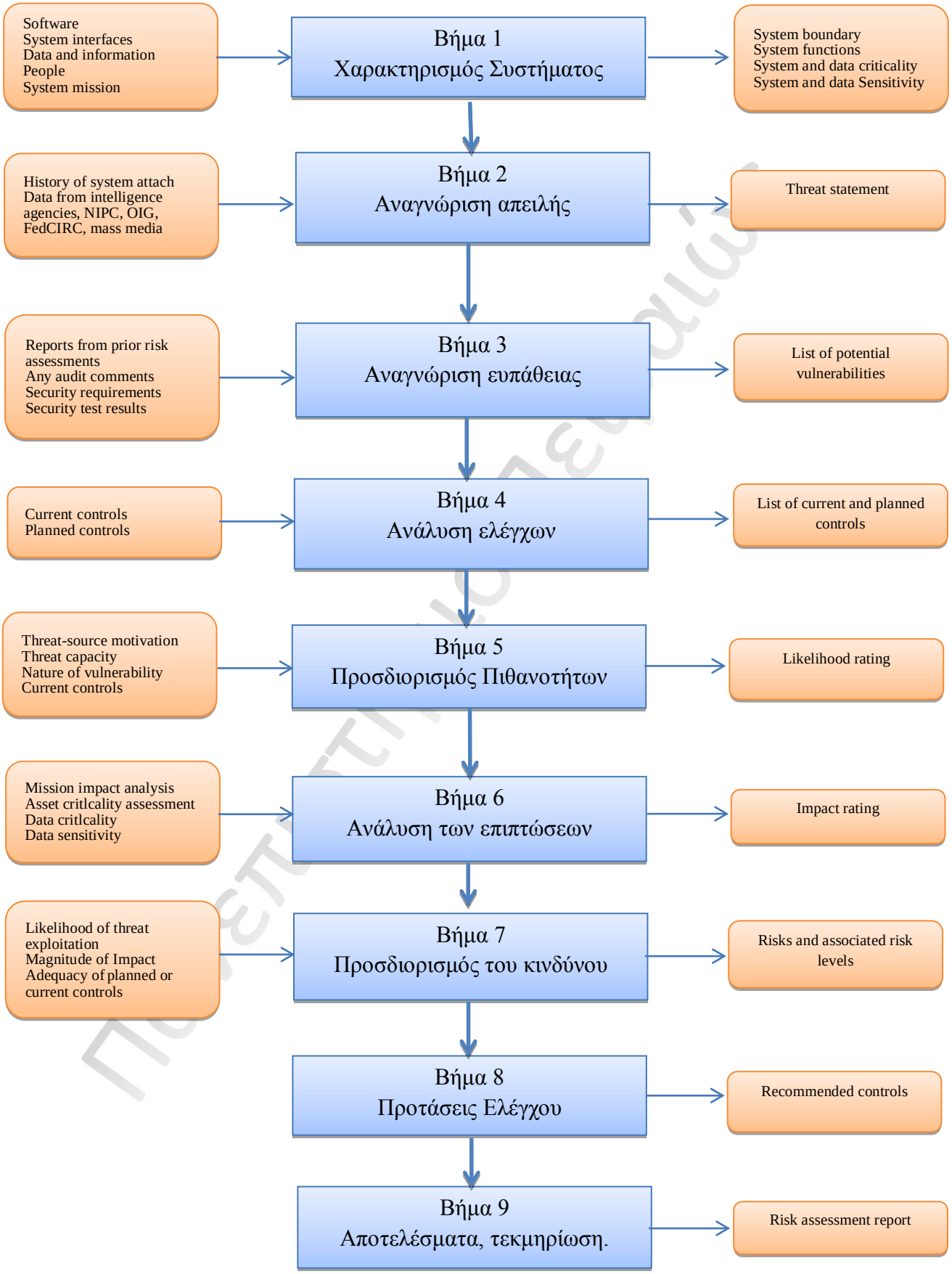
Βήμα 6 - Ανάλυση των επιπτώσεων

Βήμα 7 - Προσδιορισμός του κινδύνου

Βήμα 8 – Προτάσεις Ελέγχου

Βήμα 9 – Αποτελέσματα, τεκμηρίωση.

Σχήμα 3.5: Μεθοδολογία Αξιολόγησης Κινδύνου NIST



3.8.2 Συσσωρευμένος και διαδοχικός κίνδυνος

Ένα άλλο στοιχείο που πρέπει να εξεταστεί είναι ο συσσωρευμένος κίνδυνος. Μπορεί να υπάρχουν περιπτώσεις που μια συγκεκριμένη απειλή επηρεάζει ένα μεγάλο αριθμό μικρής σημασίας τρωτών σημείων που, στο σύνολό τους, μπορεί να έχουν σημαντικό αντίκτυπο. Μια άλλη πιθανότητα είναι ότι ένας μεγάλος αριθμός των απειλές μπορούν να επηρεάσουν ταυτόχρονα μια σειρά μικρής σημασίας τρωτά σημεία, με αποτέλεσμα ένα μεγάλο κίνδυνο συνολικά. Σε αυτήν την περίπτωση, είναι δυνατό για ένα σύνολο κινδύνων, οι οποίοι είναι αποδεκτοί μεμονωμένα, να έχουν καταστροφικές επιπτώσεις συνολικά.

Οι διαδοχικοί κίνδυνοι μπορούν επίσης να φανερώσουν αρνητικές επιπτώσεις, ως αποτέλεσμα ανεπάρκειας, η οποία μπορεί να οδηγήσει σε μια αλυσιδωτή αντίδραση αποτυχιών (Στην ανατολική ακτή των Ηνωμένων Πολιτειών, μια βλάβη σε ένα μικρό δίκτυο ηλεκτροδότησης στις μεσοδυτικές πολιτείες προκάλεσε έναν καταιγισμό από βλάβες σε όλο το δίκτυο ρεύματος, πλήττοντας τελικά το μεγαλύτερο βορειοανατολικό κομμάτι των Ηνωμένων Πολιτειών). Ομοίως, στο βαθμό που τμήματα της πληροφορικής της επιχείρησης και άλλες δραστηριότητες έχουν στενά συνδεδεμένες εξαρτήσεις, ο διευθυντής της ασφάλειας πληροφοριών πρέπει να εξετάσει πώς κάποια συγκεκριμένη βλάβη ή συνδυασμός από βλάβες θα επηρεάσουν τα εξαρτώμενα τα συστήματα.

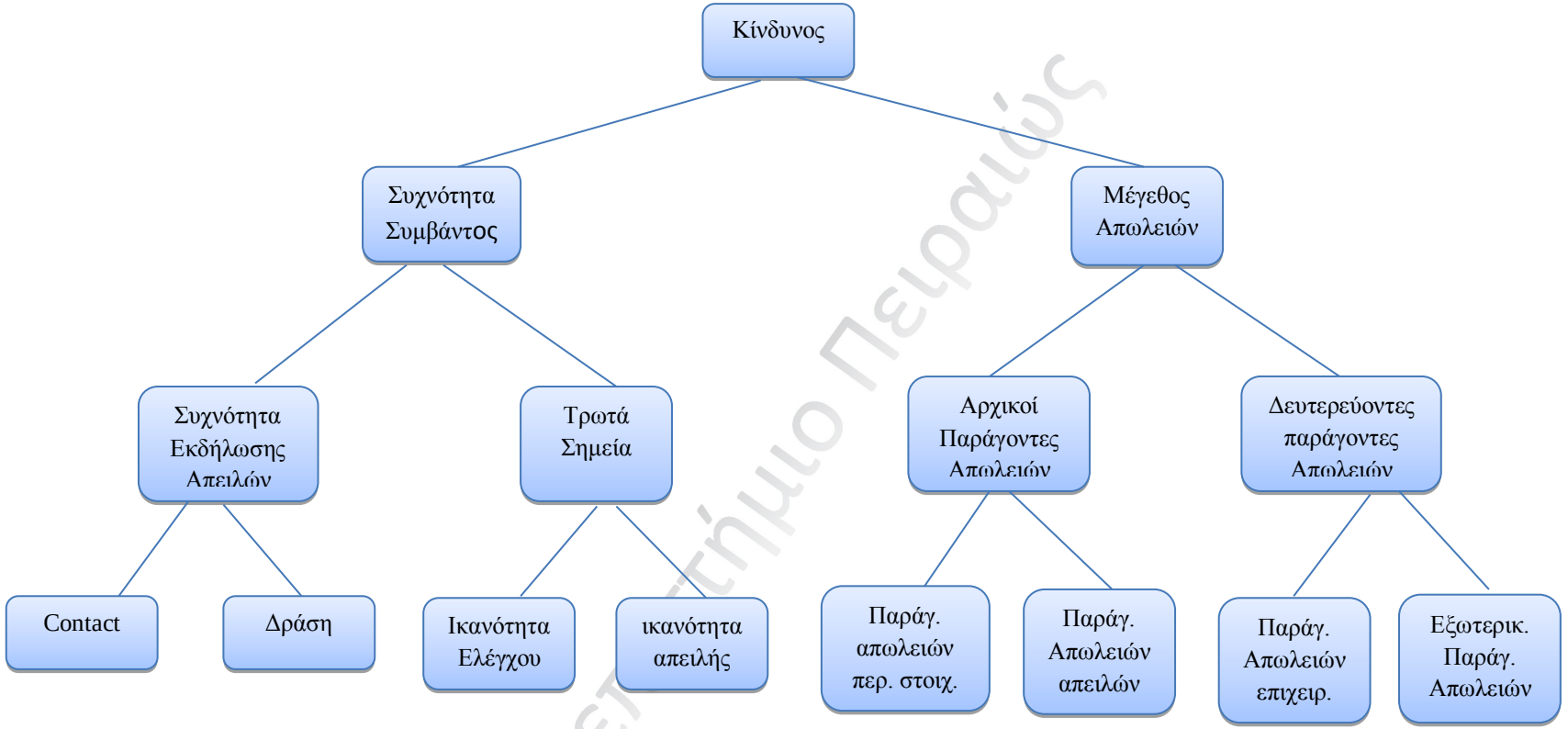
3.8.3 Άλλες προσεγγίσεις αξιολόγησης του κινδύνου.

Οι εξελίξεις κατά τη διάρκεια των τελευταίων δεκαετιών έχουν οδηγήσει σε σημαντικές βελτιώσεις σε ορισμένους τομείς για τον καθορισμό των ορίων των πιθανών κινδύνων. Ωστόσο, λίγοι από αυτούς αντιμετωπίζουν άμεσα και αποτελεσματικά τους κινδύνους της ασφάλειας πληροφοριών. Μερικοί αρχίζουν να πιστεύουν στην υιοθέτηση μέτρων στον τομέα της ασφάλειας των πληροφοριών και είναι πιθανό ότι τα επόμενα χρόνια θα επικρατήσει η χρήση των πιο εξελιγμένων τεχνικών και μεθόδων. Μερικές από τις μεθόδους αυτές περιγράφονται στην ακόλουθη ενότητα.

Factor Analysis of Information Risk

Μια πολλά υποσχόμενη προσέγγιση για την αποσύνθεση των κινδύνων και την κατανόηση των συστατικών τους είναι η Factor Analysis of Information Risk (FAIR). Η προσέγγιση αυτή προσφέρει μια αιτιολογημένη, λεπτομερή ανάλυση της διαδικασίας, όπως παρουσιάζεται και στο ακόλουθο σχήμα 3.6:

Σχήμα 3.6: Factor Analysis of Information Risk (FAIR)



Η FAIR παρέχει τα ακόλουθα:

- **Ταξινόμηση** των παραγόντων που συνθέτουν τον κίνδυνο πληροφοριών. Αυτή η ταξινόμηση παρέχει μια θεμελιώδη κατανόηση του κινδύνου των πληροφοριών, χωρίς την οποία δεν μπορούμε να προχωρήσουμε στα υπόλοιπα βήματα. Παρέχει επίσης μια σειρά τυποποιημένων ορισμών για τους όρους.
- **Μια μέθοδος για τη μέτρηση** των παραγόντων του κινδύνου των πληροφοριών, συμπεριλαμβανομένης της Συχνότητα Εκδήλωσης Απειλών, των Τρωτών Σημείων και των απωλειών.
- **Μια υπολογιστική μηχανή** που εξάγει τον κίνδυνο, προσομοιώνοντας μαθηματικά τις σχέσεις μεταξύ των παραγόντων.
- **Ένα μοντέλο προσομοίωσης** που επιτρέπει στο χρήστη να εφαρμόσει την ταξινόμηση, τη μέθοδο μέτρησης και την υπολογιστική μηχανή για να δομήσουν και να αναλύσουν τα σενάρια κινδύνου σχεδόν οποιουδήποτε μεγέθους και πολυπλοκότητας.

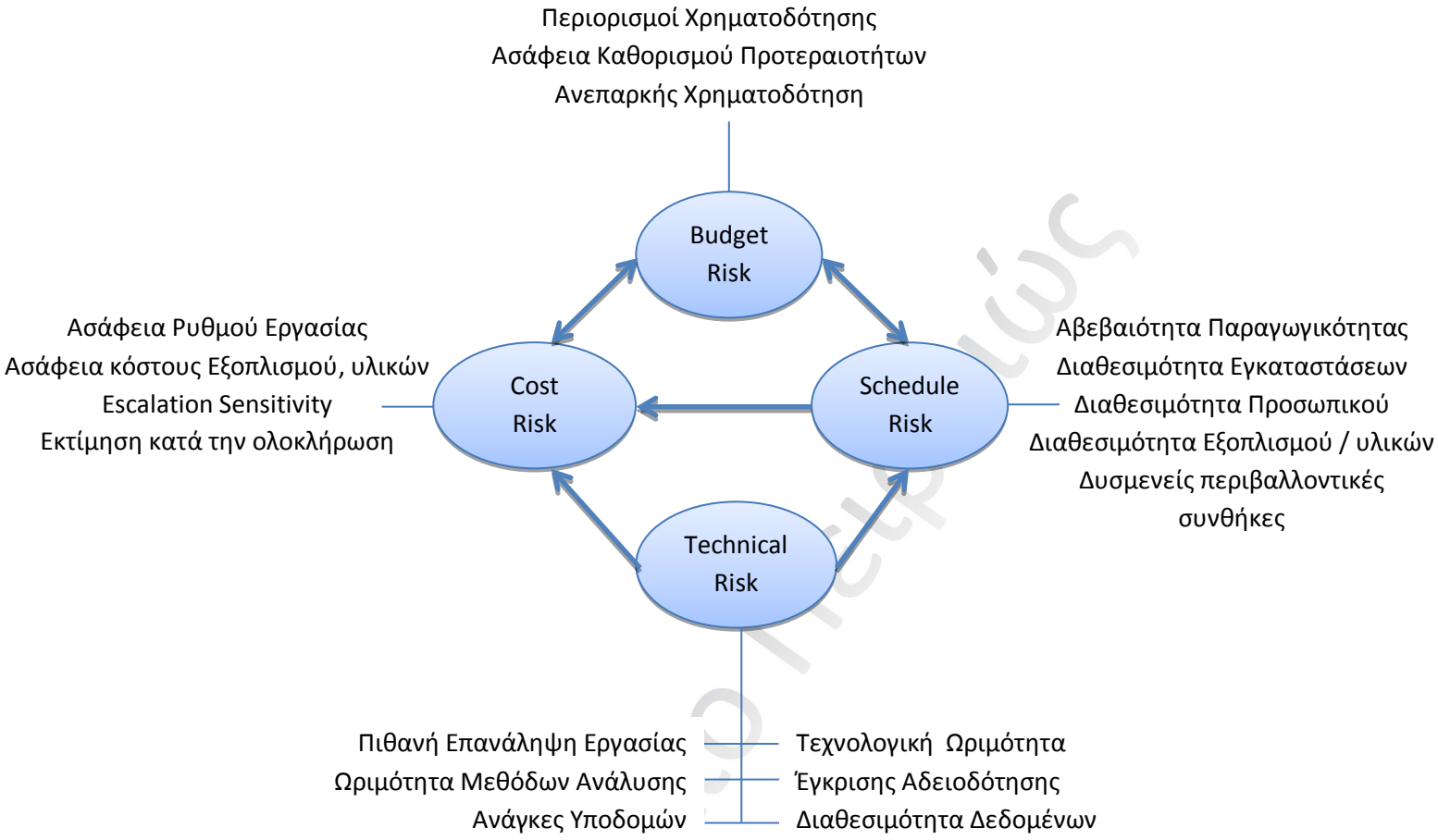
Υπάρχουν τέσσερις κύριες συνιστώσες της ταξινόμησης των κινδύνων για τις οποίες κάποιος θέλει να προσδιορίσει τα χαρακτηριστικά του παράγοντα απειλής, χαρακτηριστικά που επηρεάζουν:

- Την συχνότητα με την οποία οι παράγοντες κινδύνου έρχονται σε επαφή με έναν οργανισμό ή τα περιουσιακά του στοιχεία
- Την πιθανότητα ότι οι παράγοντες κινδύνου θα δράσουν κατά ενός οργανισμού
- Την πιθανότητα οι ενέργειες των απειλών να είναι επιτυχημένες στην παράκαμψη των ελέγχων προστασίας
- Την φύση (το είδος και τη σοβαρότητα) των επιπτώσεων στα περιουσιακά στοιχεία.

Risk Factor Analysis

Άλλη μια προσέγγιση για την αποσύνθεση και την ανάλυση του κινδύνου αποτελεί και η ακόλουθη εργασία που διεξήχθη στο Los Alamos National Laboratory και απεικονίζεται στο ακόλουθο σχήμα 2.7:

Σχήμα 3.7: Risk Factor Analysis



	Κατηγορίες Κινδύνου		
	Non/Low (0/1)	**Medium (2)**	**High (3)**
Τεχνολογική Ωριμότητα	Οι εγκαταστάσεις και ο εξοπλισμός περιλαμβάνουν μόνο αποδεδειγμένη τεχνολογία (ή νέα τεχνολογία για τις ΜΗ κρίσιμες δραστηριότητες.)	Οι εγκαταστάσεις και ο εξοπλισμός απαιτούν την **προσαρμογή** των εφαρμογών, των κατασκευών και των λειτουργιών στις νέες τεχνολογίες για το έργο αυτό	Οι εγκαταστάσεις και ο εξοπλισμός απαιτούν την **ανάπτυξη** νέας τεχνολογίας στις κατασκευές και τις λειτουργίες για το έργο αυτό
Αβεβαιότητα Παραγωγικότητας	Ο προβλεπόμενος ρυθμός προόδου που απαιτείται για την ολοκλήρωση του έργου είναι **συντηρητικός** και εντός των σημείων αναφοράς που καταγράφηκαν σε παρόμοια έργα	Ο προβλεπόμενος ρυθμός προόδου που απαιτείται για την ολοκλήρωση του έργου είναι **επιθετικός** και πάλι εντός των σημείων αναφοράς που καταγράφηκαν σε παρόμοια έργα	Ο προβλεπόμενος ρυθμός προόδου που απαιτείται για την ολοκλήρωση του έργου είναι **εξαιρετικά επιθετικός** ή χωρίς διαθέσιμα σημεία αναφοράς για την ορθότητα του ρυθμού αυτού
Ασάφεια κόστους Εξοπλισμού, υλικών	Το κόστος του εξοπλισμού και των υλικών είναι **σωστά θεσπισμένο** και **ρυθμίζεται** από συμβόλαια ή δυνάμεις του ανταγωνισμού.	Το κόστος του εξοπλισμού και των υλικών είναι **σωστά θεσπισμένο** αλλά **πρέπει να ρυθμιστεί** από δυνάμεις του ανταγωνισμού	Το κόστος του εξοπλισμού και των υλικών **δεν είναι σωστά θεσπισμένο** και **δεν υπόκειται** σε δυνάμεις του ανταγωνισμού

Πιθανολογική Αξιολόγηση Κινδύνων.

Η πιθανολογική εκτίμηση κινδύνων (Probabilistic risk assessment - PRA) είναι μια συστηματική και ολοκληρωμένη μεθοδολογία για την αξιολόγηση των κινδύνων οι οποίοι συνδέονται με σύνθετους φορείς τεχνολογίας (αεροπλάνα, πυρηνικά εργοστάσια) που χρησιμοποιούνται ευρέως (συμπεριλαμβανομένης της Πυρηνικής Ρυθμιστικής Επιτροπής των ΗΠΑ).

Ο κίνδυνος κατά την PRA ορίζεται ως το επιζήμιο αποτελέσματα μιας δραστηριότητας ή ενέργειας. Στην PRA, ο κίνδυνος χαρακτηρίζεται από δύο μέρη:

1. Το μέγεθος (σοβαρότητα) των πιθανών δυσμενών συνεπειών

2. Την πιθανότητα εμφάνισης των συνεπειών.

Οι συνέπειες εκφράζονται αριθμητικά (π.χ. ο αριθμός των ανθρώπων που ενδεχομένως να επηρεάστηκαν) και η πιθανότητα εμφάνισής τους εκφράζεται ως πιθανότητα ή συχνότητα (δηλ. ο αριθμός των περιστατικών ή η πιθανότητα εμφάνισης ανά μονάδα χρόνου). Ο συνολικός κίνδυνος είναι το άθροισμα των γινομένων των συνεπειών επί των πιθανοτήτων τους. Το φάσμα των κινδύνων μεταξύ των κατηγοριών των γεγονότων είναι επίσης ενδιαφέρον και οι κίνδυνοι ελέγχονται συνήθως μέσα από τις διαδικασίες Αδειοδότησης (θα ήταν ανησυχητικό εάν σπάνια γεγονότα αλλά με σοβαρές συνέπειες κυριαρχούσαν στο συνολικό κίνδυνο).

Η PRA συνήθως απαντά σε τρία βασικά ερωτήματα:

1. Τι μπορεί να πάει στραβά στον φορέα τεχνολογίας ή ποια είναι τα πρωταρχικά γεγονότα (ανεπιθύμητα γεγονότα έναρξης) που οδηγούν σε δυσμενείς επιπτώσεις;
2. Ποιές και πόσο σοβαρές είναι οι πιθανές ζημίες ή οι δυσμενείς συνέπειες που μπορεί να έχει ο φορέας τεχνολογίας;
3. Πόσο πιθανή είναι η εμφάνιση αυτών των ανεπιθύμητων συνεπειών ή ποιες είναι οι πιθανότητες ή οι συχνότητες τους? Δύο μέθοδοι που απαντούν τα ερωτήματα αυτά είναι η **event tree analysis** και η **fault tree analysis**.

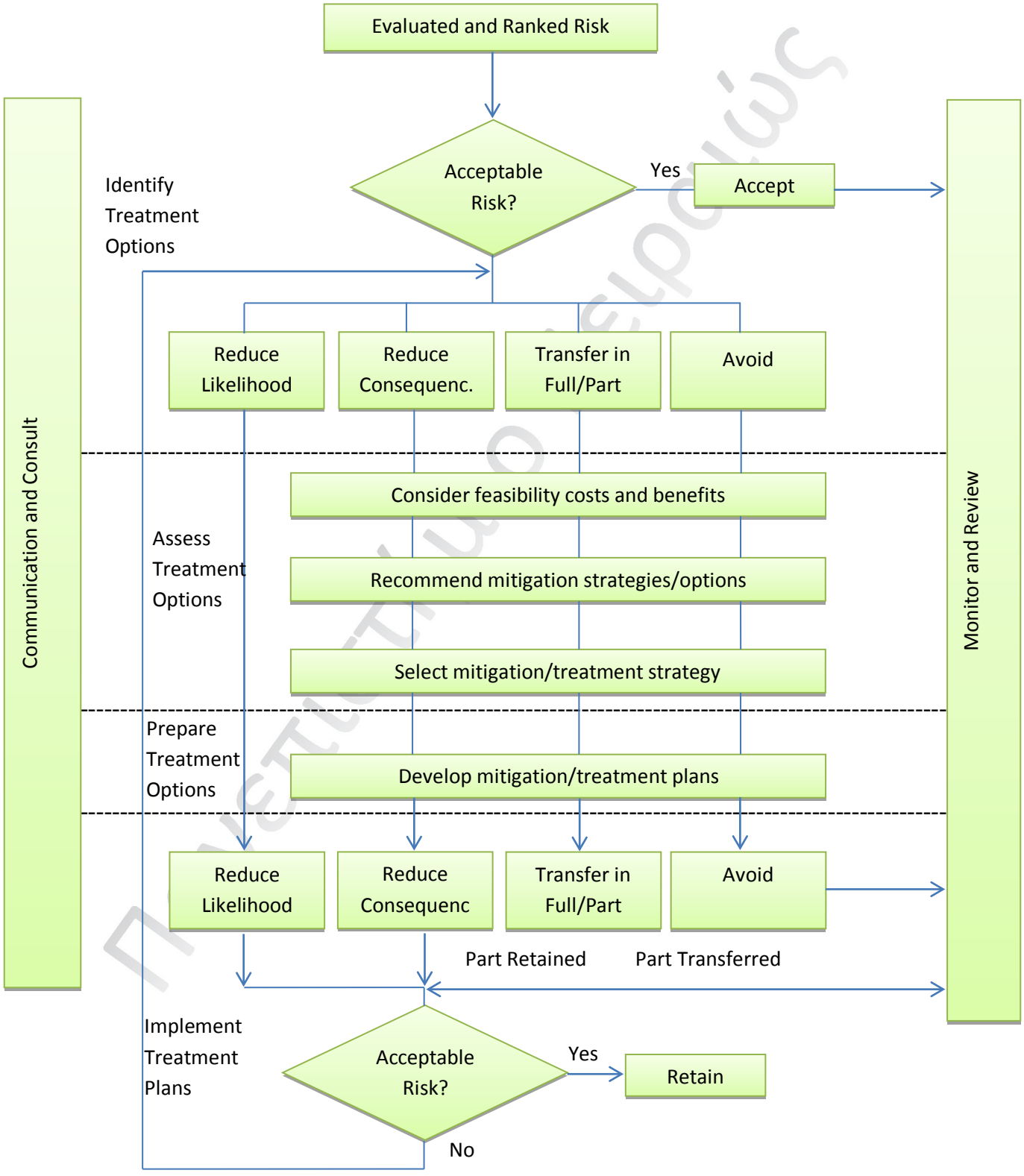
Εκτός από τις παραπάνω μεθόδους, οι PRA μελέτες απαιτούν ειδικά και συχνά πολύ σημαντικά εργαλεία ανάλυσης, όπως είναι η **human reliability analysis** (HRA) και η **common-cause-failure analysis** (CCF). Η HRA ασχολείται με μεθόδους για την μοντελοποίηση του ανθρώπινου λάθους, ενώ η CCF ασχολείται με μεθόδους για την αξιολόγηση της επίδρασης από την αλληλεξάρτηση των inter– intra- συστημάτων, οι οποίες τείνουν να προκαλούν ταυτόχρονες αποτυχίες και συνεπώς σημαντικές αυξήσεις στο συνολικό κίνδυνο.

Οι PRA μελέτες έχουν πραγματοποιηθεί με επιτυχία σε σύνθετα τεχνολογικά συστήματα σε όλες τις φάσεις του κύκλου ζωής τους, από τον ορισμό και τον σχεδιασμό τους μέχρι την

ασφαλή αποσύνδεσή τους από τη λειτουργία. Για παράδειγμα, η Ρυθμιστική Πυρηνική Επιτροπή (NRC) απαιτεί σε κάθε πυρηνικό σταθμό στις Ηνωμένες Πολιτείες να πραγματοποιείται εξέταση των εγκαταστάσεων για τον εντοπισμό και τον προσδιορισμό των τρωτών σημείων, τις αστοχίες υλικού και τα ανθρώπινα λάθη στο σχεδιασμό και τη λειτουργία. Αν και καμία μέθοδος δεν εξειδικεύεται στην εκτέλεση μιας τέτοιας αξιολόγησης, οι απαιτήσεις του NRC για την ανάλυση θα μπορούσαν να επιτευχθούν μόνο με την εφαρμογή της μεθόδου PRA.

Το κλειδί για τη Διαχείριση Επικινδυνότητας είναι η μείωση του κινδύνου ή η αντιμετώπισή του. Ως παράδειγμα άλλων προσεγγίσεων, η διαδικασία της αντιμετώπισης του κινδύνου παρουσιάζεται στο ακόλουθο σχήμα 3.8

Σχήμα 3.8: Διαδικασία αντιμετώπισης κινδύνου



3.8.4 Προσδιορισμός των Κινδύνων

Οι τεχνικές μέθοδοι, συμπεριλαμβανομένης της χρήσης του λογισμικού, μπορούν να χρησιμοποιηθούν για τον εντοπισμό και την παρακολούθηση των κινδύνων καθώς και για την παροχή εργαλείων για αναφορές κατά την καταγραφή της ανάλυσης των κινδύνων. Όπως με οποιαδήποτε διαδικασία, το καλύτερο εργαλείο που μπορεί να χρησιμοποιηθεί είναι αυτό που ταιριάζει καλύτερα και ανταποκρίνονται στις ανάγκες του οργανισμού - επιχείρησης. Κατά την εφαρμογή των μεθόδων ανάλυσης και προσδιορισμού του κινδύνου, ο διευθυντής της ασφάλειας πληροφοριών πρέπει να καθορίσει τους απαιτούμενους πόρους και να καταρτίσει τον προϋπολογισμό και το χρονοδιάγραμμα αυτών των σημαντικών καθηκόντων.

Ένα από τα αρχικά στάδια σχεδιασμού ενός προγράμματος Διαχείρισης Επικινδυνότητας είναι η δημιουργία μιας ολοκληρωμένης λίστας των πηγών των απειλών, των κινδύνων και των γεγονότων που θα μπορούσαν να έχουν αντίκτυπο στην ικανότητα της επιχείρησης να επιτύχει τους στόχους της, όπως προσδιορίζονται στον προσδιορισμός του πεδίου εφαρμογής και το πλαίσιο του προγράμματος. Τα γεγονότα αυτά μπορούν να αποτρέψουν, να υποβαθμίσουν, να καθυστερήσουν ή να ενισχύσουν την επίτευξη των στόχων αυτών.

Σε γενικές γραμμές, ο κίνδυνος μπορεί να συνδέεται ή να χαρακτηρίζεται από τα ακόλουθα:

- **Την προέλευσή του**. Για παράδειγμα, παράγοντες κινδύνου όπως οι εργαζόμενοι οι οποίοι δεν είναι κατάλληλα εκπαιδευμένοι, οι ανταγωνιστές, οι κυβερνήσεις, κλπ
- **Δραστηριότητα, γεγονός ή ατύχημα**. Για παράδειγμα, υποκλοπή εμπιστευτικών δεδομένων, ανάπτυξη νέας πολιτικής μάρκετινγκ από τους ανταγωνιστές, νέες ή αναθεωρημένες ρυθμίσεις περί προστασίας των δεδομένων, μια εκτεταμένη διακοπή ρεύματος κλπ.
- **Τις συνέπειες του και τα αποτελέσματα των επιπτώσεων του**. Για παράδειγμα η μη διαθεσιμότητα των υπηρεσιών, η απώλεια ή η αύξηση του μεριδίου αγοράς / κερδών, η αύξηση ρυθμιστικών μέτρων, η αύξηση ή η μείωση της ανταγωνιστικότητας, οι κυρώσεις, κλπ.
- **Συγκεκριμένοι λόγοι εμφάνισης**. Για παράδειγμα, σφάλμα στο σχεδιασμό του συστήματος, η ανθρώπινη παρέμβαση, σωστή ή εσφαλμένη πρόβλεψη των δραστηριοτήτων των ανταγωνιστών.
- **Μηχανισμούς προστασίας και ελέγχου** (μαζί με πιθανή έλλειψη αποτελεσματικότητας τους). Για παράδειγμα, ο έλεγχος πρόσβασης και τα συστήματα ανίχνευσης, πολιτικές, εκπαίδευση σε θέματα ασφάλειας, έρευνα αγοράς.
- **Χρόνος και τόπος των περιστατικών**. π.χ., μια πλημμύρα στην αίθουσα ηλεκτρονικών υπολογιστών κατά τη διάρκεια ακραίων περιβαλλοντικών συνθηκών.

Οι υψηλής ποιότητας πληροφορίες και η βαθειά γνώση της επιχείρησης και του εσωτερικού και εξωτερικού περιβάλλοντος της είναι πολύ σημαντικοί στον εντοπισμό των κινδύνων. Τα

ιστορικά στοιχεία των επιχειρήσεων ή παρόμοιων οργανισμών (ανταγωνιστών ή όχι) μπορούν επίσης να αποδειχθούν πολύ χρήσιμες πληροφορίες μιας και μπορούν να οδηγήσουν σε λογικές προβλέψεις πάνω σε θέματα που δεν έχει ακόμη αντιμετωπίσει η επιχείρηση.

Ο προσδιορισμός του τι μπορεί να συμβεί είναι πολύ σπάνια επαρκής. Το γεγονός ότι υπάρχουν πολλοί τρόποι για να συμβεί ένα γεγονός αυτόματα καθιστά σημαντική την ενδελεχή μελέτη όλων των πιθανών και σημαντικών αιτίων και σεναρίων. Οι Μέθοδοι και τα εργαλεία που χρησιμοποιούνται για τον εντοπισμό των κινδύνων και της εμφάνισής τους περιλαμβάνουν λίστες ελέγχου (checklists), αποφάσεις με βάση την εμπειρία και αρχεία, διαγράμματα ροής, brainstorming, ανάλυση συστημάτων και ανάλυση σεναρίων.

Κατά την επιλογή μεθοδολογίας για τον προσδιορισμό του κινδύνου, οι ακόλουθες τεχνικές θα πρέπει να λαμβάνονται υπόψη:

- **Brainstorming** (βασισμένο σε ομάδα), όπου τα workshops μπορούν να αποδειχθούν αποτελεσματικά στην αξιοποίηση διαφορετικών εμπειριών.
- **Δομημένες τεχνικές** όπως τα διαγράμματα ροής, η επισκόπηση του σχεδιασμού του συστήματος, η ανάλυση των συστημάτων, οι μελέτες κινδύνου και λειτουργικότητας καθώς και η μοντελοποίηση των λειτουργιών.
- Η "**what-if" ανάλυση και η ανάλυση σεναρίων** για λιγότερο σαφώς καθορισμένες περιπτώσεις, όπως ο προσδιορισμός των στρατηγικών κινδύνων και διαδικασιών με μια πιο γενική διάρθρωση.

3.8.5 Απειλές

Οι απειλές στις πηγές πληροφόρησης και η πιθανότητα εμφάνισής τους πρέπει να αξιολογηθούν. Στο πλαίσιο αυτό, απειλές ενδέχεται να είναι οποιεσδήποτε περιστάσεις ή γεγονότα που έχουν τη δυναμική να προκαλέσουν βλάβη σε μια πηγή πληροφοριών, εκμεταλλευόμενα τα τρωτά σημεία του συστήματος. Οι απειλές συνήθως κατηγοριοποιούνται ως εξής:

- **Φυσικές**: πλημμύρες, πυρκαγιές, κυκλώνες, βροχή / χαλάζι, επιδημίες και σεισμοί
- **Ακούσιες**: φωτιά, νερό, ζημιά / κατάρρευση κτιρίου, απώλεια των υπηρεσιών κοινής ωφέλειας και κατάσχεση του εξοπλισμού
- **Εκούσιες σωματικές**: Βόμβες, φωτιά, νερό και κλοπή
- **Εκούσιες μη σωματικές**: απάτη, κατασκοπεία, πειρατεία, κλοπή ταυτότητας, κακόβουλο λογισμικό, κοινωνική εργασία, ηλεκτρονικό «ψάρεμα» και Denial-Of-Service attacks (DoS attacks)

3.8.6 Τρωτά Σημεία

Ο όρος αυτός χρησιμοποιείται συχνά σαν να είναι μια δυαδική κατάσταση. Κάτι "είναι ευάλωτο" ή "δεν είναι ευάλωτο». Ακριβέστερα, τα περιουσιακά στοιχεία είναι ευάλωτα σε διαφορετικούς βαθμούς, δηλαδή, μια συγκεκριμένη κατάσταση ελέγχου θα μπορούσε να αντιπροσωπεύσει έναν υψηλό βαθμό επισφάλειας, ενώ μια άλλη κατάσταση του ελέγχου αντιπροσωπεύει ένα μικρότερο βαθμό επισφάλειας. Η διάκριση αυτή καθίσταται καθοριστική στη διαδικασία των προτεραιοτήτων των προσπαθειών διαχείρισης κινδύνου, κατά τον καθορισμό του επιπέδου του κινδύνου μέσα σε ένα σενάριο και, επίσης, κατά την εξήγηση των συμπερασμάτων και των προτάσεων για τη διαχείριση.

Η εκτίμηση του βαθμού τρωτότητας μπορεί να επιτευχθεί μέσω διαφόρων μορφών ελέγχου (όταν ο χρόνος το επιτρέπει και όταν το διακύβευμα είναι υψηλό) ή μέσω αντικειμενικών αξιολογήσεων από εμπειρογνώμονες. Όπως και με άλλες εκτιμήσεις, αυτές μπορεί να είναι ποσοτικές ή ποιοτικές. Όπως με οποιοδήποτε ποσοτικό μέτρο ή εκτίμηση, είναι σημαντικό να είναι συμβατό με τον ασαφή χαρακτήρα της αξίας έτσι ώστε η διοίκηση να μην παραπλανηθεί.

Ο προσδιορισμός του απόλυτου συσχετισμού ενός αδύναμου ελέγχου απαιτεί επίσης την κατανόηση των άλλων συνεργαζόμενων ελέγχων που μπορούν να μειώσουν τη συνολική έκθεση. Θα ήταν ανακριβές και ζημιογόνο να απεικονίσει κανείς ένα στοιχείο ελέγχου σαν ένα σοβαρό πρόβλημα, όταν στην πραγματικότητα, η συνολική κατάσταση του ελέγχου είναι σχετικά ισχυρή.

Δεδομένου ότι είναι φυσιολογικό σε μια επιχείρηση να βρεθούν μια σειρά από έλεγχους σε διάφορα μέρη μιας τυπικής διαδικασίας, είναι σημαντικό να κατανοήσουμε την όλη διαδικασία από άκρη σε άκρη.

Ενώ η διαστρωμάτωση των ελέγχων είναι μια συνετή προσέγγιση, ένας υπερβολικά μεγάλος αριθμός ελέγχων για την αντιμετώπιση των ίδιων κινδύνων είναι περιττός. Είναι επίσης σημαντικό να διασφαλιστεί ότι οι έλεγχοι δεν υπόκεινται στους ίδιους κινδύνους που να ακυρώνουν το σκοπό της διαστρωμάτωσης τους. Για να είναι οι αξιολογήσεις του κινδύνου αποτελεσματικές και ακριβείς, είναι απαραίτητο να εξασφαλιστεί ότι αυτές διεξάγονται από την αρχή των διαδικασιών μέχρι το τέλος. Για να γίνει κατανοητό το παραπάνω, οι έλεγχοι upstream μπορούν να ελαχιστοποιήσουν ή την εξαλείψουν ορισμένους κινδύνους και να αποκλείσουν την ανάγκη για περαιτέρω ελέγχους. Επίσης μπορούν να βοηθήσουν στην να γίνει αντιληπτό εάν υπάρχει περιττός πλεονασμός ή επανάληψη του ελέγχου.

Πολλές αδυναμίες του συστήματος πληροφορικής αναγνωρίζονται με τη χρήση αυτοματοποιημένου εξοπλισμού σάρωσης. Τα ευάλωτα σημεία διαδικασιών και απόδοσης είναι πιο δύσκολο να εξακριβωθούν και ενδεχομένως να απαιτούν προσεκτική ανάλυση για να αποκαλυφθούν. Η αξιολόγηση πρέπει να συνυπολογίσει διαδικασίες και διαδικαστικές και φυσικές αδυναμίες εκτός από τις αδυναμίες της τεχνολογίας. Ας εξετάσουμε μια επιχείρηση

που δεν έχει εκπαίδευση σε προγράμματα με θέματα ασφάλειας, ενημέρωσης και ευαισθητοποίησης. Τα τρωτά σημεία σε αυτή την περίπτωση θα προέκυπταν από την έλλειψη συνειδητοποίησης των χρηστών των πολιτικών ασφάλειας, των πρότυπων και των κατευθυντήριων γραμμών. Αδυναμίες μπορούν επίσης να απορρέουν από την έλλειψη των διαδικασιών για τον έλεγχο, την πιστοποίηση και την διαπίστευση των συστημάτων.

Οι έλεγχοι είναι χρήσιμοι για τον εντοπισμό των τρωτών σημείων.

Μερικά παραδείγματα από τα ευάλωτα σημεία είναι:

• Ελαττωματικό software

• Ακατάλληλα ρυθμισμένος εξοπλισμός

• Ανεπαρκής επιβολή συμμόρφωσης

• Κακή μελέτη δικτύου

• Ανεξέλεγκτες ή ελαττωματικές διαδικασίες

• Ανεπαρκής διαχείριση

• Ανεπαρκής προσωπικό

• Έλλειψη γνώσης για την υποστήριξη των χρηστών ή την εκτέλεση των διαδικασιών

• Έλλειψη λειτουργικότητας ασφάλειας

• Έλλειψη κατάλληλης συντήρησης

• Κακή επιλογή κωδικών πρόσβασης

• Μη δοκιμασμένη τεχνολογία

• Απροστάτευτες επικοινωνίες

• Έλλειψη εφεδρικών

• Κακή διαχείριση επικοινωνιών

3.8.7 Είδη Κινδύνων

Ο διαχειριστής της ασφάλειας των πληροφοριών πρέπει να κατανοήσει το προφίλ κινδύνου της επιχείρησης. Κανένα μοντέλο δεν παρέχει μια πλήρη εικόνα, αλλά με την κατηγοριοποίηση των περιοχών που διατρέχουν κίνδυνο σε ένα οργανισμό (όπως φαίνεται στο ακόλουθο σχήμα 3.9) διευκολύνει την επικέντρωση στις βασικές στρατηγικές διαχείρισης επικινδυνότητας και στις αποφάσεις. Επιτρέπει επίσης στην επιχείρηση την ανάπτυξη και υλοποίηση των μέτρων μείωσης του κινδύνου που σχετίζονται με την επιχείρηση και είναι οικονομικά αποδοτικά.

Σχήμα 3.9: Κατηγορίες Λειτουργικού Κινδύνου

Λειτουργικές περιοχές κινδύνου	Περιγραφή	Πληροφορίες (IT mapping)
Κίνδυνοι εγκαταστάσεων και περιβάλλοντος εργασίας	Απώλειες ή ζημιές λειτουργικών δυνατοτήτων που προκαλούνται από προβλήματα των εγκαταστάσεων, των υπηρεσιών ή του εξοπλισμού	Διαχείριση Επιχειρησιακής Συνέχειας για τις IT εγκαταστάσεις
Κίνδυνοι Υγείας / Ασφάλειας	Απειλές για την υγεία και την ασφάλεια του προσωπικού, των πελατών και του κοινού	Εμπιστευτικότητα στις διευθύνσεις κατοικίας, στις ταξιδιωτικές πληροφορίες κα
Κίνδυνοι Ασφάλειας Πληροφοριών	Η μη εξουσιοδοτημένη γνωστοποίηση ή τροποποίηση των πληροφοριών, η απώλεια της διαθεσιμότητας ή η ακατάλληλη χρήση των πληροφοριών	Όλες οι πτυχές της ασφάλειας πληροφοριών και IT
Κίνδυνοι Ελέγχων	Ανεπαρκής σχεδιασμός ή επιδόσεις της υπάρχουσας υποδομής της διαχείρισης επικινδυνότητας	Ανάλυση επιχειρησιακών διαδικασιών για τον εντοπισμό των κρίσιμων ροών των πληροφοριών και των σημείων ελέγχου
Κίνδυνοι Νομικής και ρυθμιστικής συμμόρφωσης	Η μη συμμόρφωση με τους νόμους των χωρών στις οποίες οι επιχειρηματικές δραστηριότητες πραγματοποιούνται. Αποτυχία συμμόρφωσης με οποιαδήποτε ρυθμιστικά πρότυπα, πρότυπα φορολόγησης και υποβολής εκθέσεων. Αποτυχία συμμόρφωσης με τις	Συμμόρφωση με τη νομοθεσία περί προστασίας δεδομένων, κρυπτογραφικοί κανονισμοί ελέγχου. Ακρίβεια, επικαιρότητα και ποιότητα των πληροφοριών που αναφέρονται στις ρυθμιστικές αρχές. Η διαχείριση περιεχόμενου όλων των πληροφοριών που αποστέλλονται σε άλλα μέρη

	συμβάσεις ή Αποτυχία των συμβάσεων να προστατεύσουν τα επιχειρηματικά συμφέροντα	
Κίνδυνος επιχειρησιακής διακυβέρνησης	Η αποτυχία των διευθυντών να εκπληρώσουν τις νομικές υποχρεώσεις τους όσον αφορά τη διαχείριση και τον έλεγχο της εταιρείας	Χάραξη πολιτικής για την ασφάλεια Πληροφοριών, τη μέτρηση των επιδόσεων και την υποβολή εκθέσεων
Κίνδυνος Υπόληψης	Οι αρνητικές επιπτώσεις της κοινής γνώμης, η γνώμη των πελατών και η φήμη στην αγορά. Η ζημία που προκλήθηκε στην επιχείρηση από την αποτυχία διαχείρισης των δημοσίων σχέσεων	Έλεγχος της δημοσιοποίησης εμπιστευτικών πληροφοριών, Η δημόσια εικόνα μιας καλά οργανωμένης επιχείρησης
Κίνδυνος Στρατηγικής	Η μη τήρηση των μακροπρόθεσμων στρατηγικών στόχων της επιχείρησης, περιλαμβανομένης της εξάρτησης σε οποιαδήποτε εκτίμηση ή προγραμματισμένα αποτελέσματα που μπορεί να είναι στον έλεγχο τρίτων	Διαχείριση της ποιότητας και της λεπτότητας των πληροφοριών στις οποίες οι στρατηγικές αποφάσεις των επιχειρήσεων βασίζονται (π.χ., συγχωνεύσεις, εξαγορές, πωλήσεις)
Κίνδυνοι διαδικασιών και συμπεριφοράς	Προβλήματα με υπηρεσίες που προκαλούνται από την αποτυχία των εσωτερικών ελέγχων, τα συστήματα πληροφοριών, την ακεραιότητα των εργαζομένων, τα λάθη και τα σφάλματα τους, ή αδυναμίες των λειτουργικών διαδικασιών	Όλες οι πτυχές της ασφάλειας πληροφοριακών συστημάτων και της ασφάλειας που σχετίζεται με τη συμπεριφορά των εργαζομένων κατά την άσκηση των καθηκόντων τους.
Κίνδυνος Τεχνολογίας	Η αποτυχία στη σχεδίαση, στη διαχείριση και στην παρακολούθηση της επίδοσης σε έργα που σχετίζονται με την τεχνολογία, προϊόντα, υπηρεσίες, διαδικασίες, το προσωπικό και τα κανάλια διανομής	Αποτυχία των συστημάτων πληροφορικής και επικοινωνιών και η ανάγκη για τη διαχείριση της επιχειρησιακής συνέχειας
Κίνδυνος Διαχείρισης Έργων	Η αποτυχία στη σχεδίαση και την διαχείριση των πόρων	Διαχείριση όλων των έργων που σχετίζονται με την

	που απαιτούνται για την επίτευξη των στόχων του έργου, οδηγεί σε υπερβάσεις προϋπολογισμού, υπερβάσεις του χρόνου ή και τα δύο, που τελικά οδηγούν σε μη ολοκλήρωση του έργου. Η τεχνική βλάβη ενός έργου ή η αδυναμία να διαχειριστεί τις πτυχές της ολοκλήρωσης με τα υπάρχοντα τμήματα της επιχείρησης και τον αντίκτυπο που μπορεί να έχουν οι αλλαγές στις επιχειρηματικές δραστηριότητες	ασφάλεια πληροφοριών
Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων	Απώλεια ή ζημία που προκαλείται από απάτη, κλοπή, εσκεμμένη αμέλεια, βαριά αμέλεια, βανδαλισμούς, σαμποτάζ, εκβιασμό, κλπ	Παροχή υπηρεσιών ασφαλείας και μηχανισμοί για την πρόληψη όλων των ειδών εγκλήματος στον κυβερνοχώρο
Κίνδυνος Ανθρώπινων Πόρων	Εσφαλμένη πρόσληψη, ανάπτυξη ή διατήρηση των εργαζομένων με τις κατάλληλες δεξιότητες και γνώσεις ή αποτυχία κατά τη διαχείριση των σχέσεων των εργαζομένων	Ανάγκη για πολιτικές προστασίας των εργαζομένων από σεξουαλική παρενόχληση, ρατσιστικές ύβρεις, κλπ., μέσω των εταιρικών συστημάτων ηλεκτρονικού ταχυδρομείου, κλπ.
Κίνδυνος Προμηθευτών	Αποτυχία αξιολόγησης επαρκώς των ικανοτήτων των προμηθευτών που οδηγεί σε σφάλματα στη διαδικασία προμήθειας ή στην παράδοση των παρεχόμενων αγαθών και υπηρεσιών. Αποτυχία κατανόησης και διαχείρισης των ζητημάτων της αλυσίδας εφοδιασμού	Outsourced παροχή υπηρεσιών των συστημάτων πληροφορικής ή άλλων δραστηριοτήτων επεξεργασίας επιχειρηματικών πληροφοριών
Κίνδυνος διαχείρισης πληροφοριών	Ανεπαρκής, ανακριβής, ελλιπής ή εκτός χρόνου παροχή πληροφοριών για την διαδικασία υποστήριξης λήψης διοικητικών αποφάσεων	Διαχείριση με ακρίβεια, ακεραιότητα, επικαιρότητα και ποιότητα των πληροφοριών που χρησιμοποιούνται για την υποστήριξη λήψης αποφάσεων
Κίνδυνοι Ηθικής	Ζημιές που προκλήθηκαν	Ηθική συλλογή, αποθήκευση

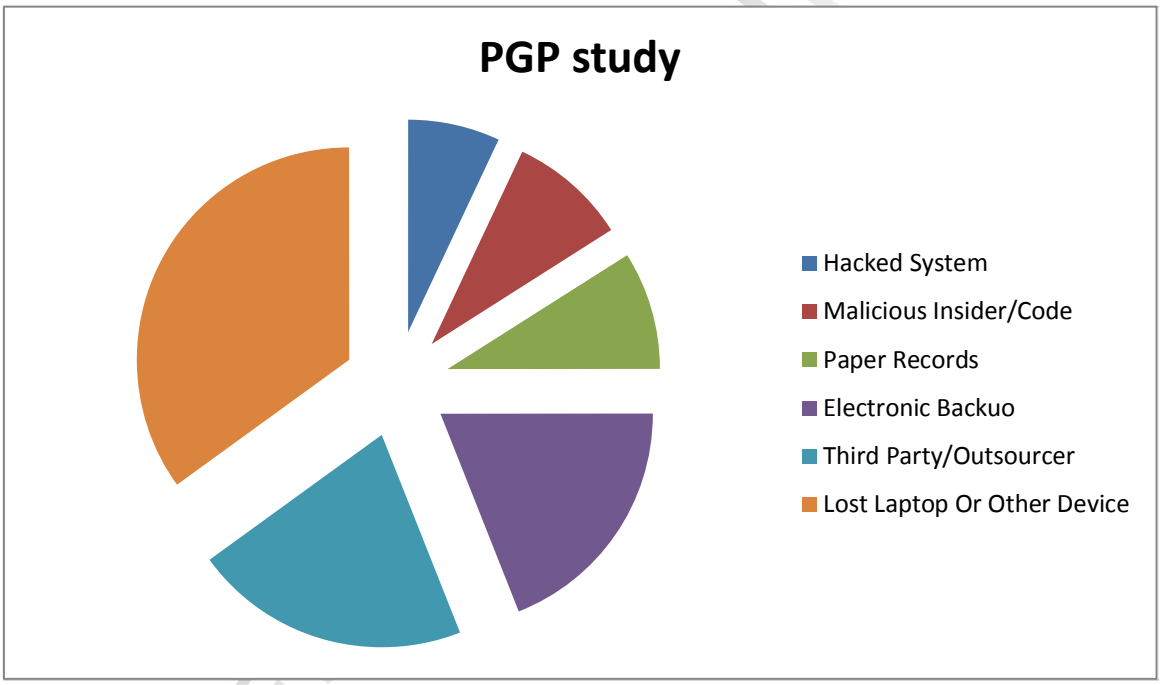
	από ανήθικες επιχειρηματικές πρακτικές, συμπεριλαμβανομένων εκείνων που σχετίζονται με τους επιχειρηματικούς εταίρους. Τα θέματα αυτά περιλαμβάνουν φυλετικές και θρησκευτικές διακρίσεις, την εκμετάλλευση της παιδικής εργασίας, τη ρύπανση, περιβαλλοντικά θέματα, τη συμπεριφορά στις ομάδες μειοψηφίας κλπ.	και χρήση των πληροφοριών. Διαχείριση του περιεχόμενου των πληροφοριών των Web sites, Intranets, και εταιρικών e-mail.
Γεωπολιτικοί Κίνδυνοι	Απώλεια ή ζημιά σε ορισμένες χώρες, που προκαλείται από την πολιτική αστάθεια, την κακή ποιότητα των υποδομών των αναπτυσσόμενων περιοχών ή πολιτισμικές διαφορές.	Διαχείριση όλων των πτυχών της ασφάλειας των πληροφοριών και των συστημάτων ασφάλειας του IT σε περιοχές όπου η επιχείρηση έχει επιχειρηματικές δραστηριότητες, αλλά υπάρχουν ειδικοί γεωπολιτικοί κίνδυνοι.
Κίνδυνοι Κουλτούρας	Η μη αντιμετώπιση πολιτιστικών θεμάτων που αφορούν τους εργαζομένους, τους πελάτες ή άλλους ενδιαφερόμενους. Αυτά τα θέματα περιλαμβάνουν τη γλώσσα, τη θρησκεία, την ηθική και άλλα έθιμα και πρακτικές της εκάστοτε κοινωνίας.	Διαχείριση του περιεχομένου των ιστοσελίδων, των intranets και των εταιρικά e-mail
Κίνδυνοι Κλιματολογικοί και καιρικών φαινομένων	Απώλεια ή ζημία που προκαλείται από ασυνήθιστες κλιματικές συνθήκες, συμπεριλαμβανομένης της ξηρασίας, της θερμότητας, της πλημμύρας, του κρύου, καταιγίδες, ανέμους κλπ.	Διαχείριση επιχειρησιακής συνέχειας για τις εγκαταστάσεις του IT

Ο κίνδυνος αποτελεί αναπόσπαστο μέρος των επιχειρήσεων και δεδομένου ότι είναι ανέφικτη και δαπανηρή η εξάλειψη όλων των κινδύνων, κάθε επιχείρηση έχει ένα αποδεκτό επίπεδο κινδύνου. Για τον προσδιορισμό του εύλογου επιπέδου του αποδεκτού κινδύνου, ο

διαχειριστής του κινδύνου πρέπει να καθορίσει ένα βέλτιστο σημείο στο οποίο το κόστος των ζημιών διασταυρώνεται με το κόστος της μείωσης κινδύνου.

Για τους περισσότερους οργανισμούς η αδυναμία σωστής εκτίμησης, ανάλυσης και διαχείρισης των κινδύνων έχει ως αποτέλεσμα οι προσπάθειες της διαχείρισης επικινδυνότητας να μην κατανέμονται σωστά και να μην κατευθύνονται στη μεγαλύτερη πηγή των ζημιών. Μια σε μελέτη εις βάθος που διεξήχθη από την PGP-Vontu από 31 οργανισμούς σε κίνδυνο προσδιορίστηκε η πηγή των ζημιών όπως φαίνεται στο παρακάτω σχήμα 3.10. Είναι δίκαιο να πούμε ότι, για τους περισσότερους οργανισμούς, οι πρωτογενείς προσπάθειες διαχείρισης του κινδύνου κατά κανόνα απευθύνονται στον έλεγχο μη εξουσιοδοτημένης πρόσβασης, η οποία, κατά μέσο όρο, αντιπροσώπευαν όμως μόνο το 7% των ζημιών σε αυτή τη μελέτη, ενώ η πλειοψηφία των ζημιών από τις άλλες αιτίες γενικά έλαβαν σχετικά λίγη προσοχή.

Σχήμα 3.10: Πηγή Απωλειών



3.8.8 Ανάλυση σχετικών Κινδύνων

Η ανάλυση κινδύνου είναι η φάση όπου το επίπεδο του κινδύνου και η φύση του αξιολογούνται και γίνονται αντιληπτά. Η πληροφορία αυτή είναι η πρώτη είσοδος στους φορείς λήψης αποφάσεων, σχετικά με το αν οι κίνδυνοι πρέπει να αντιμετωπίζονται ή πρέπει να γίνουν αποδεκτοί, καθώς και η πλέον κατάλληλη και αποδοτική μέθοδος αντιμετώπισης του κινδύνου.

Η ανάλυση κινδύνου περιλαμβάνει:

- Την ενδελεχή εξέταση των πηγών κινδύνου.
- Τις θετικές και αρνητικές συνέπειες τους.
- Την πιθανότητα οι συνέπειες αυτές να συμβούν (και τους παράγοντες που τις επηρεάζουν)
- Την εκτίμηση των υπαρχόντων ελέγχων ή διαδικασιών με σκοπό να ελαχιστοποιήσουν τους αρνητικούς κινδύνους ή να ενισχύσουν τους θετικούς (οι έλεγχοι αυτοί μπορεί να προέρχονται από ένα ευρύτερο σύνολο standards, ελέγχων ή πρακτικών που επελέγησαν σύμφωνα την δυνατότητα εφαρμογής τους και μπορούν επίσης να προέρχονται από προηγούμενες δραστηριότητες της αντιμετώπισης του κινδύνου).

Το επίπεδο του κινδύνου μπορεί να υπολογιστεί με διάφορους τρόπους, συμπεριλαμβανομένης της χρήσης στατιστικής ανάλυσης και υπολογισμών που συνδυάζουν την πιθανότητα και τις επιπτώσεις. Κάθε τύποι και μέθοδοι για να συνδυαστούν πρέπει να είναι σύμφωνοι με τα κριτήρια που ορίζονται κατά τη θέσπιση του περιεχομένου της διαχείρισης επικινδυνότητας. Αυτό συμβαίνει επειδή ένα γεγονός μπορεί να έχει πολλαπλές συνέπειες και επιπτώσεις σε διαφορετικούς τομείς. Ως εκ τούτου, οι επιπτώσεις και η πιθανότητα πρέπει να συνδυαστούν για να υπολογιστεί το επίπεδο του σχετικού κινδύνου. Αν δεν υπάρχουν αξιόπιστα ή στατιστικά αξιόπιστα και σχετικά στοιχεία του παρελθόντος διαθέσιμα (π.χ. να διατηρούνται σε μια βάση δεδομένων περιστατικών), πιθανότατα να μπορούν να γίνουν διαφορετικές εκτιμήσεις, εφ 'όσον όμως έχουν κοινοποιηθεί δεόντως και έχουν εγκριθεί από τους υπεύθυνους λήψης αποφάσεων.

Οι πληροφορίες που χρησιμοποιούνται για την εκτίμηση των επιπτώσεων και των πιθανοτήτων προέρχεται συνήθως από:

- την εμπειρία του παρελθόντος ή δεδομένα και αρχεία (π.χ. αναφορές συμβάντων).
- αξιόπιστες πρακτικές, διεθνή πρότυπα ή κατευθυντήριες γραμμές.
- έρευνα και ανάλυση αγοράς.
- τα πειράματα και τα πρωτότυπα.
- Οικονομικά μοντέλα, μοντέλα μηχανικής ή άλλα μοντέλα.
- εξειδικευμένους σύμβουλους και εμπειρογνώμονες.

Οι Τεχνικές ανάλυσης κινδύνου περιλαμβάνουν:

- **συνεντεύξεις** με εμπειρογνώμονες στον τομέα ενδιαφέροντος και ερωτηματολόγια,
- τη **χρήση των υπαρχόντων μοντέλων** και προσομοιώσεων.

Η ανάλυση κινδύνων μπορεί να διαφέρει σε λεπτομέρειες ανάλογα με τον κίνδυνο, τον σκοπό της ανάλυσης και το απαιτούμενο επίπεδο προστασίας των σχετικών πληροφοριών, στοιχείων και πόρων. Η ανάλυση μπορεί να είναι **ποιοτική, ποσοτική ή ημι-ποσοτική** (qualitative, semiquantitative or quantitative) ή συνδυασμός αυτών. Σε κάθε περίπτωση, το είδος της ανάλυσης που εφαρμόζεται πρέπει, όπως προαναφέρθηκε, να είναι σύμφωνο με τα κριτήρια που έχουν αναπτυχθεί, ως μέρος του περιεχομένου της διαχείρισης επικινδυνότητας.

Στην συνέχεια ακολουθεί περιγραφή των τριών αυτών τύπων ανάλυσης.

Ποιοτική Ανάλυση

Στην ποιοτική ανάλυση, το μέγεθος και η πιθανότητα για ενδεχόμενες συνέπειες παρουσιάζονται και περιγράφονται αναλυτικά. Οι κλίμακες που χρησιμοποιούνται μπορεί να προσαρμοστούν ανάλογα με τις περιστάσεις ενώ διαφορετικές περιγραφές μπορούν να χρησιμοποιηθούν για διαφορετικούς κινδύνους. Η ποιοτική ανάλυση μπορεί να χρησιμοποιηθεί:

- ως μια αρχική εκτίμηση για τον εντοπισμό των κινδύνων που θα αποτελέσουν το αντικείμενο περαιτέρω λεπτομερή ανάλυση.
- Εκεί που άυλες πτυχές των κινδύνων πρέπει να υπολογιστούν (π.χ. φήμη, κουλτούρα, εικόνα επιχείρησης κλπ.)
- όπου υπάρχει έλλειψη κατάλληλων πληροφοριών και αριθμητικών δεδομένων ή πόρων, οι οποίοι απαιτούνται για μια στατιστικά αποδεκτή ποσοτική προσέγγιση.

Μια ποιοτική ανάλυση μπορεί να επιτευχθεί με τη χρήση 5 X 5 πινάκων, όπως φαίνεται στο ακόλουθο σχήμα 3.11.

Ημι-ποσοτική ανάλυση

Στην ημι-ποσοτική ανάλυση, ο στόχος είναι να εκχωρήσετε τιμές στις κλίμακες που χρησιμοποιούνται για την ποιοτική αξιολόγηση. Αυτές οι τιμές είναι συνήθως ενδεικτικές και όχι πραγματικές, κάτι το οποίο είναι η προϋπόθεση για την ποσοτική προσέγγιση. Ως εκ τούτου, καθώς η τιμή που αποδίδεται σε κάθε κλίμακα δεν είναι μια ακριβής αναπαράσταση του πραγματικού μεγέθους του αντίκτυπου ή του ενδεχόμενου, οι αριθμοί που χρησιμοποιούνται πρέπει να συνδυαστούν μόνο με τύπους που εμπεριέχουν τους

περιορισμούς ή παραδοχές που έγιναν κατά την περιγραφή των χρησιμοποιούμενων κλιμάκων. Πρέπει επίσης να αναφερθεί ότι η χρήση της ημι-ποσοτικής ανάλυσης μπορεί να οδηγήσει σε ορισμένες ανακολουθίες εξαιτίας του γεγονότος ότι οι αριθμοί που επιλέχθηκαν ενδεχομένως να μην αντανακλούν σωστές αναλογίες ανάμεσα στους κινδύνους, ιδιαίτερα όταν είτε οι συνέπειες είτε οι πιθανότητες είναι ακραίες.

Οι τιμές που επιλέγονται θα πρέπει να είναι ενδεικτικές και γενικά επαρκείς για την ιεράρχηση των κινδύνων απέναντι σε άλλους κινδύνους. Κάθε διαδικασία για να λειτουργήσει με επιτυχία θα πρέπει να υπάρχει μια κοινή αντίληψη αυτών των αξιών και των χρησιμοποιουμένων όρων. Οι ορισμοί που παρουσιάζονται παρακάτω μπορούν να αντικατασταθούν με εκείνους που βρίσκονται ήδη σε χρήση εντός του οργανισμού και ενδεχομένως να χρησιμοποιεί ένα υποσύνολο από τη διαχείριση του επιχειρηματικού κινδύνου (ERM), όπου αυτή υπάρχει.

Τυπικές τιμές για τις επιπτώσεις είναι:

- **Ασήμαντη** (τιμή = 1): καμία ουσιαστική ή περιορισμένη επίπτωση.
- **Μικρή** (τιμή = 2): αντίκτυπο σε μικρό μέρος των επιχειρήσεων μόνο, ή αντίκτυπο λιγότερο του 1 εκατομμυρίου δολαρίων ΗΠΑ.
- **Μείζονα** (τιμή = 3): Επιπτώσεις στο brand της εταιρείας, ή αντίκτυπος περισσότερο του 1 εκατομμυρίου δολαρίων ΗΠΑ.
- **Υλική** (τιμή = 4): Επιπτώσεις μεγαλύτερες από 200 εκατομμύρια δολάρια ΗΠΑ οι οποίες απαιτούν εξωτερική αναφορά.
- **Καταστροφική** (τιμή = 5): Αποτυχία ή σημαντική μείωση του μεγέθους της εταιρείας

Τυπικές τιμές για τις πιθανότητες είναι:

- **Σπάνιες** (τιμή = 1).
- **Απίθανες** (τιμή = 2): Δεν παρατηρήθηκαν εντός των τελευταίων 5 ετών.
- **Μέτριες** (τιμή = 3): Παρατηρήθηκαν τα τελευταία 5 χρόνια, αλλά όχι το τελευταίο έτος
- **Πιθανές** (τιμή = 4): Παρατηρήθηκε το τελευταίο έτος.
- **Συχνές** (τιμή = 5): Συμβαίνει σε τακτική βάση.

Οι τιμές αυτές πρέπει να είναι επαρκής ώστε να επιτρέπουν την ιεράρχηση των κινδύνων σύμφωνα με την ημι-ποσοτική προσέγγιση.

Τυπικά, ο κίνδυνος μπορεί να υπολογιστεί ως:

Κίνδυνος = πιθανότητα x επιπτώσεις (πχ. Κίνδυνος = 4 (υλική) x 3 (μέτρια) = 12)

Παράδειγμα ημι-ποσοτικής ανάλυσης

Η αξία της προσέγγισης που παρουσιάζεται εδώ προέρχεται από την ποικιλία των συμμετεχόντων, την ποιότητα της συζήτησης και των ομόφωνων αποφάσεων που επιτεύχθηκαν στο πλαίσιο ενός workshop. Αν η ανάλυση αυτή επιχειρείται «απομονωμένο», είναι πιθανό ότι τα αποτέλεσμα θα είναι εσφαλμένα και ελλιπή.

Βήμα 1. Ποια είναι τα στοιχεία του ενεργητικού της επιχείρησης? Δημιουργία μητρώου των περιουσιακών στοιχείων που προσδιορίζει και εκτιμά τα περιουσιακά αυτά στοιχεία. Εντοπισμός κρίσιμων περιουσιακών στοιχείων στο μητρώο. Αυτό πρέπει να επιτευχθεί σε συνεργασία με τους ιδιοκτήτες των επιχειρήσεων και άλλα ενδιαφερόμενα μέρη.

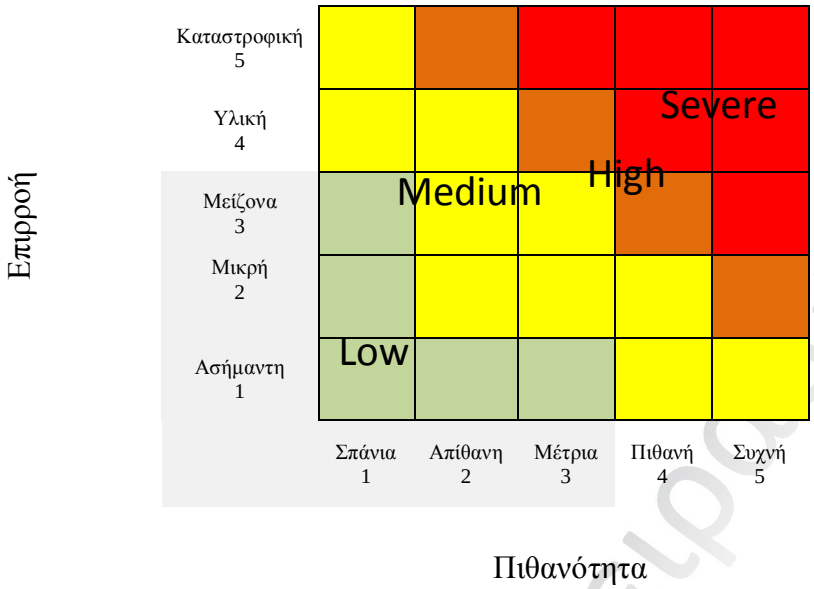
Βήμα 2. Ποιές πιθανές απειλές θέτουν τα περιουσιακά στοιχεία του οργανισμού σε κίνδυνο? Προσδιορισμός των πιθανών απειλών.

Βήμα 3. Για κάθε απειλή, ποια θα ήταν η επίδραση τους στα περιουσιακά στοιχεία της επιχείρησης αν η απειλή αυτή υλοποιηθεί? Προσδιορισμός και ποσοτικοποίηση αυτών των επιπτώσεων από την συσχέτιση των περιουσιακών στοιχείων με το μητρώο. Για κάθε περιουσιακό στοιχείο, προσδιορίζεται ο αντίκτυπος, αν το περιουσιακό στοιχείο δεν είναι πλέον διαθέσιμο, καθώς και η πιθανότητα των εν λόγω επιπτώσεων. Αυτό θα πρέπει να διεξάγεται σε workshops στα οποία συμμετέχουν οι ιδιοκτήτες των επιχειρήσεων, ιδιοκτήτες συστημάτων, εμπειρογνώμονες σε θέματα υποδομών (π.χ. αρχιτέκτονες) και σε θέματα ασφάλειας.

Σε αυτό το μοντέλο, οι επιπτώσεις περιγράφεται ως το κόστος για την επιχείρηση (π.χ. διακοπή λειτουργίας = απώλεια εσόδων), στην περίπτωση κατά την οποία ένα περιουσιακό στοιχείο δεν είναι διαθέσιμο για κάποιο χρονικό διάστημα.

Για να δοθεί περαιτέρω η δυνατότητα στους συμμετέχοντες στα workshops να απεικονίσουν τον κίνδυνο για τα περιουσιακά στοιχεία της επιχείρησης, μπορεί να χρησιμοποιηθεί ένα μεγάλο έντυπο (μερικές φορές χειρόγραφο) πλέγμα. Τα περιουσιακά στοιχεία είναι γραμμένα σε σημειώσεις και τοποθετούνται σε έναν πίνακα ή πλέγμα κίνδυνου. Ο συντονιστής στη συνέχεια δίνει την δυνατότητα στους συμμετέχοντες των workshops να αποφασίσουν για τον αντίκτυπο και τις πιθανότητες για τα περιουσιακά στοιχεία. Ένα τέτοιο πλέγμα παρουσιάζεται στο ακόλουθο σχήμα 3.11.

Σχήμα 3.11: Πίνακας Ημιποσοτικής Επίπτωσης



Σε αυτό το σημείο της διαδικασίας, μπορεί να χρησιμοποιηθεί ένα template για την συλλογή των κινδύνων που έχουν τοποθετηθεί στις υψηλές (high) και σοβαρές (severe) περιοχές του πίνακα. Το πρότυπο αυτό χρησιμοποιείται για την καταγραφή των αποτελεσμάτων από τα παρακάτω βήματα.

Βήμα 1. Αν οι επιπτώσεις είναι αρκετά σημαντικές ώστε να προκαλούν ανησυχία, ποιά τρωτά σημεία και ποιες αδυναμίες μπορεί να υπάρξουν έτσι ώστε να επιτραπεί αυτή στην απειλή την αξιοποίηση των περιουσιακών στοιχείων του οργανισμού, προκαλώντας επιπτώσεις? Τα τρωτά σημεία ή οι αδυναμίες σε συνδυασμό με την γνωστή απειλή θα αλλάξουν την πιθανότητα εκδήλωσης του συμβάντος. Προσδιορισμός και ποσοτικοποίηση αυτών των τρωτών σημείων ή αδυναμιών.

Βήμα 2. Μπορεί αυτές τα τρωτά σημεία ή οι αδυναμίες να εισαχθούν από την εισαγωγή πρόσθετων ελέγχων? Προσδιορισμός των πιθανών στρατηγικών ελέγχου και ποσοτικοποίηση του κόστους (συνολικό κόστος ιδιοκτησίας) για τους ελέγχους αυτούς.

Βήμα 3. Ποια είναι τα αποτελέσματα της ανάλυσης “cost-benefit” τα οποία και προκύπτουν από το επίπεδο της μείωσης των πιθανών επιπτώσεων στις επιχειρήσεις (δηλ. το όφελος) το οποίο σταθμίζεται με το κόστος του πρόσθετου ελέγχου? Ποσοτικοποίηση του οφέλους και του κόστους.

Ποσοτική Ανάλυση

Στην ποσοτική ανάλυση οι αριθμητικές τιμές αποδίδονται εξίσου στις επιπτώσεις και τις πιθανότητες. Αυτές οι τιμές προέρχονται από ποικίλες πηγές. Η ποιότητα της συνολικής ανάλυσης εξαρτάται από την ακρίβεια των τιμών αυτών και την εγκυρότητα των στατιστικών μοντέλων που χρησιμοποιούνται. Οι επιπτώσεις μπορούν να καθοριστούν από την αξιολόγηση και την επεξεργασία των διαφόρων αποτελεσμάτων ενός γεγονότος ή με προέκταση πειραματικών μελετών ή δεδομένων του παρελθόντος. Οι συνέπειες μπορούν να εκφραστούν με διάφορους όρους:

- Χρηματικούς
- Τεχνικούς
- Λειτουργικούς
- Ανθρώπινο παράγοντα

Όπως γίνεται σαφές από την ανωτέρω ανάλυση, ο καθορισμός του επιπέδου του κινδύνου δεν είναι μοναδικός. Οι επιπτώσεις και η πιθανότητα μπορούν να εκφραστούν ή να συνδυαστούν με διαφορετικούς τρόπους, ανάλογα με το είδος του κινδύνου και το πεδίο εφαρμογής και το αντικείμενο της διαδικασίας διαχείρισης επικινδυνότητας.

Προδοκούμενη Ετήσια Απώλεια (Annual Loss Expectancy)

Η ποσοτική εκτίμηση των κινδύνων θα προσπαθήσει να καταλήξει σε μια αριθμητική τιμή, συνήθως εκφρασμένη σε οικονομικούς όρους. Η πιο κοινή μορφή είναι είτε η **single loss expectancy (SLE)** είτε η **annual loss expectancy (ALE)**.

Η SLE είναι το γινόμενο της αξίας του ενεργητικού (Asset Value - AV) πολλαπλασιασμένο με το συντελεστή έκθεσης (EF): SLE=AV*EF .

Η EF είναι η πιθανότητα ότι ένα γεγονός θα συμβεί και ισούται με το ποσοστό της απώλειας των περιουσιακών στοιχείων που προκαλούνται από την απειλή. Το αποτέλεσμα είναι ότι όσο μεγαλύτερη είναι η τιμή αυτή, τόσο μεγαλύτερος είναι ο ενδεχόμενος κίνδυνος της απώλειας.

Η ALE προσθέτει το **ετήσιο ποσοστό εμφάνισης** (annualized rate of occurrence - ARO) στην εξίσως,η με αποτέλεσμα πολλές εμφανίσεις να οδηγούν σε μεγαλύτερες πιθανές απώλειες. Η ALE εκφράζεται συνήθως ως εξής: ALE = SLE*ARO.

Η ALE είναι η αναμενόμενη ετήσια οικονομική ζημία στα περιουσιακά στοιχεία, η οποία προκύπτει από μια συγκεκριμένη απειλή.

Το ετήσιο ποσοστό εμφάνισης (annualized rate of occurrence - ARO), είναι ο αριθμός των φορών που αναμένεται να συμβεί η απειλή σε ένα περιουσιακό στοιχείο. Όσο υψηλότερος

είναι ο κίνδυνος που συνδέεται με την απειλή, τόσο μεγαλύτερη είναι η ARO. Για παράδειγμα, εάν τα δεδομένα ασφαλείας δείχνουν ότι μια σοβαρή πυρκαγιά είναι πιθανό να συμβεί μία φορά σε 25 χρόνια, τότε το ετήσιο ποσοστό εμφάνισης είναι 1/25 = 0,04.

Η EF αντιπροσωπεύει το ποσοστό της απώλειας που θα μπορούσε να έχει μια απειλή σε ένα συγκεκριμένο περιουσιακό στοιχείο, όταν η συγκεκριμένη απειλή αντιστοιχίζεται με ένα συγκεκριμένο τρωτό σημείο. Με άλλα λόγια, **η EF είναι το ποσοστό της αξίας ενός περιουσιακού στοιχείου που είναι πιθανό να καταστραφεί από ένα συγκεκριμένο κίνδυνο.**

Value at Risk (VAR)

Μια άλλη προσέγγιση που απαιτείται σε ορισμένους χρηματοπιστωτικούς τομείς είναι η value at risk (VAR), η οποία μπορεί επίσης να έχει οφέλη και γενική χρησιμότητα στη διαχείριση επικινδυνότητας. Η προσέγγιση αυτή έχει μελετηθεί από διάφορους ερευνητές, γεγονός που υποδηλώνει την καταλληλότητα της προσέγγισης για τη διαχείριση της ασφάλειας των πληροφοριών.

Η VAR είναι ένας υπολογισμός με βάση τα ιστορικά δεδομένα της κατανομής πιθανοτήτων των απωλειών για μια δεδομένη χρονική περίοδο με παράγοντα ασφάλειας 95% ή 99%. Η κατανομή πιθανοτήτων προέρχεται από τη χρήση προσομοιώσεων Monte Carlo που εκτελούνται μέσα από χιλιάδες επαναλήψεις με τυχαίες μεταβλητές, βασισμένες σε ιστορικές πληροφορίες.

Η VAR μπορεί να χρησιμοποιηθεί με επιτυχία στη διαχείριση επικινδυνότητας της ασφάλειας πληροφοριών:

Τα περισσότερα από τα εργαλεία που χρησιμοποιούνται για την εκτίμηση κινδύνου είναι ποιοτικού χαρακτήρα και δεν στηρίζονται στη θεωρία. Η VAR είναι ένα χρήσιμο εργαλείο στα χέρια ενός ειδικού στην ασφάλεια των πληροφοριών, καθώς παρέχει ένα ποσοτικό μέτρο, βασισμένο στη θεωρία, του κινδύνου της ασφάλειας πληροφοριών. Χρησιμοποιώντας αυτό το μέτρο του κινδύνου, μπορεί να επιτευχθεί η καλύτερη δυνατή ισορροπία ανάμεσα στον κίνδυνο και το κόστος για την παροχή ασφάλειας. Οι περισσότεροι οργανισμοί, ιδίως οι μεγάλες επενδύσεις στο ηλεκτρονικό εμπόριο, έχουν ήδη καθορίσει το αποδεκτό επίπεδο κινδύνου. Στη συνέχεια υπολογίζεται το χρηματικό ποσό του κινδύνου αυτού. Όταν το συνολικό VAR ενός οργανισμού υπερβαίνει αυτό το ποσό, η επιχείρηση είναι σε εγρήγορση καθώς απαιτείται αυξημένη έρευνα ασφαλείας.

3.8.9 Αξιολόγηση των κινδύνων

Κατά τη διάρκεια της φάσης αξιολόγησης των κινδύνων, πρέπει να ληφθούν οι αποφάσεις που αφορούν τους κινδύνους που χρειάζονται αντιμετώπιση καθώς και οι προτεραιότητες αντιμετώπισης με βάση την προηγούμενη ανάλυση. Οι αναλυτές πρέπει να συγκρίνουν το επίπεδο του κινδύνου που καθορίζεται κατά τη διαδικασία ανάλυσης των κινδύνων με τα κριτήρια που καθορίζονται στο πλαίσιο της διαχείρισης επικινδυνότητας (στο στάδιο προσδιορισμού κριτηρίων κινδύνου). Είναι σημαντικό να σημειωθεί ότι, σε ορισμένες περιπτώσεις, η αξιολόγηση του κινδύνου μπορεί να οδηγήσει στην απόφαση να προβούμε σε περαιτέρω ανάλυση.

Τα κριτήρια που χρησιμοποιούνται από την ομάδα διαχείρισης επικινδυνότητας πρέπει επίσης να λαμβάνουν υπόψη τους στόχους της οργάνωσης, τις απόψεις των ενδιαφερομένων μερών και, φυσικά, το πεδίο εφαρμογής και τους στόχους της διαδικασίας διαχείρισης επικινδυνότητας, καθώς και πιθανά περιθώρια λάθους. Οι αποφάσεις λαμβάνονται συνήθως με βάση το επίπεδο του κινδύνου, αλλά μπορεί επίσης να σχετίζονται με:

- Τις συνέπειες (επιπτώσεις)
- Την πιθανότητα των γεγονότων
- Την συνολική (συγκεντρωτική) επίπτωση από μια σειρά γεγονότων που θα μπορούσαν να συμβαίνουν ταυτόχρονα.

3.8.10 Επιλογές Διαχείρισης Επικινδυνότητας

Αντιμέτωποι με τον κίνδυνο, οι οργανισμοί έχουν τέσσερις στρατηγικές επιλογές:

- Τερματισμός της δραστηριότητας που οδηγεί σε κίνδυνο.
- Μεταφορά του κινδύνου.
- Αντιμετώπιση του κίνδυνου με τα κατάλληλα μέτρα ελέγχου ή μηχανισμούς.
- Αποδοχή κινδύνου.

Μια άλλη εναλλακτική λύση είναι ότι ένας οργανισμός μπορεί να επιλέξει να αποδεχθεί τον κίνδυνο αγνοώντας τον, το οποίο μπορεί να είναι επίσης επικίνδυνο. Αγνοώντας τον κίνδυνο με την πάροδο του χρόνου, μπορεί να οδηγηθεί σε σοβαρή υποτίμηση του μεγέθους του κινδύνου. Κατά συνέπεια, αυτό γενικά δεν συνιστάται ως πορεία δράσης. Η μοναδική φορά που μπορεί να είναι φρόνιμο να αγνοηθεί ο κίνδυνος, είναι όταν η πιθανότητα, η έκθεση ή οι επιπτώσεις είναι τόσο μικρές ώστε ο κίνδυνος να μην θεωρείται σημαντικός για τον οργανισμό.

Τα μέτρα (μετρήσεις ασφαλείας) μπορεί να επιλεχθούν από σειρές μετρήσεων ασφαλείας που χρησιμοποιούνται στο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) της επιχείρησης, όπως ορίζεται από το ISO / IEC 27001. Σε αυτό το επίπεδο, τα μέτρα ασφάλειας

είναι λεκτικές περιγραφές των διαφόρων λειτουργιών ασφαλείας που εφαρμόζονται τεχνικά (π.χ. software, hardware) ή οργανωτικά (π.χ. καθιερωμένες διαδικασίες).

Τερματισμός της δραστηριότητας που οδηγεί σε κίνδυνο.

Υπάρχουν περιπτώσεις στις οποίες οι δραστηριότητες μπορεί να τροποποιηθούν ή διαδικασίες να αναδιοργανωθούν έτσι ώστε να χρησιμεύσουν για τον περιορισμό ή τη διαχείριση των κινδύνων σε αποδεκτά επίπεδα. Η ανάλυση των δραστηριοτήτων μπορεί επίσης να οδηγήσει στο συμπέρασμα ότι δεν αξίζει κάποιος κίνδυνος.

Μεταφορά του κινδύνου

Ένα παράδειγμα της μεταβίβασης του κινδύνου είναι η απόφαση μιας επιχείρησης να αγοράσει ασφάλεια για την αντιμετώπιση των περιοχών του κινδύνου. Όταν μια εταιρεία αγοράζει ασφάλιση, ο κίνδυνος μεταφέρεται προς την ασφαλιστική εταιρεία σε αντάλλαγμα για την πληρωμή των ασφαλίστρων που αντικατοπτρίζουν την εκτίμηση της ασφαλιστικής εταιρείας του βαθμού του κινδύνου που αναλαμβάνει.

Ο κινδύνου μπορεί επίσης να μεταφερθεί με outsourcing των IT λειτουργιών σε τρίτους παρόχους. Ωστόσο, στη μεταφορά του κινδύνου αυτού, οι συμφωνίες με τρίτους και οι συμβάσεις πρέπει να αφορούν ειδικά την ευθύνη και τις αρμοδιότητες των δύο μερών σε συγκεκριμένες ρήτρες αποζημίωσης.

Τα συμβόλαια αποζημίωσης είναι μέρος της εξωτερικής ανάθεσης της παροχής υπηρεσιών και παρέχουν ένα επίπεδο προστασίας από τα επιβλαβή περιστατικά. Ενώ οι πιθανές οικονομικές επιπτώσεις που συνδέονται με τον κίνδυνο μπορούν να μεταφερθούν, η νομική ευθύνη για τις συνέπειες του συμβιβασμού δεν μπορούν να μεταβιβαστούν.

Οι κίνδυνοι συνήθως μεταφέρονται στις ασφαλιστικές εταιρείες, όταν η πιθανότητα ενός ατυχήματος είναι χαμηλή, αλλά ο αντίκτυπος είναι υψηλός. Ένα παράδειγμα θα ήταν η ασφάλιση από σεισμό ή πλημμύρα. Για τον διευθυντή της ασφάλειας πληροφοριών αυτό σημαίνει ότι ένα καλά οργανωμένο πρόγραμμα κινδύνου πρέπει να συνδέεται κατάλληλα με τους άλλους παρόχους διασφάλισης.

Αντιμετώπιση του Κίνδυνου

Ο κίνδυνος μπορεί να αντιμετωπιστεί με διάφορους τρόπους. Ο κίνδυνος μπορεί να μειωθεί με την εφαρμογή ή τη βελτίωση των ελέγχων ασφαλείας ή τη θέσπιση αντιμέτρων. Οι έλεγχοι αυτοί μπορούν να αντιμετωπίσουν άμεσα τον κίνδυνο ή μπορούν να είναι έλεγχοι αντιστάθμισης που μειώνουν τις επιπτώσεις των συμβάντων. Οι πιθανές επιπτώσεις μπορούν να μειωθούν μέσω διαδικασιών ή τεχνικών μεθόδων. Οι απειλές και τα τρωτά σημεία μπορούν να αντιμετωπιστούν άμεσα μειώνοντας την πιθανότητα εκμετάλλευσης.

Ανοχή / αποδοχή του κίνδυνου

Υπάρχουν διάφορες περιπτώσεις στις οποίες ο κίνδυνος μπορεί να γίνει αποδεκτός. Προϋπόθεση είναι, αν το κόστος μείωσης του είναι πολύ υψηλό σε αναλογία με την αξία του περιουσιακού στοιχείου. Σε άλλες περιπτώσεις μπορεί απλώς να μην είναι εφικτό ο κίνδυνος να αντιμετωπισθεί αποτελεσματικά ή οι ενδεχόμενες επιπτώσεις μπορεί να είναι χαμηλές. Γενικά, υπάρχει ένα βέλτιστο σημείο όπου το κόστος του μετριασμού του κινδύνου είναι ίσο με τη χρηματοοικονομική επίπτωση του συμβιβασμού.

Στοιχεία όπως η εμπιστοσύνη των πελατών, η νομική ευθύνη ή η παραβίαση των κανονιστικών απαιτήσεων μπορεί να χρειαστούν επίσης να εξεταστούν. Σε κάθε περίπτωση, η διαδικασία διαχείρισης επικινδυνότητας, πρέπει να επιτρέπει την ακριβή και κατάλληλη τεκμηρίωση του κινδύνου, προκειμένου ο διαχειριστής των επιχειρήσεων να πάρει την απόφαση να αποδεχτεί τον κίνδυνο με βάση την επαρκή γνώση και κατανόηση. Η αποδοχή των κινδύνων θα πρέπει να επανεξετάζεται τακτικά προκειμένου να εξασφαλιστεί ότι το σκεπτικό για την αρχική αποδοχή εξακολουθεί να ισχύει εντός του ισχύοντος πλαισίου των επιχειρήσεων.

Πλαίσιο Αποδοχής Κίνδυνου

Το πλαίσιο αποδοχής των κινδύνων αποτελεί ένα σημαντικό εργαλείο. Με αυτό, η επιχείρηση μπορεί να διασφαλίσει ότι η αποδοχή του κινδύνου εκτελείται στο σωστό επίπεδο διαχείρισης.

Ένα τυπικό πλαίσιο αποδοχής κινδύνου παρουσιάζεται παρακάτω στον σχήμα 3.12.

Σχήμα 3.12: Πλαίσιο Αποδοχής Κίνδυνου

Πλαίσιο Αποδοχής Κίνδυνου	
Επίπεδο Κινδύνου	**Απαιτούμενο διοικητικό επίπεδο για την αποδοχή του κινδύνου**
Χαμηλό	Η Αποδοχή του κινδύνου είναι εφικτή από την τοπική διαχείριση
Μεσαίο	Η Αποδοχή του κινδύνου είναι εφικτή από τον chief information officer (CIO)
Υψηλό	Η Αποδοχή του κινδύνου είναι εφικτή από τον CIO, τον διευθυντή ή τον γενικό διευθυντή της ασφάλειας πληροφοριών (CISO), ανάλογα τις ενδεχόμενες επιπτώσεις
Κρίσιμο	Αποδοχή του κινδύνου μόνο σε επίπεδο διοικητικού συμβουλίου, ανάλογα με τις ενδεχόμενες επιπτώσεις. Η μείωση του κινδύνου είναι υποχρεωτική, μέσω αυστηρών ελέγχων και παρακολούθησης. Απαιτείται η διαδικασία κοινοποίησης στη Διοίκηση.

3.8.11 Επιπτώσεις

Οι επιπτώσεις είναι η κατώτατη γραμμή για τη διαχείριση του κινδύνου. Τελικά, όλες οι δραστηριότητες διαχείρισης επικινδυνότητας αποσκοπούν στη μείωση των επιπτώσεων σε αποδεκτά επίπεδα. Το αποτέλεσμα οποιαδήποτε τρωτού σημείου το οποίο και εκμεταλλεύεται η απειλή και προκαλεί απώλεια, είναι οι επιπτώσεις. Οι απειλές και τα τρωτά σημεία που δεν προκαλούν επιπτώσεις είναι συνήθως άσχετα.

Σε εμπορικούς οργανισμούς, οι επιπτώσεις γενικά ποσοτικοποιούνται ως άμεση οικονομική ζημία σε σύντομο χρονικό διάστημα ή απόλυτη (έμμεση) οικονομική ζημία σε μακροπρόθεσμη βάση. Παραδείγματα τέτοιων ζημιών περιλαμβάνουν τα ακόλουθα:

- Άμεση απώλεια χρημάτων (μετρητά ή πιστωτική)
- Ποινική ή αστική ευθύνη Απώλεια της φήμης / υπεραξίας / εικόνας
- Μείωση της αξίας της μετοχής
- Σύγκρουση συμφερόντων για το προσωπικό ή τους πελάτες ή τους μετόχους
- Παραβίαση της εμπιστοσύνης / ιδιωτικής ζωής
- Απώλεια επιχειρηματική ευκαιρία / ανταγωνισμού
- Απώλεια μεριδίου αγοράς
- Μείωση της λειτουργικής αποδοτικότητας / απόδοσης
- Διακοπή της επιχειρηματικής δραστηριότητας
- Μη συμμόρφωση με νόμους και κανονισμούς που προκύπτουν σε κυρώσεις

Όπως με τους υπολογισμούς του κινδύνου έτσι και οι υπολογισμοί των επιπτώσεων μπορεί να γίνουν είτε **ποιοτικά** είτε **ποσοτικά**. Ορισμένες επιπτώσεις επιδέχονται ποσοτικό υπολογισμό, όπως το εύρος των πιθανών οικονομικών επιπτώσεων. Άλλες, όπως η απώλεια της φήμης ή του μεριδίου αγοράς, μπορεί να είναι πιο δύσκολες και μπορεί να υπολογίζονται επαρκώς από ποιοτικούς υπολογισμούς. Οι επιπτώσεις καθορίζονται από την εκτέλεση μιας αξιολόγησης των επιπτώσεων των επιχειρήσεων και την επακόλουθη ανάλυση. Η ανάλυση αυτή θα καθορίσει την κρισιμότητα και την ευαισθησία των πηγών πληροφόρησης. Παρέχει τη βάση για τον καθορισμό των αδειών πρόσβασης και το σχεδιασμό της επιχειρηματικής συνέχειας (BCP), ενώ περιλαμβάνει τους στόχους για τους χρόνους αποκατάστασης (RTOs). Χρησιμεύει για να δοθεί προτεραιότητα στη διαχείριση επικινδυνότητας και, σε συνδυασμό με τις αποτιμήσεις των περιουσιακών στοιχείων, παρέχει τη βάση για τα επίπεδα και είδη προστασίας που απαιτούνται, καθώς και την βάση για την ανάπτυξη της επιχείρησης.

3.9 Έλεγχοι και Αντιμέτρα

Ο καθορισμός των στρατηγικών επιλογών και των προτεραιοτήτων για τη μείωση των κινδύνων σε επίπεδα αποδεκτά για την επιχείρηση, αποτελούν βασικές αρμοδιότητες του διαχειριστή της ασφάλειας πληροφοριών. Καθώς οι κίνδυνοι που αντιμετωπίζει ένας οργανισμός εντοπίζονται και ιεραρχούνται και τα περιουσιακά στοιχεία αποτιμώνται και κατηγοριοποιούνται, ο διευθυντής της ασφάλειας πληροφοριών μπορεί να προσαρμόσει τις στρατηγικές ασφάλειας και να ιεραρχήσει τις επιλογές για τον περιορισμό αυτών των κινδύνων. Οι έλεγχοι μπορεί να περιλαμβάνουν:

- **Αποτρεπτικοί έλεγχοι** για την μείωση της πιθανότητας ή της ευπάθειας στις απειλές
- **Προληπτικοί έλεγχοι** για τη μείωση των τρωτών σημείων και την αποτυχία μιας επίθεσης ή την μείωση των επιπτώσεών της.
- **Διορθωτικοί έλεγχοι** για τη μείωση των επιπτώσεων
- **Αντισταθμιστικοί έλεγχοι**, για την αντιστάθμιση των αυξημένων κίνδυνων
- **Ανιχνευτικοί έλεγχοι** για την ανακάλυψη επιθέσεων και την ενεργοποίηση προληπτικών ή διορθωτικών ελέγχων.

Ο διαχειριστής της ασφάλειας πληροφοριών θα πρέπει να γνωρίζει τα διάφορα εργαλεία και τις διαδικασίες για την μείωση των κινδύνων εντός της δομής της οργάνωσης και πρέπει να εξισορροπήσει τις διαθέσιμες επιλογές από ό,τι είναι αποδεκτό από την επιχείρηση. Πρέπει να εξετάσει το κόστος και τον αντίκτυπο των μέτρων ασφαλείας σύμφωνα με την κουλτούρα της επιχείρησης και την ικανότητά της να ολοκληρώσει τους επιχειρησιακούς της στόχους. Πρέπει να γνωρίζει ότι ένα ακατάλληλο σύνολο από στρατηγικές και επιλογές θα μπορούσε να εμποδίσει τις συνήθεις εμπορικές πράξεις. Ένα παράδειγμα θα μπορούσε είναι η περιορισμένη πρόσβαση στο Διαδίκτυο από τους εργαζομένους. Ενώ αυτό μειώνει ορισμένους κινδύνους, ο οργανισμός μπορεί να χρειάζεται το Διαδίκτυο για την έρευνα και περιορίζοντας την πρόσβαση ενδεχομένως να οδηγήσει σε μειωμένη αποτελεσματικότητα των εργαζομένων.

Όπως αναφέρθηκε προηγουμένως, ***το κόστος του ελέγχου δεν θα πρέπει ποτέ να υπερβαίνει το όφελος που συνεπάγεται***. Οι υπολογισμοί του κόστους πρέπει να περιλαμβάνουν κάθε επαναλαμβανόμενες εργασίες ή χρόνους που απαιτούνται από το προσωπικό και κόστη εκτός προϋπολογισμού, ως αποτέλεσμα της εγκατάστασης ελέγχου ή εν εξελίξει διαχείριση και διοίκηση.

Το κλειδί για τη διαχείριση του κινδύνου είναι η μείωση του κινδύνου ή η αντιμετώπιση (πώς ο αξιολογούμενος κίνδυνος αντιμετωπίζεται από την επιχείρηση). Η διαδικασία αντιμετώπισης του κινδύνου παρουσιάζεται στο σχήμα 2.9.

3.9.1 Θέματα Σχεδιασμού ελέγχων

Με την εφαρμογή των πλαισίων όπως είναι το COBIT και το ISO 27001, ο σχεδιασμός των ελέγχων που εφαρμόζονται πρέπει να περιλαμβάνει την δυνατότητα **μέτρησης των ελέγχων** αυτών. ***Η αποτελεσματικότητα των ελέγχων δεν μπορεί να αξιολογηθεί εάν αυτοί δεν μπορούν να ελεγχθούν και να μετρηθούν***. Επιπλέον, τα επίπεδα εμπιστοσύνης και η δειγματοληψία για τον έλεγχο της αποτελεσματικότητας των ελέγχων αυτών αντικατοπτρίζουν άμεσα τα αντικείμενα των ελεγκτικών μηχανισμών και της κανονιστικής συμμόρφωσης. Για παράδειγμα, κατά τον σχεδιασμό ενός ελέγχου για το σύστημα καθημερινής ανίχνευσης εισβολών (intrusion detection system - IDS) σε μια εταιρεία που υπόκειται στο νόμο Sarbanes-Oxley Act (SOX) των ΗΠΑ, είναι λογικό να δημιουργηθεί μια διαδικασία καθημερινών αναφορών και δειγματοληψίας που να ακολουθεί τις απαιτήσεις δοκιμών SOX με βάση τη συχνότητα του ελέγχου, δηλαδή 25 δείγματα καθημερινά, 10 εβδομαδιαία, 3 σε μηνιαία βάση. Αν οι έλεγχοι της ασφάλειας των πληροφοριών δοκιμάζονται με συνέπεια, η συμμόρφωση είναι ενσωματωμένη.

Όσον αφορά τη συμμόρφωση, ο κύριος ρόλος του διαχειριστή της ασφάλειας των πληροφοριών είναι η διασφάλιση ότι ο οργανισμός είναι σε συμμόρφωση με τις σχετικές νομικές και κανονιστικές απαιτήσεις.

3.9.2 Η ισχύς των ελέγχων

Η ισχύς των ελέγχων μπορεί να μετρηθεί από το είδος του ελέγχου που αξιολογείται κάθε φορά (προληπτικός, διερευνητικός, αυτοματοποιημένος κ.λπ.) και τα συμμορφούμενα ποσοτικά και ποιοτικά αποτελέσματα δοκιμών. Ως εκ τούτου, αν και ένας αυτοματοποιημένος έλεγχος είναι εξ ορισμού ισχυρότερος από ένα χειροκίνητο έλεγχο, μια λεπτομερής ανάλυση μπορεί να αποκαλύψει ότι ένας χειροκίνητος έλεγχος είναι καλύτερος. Ο σχεδιασμός ενός αυτοματοποιημένου ελέγχου μπορεί να δημιουργήσει συναγερμούς και να παράγει αυτόματες αναφορές. Ωστόσο, μετά από προσεκτική εξέταση της διαδικασίας, μπορεί κανείς να διαπιστώσει ότι α) δεν μπορεί να παραχθεί κανένα αποδεικτικό στοιχείο αναθεώρησης της άνωθεν διαδικασίας και β) οι επακόλουθες ενέργειες δεν μπορούν να υπολογιστούν. Σε αυτή την περίπτωση ο έλεγχος αποτυγχάνει.. Από την άλλη πλευρά, αν οι χειρόγραφες σημειώσεις καταγράφονταν σε αναφορές ημερήσιας βάσης με ημερομηνίες, και οι ίδιες σημειώσεις περιλάμβαναν ανάλυση, σχέδια δράσης κλπ τότε ο χειροκίνητος έλεγχος θα ήταν πολύ πιο αποτελεσματικός από έναν αυτοματοποιημένο. Φυσικά, δεν μπορεί να προκύψει κανένα συμπέρασμα ως προς την ισχύ του ελέγχου μέχρι αυτός να δοκιμασθεί επαρκώς.

Πρέπει να τονιστεί στη διοίκηση ότι οι κίνδυνοι του IT είναι επιχειρηματικοί κίνδυνοι, και η προσυπογραφή της διοίκησης σε κάθε διαχείριση επικινδυνότητας, ιδιαίτερα ως προς την αποδοχή των υπολειμματικών κινδύνων, καθίσταται απαραίτητη.

Προκειμένου η μείωση του κινδύνου να αποδείξει την αξία και την ευθυγράμμιση της με τους επιχειρηματικούς στόχους, πρέπει να συνδέεται με τις υποστηριζόμενες λειτουργίες της επιχείρησης. Αυτό εξασφαλίζει ότι η ασφάλεια πληροφοριών και οι πρωτοβουλίες της διακυβέρνησης του IT πειθαρχούν και η αιτιολόγηση του κόστους για τη διαδικασία αντιμετώπισης είναι άμεσα διαθέσιμη και αυτονόητη. Αυτό επιβεβαιώνει την βασική αρχή ότι οι κίνδυνοι του IT αποτελούν επιχειρηματικούς κινδύνους.

Το κλειδί για τη διαχείριση του κινδύνου είναι η μείωση του κινδύνου ή η αντιμετώπισή του. Η διαδικασία αντιμετώπισης του κινδύνου απεικονίζεται στο σχήμα 2.9 . Μόλις οι κίνδυνοι εντοπιστούν, γίνεται αξιολόγηση των υπαρχόντων έλεγχων και των αντίμετρων ή σχεδιάζονται νέοι για τον περιορισμό των κινδύνων σε αποδεκτά επίπεδα.

3.9.3 Μέθοδοι Ελέγχων

Οι έλεγχοι ασφαλείας περιλαμβάνουν τη χρήση τεχνικών και μη τεχνικών μεθόδων. Οι τεχνικοί έλεγχοι αποτελούν παράγοντες ασφαλείας, ενσωματωμένοι στο hardware, software και firmware των υπολογιστών (π.χ. μηχανισμοί ελέγχου πρόσβασης, μηχανισμοί αναγνώρισης και πιστοποίησης, μέθοδοι κρυπτογράφησης, λογισμικό ανίχνευσης εισβολής). Οι μη τεχνικοί έλεγχοι είναι οι διοικητικοί και λειτουργικοί, όπως είναι οι πολιτικές ασφάλειας, οι επιχειρησιακές διαδικασίες, το ανθρώπινο δυναμικό και η σωματική και περιβαλλοντική ασφάλεια.

Τα στοιχεία των ελέγχων που πρέπει να εξεταστούν κατά την αξιολόγηση της ισχύος του ελέγχου περιλαμβάνουν εάν οι έλεγχοι είναι προληπτικοί ή διερευνητικοί, χειροκίνητοι ή αυτοματοποιημένοι, και formal (τεκμηριωμένοι στα εγχειρίδια διαδικασιών) ή ad hoc.

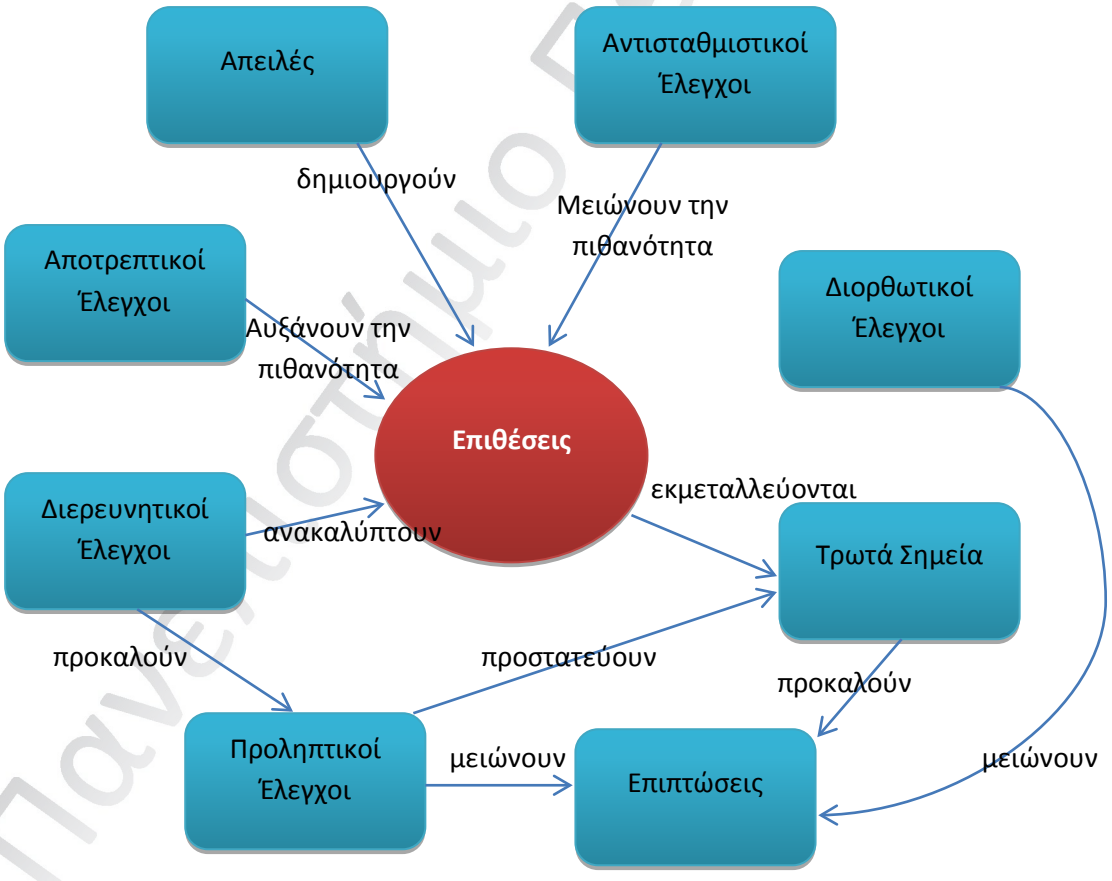
3.9.4 Κατηγορίες Ελέγχων

Όπως αναφέρθηκε προηγουμένως, οι έλεγχοι μπορούν να κατηγοριοποιηθούν ως εξής:

- **Προληπτικοί**: Οι προληπτικοί έλεγχοι εμποδίζουν τις προσπάθειες παραβίασης της πολιτικής ασφάλειας και περιλαμβάνουν ελέγχους πρόσβασης, κρυπτογράφησης και ελέγχους ταυτότητας.
- **Διερευνητικοί**: Οι διερευνητικοί έλεγχοι προειδοποιούν για παραβιάσεις ή απόπειρα παραβίασης της πολιτικής ασφάλειας και περιλαμβάνουν τους ελέγχους όπως είναι τα audit trails, μεθόδους ανίχνευσης εισβολής και checksums.

- **Διορθωτικοί**: Οι διορθωτικοί έλεγχοι είναι υπεύθυνοι για την αποκατάσταση των τρωτών σημείων. Οι διαδικασίες αντιγράφων ασφαλείας και επαναφοράς των συστημάτων είναι ένα διορθωτικό μέτρο καθώς επιτρέπει την ανάκτηση ενός συστήματος σε περίπτωση που η βλάβη είναι τόσο εκτεταμένη ώστε η επεξεργασία να μην μπορεί να συνεχιστεί χωρίς την προσφυγή σε διορθωτικά μέτρα.
- **Αντισταθμιστικοί**: Οι αντισταθμιστικοί έλεγχοι αντισταθμίζουν τον αυξημένο κίνδυνο με την προσθήκη βημάτων ελέγχου που μειώνουν τον κίνδυνο.
- **Αποτρεπτικοί**: Οι αποτρεπτικοί έλεγχοι παρέχουν προειδοποιήσεις που μπορούν να αποτρέψουν πιθανούς συμβιβασμούς, όπως η προσφορά αμοιβής για τη σύλληψη των χάκερς. Οι έλεγχοι και η επίδρασή τους φαίνεται στο ακόλουθο σχήμα.

Σχήμα 3.14: Είδη ελέγχων



Οι έλεγχοι ορίζονται ως οι πολιτικές, οι διαδικασίες, οι πρακτικές και οι κατευθυντήριες γραμμές που αποσκοπούν στην παροχή εύλογης βεβαιότητας ότι οι επιχειρηματικοί στόχοι

θα επιτευχθούν και ότι τα ανεπιθύμητα συμβάντα θα προληφθούν ή θα εντοπιστούν και θα διορθωθούν.

Τα αντίμετρα μειώνουν άμεσα την απειλή ή τα τρωτά σημεία και μπορεί να θεωρηθούν στοχοθετημένοι έλεγχοι. Η παύση μιας δραστηριότητας που δημιουργεί κίνδυνο είναι ένα παράδειγμα ενός αντίμετρου. Η κατάτμηση του δικτύου είναι επίσης ένα αντίμετρο, δεδομένου ότι μειώνει την ευπάθεια του δικτύου σε περίπτωση παραβίασης. Έχοντας πολλαπλούς παρόχους υπηρεσιών Διαδικτύου (ISP) είναι ένα αντίμετρο που μειώνει την πιθανότητα μιας συνολικής διακοπής του Διαδικτύου.

Η δύναμη του ελέγχου μπορεί να μετρηθεί από την δύναμη του σχεδιασμού και την πιθανότητα της αποτελεσματικότητάς του. Ένα παράδειγμα ενός εκ φύσεως ισχυρού έλεγχου είναι ο διαχωρισμός αρμοδιοτήτων μεταξύ πολλαπλών υπαλλήλων. Ένα παράδειγμα ενός εκ φύσεως ισχυρού σχεδιαστικού έλεγχου είναι η απαίτηση διπλού ελέγχου πρόσβασης σε ευαίσθητες περιοχές ή υλικά.

3.9.5 Προτάσεις Ελέγχου

Τα στοιχεία των ελέγχων που πρέπει να εξεταστούν κατά την αξιολόγηση της ισχύος του ελέγχου περιλαμβάνουν εάν οι έλεγχοι είναι προληπτικοί ή διερευνητικοί, χειροκίνητοι ή αυτόματοι και formal ή ad-hoc. Κατά την διάρκεια αυτού του βήματος της διαδικασίας, διατίθενται οι έλεγχοι που μπορεί να μειώσουν ή να άρουν τους διαπιστωμένους κινδύνους (σύμφωνα με τις δραστηριότητες της επιχείρησης). Ο στόχος των προτεινόμενων ελέγχων είναι να μειώσουν το επίπεδο του κινδύνου στις πηγές πληροφόρησης σε αποδεκτά επίπεδα. Οι ακόλουθοι παράγοντες πρέπει να εξεταστούν για την ελαχιστοποίηση ή την εξάλειψη των κινδύνων που εντοπίζονται, κατά τη σύσταση των ελέγχων και των εναλλακτικών λύσεων:

- **Αποτελεσματικότητα** των συνιστώμενων επιλογών (π.χ. συμβατότητα του συστήματος)
- **Νομοθεσία και κανονιστικές ρυθμίσεις**
- **Οργανωτική πολιτική**
- **Λειτουργικές επιπτώσεις**
- **Ασφάλεια και αξιοπιστία**

Οι προτάσεις ελέγχου είναι τα αποτελέσματα της διαδικασίας αξιολόγησης των κινδύνων και συνεισφέρουν στη διαδικασία μείωσης του κινδύνου. Κατά τη διάρκεια της διαδικασίας μείωσης του κινδύνου, οι συνιστώμενοι, οι διαδικαστικοί και οι τεχνικοί έλεγχοι ασφαλείας αξιολογούνται, ιεραρχούνται και εφαρμόζονται. Δεν μπορούν να υλοποιηθούν όλοι οι πιθανοί έλεγχοι για να μειωθούν οι απώλειες. Για να προσδιοριστεί ποιοι είναι απαραίτητοι και κατάλληλοι για τη συγκεκριμένη επιχείρηση, μία ανάλυση κόστους-οφέλους πρέπει να διεξαχθεί για τους συνιστώμενους ελέγχους, για να αποδείξει ότι το κόστος της εφαρμογής των ελέγχων μπορεί να δικαιολογηθεί από τη μείωση του επιπέδου του κινδύνου. Επιπλέον,

οι λειτουργικές επιπτώσεις (π.χ. η επίδραση στην απόδοση του συστήματος) και η σκοπιμότητα (π.χ. τεχνικές προδιαγραφές, η αποδοχή των χρηστών) της εισαγωγής της προτεινόμενης επιλογής πρέπει να αξιολογηθεί προσεκτικά κατά τη διάρκεια της διαδικασίας μείωσης του κινδύνου.

3.9.6 Υπολειπόμενος Κίνδυνος (Residual Risk)

Ο κίνδυνος που εξακολουθεί να παραμένει μετά τα αντίμετρα και τους ελέγχους που εφαρμόζονται λέγεται υπολειπόμενος κίνδυνος. Χρησιμοποιώντας το παράδειγμα του διπλού ελέγχου που απαιτείται για την πρόσβαση σε ευαίσθητες πληροφορίες, ένας υπολειπόμενος κίνδυνος είναι δύο άτομα συνωμοτούν για την παροχή μη εξουσιοδοτημένης πρόσβασης.

Ο υπολειπόμενος κίνδυνος που αναφέρεται μέσα σε μια αξιολόγηση επικινδυνότητας μπορεί να χρησιμοποιηθεί από τη διοίκηση για τον εντοπισμό των τομέων στους οποίους απαιτείται περισσότερος έλεγχος για να μειωθεί ακόμη περισσότερο ο κίνδυνος. Τα αποδεκτά επίπεδα κινδύνου αποτελούν μέρος της ανάπτυξης μιας στρατηγικής για την ασφάλεια των πληροφοριών, όπως περιγράφεται στο προηγούμενο κεφάλαιο. Εάν η στρατηγική δεν έχει αναπτυχθεί, η διαχείριση πρέπει να καθορίσει τα αποδεκτά επίπεδα κινδύνου, συνήθως από την άποψη των επιτρεπόμενων επιπτώσεων. Οι κίνδυνοι που υπερβαίνουν αυτό το επίπεδο θα πρέπει να μειωθούν με την εφαρμογή αυστηρότερων ελέγχων ή αντίμετρων. Οι κίνδυνοι κάτω από αυτό το επίπεδο θα πρέπει να αξιολογούνται ώστε να καθοριστεί αν είναι υπερβολικό το επίπεδο των αντισταθμιστικών μέτρων ή των ελέγχων που εφαρμόζονται και εάν υπάρχει δυνατότητα μείωσης του κόστους, με την αφαίρεση ή την τροποποίηση τους. Η οριστική αποδοχή των υπολειμματικών κινδύνων λαμβάνει υπόψη τα ακόλουθα:

- Κανονιστική συμμόρφωση
- Οργανωτική πολιτική
- Ευαισθησία και κρισιμότητα των σχετικών περιουσιακών στοιχείων
- Αποδεκτά επίπεδα των δυνητικών επιπτώσεων
- Αβεβαιότητα ενσωματωμένη στην αξιολόγηση του κινδύνου.
- Κόστος και αποτελεσματικότητα της εφαρμογής

Κατά την αξιολόγηση της καταλληλότητας των ελέγχων ή των αντίμετρων, το κόστος εφαρμογής και λειτουργίας ειδικών μέτρων ή μηχανισμών θα πρέπει να σταθμίζεται έναντι του κινδύνου που αντιμετωπίζεται.

Η απόφαση αυτή περιλαμβάνει εκτίμηση των δύο συνιστωσών:

- Της πιθανότητας (πιθανότητα εμφάνισης) της απώλειας ή ζημίας σε συγκεκριμένα περιουσιακά στοιχεία
- Του μεγέθους και της οικονομικής ή άλλης επίπτωσης τέτοιων περιστατικών

Ο προσδιορισμός της πιθανότητας εμφάνισης περιλαμβάνει επιχειρηματική κρίση, όπως στα ακόλουθα παραδείγματα:

- Η ακεραιότητα και το στυλ λειτουργίας της διαχείρισης ενός οργανισμού και η ομάδα του επηρεάζει τη συνείδηση του ελέγχου του συνόλου του προσωπικού. Αν η κουλτούρα της ασφάλειας είναι αδύναμη, ακόμα και με τα καλύτερους ελέγχους, η αδύναμη τήρηση ή καταστρατήγηση μπορεί να αυξήσει την πιθανότητα εμφάνισης ζημιών.
- Η φύση των επιχειρηματικών διαδικασιών (π.χ. απομακρυσμένες / χωρίς επίβλεψη εργασίες, έλλειψη διαχωρισμού καθηκόντων κλπ) μπορεί επίσης να καθορίσει την πιθανότητα της απώλειας ή ζημιάς.
- Η ελκυστικότητα των περιουσιακών στοιχείων οδηγεί σε μεγαλύτερη έκθεση, σε κίνδυνο και εμφάνιση ζημιών.

3.9.7 Κόστη και Οφέλη

Όταν έχουν προγραμματιστεί έλεγχοι ή αντίμετρα, ένας οργανισμός πρέπει να εξετάσει τα κόστη και τα οφέλη. Αν το κόστος των ελέγχων ή των αντίμετρων δεν υπερβαίνουν τα οφέλη, ένας οργανισμός μπορεί να επιλέξει να αποδεχθεί τον κίνδυνο αντί να επιβαρυνθεί με επιπρόσθετα κόστη για την εξασφάλιση των συστημάτων του. Αυτό ακολουθεί τη γενική αρχή ότι το κόστος του ελέγχου δεν πρέπει να υπερβαίνει το αναμενόμενο όφελος. Αυτή είναι η αρχή της αναλογικότητας που περιγράφεται στις γενικά αποδεκτές αρχές των συστημάτων ασφάλειας (GASSP) ή του διάδοχού του, τις γενικά αποδεκτές αρχές της ασφάλειας πληροφοριών (GAISP).

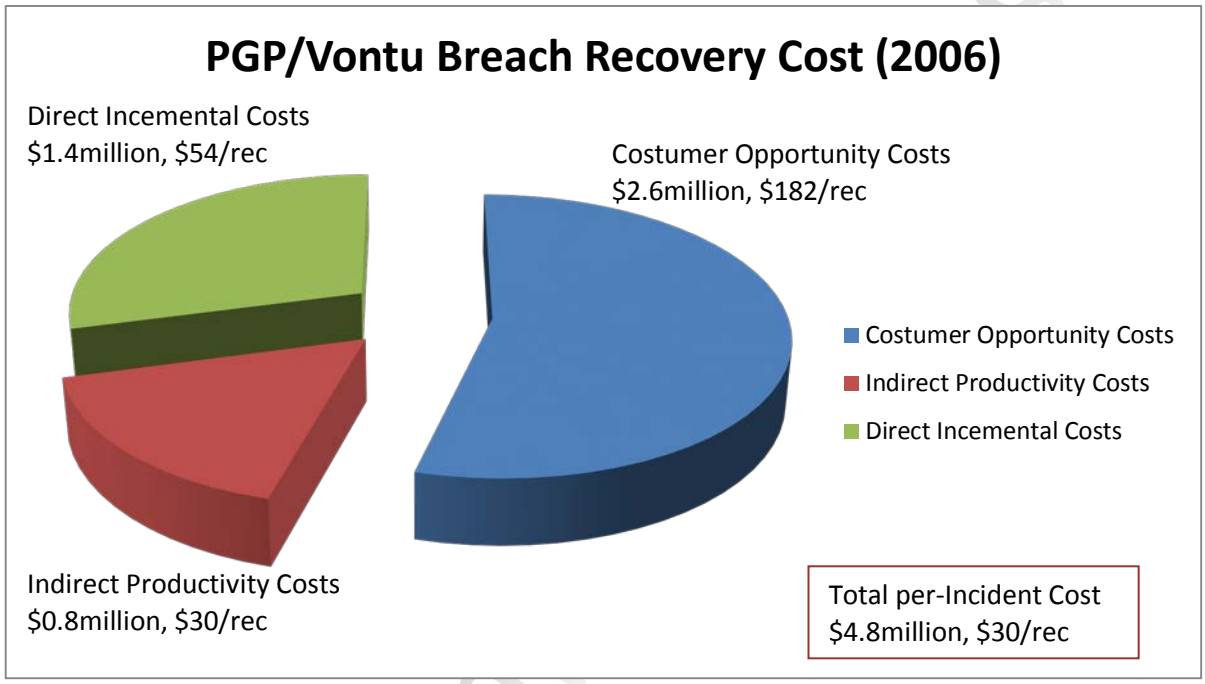
Η ανάλυση κόστους-οφέλους βοηθά στην παροχή μιας οικονομικής άποψης των επιπτώσεων των κινδύνων και στον καθορισμό του κόστους της προστασίας της σημαντικότητας. Ωστόσο, με την ανάλυση κόστους-οφέλους γίνονται έξυπνες επιλογές με βάση τις πιθανές δαπάνες μείωσης του κινδύνου έναντι των πιθανών απωλειών.

Δυστυχώς, στα περισσότερα εγκλήματα της ασφάλειας πληροφοριών οι μετρήσεις απώλειας δεν είναι καθιερωμένες, όπως η κλοπή στατιστικών. Στην ετήσια έρευνα (CSI Computer Security Institute) εγκλήματος πληροφορικής και ασφάλειας υπήρξε μία και μόνη μέτρηση που αφορούσε απώλειες στο χώρο της ασφάλειας των πληροφοριών αλλά ορισμένοι νομικοί πιστεύουν ότι τα αριθμητικά στοιχεία της απώλειας είναι υποτιμημένα, ενώ άλλοι πιστεύουν ότι έχουν υπερεκτιμηθεί.

Αντί να γίνεται συζήτηση για την ισχύ αυτών των μέτρων, μπορεί να είναι πιο χρήσιμο να δούμε μετρήσεις τις οι περισσότεροι οργανισμοί μπορούν να ποσοτικοποιήσουν με ακρίβεια. Τρεις από τις μετρήσεις των πιθανών απωλειών είναι **οι επιπτώσεις στην παραγωγικότητα των εργαζομένων, οι απώλειες εσόδων και τα γεγονότα απωλειών άμεσου κόστους**. Τα

περιστατικά ιών και σκουληκιών είναι αυτά που αναφέρονται συχνότερα κατά τη συζήτηση των επιπτώσεων στην παραγωγικότητα. Ένα άλλο είναι το αποτέλεσμα είναι οι ζημίες των αναγνωρίσιμων προσωπικών πληροφοριών (personally identifiable information - PII) ως αποτέλεσμα περιστατικού που σχετίζεται με την ασφάλεια, όπως φαίνεται στο ακόλουθο σχήμα 3.15 και περιγράφει λεπτομερώς τις συνέπειες των ζημιών σε 31 οργανισμούς που αναλύθηκαν από την PGP-Vontu.

Σχήμα 3.15: Έρευνα PGP-Vontu



Ένα παράδειγμα της προτεινόμενης προσέγγισης θα μπορούσε να είναι το αποτέλεσμα ενός κακόβουλου λογισμικού που μολύνει 10.000 υπαλλήλους σε μια επιχείρηση με 40.000 άτομα. Κάθε μολυσμένο σύστημα στοιχίζει στον κάθε εργαζόμενος που επηρεάζει μία ώρα παραγωγικότητας. Εάν κάθε εργαζόμενος έχει ωρομίσθιο των $30, τότε αυτό υπολογίζεται σε αντίκτυπο των 300.000 δολαρίων. Έτσι όταν ο πιθανός αριθμός απωλειών έχει προσδιοριστεί, είναι ευκολότερο να ληφθούν αποφάσεις αποκατάστασης του κινδύνου.

Η απώλεια εσόδων μπορεί επίσης να καθοριστεί με παρόμοιο τρόπο. Εάν μια επιχείρηση έχει ιστοσελίδα ηλεκτρονικού εμπορίου που παράγει 1 εκατ. Δολάρια ΗΠΑ έσοδα κάθε μέρα, τότε η επίθεση με απώλεια της υπηρεσίας (DoS) που διαρκεί μισή ημέρα δημιουργεί απώλεια 500.000 δολαρίων ΗΠΑ. Είναι αμφίβολο αν αυτό το είδος της επίθεσης θα αναγκάσει τους πελάτες απλώς να καθυστερήσουν τις αγορές τους, ή αν απλά θα πάνε σε έναν άλλο ανταγωνιστή. Ωστόσο, η δημόσια αντίληψη για τον οργανισμό που είναι θύμα μιας τέτοιας εισβολής - επίθεσης, θέτοντας ευαίσθητες πληροφορίες σε κίνδυνο ή όχι, έχουν συχνά ως αποτέλεσμα την απώλεια της εμπιστοσύνης των πελατών.

Ενώ η παραγωγικότητα και οι απώλειες εσόδων θεωρούνται άμεσες απώλειες, έμμεσες απώλειες ενδέχεται να περιλαμβάνουν τον αριθμό των ωρών υπερεργασίας, κατά τον οποίο

οι εργαζόμενοι πρέπει να εργαστούν για να ανταποκριθούν και να ανακτήσουν ένα τέτοιο συμβάν. Ένα άλλο άμεσο κόστος μπορεί να είναι οι πρόσθετες προσπάθειες προστασίας που προκύπτουν από έναν συμβιβασμό.

Κατά την εξέταση των δαπανών, το συνολικό κόστος ιδιοκτησίας (TCO) πρέπει να υπολογιστεί για τον πλήρη κύκλο ζωής του ελέγχου ή των αντιμέτρων. Αυτό μπορεί να περιλαμβάνει στοιχεία όπως:

- Κόστος απόκτησης
- το κόστος ανάπτυξης και υλοποίησης
- Επαναλαμβανόμενο κόστος συντήρησης
- δαπάνες δοκιμών και αξιολόγησης
- παρακολούθηση της συμμόρφωσης και επιβολής
- Ταλαιπωρία για τους χρήστες
- Μειωμένη απόδοση των ελεγχόμενων διαδικασιών
- Κατάρτιση στις νέες διαδικασίες ή τεχνολογίες.

3.10 Πληροφορίες Αποτίμησης Πόρων

Η διαδικασία αποτίμησης, η οποία αποτελείται από την συσχέτιση των αξιών σε μία κοινή οικονομική μορφή, μπορεί να είναι απλή για ορισμένα περιουσιακά στοιχεία. Το Hardware μπορεί εύκολα να αποτιμηθεί με βάση το κόστος αντικατάστασης. Η αξία, σε ορισμένες περιπτώσεις, είναι το κόστος της ανάπλασης ή αποκατάστασης. Σε άλλες περιπτώσεις, η τιμή συνδέεται με τις επακόλουθες δαπάνες και την πιθανή κανονιστική παραβίαση της δημοσιοποίησης των ιδιωτικών πληροφοριών. Ο αντίκτυπος και οι συνέπειες που μπορούν να προκύψουν από κανονιστικές κυρώσεις μπορεί να περιλαμβάνουν κατάθεση αγωγών για αποζημίωση ή ζημιές στη φήμη της επιχείρησης με αποτέλεσμα την απώλεια της αξίας της μετοχής. Σαφώς, στην περίπτωση αυτή, η αποτίμηση δεν μπορεί να βασίζεται στην πραγματική αξία των πληροφοριών, που μπορεί να είναι χαμηλή ή μηδενική. Αντιθέτως, η αποτίμηση πρέπει να βασίζεται στις πιθανές απώλειες και τις επιπτώσεις. Με άλλα λόγια, η αξία των πληροφοριών πιθανώς να χρειαστεί να εξεταστεί από την προοπτική της πιθανής ζημίας ή σημαντικών συνεπειών που απορρέουν από την εισβολή, αλλοίωση ή ακούσια αποκάλυψη.

Οι πληροφορίες του μάρκετινγκ είναι ένα άλλο είδος των πληροφοριών που δεν έχουν εγγενή αξία, αλλά οι οποίες μπορούν ωστόσο να οδηγήσουν σε ανεπιθύμητες υποχρεώσεις και, συνεπώς, κίνδυνους που πρέπει να εξεταστούν. Ανακριβή αναπαραστάσεις των προϊόντων ή υπηρεσιών ή πληροφορίες που θα οδηγήσουν σε λανθασμένες αποφάσεις των επενδυτών μπορεί να οδηγήσουν και πάλι σε σημαντικές απώλειες, ως συνέπεια των διαφόρων νομικών ενεργειών. Ως εκ τούτου, μια συνετή οργάνωση πρέπει να εξετάσει τη διασφάλιση συστηματικής αξιολόγησης και ελέγχου των πληροφοριών για τη διαχείριση του κινδύνου πιθανών ευθυνών που δημιουργούνται από δημοσιοποιημένες πληροφορίες.

Παραδείγματα τυπικών πληροφοριών των περιουσιακών στοιχείων περιλαμβάνουν:

- Πληροφορίες (δεδομένα, φωνή και εικόνες)
- Hardware
- Software
- Υπηρεσίες
- Πνευματική ιδιοκτησία (έγγραφα, σχέδια, γραφικά, κλπ.)
- Προσωπικό

3.10.1 Στρατηγικές Αποτίμησης Πόρων

Οι εταιρείες συνήθως βρίσκουν δύσκολη την αποτίμηση πόρων. Σε πολλές περιπτώσεις, είναι δύσκολο να δοθεί η ακριβής αξία ενός περιουσιακού στοιχείου. Είναι πολύ πιο δύσκολο να αξιολογηθεί η απώλεια του περιουσιακού στοιχείου (σε πολλές περιπτώσεις αυτό εξαρτάται

από τον τρόπο έχασε περιουσιακό στοιχείο χρησιμοποιείται. Όταν ένα χαμένο περιουσιακό στοιχείο κυριαρχεί, το κόστος για την εταιρεία από την άποψη των δικαστική και την αξία των μέτοχων μπορεί να είναι τεράστιο, έως απίστευτο) μέχρι να συμβεί.

Η αποτελεσματική αποτίμηση των πόρων είναι καλύτερα βασισμένη στα σενάρια απώλειας. Οι πληροφορίες μπορούν να ταξινομηθούν και να τεθούν σε ένα πίνακα με κάθε σενάριο απώλειας να κάνει ένα σύνθετο πρόβλημα πιο εύχρηστο και κατανοητό. Βλέπε σχήμα 3.16

Σχήμα 3.16: Πίνακας σεναρίων απώλειας

Πίνακας σεναρίων απώλειας								
Σενάριο	**Τύπος Δεδομένων**	**Μέγεθος Απώλειας**	**Απώλειες Φήμης**	**Απώλειες Αγωγών**	**Πρόστιμα**	**Απώλειες Αγοράς**	**Αναμενόμενη Ετήσια Απώλεια**	**Σημειώσεις**
Hackers κλέβουν δεδομένα	Δεδομένα Πελατών	1K ~ 10K εγγραφές	US $1-20M	US $1~10M	US $1~35M	US $1~5M	US $10M	
Εργαζόμενοι κλέβουν δεδομένα	Στρατηγικό πλάνο	Πλάνο τριετίας	Ελάχιστο	Ελάχιστο	Ελάχιστο	Ελάχιστο	US $20M	Ενίσχυση ανταγων.
Ανάδοχοι έργου κλέβουν δεδομένα	Δεδομένα Εργατών	10K εγγραφές	US $5M	US $10M	Ελάχιστο	Ελάχιστο	US $200,00	
Backup Tapes στα σκουπίδια.	Δεδομένα Πελατών	10M εγγραφές	US $20M	US $20M	US $10M	US $5M	US $200,00	

Η ακρίβεια της αποτίμησης δεν είναι τόσο κρίσιμη, όπως μια προσέγγιση για την ιεράρχηση των προσπαθειών. Οι τιμές της ίδιας τάξης μεγέθους με την πραγματική απώλεια (σε περίπτωση που συμβεί) είναι επαρκής για σκοπούς σχεδιασμού. Δυστυχώς, υπάρχει μια σειρά από καλά τεκμηριωμένα σενάρια απώλειας και ζημιών στις οποίες μπορεί να βασιστεί η αποτίμηση. Μια καλή πηγή πληροφοριών είναι η www.attrition.org η οποία διατηρεί μια βάση δεδομένων των παραβιάσεων των δεδομένων και των ζημιών.

3.10.2 Μεθοδολογία Αποτίμησης

Η αποτίμηση των περιουσιακών στοιχείων ή των πόρων μπορεί να είναι πολύπλοκη και χρονοβόρα αλλά και ουσιαστική. Η αξιολόγηση των πηγών πληροφορίας μπορεί να εξετάσει πολλές διαφορετικές μεταβλητές. Οι μεταβλητές αυτές μπορούν να περιλαμβάνουν το επίπεδο της τεχνικής πολυπλοκότητας και το επίπεδο των πιθανών άμεσων και επακόλουθων οικονομικών απωλειών. Οι ποσοτική αποτιμήσεις είναι γενικά οι πιο ακριβείς αλλά μπορεί να είναι αρκετά πιο περίπλοκες όταν οι πραγματικές επιπτώσεις αναλυθούν. Μια άλλη μορφή

της αποτίμησης που χρησιμοποιείται μερικές φορές είναι η ποιοτικού χαρακτήρα, στην οποία μια απόφαση λαμβάνεται με βάση τη γνώση των επιχειρήσεων, των οδηγιών της διοίκησης, των ιστορικών προοπτικών, των επιχειρηματικών στόχων και των περιβαλλοντικών παραγόντων. Υπάρχουν καταστάσεις στις οποίες τα ποσοτικά στοιχεία δεν είναι διαθέσιμα και αυτή η εναλλακτική μέθοδος είναι επιθυμητή. Πολλοί διαχειριστές συστημάτων πληροφοριών χρησιμοποιούν ένα συνδυασμό τεχνικών. Σε ορισμένες περιπτώσεις, δίνοντας απλά αξία βασισμένη σε μια υποκειμενική κλίμακα για το χαμηλό, μεσαίο και υψηλό επίπεδο μπορεί να είναι ικανοποιητική.

Η πιο απλή προσέγγιση είναι η νομισματική αξία που αντιπροσωπεύει την τιμή αγοράς, το κόστος αντικατάστασης ή την λογιστική αξία αν αυτό είναι αντιπροσωπευτικό της σημαντικότητας στην επιχείρηση. Εάν δεν είναι, άλλες προσεγγίσεις θα πρέπει να λαμβάνονται υπόψη. Αν πρόκειται για ένα περιουσιακό στοιχείο που δημιουργεί άμεσα έσοδα, μια τιμή όπως η καθαρή παρούσα αξία (ΚΠΑ) μπορεί να είναι μια λογική προσέγγιση.

Μια άλλη προσέγγιση είναι να εξεταστεί η φορολογία ή άλλες πιο αόριστες, αλλά αναμφισβήτητα πιο σημαντικές αξίες. Για παράδειγμα, μια εφαρμογή ηλεκτρονικού εμπορίου και ο server μπορεί να έχει μόνο hardware και software κόστος των $50.000, αλλά είναι ένα ουσιαστικό στοιχείο για τη δημιουργία εσόδων εκατομμύριων κάθε μήνα. Σε αυτήν την κατάσταση, η αξία μπορεί να υπολογιστεί από την άποψη της δημιουργίας εσόδων και των οικονομικών επιπτώσεων από οποιαδήποτε απρόβλεπτη διακοπή της υπηρεσίας.

Αόριστα περιουσιακά στοιχεία που μπορεί να αποδειχθούν δύσκολα να ποσοτικοποιηθούν αποτελούν η φήμη του οργανισμού και η εμπιστοσύνη των καταναλωτών. Παρά το γεγονός ότι ένα περιστατικό πειρατείας από μόνο του δεν μπορεί να δημιουργήσει άμεσες απώλειες, οι πελάτες μπορεί να φύγουν λόγω της έλλειψης εμπιστοσύνης στην εταιρεία, ειδικά αν υπάρχουν ισχυροί ανταγωνιστές. Ένα άλλο παράδειγμα θα μπορούσε να προκύψει από κάποιον που κλέβει τα προσωπικά δεδομένα των πιστωτικών των πελατών. Αυτό θα μπορούσε να προκαλέσει επιβάρυνση του οργανισμού με το κόστος της κοινοποίησης σε ένα μεγάλο αριθμό ανθρώπων του περιστατικού αυτού (σύμφωνα με τη νομοθεσία). Επιπλέον, αυτό το είδος του συμβάντος θα μπορούσε να οδηγήσει σε δυνητικό κόστος που σχετίζεται με τη νομική κάλυψη.

Η πιθανή απώλεια των πελατών πρέπει επίσης να εξεταστεί στο πλαίσιο των προσπαθειών αποτίμησης. Η προαναφερθείσα PGP-Vontu μελέτη σε 31 οργανισμούς σε κίνδυνο διαπίστωσε ότι το 19% των πελατών έπαψε συνεργάζεται με τους οργανισμούς αυτούς και ένα άλλο 40% σκέπτονται να το πράξουν. Μια τέτοια δραματική εξέλιξη είναι πιθανό να έχει σοβαρές οικονομικές επιπτώσεις σε κάθε οργανισμό.

Ενώ η λεπτομερής συζήτηση σχετικά με μεθόδους καθιέρωσης αόριστων αξιών περιουσιακών στοιχείων είναι πέρα από το πεδίο εφαρμογής της παρούσας εργασίας, είναι σημαντικό ο διευθυντής της ασφάλειας πληροφοριών να κατανοήσει τις προσεγγίσεις αποτίμησης και την ανάγκη της δραστηριότητας αυτής.

Σε μια εισηγμένη εταιρεία, τα άυλα περιουσιακά στοιχεία αντιπροσωπεύουν την διαφορά μεταξύ των υλικών περιουσιακών στοιχείων και την αξία κεφαλαιοποίησης της εταιρείας. Για παράδειγμα, μια εταιρεία με κεφαλαιοποίηση 5 δις δολαρίων ΗΠΑ στην αγορά έχει 1 δις δολάρια σε υλικά στοιχεία και 4 δισεκατομμύρια δολάρια σε άυλα στοιχεία ενεργητικού. Ως εκ τούτου, το 80% της αξίας της εταιρείας (4 δισεκατομμύρια δολάρια) αποτελείται από άυλα περιουσιακά στοιχεία. Τα άυλα περιουσιακά στοιχεία συνήθως αποτελούνται από δικαιώματα πνευματικής ιδιοκτησίας, όπως διπλώματα ευρεσιτεχνίας, εμπορικά μυστικά, πνευματικά δικαιώματα, φήμη, την εταιρική κουλτούρα, την αφοσίωση και την εμπιστοσύνη των πελατών και την καινοτομία. Είναι προφανές ότι τα περισσότερα από αυτά τα άυλα περιουσιακά στοιχεία εμπίπτουν στην αρμοδιότητα της ασφάλειας πληροφοριών για τους σκοπούς της προστασίας τους και την διατήρηση την αξία τους.

Επιπλέον, ο διευθυντής της ασφάλειας πληροφοριών πρέπει να είναι ενημερωμένος για τις τρέχουσες αλλαγές στην επιχείρηση και θα πρέπει να τροποποιήσει τη χρήση των μεθόδων αποτίμησης για να ανταποκρίνονται καλύτερα στις ανάγκες αυτής, ως αποτέλεσμα αυτών των αλλαγών. Εάν τα ποσοτικά στοιχεία είναι ξεπερασμένα και δεν μπορούν να ενημερωθούν σε ένα εύλογο χρονικό διάστημα, μπορεί να είναι επιθυμητό να χρησιμοποιούν ποιοτικά δεδομένα, είτε στη θέση τους είτε αυξάνοντας τα ποσοτικά δεδομένα.

3.10.3 Ταξινόμηση Πληροφοριών Περιουσιακών στοιχείων

Η ταξινόμηση των πληροφοριών των περιουσιακών στοιχείων απαιτείται για τον προσδιορισμό της σχετικής ευαισθησίας και της κρισιμότητας των πληροφοριών αυτών, κατι το οποίο παρέχει τη βάση για τις προσπάθειες προστασίας, BCP και τον έλεγχο πρόσβασης. Για τις μεγαλύτερες επιχειρήσεις αυτό μπορεί να είναι ένα δύσκολο έργο, δεδομένου ότι υπάρχουν πιθανότητες ηλεκτρονικών δεδομένων της τάξης των terabyte, warehouses εγγράφων και χιλιάδες συσκευών. Ωστόσο, χωρίς τον προσδιορισμό της αξίας, της ευαισθησίας και της κρισιμότητας (όλο και περισσότερο νομικών και κανονιστικών απαιτήσεων) των πληροφοριακών πηγών, δεν είναι δυνατόν να αναπτυχτεί ένα αποτελεσματικό πρόγραμμα διαχείρισης επικινδυνότητας που να παρέχει την κατάλληλη προστασία, ανάλογη με την ευαισθησία, την αξία και κρισιμότητα.

Σε άλλες περιπτώσεις όπου η ταξινόμηση δεν είναι δυνατή λόγω των περιορισμένων πόρων ή για άλλους λόγους, μια λιγότερο αποτελεσματική επιλογή είναι η εκτίμηση της εξάρτησης των επιχειρήσεων,η οποία μπορεί να χρησιμοποιηθεί για να αποτελέσει τη βάση για την κατανομή των δραστηριοτήτων προστασίας. Η προσέγγιση αυτή βασίζεται στις πηγές πληροφόρησης που χρησιμοποιούν οι κρίσιμες επιχειρηματικές λειτουργίες.

Το πρώτο βήμα στη διαδικασία ταξινόμησης είναι ο εντοπισμός και η αναγνώριση των πηγών πληροφόρησης. Σε πολλούς οργανισμούς, αυτό μπορεί να αποδειχθεί δύσκολο δεδομένου ότι συχνά δεν υπάρχει πλήρης καταγραφή των πληροφοριών που σχετίζονται με

τα περιουσιακά στοιχεία. Αυτό μπορεί να ισχύει ιδιαίτερα σε μεγαλύτερες επιχειρήσεις με πολλαπλές ανεξάρτητες επιχειρηματικές μονάδες που δεν διαθέτουν ισχυρή κεντρική λειτουργία ασφαλείας. Η διαδικασία ταυτοποίησης περιλαμβάνει τον καθορισμό των ιδιοκτητών, των χρηστών και των εξωτερικών παρόχων υπηρεσιών. Οι πάροχοι υπηρεσιών μπορούν να περιλαμβάνουν επιχειρήσεις, διαδικασίες αλληλογραφίας που περιέχουν πληροφορίες της εταιρείας, επιχειρήσεις courier ή μεταφορικές, third-party παρόχους υπηρεσιών. Οι πάροχοι υπηρεσιών μπορούν να περιλαμβάνουν data centers, hosting παροχής υπηρεσιών, υπηρεσίες μισθοδοσίας και διαχείρισης της ασφάλισης υγείας.

Ο διαχειριστής της ασφάλειας πληροφοριών σε συνεργασία με τις επιχειρηματικές μονάδες θα πρέπει να διαπιστώσει την κατάλληλη ταξινόμηση πληροφοριών ή τα επίπεδα της ευαισθησίας και της κρισιμότητας των πληροφοριών αυτών και να εξασφαλίσει ότι η διοίκηση της εταιρείας εγκρίνει τις καθιερωμένες κατευθυντήριες γραμμές για το επίπεδο των ελέγχων πρόσβασης. Ο αριθμός των επιπέδων πρέπει να περιορίζεται στο ελάχιστο. Οι ονοματολογίες πρέπει να είναι απλές, όπως ονομασίες από διαφορετικούς βαθμούς ευαισθησίας και κρισιμότητας. Οι End-users διαχειριστές σε συνεργασία με το διαχειριστή ασφαλείας μπορούν να χρησιμοποιήσουν αυτές τις ταξινομήσεις σε διαδικασία εκτίμησης των κινδύνων τους και να βοηθήσουν με τον προσδιορισμό των επιπέδων πρόσβασης.

Ένα σημαντικό πλεονέκτημα της ταξινόμησης των περιουσιακών στοιχείων των πληροφοριών είναι η μείωση του κινδύνου underprotecting και το overprotecting κόστος των πηγών πληροφοριών, μέσω δεσμεύσεων ασφαλείας, στους επιχειρηματικούς στόχους. Αν και πρόκειται για μια περίπλοκη διαδικασία η εφαρμογή της ταξινόμησης των δεδομένων, τα μακροπρόθεσμα οφέλη στον οργανισμό είναι σημαντικά.

Υπάρχουν μια σειρά από ερωτήματα που πρέπει να ζητηθούν σε οποιοδήποτε μοντέλο ταξινόμησης των περιουσιακών στοιχείων των πληροφοριών, συμπεριλαμβανομένων των (αλλά δεν περιορίζονται μόνο σε αυτά):

- Πόσα επίπεδα κατάταξης είναι κατάλληλα για την επιχείρηση;
- Πώς θα πρέπει να βρίσκονται οι πληροφορίες;
- Ποια διαδικασία χρησιμοποιείται για τον προσδιορισμό της ταξινόμησης;
- Πώς αναγνωρίζονται οι ταξινομημένες πληροφορίες;
- Πώς θα αντιμετωπιστούν;
- Πώς θα μεταφερθούν;
- Πώς πρέπει να αποθηκεύονται και αρχειοθετούνται οι εμπιστευτικές πληροφορίες;
- Ποια είναι η διάρκεια του κύκλου ζωής των πληροφοριών (δημιουργία, ενημέρωση, ανάκτηση, αρχειοθέτηση, διάθεση);
- Ποιες είναι οι διαδικασίες που συνδέονται με τα διάφορα στάδια του κύκλου ζωής των πληροφοριών περιουσιακών στοιχείων;
- Πώς πρέπει να διατηρούνται σύμφωνα με την πολιτική ή τους νόμους;
- Πώς θα καταστρέφονται ασφαλώς στο τέλος της περιόδου διατήρησης;
- Ποιος έχει την κυριότητα των πληροφοριών;

- Ποιος έχει τα δικαιώματα πρόσβασης;
- Ποιος έχει την εξουσία για τον προσδιορισμό της πρόσβασης στα δεδομένα;
- Ποιές εγκρίσεις απαιτούνται για την πρόσβαση;

Ένα σημαντικό μέρος της ταξινόμησης πληροφοριών δεν εφαρμόζει απλά μια ετικέτα ταξινόμησης σε κάθε κομμάτι των πληροφοριών αλλά προσδιορίζει και τα μέτρα ασφαλείας που μπορούν με συνέπεια να εφαρμοστούν σε κάθε διαφορετικό επίπεδο. Καθώς το επίπεδο της ευαισθησίας ή της κρισιμότητας αυξάνει, τα μέτρα ασφαλείας θα πρέπει να αυξηθούν σε αυστηρότητα, έτσι ώστε στο υψηλότερο επίπεδο οι μηχανισμοί ασφαλείας να είναι οι πιο αυστηροί ή να απαιτούν το μεγαλύτερο επίπεδο προστασίας για να εξασφαλιστεί η διαθεσιμότητα. Πρέπει επίσης να θυμόμαστε ότι η ευαισθησία και η κρισιμότητα απαιτεί διαφορετικούς μηχανισμούς ασφαλείας και διαδικασίες. Για οποιαδήποτε πληροφορία, ένας ιδιοκτήτης μπορεί να πρέπει να διαχειριστεί τόσο την ευαισθησία όσο και την απόφαση της κρισιμότητας. Οι χρήστες θα πρέπει να είναι ικανοποιημένοι με το προϊόν της εν λόγω κατάταξης. Εάν υπάρχουν τρία επίπεδα ευαισθησίας και τρία επίπεδα της κρισιμότητας, ένα κομμάτι των πληροφοριών ενδέχεται να πρέπει να χωρέσει σε ένα πίνακα 3 x 3, που μπορεί να φιλοξενεί εννέα διαφορετικούς συνδυασμούς διασφάλισης και συνέχισης.

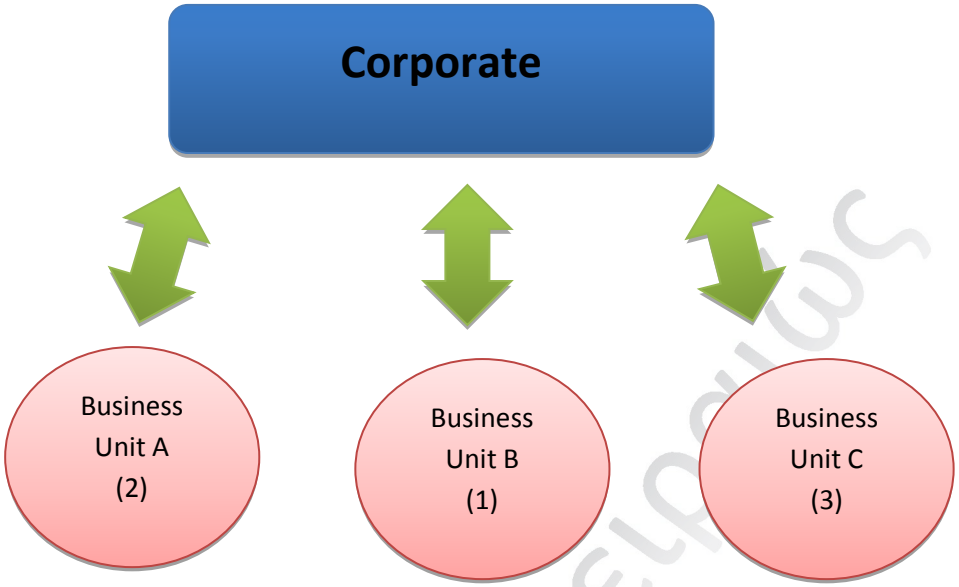
Μέθοδοι προσδιορισμού της κρισιμότητας των πόρων και των επιπτώσεων των ανεπιθύμητων συμβάντων.

Υπάρχει μια σειρά από μεθόδους για τον προσδιορισμό της ευαισθησίας και της κρισιμότητας των πηγών πληροφόρησης καθώς και του αντίκτυπου των ανεπιθύμητων ενεργειών. Μια ανάλυση BIA εκτελείται συχνά για τον προσδιορισμό της επίπτωσης των ανεπιθύμητων ενεργειών. Οι μέθοδοι που περιγράφονται στα COBIT, NIST και στο Software Engineering Institute’s Octave framework είναι αντιπροσωπευτικές των πόρων που ο διευθυντής της ασφάλειας πληροφοριών μπορεί να χρησιμοποιήσει σε αυτή την προσπάθεια.

Είναι γενικά αποδεκτή πρακτική η εστίαση στον αντίκτυπο της απώλειας των πηγών των πληροφοριών που σχετίζονται με την επιχείρηση και όχι σε μια συγκεκριμένη ανεπιθύμητη ενέργεια. Δεδομένου ότι υπάρχουν πολλές ανεπιθύμητες ενέργειες, που θα μπορούσαν να συμβούν, είναι δύσκολο έργο ένας πλήρης κατάλογος αυτών. Μια τέτοια προσπάθεια, προφανώς, δεν είναι πρακτικά ή οικονομικά αποδοτική.

Το πρώτο βήμα για τον προσδιορισμό της σημασία των πηγών των πληροφοριών είναι να διαιρεθεί η εταιρική ή οργανωτική δομή σε επιχειρηματικές μονάδες ή τμήματα. Βλέπε σχήμα 2.17. Σύμφωνα με την εταιρική ή ανώτερου επιπέδου οργανωτική δομή, καθεμία από τις επιχειρηματικές μονάδες θα πρέπει να αξιολογηθεί από την σημασία ή την αξία της στην επιχείρηση.
Στο σχήμα 3.17, στην Επιχειρηματική Μονάδα Β δίνεται ο αριθμός **ένα** ως βαθμολογία, δεδομένου ότι είναι η πιο σημαντική. Η σημασία ισοδυναμεί συνήθως με τα έσοδα, αλλά η αξία μπορεί να ισοδυναμεί με κρίσιμες λειτουργίες που εκτελούνται.

Σχήμα 3.17: ανώτερου επιπέδου οργανωτική δομή

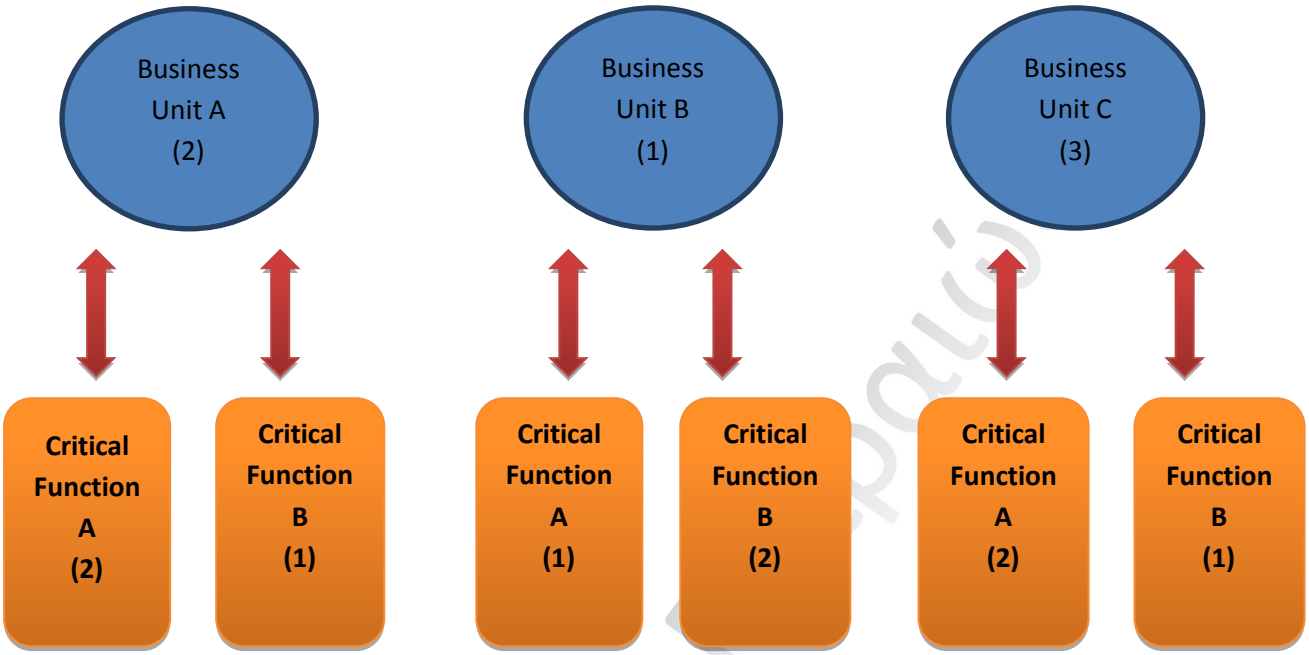


Η βαθμολογία θα πρέπει να γίνει από την ομάδα διοίκησης, με βάση την κατανόησή τους για την επιχείρηση. **Αυτό είναι το θεμέλιο για την ίδρυση της δομής διαχείρισης επικινδυνότητας**. Η σχετική αξία της σημασία των επιχειρηματικών μονάδων ή τμημάτων πρόκειται να ρέει προς τα κάτω σε περιουσιακά στοιχεία ζωτικής σημασίας λειτουργίες και πόρους.

Το επόμενο βήμα είναι η αναγνώριση των κρίσιμων οργανωτικών λειτουργιών. Η εστίαση σε κάθε επιχειρηματική μονάδα ή τμήμα πρόκειται να καθορίσει ποια καθήκοντα είναι σημαντικά για τη μονάδα στην επίτευξη των στόχων της. Μπορεί να υπάρξει μια δομή δύο επιπέδων, κατά τις κρίσιμες λειτουργίες έτσι ώστε να εκπροσωπεί τις πολύπλοκες λειτουργίες. Οι κρίσιμες επιχειρηματικές λειτουργίες είναι επίσης αριθμητικά βαθμονομημένες για να βοηθήσουν με την ιεράρχηση των επακόλουθων προσπαθειών αποκατάστασης του κίνδυνου.

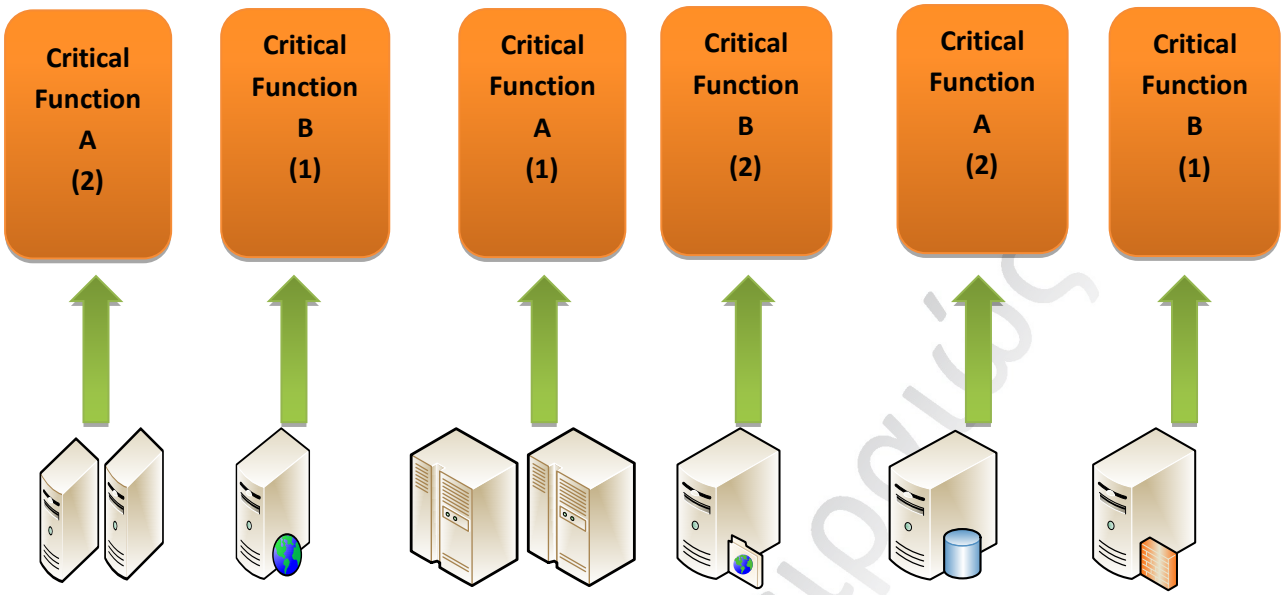
Μόλις οι κρίσιμες λειτουργίες εντοπιστούν, όπως φαίνεται στο σχήμα 3.18 , η βασική δομή της οργάνωσης έχει χαρτογραφηθεί. Είναι σημαντικό να αναγνωρίσουμε ότι η δομή έχει επικεντρωθεί μόνο στα επιχειρησιακά στοιχεία και όχι στις τεχνολογίες, τις εφαρμογές και τα δεδομένα. Αυτή η προοδευτική δομή προς τα κάτω μοιάζει με την ανάλυση BIA που εκτελείται κατά την BCP. Η δομή αυτή παρέχει μια οπτική του κινδύνου διοικητικού επιπέδου και που εντοπίζεται αυτός στην επιχείρηση.

Σχήμα 3.18: Κρίσιμες Λειτουργίες



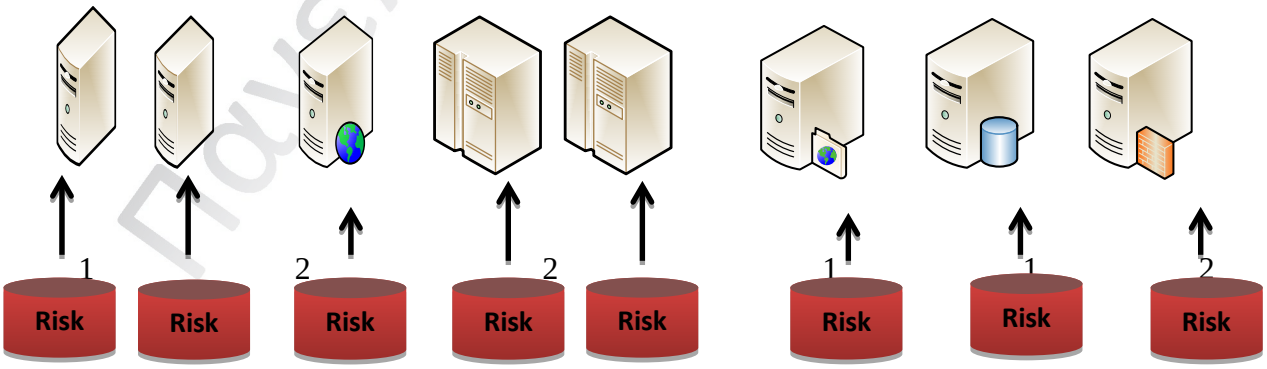
Στη δομή φαίνεται στο ακόλουθο σχήμα 3.19, τα περιουσιακά στοιχεία και οι πόροι είναι οι φορείς του κινδύνου. Επειδή υπάρχουν τρωτά σημεία που εντοπίζονται στα περιουσιακά στοιχεία, τα οποία μπορούν να αξιοποιηθούν από τις απειλές, υπάρχει κίνδυνος. Τα περιουσιακά στοιχεία, όπως οι επιχειρηματικές μονάδες και οι κρίσιμες λειτουργίες, επίσης βαθμονομούνται αριθμητικά. Επειδή τα περιουσιακά στοιχεία συνδέονται με τις κρίσιμες επιχειρηματικές λειτουργίες που υποστηρίζουν, θα πρέπει να αξιολογηθούν από το πιο σημαντικό προς το λιγότερο σημαντικό στην ομάδα τους.

Σχήμα 3.19



Οι κίνδυνοι που αναπαριστούνται στο ακόλουθο σχήμα 3.20, είναι μία σύνθεση των τρωτών σημείων που μια απειλή μπορεί να εκμεταλλευτεί για να προκαλέσει αρνητικές επιπτώσεις σε ένα περιουσιακό στοιχείο. Με την προσέγγιση που παρουσιάστηκε στα προηγούμενα διαγράμματα, ένας οργανισμός μπορεί να δει από πού προέρχεται ο κίνδυνος και πώς μπορούν να επηρεάσουν ενδεχομένως οι επιχειρηματικές δραστηριότητες. Η roll-up και drill-down φύση αυτής της προσέγγισης είναι χρήσιμη για τη διαχείριση όλης της επιχείρησης. Για παράδειγμα, οι ιδιοκτήτες των επιχειρήσεων μπορεί να θέλουν να δουν σε ποιο επίπεδο του κινδύνου βρίσκονται οι κρίσιμες λειτουργίες τους, ώστε να είναι σε θέση να θέσει ένα χρονοδιάγραμμα για τον καθορισμό των προτεραιοτήτων ή την ιεράρχηση των τρωτών σημείων των προσπαθειών προστασίας.

Σχήμα 3.20: Τρωτά σημεία περιουσιακών στοιχείων



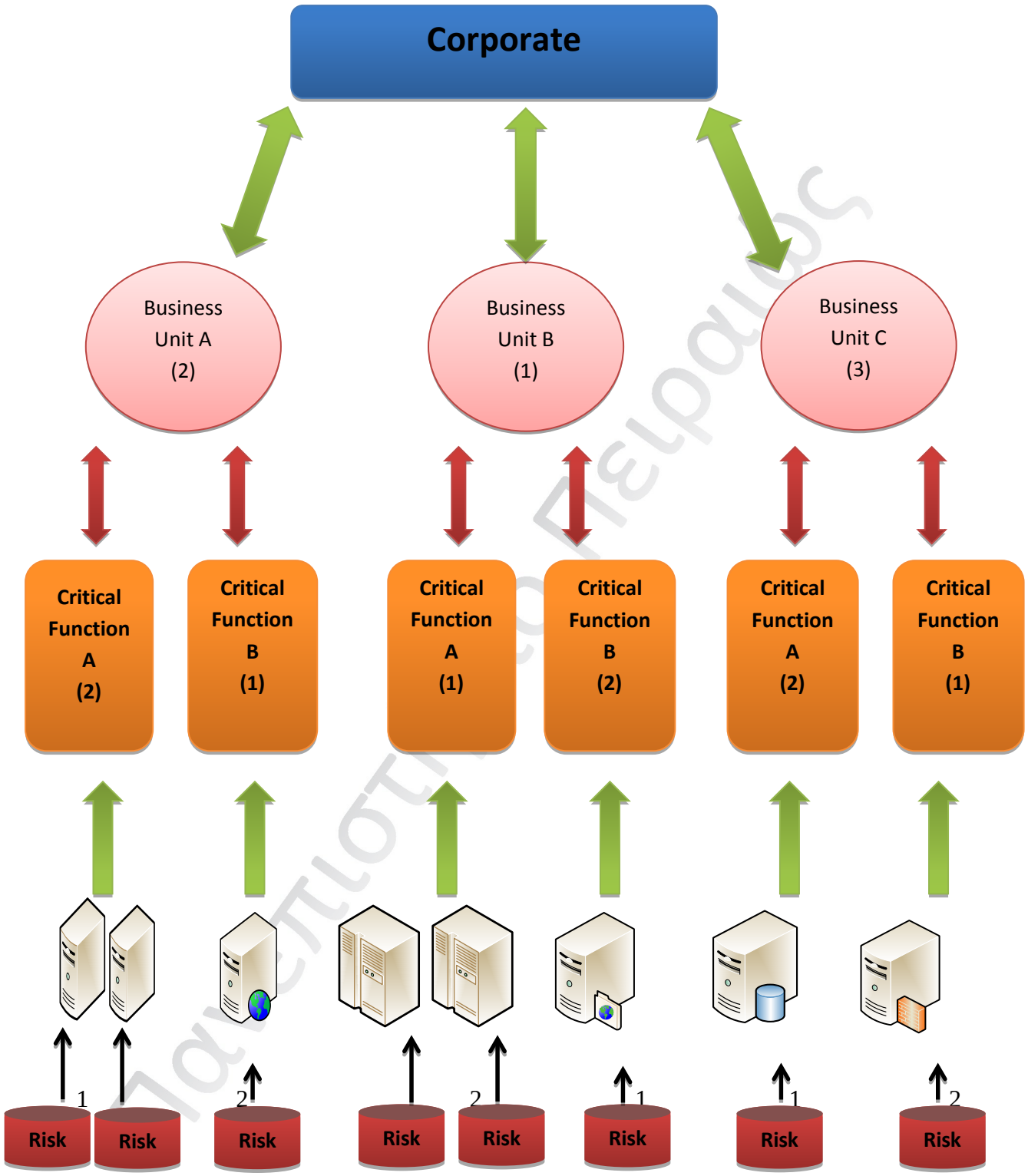
Η ικανότητα προσδιορισμού του τρόπο που ο κίνδυνος μπορεί να επηρεάσει τις επιχειρησιακές λειτουργίες παρουσιάζεται στο σχήμα 3.21, στο οποίο βρίσκονται τα στοιχεία που συζητήθηκαν παραπάνω. Αυτό δείχνει το πώς η έκθεση του κινδύνου μπορεί να επηρεάσει δυνητικά μερικά από τα πιο πολύτιμα περιουσιακά στοιχεία της εταιρείας. Η δομή που φαίνεται στο διάγραμμα βοηθά τόσο την ομάδα διοίκησης όσο και την ομάδα ασφαλείας να ευθυγραμμιστούν και να ιεραρχήσουν τις προσπάθειες τους αναλόγως.

3.10.4 Αξιολόγηση Επιπτώσεων και Ανάλυση.

Μια κοινή προσέγγιση για την εκπόνηση μελετών επιπτώσεων είναι ο προσδιορισμός της αξίας ενός περιουσιακού στοιχείου στην επιχείρηση όσον αφορά:

- Το κόστος αντικατάστασης
- Τις επιπτώσεις που συνδέονται με την απώλεια της ακεραιότητας.
- Επιπτώσεις που συνδέονται με την απώλεια της διαθεσιμότητας
- Οι επιπτώσεις που συνδέονται με την απώλεια της εμπιστευτικότητας

Σχήμα 3.21: Δομή της συνδυασμένης επιρροής του κινδύνου



Δυστυχώς, είναι σύνηθες για τις αξιολογήσεις αυτές να προσδιορίζουν μόνο το αποτέλεσμα της χειρότερης περίπτωσης, το οποίο εμπειρικά εμφανίζεται σε μια μειοψηφία γεγονότων. Ως αποτέλεσμα αυτού, η διοίκηση προεξοφλεί συχνά αυτές τις αξιολογήσεις ως μη ρεαλιστικές.

Μια πιο αποτελεσματική προσέγγιση περιλαμβάνει τη διενέργεια ενός εύλογα μικρού συνόλου από σενάρια - αναλύσεις με τους βασικούς ενδιαφερόμενους φορείς της επιχείρησης, στο οποίο καθορίζονται μια σειρά από πιθανά αποτελέσματα. Αυτή η σειρά των αποτελεσμάτων στη συνέχεια χρησιμοποιείται για να καθορίσει μια ποσοτική κατανομή των μεγεθών των επιπτώσεων, συμπεριλαμβανομένων των ελάχιστων, των μέγιστων και των πιο πιθανών, συμπεριλαμβανομένων των τιμών καθώς και των επίπεδων εμπιστοσύνης. Οι τιμές αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν ως εισροές για τις μεθόδους ποσοτικής ανάλυσης (π.χ., προσομοιώσεις Monte Carlo για τον καθορισμό της πιθανότητας κατανομής) που περιγράφουν με μεγαλύτερη ακρίβεια τις πραγματικές πιθανές επιπτώσεις για τη διοίκηση

Το άλλο πλεονέκτημα που παρέχει είναι ότι μοιάζει περισσότερο με το είδος των δεδομένων που επηρεάζονται τα οποία η διοίκηση λαμβάνει από άλλους τομείς επιχειρηματικού κινδύνου (π.χ., τις επενδύσεις, την εμπορία, κλπ.). Η ευθυγράμμιση αυτή βελτιώνει την ικανότητα της διοίκησης να προβεί σε συγκρίσεις και καλά τεκμηριωμένες αποφάσεις κινδύνου.

Το επόμενο σημαντικό βήμα για τη μέτρηση του επίπεδου του κινδύνου είναι ο προσδιορισμός των δυσμενών επιπτώσεων που προκύπτουν από μια επιτυχημένη απειλή που εκμεταλλεύεται ένα τρωτό σημείο. Πριν αρχίσει η ανάλυση των επιπτώσεων ενός συγκεκριμένου συνόλου των πόρων, είναι απαραίτητο να ληφθούν οι ακόλουθες πληροφορίες:

- **Η αποστολή του συστήματος** (π.χ., οι διαδικασίες που εκτελούνται από το IT σύστημα)
- **Η κρισιμότητας του συστήματος και των δεδομένων** (π.χ., η αξία του συστήματος ή η σημασία του σε έναν οργανισμό)
- **Η ευαισθησία του συστήματος και των δεδομένων** (οι επιπτώσεις που σχετίζονται με την ακούσια αποκάλυψη)

Αυτές οι πληροφορίες μπορούν να ληφθούν από την εκτέλεση ανάλυσης BIA ή από υπάρχοντα οργανωτικά έγγραφα, όπως **η αναφορά της ανάλυσης επιπτώσεων** ή την **έκθεση εκτίμηση της κρισιμότητας των περιουσιακών στοιχείων**, εφόσον αυτά υπάρχουν. Μια ανάλυση των επιπτώσεων (BIA) ιεραρχεί τα επίπεδα επιπτώσεων που συνδέονται με τον συμβιβασμό των περιουσιακών στοιχείων πληροφοριών ενός οργανισμού, βασισμένη σε μια ποιοτική ή ποσοτική αξιολόγηση της ευαισθησίας και της κρισιμότητας των εν λόγω περιουσιακών στοιχείων. Η εκτίμηση της κρισιμότητας ενός περιουσιακού στοιχείου εντοπίζει και ιεραρχεί τις ευαίσθητες και κρίσιμες πληροφορίες των περιουσιακών στοιχείων του οργανισμού (π.χ., hardware, software, συστήματα, υπηρεσίες και σχετικά

τεχνολογικά περιουσιακά στοιχεία) τα οποία υποστηρίζουν τις κρίσιμων αποστολές της επιχείρησης.

Αν τα έγγραφα αυτά δεν υπάρχουν ή τέτοιες εκτιμήσεις για τα περιουσιακά στοιχεία του οργανισμού δεν έχουν πραγματοποιηθεί, η ευαισθησία του συστήματος και τα δεδομένα μπορούν να καθοριστούν με βάση το επίπεδο προστασίας που απαιτείται για να διατηρήσει τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα του συστήματος και των δεδομένων.

Οι δυσμενείς επιπτώσεις ενός συμβάντος ασφάλειας μπορεί να περιγραφούν από την άποψη της απώλειας ή υποβάθμισης ή οποιονδήποτε συνδυασμό της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας.

- **Απώλεια της ακεραιότητας**: Η ακεραιότητα του συστήματος και των δεδομένων αναφέρεται στην απαίτηση ότι οι πληροφορίες πρέπει να προστατεύονται από ενδεχόμενη ακατάλληλη τροποποίηση. Η ακεραιότητα χάνεται αν μη εξουσιοδοτημένες αλλαγές γίνονται στα δεδομένα ή στα IT συστήματα είτε σκόπιμα είτε από ακούσιες πράξεις. Εάν η απώλεια της ακεραιότητας του συστήματος ή των δεδομένων δεν διορθωθεί, η συνεχιζόμενη χρήση ενός μολυσμένου συστήματος ή αλλοιωμένων δεδομένων θα μπορούσε να οδηγήσει σε ανακρίβεια, απάτη, ή λανθασμένες αποφάσεις. Επίσης, η παραβίαση της ακεραιότητας μπορεί να είναι το πρώτο βήμα σε μια επιτυχημένη επίθεση εναντίον της διαθεσιμότητα του συστήματος ή της εμπιστευτικότητας του.
- **Απώλεια διαθεσιμότητας**: Εάν ένα σημαντικό IT σύστημα δεν είναι διαθέσιμο στους τελικούς χρήστες του, η αποστολή του οργανισμού μπορεί να επηρεαστεί. Η απώλεια της λειτουργικότητας του συστήματος και της επιχειρησιακής αποτελεσματικότητας, για παράδειγμα, μπορεί να οδηγήσει σε απώλεια παραγωγικού χρόνου, εμποδίζοντας έτσι την απόδοση των τελικών χρηστών στα καθήκοντα τους στην υποστήριξη της αποστολής του οργανισμού.
- **Απώλεια της εμπιστευτικότητας**: Η εμπιστευτικότητα των συστημάτων και των δεδομένων αναφέρεται στην προστασία των πληροφοριών από μη εξουσιοδοτημένη αποκάλυψη. Οι επιπτώσεις της μη εξουσιοδοτημένης αποκάλυψης εμπιστευτικών πληροφοριών μπορεί να κυμαίνονται από την έκθεση σε κίνδυνο της εθνικής ασφάλειας έως την αποκάλυψη των προσωπικών δεδομένων. Η μη εξουσιοδοτημένη, απρόβλεπτη, ή ακούσια αποκάλυψη θα μπορούσε να οδηγήσει σε απώλεια της εμπιστοσύνης του κοινού, αμηχανία, ή νομικών κυρώσεων κατά της επιχείρησης.

Μερικές υλικές επιπτώσεις μπορούν να μετρηθούν ποσοτικά με τα διαφυγόντα έσοδα, το κόστος της επισκευής του συστήματος ή το επίπεδο της προσπάθειας που απαιτείται για την επίλυση προβλημάτων που προκαλούνται από έναν συμβιβασμό. Άλλες επιπτώσεις (π.χ. απώλεια της εμπιστοσύνης του κοινού, η απώλεια της αξιοπιστίας, της βλάβης προς το συμφέρον ενός οργανισμού) δεν μπορούν να μετρηθούν σε συγκεκριμένες μονάδες, αλλά

μπορεί να θεωρηθούν ή να περιγραφούν με όρους υψηλών, μεσαίων και χαμηλών επιπτώσεων.

Κατά τη διεξαγωγή ανάλυσης επιπτώσεων, θα πρέπει να ληφθούν υπόψη τα πλεονεκτήματα και τα μειονεκτήματα των ποσοτικών έναντι των ποιοτικών αξιολογήσεων. Το κύριο πλεονέκτημα της ποιοτικής ανάλυσης των επιπτώσεων είναι ότι ιεραρχεί τους κινδύνους και εντοπίζει τους τομείς που χρίζουν άμεσης βελτίωσης κατά την αντιμετώπιση των τρωτών σημείων. Το μειονέκτημα της ποιοτικής ανάλυσης είναι ότι δεν παρέχει συγκεκριμένες ποσοτικοποιημένες μετρήσεις του μεγέθους των επιπτώσεων, οπότε καθιστά την ανάλυση κόστους-οφέλους όλων των συνιστώμενων ελέγχων δύσκολη.

Το σημαντικότερο πλεονέκτημα μιας ποσοτικής ανάλυσης των επιπτώσεων είναι ότι παρέχει μια μέτρηση του μεγέθους των επιπτώσεων, η οποία μπορεί να χρησιμοποιηθεί για την ανάλυση κόστους-οφέλους των συνιστώμενων ελέγχων.

Το μειονέκτημα είναι ότι, ανάλογα με το αριθμητικό εύρος που χρησιμοποιείται για τη μέτρηση, η έννοια της ποσοτικής ανάλυσης των επιπτώσεων μπορεί να είναι ασαφής, απαιτώντας το αποτέλεσμα να πρέπει να ερμηνεύεται κατά τρόπο ποιοτικό. Πρόσθετοι παράγοντες συχνά πρέπει επίσης να ληφθούν υπόψη για τον προσδιορισμό του μεγέθους των επιπτώσεων, όπως είναι το φάσμα των πιθανών σφαλμάτων κατά την εκτίμηση ή τους υπολογισμούς.

3.11 Στόχοι των χρόνων ανάκτησης (RTOs)

Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να κατανοήσει τα RTOs και πώς αυτά εφαρμόζονται σε πηγές πληροφόρησης του οργανισμού ως μέρος της συνολικής αξιολόγησης του κινδύνου. Οι επιχειρησιακές ανάγκες του οργανισμού επιβάλουν τα RTOs, που συνήθως ορίζονται ως η ποσότητα του χρόνου για την ανάκτηση ενός αποδεκτού επιπέδου κανονικής λειτουργίας. Η λειτουργική κρισιμότητα των πηγών πληροφορίας, οι προτεραιότητες αποκατάστασης και οι αλληλεξαρτήσεις που αντισταθμίζεται από το κόστος είναι μεταβλητές οι οποίες θα καθορίσουν το RTO.

Ο καθορισμός του RTO (Recovery Time Objective) μπορεί να εξαρτάται από έναν αριθμό παραγόντων, όπως η περιοδικότητα (ημερήσιο, εβδομαδιαίο, μήνιαίο ή το ετήσιο) των πληροφοριών και του οργανισμού, οι αλληλεξαρτήσεις μεταξύ των πληροφοριών και των απαιτήσεων του οργανισμού καθώς και το κόστος των διαθέσιμων επιλογών. Οι απαιτήσεις του οργανισμού μπορεί να στηρίζονται στις ανάγκες των πελατών, στις συμβατικές υποχρεώσεις ή SLAs, στις προσδοκίες και, ενδεχομένως, στις ρυθμιστικές απαιτήσεις. Ο διαχειριστής της ασφάλειας πληροφοριών θα πρέπει να λαμβάνει υπόψη του ότι η RTO μπορεί να ποικίλλει ανάλογα με τη χρονική στιγμή του μήνα ή του έτους. Οι οικονομικές πληροφορίες μπορεί να μην είναι τόσο κρίσιμες στις αρχές του μήνα, όταν η δημοσιονομική

περίοδος ανοίγει, ενώ η ίδια πληροφορία είναι πιθανό να είναι ιδιαίτερα κρίσιμη στο τέλος του μήνα, όταν ετοιμάζονται οι μηνιαίες οικονομικές εκθέσεις και κλείνει η λογιστική περίοδος. Το χρονοδιάγραμμα των επιχειρηματικών κύκλων και η εξάρτησή τους από τις πληροφορίες πρέπει να θεωρούνται ως μέρος της ταξινόμησης πληροφοριών.

Τα RTOs καθορίζονται από την εκτέλεση μιας BIA ανάλυσης (Business Impact Analysis) σε συντονισμό με την ανάπτυξη ενός επιχειρηματικού σχεδίου BCP (Business Continuity Plan). Η BIA γενικά διενεργείται παίρνοντας συνεντεύξεις από τους κατόχους πληροφοριών ώστε να επιτευχθεί η προοπτική τους για το κόστος που συνδέεται με την εκτεταμένη διακοπή της υπηρεσίας για ένα επιχειρηματικό σύστημα ή διαδικασία. Συχνά υπάρχουν δύο προοπτικές για το RTO. Η μία είναι η προοπτική των ατόμων των οποίων η δουλειά είναι να αξιοποιήσουν τις πληροφορίες και η άλλη είναι η άποψη των ανώτερων διοικητικών στελεχών που πρέπει να εξετάσουν το κόστος και μπορεί να υπάρχει ανάγκη διαιτησίας μεταξύ των επιχειρηματικών μονάδων που ανταγωνίζονται για τους πόρους. Μια πηγή πληροφοριών για την οποία ένας υπεύθυνος τμήματος μπορεί να πιστεύει ότι είναι ζωτικής σημασίας μπορεί να μην είναι εξίσου κρίσιμη στα μάτια του αντιπροέδρου των εργασιών, ο οποίος είναι σε θέση να συνυπολογίζει τον συνολικό οργανωτικό κίνδυνο για την αξιολόγηση του RTO.

Ο διαχειριστής της ασφάλειας των πληροφοριών πρέπει να καταλάβει ότι και οι δύο προοπτικές είναι σημαντικές και εργάζονται προς την κατεύθυνση ενός RTO που τις λαμβάνει υπόψη του. Το αποτέλεσμα θα συνυπολογιστεί στο BCP, στο πεδίο εφαρμογής των υπηρεσιών που πρέπει να αποκατασταθούν και πρέπει να γίνει ιεράρχηση των προτεραιοτήτων για την αποκατάσταση των συστημάτων. Στο τέλος, η τελική απόφαση ανήκει στα ανώτερα στελέχη. Η διοίκηση είναι στην καταλληλότερη θέση για να διαιτητεύσει τις ανάγκες και απαιτήσεις των διαφόρων στοιχείων της επιχείρησης, όπως οι κανονιστικές απαιτήσεις στις οποίες υπόκειται ο οργανισμός, και να καθορίσει ποιες διαδικασίες είναι οι πιο κρίσιμες για τη διασφάλιση της επιβίωσης της επιχείρησης, καθώς και να προσδιορίσει τα αποδεκτά κόστη.

3.11.1 RTO σε συσχέτιση με το BCP

Η γνώση του RTO για τις πηγές πληροφόρησης χρειάζεται σε έναν οργανισμό για να αναπτύξει και να εφαρμόσει ένα αποτελεσματικό πρόγραμμα επιχειρηματικού σχεδιασμού BCP. Μόλις τα RTO γίνουν γνωστά, ο οργανισμός μπορεί να εντοπίσει και να αναπτύξει στρατηγικές έκτακτης ανάγκης που θα συνάδουν με τις πηγές πληροφόρησης των RTO. Το RTO θα υποδείξει τη σειρά προτεραιότητας για την αποκατάσταση των υπηρεσιών και, σε ορισμένες περιπτώσεις, την επιλογή των συγκεκριμένων τεχνολογιών αποκατάστασης σε περιπτώσεις όπου το RTO είναι σύντομο.

Ένας σημαντικός παράγοντας κατά την ανάπτυξη των διαδικασιών έκτακτης ανάγκης είναι το κόστος. Οι ιδιοκτήτες συστημάτων προτιμούν πάντα μικρότερα RTO, αλλά τα

ανταλλάγματα σε κόστος ενδεχομένως να μην δικαιολογούνται. Σύντομη στιγμιαία ανάκαμψη μπορεί να επιτευχθεί, όπου χρειάζεται, με τη χρήση τεχνολογιών mirroring των πηγών πληροφόρησης και αντιγραφής των πληροφοριών, έτσι ώστε, σε περίπτωση διακοπής ρεύματος, οι πηγές πληροφόρησης να είναι πάντα άμεσα διαθέσιμες. Σε γενικές γραμμές, το κόστος της ανάκτησης είναι μικρότερο αν το RTO για μια συγκεκριμένη πηγή είναι μεγαλύτερο.

Υπάρχει ένα νεκρό σημείο της χρονικής περιόδου για τον καθορισμό του RTO, όπου η επίδραση της βλάβης αρχίζει να είναι μεγαλύτερη από το κόστος της αποκατάστασης. Η διάρκεια αυτής της χρονικής περιόδου εξαρτάται από τη φύση της διαταραχής της δραστηριότητάς και τους εμπλεκόμενους πόρους. Ποιοτικά καθώς και ποσοτικά ζητήματα πρέπει να ληφθούν υπόψη δεδομένου ότι η απώλεια της εμπιστοσύνης των πελατών, ακόμη και αν δεν είναι μετρήσιμη, μπορεί να έχει μακροπρόθεσμες αρνητικές συνέπειες για τον οργανισμό. Οι περισσότεροι οργανισμοί μπορούν να μειώσουν τα RTO τους, αλλά υπάρχει ένα σχετικό κόστος.

3.11.2 Τρίτοι Πάροχοι Υπηρεσιών

Μια τυπική οργάνωση χρησιμοποιεί πολλές πηγές πληροφοριών για την υποστήριξη των επιχειρηματικών διαδικασιών της. Οι πόροι αυτοί μπορεί να προέρχονται από το εσωτερικό του οργανισμού ή να παρέχονται από φορείς εκτός του οργανισμού. Οι περισσότεροι οργανισμοί χρησιμοποιούν ένα συνδυασμό των δύο. Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να γνωρίζει όλες τις πηγές πληροφοριών καθώς όλες απαιτούν προστασία από διαρροές.

Για τον διευθυντή της ασφάλειας των πληροφοριών, υπάρχουν γενικά τρεις πτυχές για την αντιμετώπιση της εξωτερικής ανάθεσης (outsourcing):

- Ρύθμιση της οργάνωσης για εξωτερική ανάθεση
- Το συμβόλαιο εξωτερικής ανάθεσης περιλαμβάνει τις κατάλληλες ρήτρες διαχείρισης επικινδυνότητας πληροφοριών.
- Διαχείριση των κινδύνων των πληροφοριών για τις outsource υπηρεσίες σε ημερήσια βάση.

Κατά την outsourcing ανάθεση των υπηρεσιών, τα ακόλουθα πρέπει να ληφθούν υπόψη:

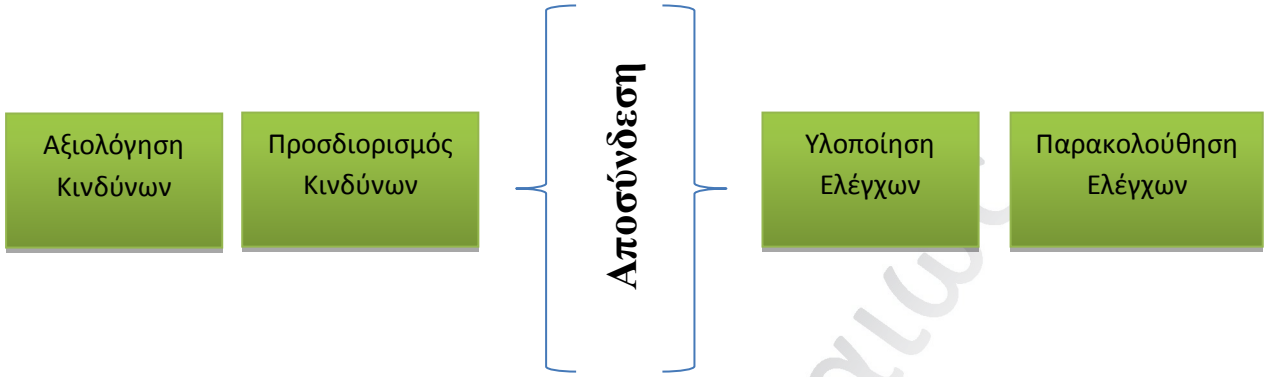
- Η ανάθεση ή ο σχεδιασμός ανάθεσης σε τρίτους, των κρίσιμων επιχειρηματικών λειτουργιών, αυξάνει τους κινδύνους των πληροφοριών.
- Η πολυπλοκότητα της διαχείρισης των κινδύνων των πληροφοριών αυξάνεται κατά την εξωτερική ανάθεση καθηκόντων, από το διαχωρισμό των ευθυνών για τις προδιαγραφές ελέγχου και την εφαρμογή του.
- Ο διαχωρισμός της ευθύνης για τις προδιαγραφές των ελέγχων και την εφαρμογή τους γεφυρώνεται από τα outsourcing συμβόλαια. Αυτό υπογραμμίζει τη

σπουδαιότητα των συμβολαίων ως την κύρια μέθοδο μέσω της οποίας ο οργανισμός μπορεί να διαχειριστεί τους κινδύνους των πληροφοριών.

- Όταν οι outsourcing επιχειρησιακές λειτουργίες δρουν μέσα στη βιομηχανία, τα συμβόλαια ανάθεσης θα πρέπει να συμμορφώνονται ρητά με τις κανονιστικές απαιτήσεις.
- Η πολυπλοκότητα της αξιολόγησης των κινδύνων των πληροφοριών αυξάνεται στην περίπτωση outsourcing διευθέτησης, δεδομένου ότι υπάρχουν τρία είδη κινδύνου πληροφοριών για την αξιολόγηση: η λειτουργία των επιχειρήσεων, ο πάροχος outsourcing και το outsourcing το ίδιο.
- Το είδος του συμβολαίου και το ποσό της καινοτομίας που συνεισφέρει ο πάροχος έχει σημαντικό αντίκτυπο στον τρόπο με τον οποίο καθορίζονται οι απαιτήσεις διαχείρισης του κινδύνου των πληροφοριών.
- Η σχέση ανάμεσα στην επιχείρηση και τον πάροχο των υπηρεσιών συμβάλλει συχνά περισσότερο στην αποτελεσματική διαχείριση των κινδύνων των πληροφοριών στην περίπτωση μιας outsourcing διευθέτησης απ' ότι στο συμβόλαιο.
- Επειδή λίγες επιχειρήσεις εξακολουθούν να είναι στατικές, η διαχείριση επικινδυνότητας εντός της outsourcing συμφωνίας πρέπει να αναπτύσσεται έτσι ώστε να εξακολουθεί να είναι σχετική με τις ανάγκες του οργανισμού.
- Η στρατηγική εξόδου από μία outsourcing συμφωνία είναι τουλάχιστον εξίσου σημαντική με την πρώτη μετάβαση. Θα πρέπει να αναπτυχθεί στο στάδιο του σχεδιασμού και να συμπεριληφθεί στο συμβόλαιο για να διευκολύνει τη συνεχή διαθεσιμότητα της outsourcing επιχειρηματικής λειτουργίας.

Οι απαιτήσεις της διαχείρισης επικινδυνότητας για τις outsourcing επιχειρηματικές λειτουργίες είναι διαφορετικές από εκείνες για τις εσωτερικές λειτουργίες και, σε πολλές περιπτώσεις, είναι μεγαλύτερες. Το συμβόλαιο με τον πάροχο είναι το κύριο όχημα μέσω του οποίου διαχειρίζονται οι κίνδυνοι των πληροφοριών. Όταν οι κίνδυνοι αναλυθούν και οι έλεγχοι καθοριστούν, οι έλεγχοι αυτοί πρέπει να καθορίζονται στο πλαίσιο του συμβολαίου για την υλοποίηση τους από τον πάροχο. Το Outsourcing έχει ως αποτέλεσμα την αποσύνδεση του καθορισμού των ελέγχων από την υλοποίηση τους. Το ακόλουθο σχήμα 3.22 δίνει μια απλοϊκή άποψη αυτού του διαχωρισμού των αρμοδιοτήτων του οργανισμού σε σχέση με εκείνες του παρόχου.

Σχήμα 3.22: διαχωρισμός αρμοδιοτήτων του οργανισμού και παρόχου



Η αποσύνδεση του καθορισμού των ελέγχων από την υλοποίηση τους σε μια outsourcing συμφωνία

Ο διαχειριστής της ασφάλειας πληροφοριών θα πρέπει να γνωρίζει ότι αν και ο οργανισμός μπορεί να αναθέσει τη διαχείριση των κινδύνων σε τρίτους, δεν μπορεί να αναθέσει μέσω outsourcing και την ευθύνη του.

Η αποσύνδεση μεταξύ του ορισμού του ελέγχου και της υλοποίησης του ελέγχου κάνει τη διαχείριση των κινδύνων που συνδέονται με την εξωτερική ανάθεση των επιχειρησιακών λειτουργιών πολύπλοκη και το συμβόλαιο ανάθεσης απαραίτητο κατά την διαχείριση των κινδύνων. Η πρόκληση για τον διευθυντή της ασφάλειας πληροφοριών είναι το πώς θα καθοριστούν και θα εφαρμοστούν οι έλεγχοι διαχείρισης των κινδύνων σε διαφορετικές outsourced επιχειρηματικές λειτουργίες στην επιχείρηση.

Το πρόβλημα των επιχειρήσεων είναι η ανάγκη καθορισμού και υλοποίησης των μέτρων διαχείρισης επικινδυνότητας για την προστασία των πληροφοριών μεταξύ των επιχειρηματικών λειτουργιών που έχουν παραδοθεί σε τρίτους παρόχους και λειτουργούν σε ημερήσια βάση.

Συστάσεις κίνδυνου για outsourcing πρωτοβουλίες:

- Η έγκαιρη συμμετοχή εξειδικευμένων της διαχείρισης επικινδυνότητας για την εξασφάλιση της αξιολόγησης των κινδύνων και του προσδιορισμού αυτών.
- Διασφάλιση ότι οι βασικοί έλεγχοι της διαχείρισης επικινδυνότητας πραγματεύονται εντός της σύμβασης.
- Διασφάλιση ύπαρξης μηχανισμών για τη διαπραγμάτευση μικρών αλλαγών σε ελέγχους διαχείρισης επικινδυνότητας, δεδομένου ότι είναι δαπανηρές.

- Διασφάλιση ότι οι αλλαγές σε ελέγχους διαχείρισης επικινδυνότητας δεν είναι δύσκολες και περίπλοκες.
- Διασφάλιση ότι οι μηχανισμοί για την λήψη πληροφοριών σχετικά με το εάν οι κίνδυνοι διαχειρίζονται αποτελεσματικά.
- Διασφάλιση μηχανισμών για την μείωση της έλλειψης εμπιστοσύνης στο προσωπικό του παρόχου

Οι outsourced πηγές πληροφορίας μπορεί να επιφέρουν στον διευθυντή της ασφάλειας πληροφοριών άλλες προκλήσεις, συμπεριλαμβανομένων των εξωτερικών οργανισμών που μπορεί να είναι απρόθυμοι να μοιραστούν τις τεχνικές λεπτομέρειες σχετικά με τη φύση και την έκταση των μηχανισμών τους προστασίας των πληροφοριών. Αυτό καθιστά πολύ σημαντική την διασφάλιση παροχής των απαραίτητων επιπέδων προστασίας εντός των SLAs και των άλλων συμβολαίων outsourcing. Μια απλή προσέγγιση είναι ο καθορισμός των απαιτήσεων για ειδικούς ελέγχους, όπως είναι το SAS 70 level 2 (Statement on Auditing Standards no. 70, Service Organization, developed by the AICPA) ή η πιστοποίηση ISO 27001. Είναι επίσης σημαντικό να αναλυθούν το SAS 70 ή άλλες εκθέσεις ελέγχου για παρατηρήσεις από εξωτερικούς ελεγκτές και, εάν υπάρχουν, παρατηρήσεις σχετικά με την αποτελεσματικότητα του ελέγχου του πελάτη και την συμμόρφωση με την πολιτική.

Από την άποψη της διαχείρισης επικινδυνότητας είναι επίσης σημαντικό η διαχείριση συμβάντων και η αντίδραση σε αυτά, η BCP / DRP και οι δοκιμασίες να περιλαμβάνουν όλες τις σημαντικές outsourcing υπηρεσίες και λειτουργίες. Αυτό περιλαμβάνει την εφαρμογή ενός καλά σχεδιασμένου και δοκιμασμένου μηχανισμού για την ανίχνευση περιστατικών, την κλιμάκωση και το σχέδιο αντίδρασης σε συνεννόηση με τους outsourcing φορείς.

Ένας άλλος συχνά παραμελημένος τομέας αφορά την οικονομική βιωσιμότητα του προμηθευτή. Δεδομένου ότι η εξωτερική ανάθεση των συμβάσεων συνήθως ανατίθενται σε χαμηλού κόστους πλειοδότες, ο κίνδυνος της outsourcing επιχείρησης να συνεχίσει να λειτουργούν σύμφωνα με τη σύμβαση και να τιμήσει όλες τις συμφωνίες αποζημίωσης μπορεί να είναι συνάρτηση των οικονομικών δυνατοτήτων τους. Οι οικονομικές πληροφορίες μπορούν να ληφθούν από διάφορες πηγές (ετήσιες εκθέσεις των εισηγμένων επιχειρήσεων κλπ.) Εάν οι πιστοποιήσεις δεν είναι διαθέσιμες, οι πληροφορίες πρέπει να λαμβάνονται από τους παρόχους (επαρκείς πληροφορίες για τον προσδιορισμό του τρόπου που οι εξωτερικοί φορείς διασφαλίζουν τα περιουσιακά στοιχεία.)

Κάποια μερίδα των κινδύνων που συνδέονται με την παροχή outsourced υπηρεσιών πληροφοριών, μπορούν να μεταφερθούν με την ενσωμάτωση όρων αποζημίωσης στα SLAs. Οι βασικές ρήτρες που πρέπει να είναι μέρος ενός SLA πρέπει να περιλαμβάνουν (αλλά δεν περιορίζονται) στα ακόλουθα:

- Δικαίωμα έλεγχου των βιβλίων των προμηθευτών.
- Δικαίωμα επανεξέτασης των διαδικασιών τους.
- Επιμονή σε τυποποιημένες διαδικασίες λειτουργίας (SOPs).

- Advanced πληροφορίες αν οι πόροι που διατίθενται πρόκειται να αλλάξουν.

3.12 Ενσωμάτωση με τις διαδικασίες στον Κύκλο Ζωής (Life Cycle)

Η διασφάλιση ότι ο εντοπισμός των κινδύνων, η ανάλυση και οι ενέργειες μείωσης αυτών είναι ενσωματωμένες στις διαδικασίες του κύκλου ζωής είναι ένα σημαντικό καθήκον της διαχείρισης της ασφάλειας πληροφοριών. Οι περισσότεροι οργανισμοί έχουν μεταβάλει τις διαδικασίες διαχείρισης έτσι ώστε να παρέχουν στο διαχειριστή της ασφάλειας πληροφοριών μια προσέγγιση για την υλοποίηση των διαδικασιών διαχείρισης επικινδυνότητας σε συνεχή βάση. Δεδομένου ότι οι αλλαγές σε κάθε πηγή πληροφοριών είναι πιθανό να περιέχουν νέα τρωτά σημεία και να αλλάξουν τη συνολική εξίσωση επικινδυνότητας, είναι σημαντικό ο διευθυντής της ασφάλειας πληροφοριών να έχει επίγνωση των προτεινόμενων τροποποιήσεων. Η προσέγγιση αυτή επιτρέπει στις δραστηριότητες εντοπισμού, ανάλυσης και μείωσης των κινδύνων να ενσωματωθούν στις διαδικασίες του κύκλου ζωής του οργανισμού.

Η αλλαγή της διαχείρισης είναι αρχή των σωστά διοικούμενων επιχειρήσεων. Αλλά, καθώς το computing έγινε κανόνας και οι αλλαγές γίνονται πιο εύκολα σε διαμοιρασμένο περιβάλλον από άτομα με περιορισμένη γνώση, οι επιχειρήσεις συχνά αντιμετωπίζουν την έλλειψη τυποποίησης στο hardware και software περιβάλλον. Αντιλαμβανόμενη αυτό, η διοίκηση στις περισσότερες επιχειρήσεις έχει κινήσει πιο ισχυρές διαδικασίες αλλαγής της διαχείρισης και, ως εκ τούτου, έχουν αρχίσει να επιτυγχάνουν καλύτερο έλεγχο των επιχειρησιακών πηγών πληροφορίας. Αυτό είναι, φυσικά, ένας κινούμενος στόχος, και οι οργανώσεις με απομακρυσμένες λειτουργίες, σε ορισμένες περιπτώσεις, εξακολουθούν να βρίσκουν την αποτελεσματική αλλαγή της διαχείρισης ένα απατηλό στόχο.

Οι οργανισμοί έχουν επίσης κινηθεί κατά κανόνα για την αλλαγή της διαχείρισης και σε άλλους τομείς της επιχειρηματικής δραστηριότητας και για μια ποικιλία επιχειρηματικών δραστηριοτήτων όπως οι περιβαλλοντικοί παράγοντες και οι εγκαταστάσεις. Το όφελος από τις δραστηριότητες αυτές είναι ότι πολλές οργανώσεις έχουν διαδικασίες αλλαγής της διαχείρισης που εκτείνονται σε ολόκληρο τον οργανισμό. Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να είναι ενήμερος για αυτές τις δραστηριότητες αλλαγής της διαχείρισης και να εξασφαλίζει ότι η ασφάλεια είναι καλά εδραιωμένη έτσι ώστε οι αλλαγές δεν γίνονται χωρίς να λαμβάνονται υπόψη οι επιπτώσεις στη συνολική ασφάλεια των πληροφοριακών πόρων του οργανισμού. Μια μέθοδος για να βοηθήσει να εξασφαλιστεί αυτό, είναι η διαχείριση της ασφάλειας πληροφοριών να συμμετάσχει ως μέλος της επιτροπής της αλλαγής τη διαχείρισης και να εξασφαλίσει ότι όλες οι σημαντικές αλλαγές υπόκεινται σε έλεγχο και έγκριση από την ασφάλεια και πληρούν τις απαιτήσεις πολιτικών και προτύπων.

Ενώ η κανονική εστίαση στην αλλαγή της διαχείρισης απευθύνεται στις αλλαγές υλικού και λογισμικού (δοκιμές κλπ.) και, ενδεχομένως, στις επιπτώσεις της ασφάλειας, η διαδικασία

αλλαγής της διαχείρισης πρέπει να επεκταθεί πέραν των ιδιοκτητών των συστημάτων και του IT. Η διαδικασία αλλαγής της διαχείρισης πρέπει να περιλαμβάνει την διαχείριση εγκαταστάσεων με προσοχή στις υποδομές των data centers και οποιαδήποτε άλλη περιοχή που μπορεί να επηρεάσει τη συνολική ασφάλεια των πληροφοριών (π.χ. φυσικό έλεγχο της πρόσβασης των ευαίσθητων ή κρίσιμων περιοχών).

Οι επιπτώσεις της αλλαγής τη διαχείρισης πρέπει να διευθετήσουν τη συντήρηση των συστημάτων και των εγκαταστάσεων με κατάλληλο προσωπικό (συχνά outsourced) και την διαχείριση επιχειρησιακής συνέχειας. Αρκετά συχνά οι αλλαγές δεν είναι τεκμηριωμένες σε έγκαιρη βάση σε αυτούς τους τομείς. Αντίστοιχα η διαχείρισης της πληροφορικής σε επίπεδο υποδομών και διαμόρφωσης μπορεί να μην έχει τα κατάλληλα έγγραφα με τις αλλαγές ή να μην ενημερώνεται έγκαιρα. Η επιχειρησιακή συνέχεια μπορεί επίσης να υστερεί σε σχετικές ενημερώσεις, όταν οι ενημερώσεις αυτές συμβαίνουν κυκλικά. Η αντιμετώπιση καταστάσεων εκτάκτου ανάγκης και επιχειρησιακής συνέχειας μπορούν επίσης να παρουσιάσουν κενά επικοινωνίας όταν οι υπάρχουσες διαδικασίες και οι διαδικασίες αλλαγής δεν αναφέρονται στις περιοχές υποδομών.

Το προσωπικό των εγκαταστάσεων έχει συχνά πρόσβαση σε συστήματα περιβαλλοντικού ελέγχου και παρακολούθησης (σύστημα διαχείρισης κτιρίων [building management system - BMS] / συστήματα εποπτικού ελέγχου και απόκτησης δεδομένων [supervisory control and data acquisition - SCADA]) για τη θέρμανση, τον εξαερισμού και τον κλιματισμό (HVAC), την ύδρευση και την παροχή ηλεκτρικής ενέργειας, ή ακόμη και για συστήματα ελέγχου φυσικής πρόσβασης. Αυτά είναι συχνά προγραμματισμένα για πρόσβαση μέσω απομακρυσμένων υπολογιστών, μια περιοχή που συχνά ξεφεύγει από την εποπτεία της ασφάλειας πληροφοριών. Φυσικά συστήματα ασφαλείας και ελέγχου έχουν σχεδιαστεί έτσι ώστε να αναπτυχθούν εντός ενός κλειστού / ελεγχόμενου περιβάλλοντος.

Τα συστήματα κλειστού κυκλώματος παρακολούθησης μέσω καμερών μόλις ρυθμιστούν για τη μετάδοση δεδομένων μέσω του δικτύου κορμού συχνά συνδυάζονται με την υποδομή του IT, μεταθέτοντας τον κίνδυνο σε αυτά τα συστήματα από τις IT εγκαταστάσεις και το δίκτυο.

Τα συστήματα IT μπορούν επίσης να τεθούν σε κίνδυνο λόγω της ευπάθειας του φυσικού συστήματος ασφαλείας. Τα συστήματα φυσικής ασφαλείας και ελέγχου, λόγω της σημασίας τους για την προστασία των εγκαταστάσεων και των ανθρώπων, μπορεί να είναι μέρος των υποδομών ζωτικής σημασίας της επιχείρησης. Η προστασία αυτών των συστημάτων, των κωδικών και των δεδομένων τους μπορεί να χρειαστεί να ενσωματωθούν σε συστήματα διαβαθμισμένης ασφαλείας. Τα συμβόλαια υπηρεσιών των εγκαταστάσεων για την υποστήριξη των φυσικών συστημάτων και των συστημάτων ελέγχου συμπεριλαμβάνουν την άμεση ανταπόκριση σε έκτακτες περιπτώσεις. Ωστόσο, τα συμβόλαια αυτά θα πρέπει να επανεξετάζονται, διότι ενδεχομένως να μην εμπεριέχουν επαρκή SLAs, ή να μην παρέχουν επαρκή στοιχεία για την επαρκή αντιμετώπιση των καταστάσεων έκτακτης ανάγκης. Μια εφαρμογή υψηλής διαθεσιμότητας μπορεί να επιφέρει απρόβλεπτες επιπτώσεις στην επιχείρηση ως αποτέλεσμα προβλήματος των εγκαταστάσεων.

Τα εσωτερικά ή εξωτερικά μέρη που διαχειρίζονται τις εγκαταστάσεις μερικές φορές παραβλέπονται από τη σκοπιά της διαχείρισης επικινδυνότητας. Αυτές είναι και οι ευάλωτες περιοχές επειδή ο ανθρώπινος παράγοντας αποτελεί τη μεγαλύτερη απειλή για την ασφάλεια των πληροφοριών. Ο άνθρωπος υπόκειται σε αμέλεια των καθιερωμένων διαδικασιών, άγνοια των γνωστών απειλών, συμμετοχή ή συναισθηματική συμπεριφορά. Είναι σημαντικό να συμπεριληφθεί αυτός ο παράγοντας στην αξιολόγηση των κινδύνων για τις κρίσιμες πηγές πληροφοριών. Παραδείγματα εσωτερικών μερών είναι οι φορείς που εγγυώνται την άμεση φυσική πρόσβαση στα συστήματα και εγκαταστάσεις. Τα εξωτερικά μέρη που ενδεχομένως να θέσουν σε κίνδυνο περιλαμβάνουν τους παράγοντες εξυπηρέτησης, π.χ. προσωπικό καθαρισμού ή συντήρησης κλπ. Οι πιθανοί έλεγχοι είναι η ετήσια υπογραφή της συμμόρφωσης με τους κώδικες δεοντολογίας ή τους όρους του συμβολαίου, στην περίπτωση των εξωτερικών μερών.

Με την ενσωμάτωση του εντοπισμού των κινδύνων, της ανάλυσης και των δραστηριοτήτων μείωσης στη διαχείριση αλλαγής (διαδικασίες του κύκλου ζωής), ο διευθυντής της ασφάλειας πληροφοριών μπορεί να διασφαλίσει ότι οι κρίσιμες πηγές πληροφοριών προστατεύονται επαρκώς. Πρόκειται για μια προληπτική προσέγγιση, που επιτρέπει στον διαχειριστή της ασφάλειας πληροφοριών τον καλύτερο προγραμματισμό και εφαρμογή πολιτικών και διαδικασιών ασφάλειας σε ευθυγράμμιση με τους επιχειρηματικούς στόχους και τους στόχους του οργανισμού. Επιτρέπει, επίσης, να ενσωματωθούν οι έλεγχοι ασφάλειας πληροφοριών σε μια δραστηριότητα που έχει μεγαλύτερες δυνατότητες υποβάθμισης των υπαρχόντων ελέγχων.

3.12.1 Η διαχείριση επικινδυνότητας για την ανάπτυξη του κύκλο ζωής των IT συστημάτων

Σύμφωνα με την δημοσίευση του NIST, 800-30, η ελαχιστοποίηση των αρνητικών επιπτώσεων σε μια επιχείρηση και η ανάγκη για μια στέρεη βάση στη διαδικασία λήψης αποφάσεων, είναι οι βασικοί λόγοι για τους οποίους οι οργανισμοί υλοποιούν την διαδικασία διαχείρισης επικινδυνότητας στα IT συστήματα τους. Η αποτελεσματική διαχείριση επικινδυνότητας θα πρέπει να ενσωματωθεί πλήρως στην ανάπτυξη του κύκλου ζωής των συστημάτων (system development life cycle - SDLC). Η SDLC ενός πληροφοριακού συστήματος έχει πέντε φάσεις: **έναρξη, ανάπτυξη ή απόκτηση, την υλοποίηση, τη λειτουργία ή τη συντήρηση και τη διάθεση**. Σε ορισμένες περιπτώσεις, ένα σύστημα πληροφορικής μπορεί να καταλάβει πολλά από τα στάδια αυτά την ίδια στιγμή. Ωστόσο, η μεθοδολογία διαχείρισης επικινδυνότητας είναι η ίδια, ανεξάρτητα από τη φάση SDLC για την οποία διεξάγεται η αξιολόγηση. Η διαχείριση επικινδυνότητας είναι μια επαναληπτική διαδικασία που πρέπει να εκτελεστεί κατά τη διάρκεια κάθε σημαντικής φάσης της SDLC. Το ακόλουθο σχήμα 2.23 περιγράφει τα χαρακτηριστικά της κάθε φάσης SDLC και δείχνει πώς η διαχείριση επικινδυνότητας μπορεί να επιτευχτεί με την υποστήριξη της κάθε φάσης.

3.12.2 Η διαχείριση επικινδυνότητας στον κύκλο ζωής της διαχείρισης έργων.

Σε γενικές γραμμές, το έργο της διαχείρισης επικινδυνότητας γίνεται από τους project managers, αλλά συνήθως χωρίς συστηματικό τρόπο και οι προσπάθειες αυτές δεν είναι τόσο ορατές στα ανώτερα διευθυντικά στελέχη. Η προσέγγιση του κύκλου ζωής πρέπει επίσης να ληφθεί υπόψη για χρήση στη διαχείριση των έργων για τον εντοπισμό, την ανάλυση, την αξιολόγηση και παρακολούθηση των κινδύνων και μπορεί επίσης να συνδεθεί με την περιοδική υποβολή εκθέσεων ώστε να αντικατοπτρίζει την έννοια earned value management (EVM) στους ιδιοκτήτες του συστήματος. Τα βασικά χαρακτηριστικά της εφαρμογής της EVM περιλαμβάνουν:

- ένα project plan που να προσδιορίζει τις εργασίες που πρέπει να υλοποιηθούν
- εκτίμηση του προγραμματισμένου έργου, που ονομάζεται planned value (PV)
- προκαθορισμένα "earning rules" (ονομάζονται και μετρήσεις) για να ποσοτικοποιήσουν την ολοκλήρωση των εργασιών, που ονομάζεται earned value (EV)

Οι EVM υλοποιήσεις για μεγάλα ή σύνθετα έργα περιλαμβάνουν πολλά περισσότερα χαρακτηριστικά, όπως οι δείκτες και οι προβλέψεις για την απόδοση του κόστους (πάνω / κάτω από τον προϋπολογισμό) και τις επιδόσεις (πίσω / μπροστά από το χρονοδιάγραμμα). Η πιο βασική απαίτηση ενός συστήματος EVM, όμως είναι ότι ποσοτικοποιεί την πρόοδο χρησιμοποιώντας τις PV και EV.

Ο διαχειριστής της ασφάλειας πληροφοριών θα πρέπει να επιδιώκει να χρησιμοποιούν τεχνικές διαχείρισης earned value ως συνέπεια της διαδικασίας μέτρησης και παρακολούθησης του κόστους, των εργαλείων υποστήριξης, εκπαίδευσης και βοήθειας για την καλύτερη κατανόηση και τη μείωση των επιπτώσεων των κινδύνων που είναι εγγενείς στον κύκλο ζωής ενός του έργου. Η προσέγγιση πρέπει να είναι top-down συστηματική, διότι η άποψη των ανώτερων διευθυντικών στελεχών για τον κίνδυνο μπορεί να χρησιμοποιηθεί για να καθοδηγήσει τη διαδικασία. Θα δώσει, επίσης, πρόσθετο βάρος και αξιοπιστία στη διαδικασία.

Θα πρέπει να σημειωθεί ότι η EVM δεν έχει διάταξη για τη μέτρηση της ποιότητας του έργου, ώστε να υποδεικνύει ότι ένα έργο είναι κάτω από τον προϋπολογισμό, μπροστά από το χρονοδιάγραμμα, ότι το πεδίο εφαρμογής του έχει εκτελεστεί πλήρως και έτσι εξακολουθεί να έχει δυσαρεστημένους πελάτες και, τελικά, ανεπιτυχή αποτελέσματα. Με άλλα λόγια, η EVM είναι μόνο ένα εργαλείο στην εργαλειοθήκη του διαχειριστή έργου.

Για να βελτιωθεί η αποδοτικότητα και η αποτελεσματικότητα, ο διευθυντής της ασφάλειας πληροφοριών θα πρέπει να εξετάσει την δυνατότητα πρόσληψής εργαλείων λογισμικού που έχουν σχεδιαστεί για την παρακολούθηση της διαχείρισης του κύκλου ζωής των κινδύνων. Αυτό είναι πλεονέκτημα γιατί επιτρέπει την μόχλευση των πεπερασμένων πόρων

προσωπικού για την κατάλληλη παρακολούθηση και την δημιουργία περιοδικών εκθέσεων για τη διαχείριση.

Σχήμα 3.23: Χαρακτηριστικά των φάσεων SDLC

Χαρακτηριστικά της SDLC φάσης		
SDLC φάσεις	Χαρακτηριστικά	Υποστήριξη από της δραστηριότητες της Διαχείρισης Επικινδυνότητας
Φάση 1η : Έναρξη	Εκφράζεται η ανάγκη για ένα IT σύστημα και τεκμηριώνεται ο σκοπός και το περιεχόμενο του IT συστήματος	Οι αναγνωρισμένοι κίνδυνοι χρησιμοποιούνται για την ανάπτυξη των απαιτήσεων του συστήματος, συμπεριλαμβανομένων των απαιτήσεων ασφάλειας και της έννοιας της ασφάλειας των λειτουργιών.
Φάση 2η : Ανάπτυξη ή Απόκτηση	Το πληροφοριακό σύστημα είναι είτε σχεδιασμένο, είτε αγορασμένο, είτε προγραμματισμένο, είτε αναπτυγμένο.	Οι κίνδυνοι που εντοπίζονται κατά τη διάρκεια αυτής της φάσης μπορεί να χρησιμοποιηθούν για τις αναλύσεις ασφάλειας των IT συστημάτων τα οποία μπορεί να οδηγήσουν σε αρχιτεκτονικούς και σχεδιαστικούς συμβιβασμούς κατά τη διάρκεια της ανάπτυξης του συστήματος
Φάση 3η : Υλοποίηση	Τα χαρακτηριστικά ασφαλείας του συστήματος θα πρέπει να ρυθμιστούν, ενεργοποιηθούν, να ελεγχθούν και να επαληθευθούν.	Η διαδικασία διαχείρισης επικινδυνότητας υποστηρίζει την υλοποίηση του μέσα σε ένα μοντελοποιημένο επιχειρησιακό περιβάλλοντος. Οι αποφάσεις σχετικά με τους κινδύνους που προσδιορίζονται πρέπει να ληφθούν πριν από τη λειτουργία του συστήματος
Φάση 4η : Λειτουργία ή Συντήρηση	Το σύστημα εκτελεί τις λειτουργίες του. Τυπικά το σύστημα βασίζεται στην προσθήκη του υλικού και του λογισμικού καθώς και σε αλλαγές οργανωτικές, στις διαδικασίες και στις	Οι δραστηριότητες διαχείρισης επικινδυνότητας διενεργούνται για την περιοδική επαναδειοδότηση των συστημάτων ή όποτε πραγματοποιούνται σημαντικές αλλαγές που στα

	πολιτικές	IT συστήματα στο λειτουργικό, ή στο περιβάλλον παραγωγής.
Φάση 5η : Διάθεση	Η φάση αυτή περιλαμβάνει τη διάθεση των πληροφοριών, του Hardware και του Software. Οι δραστηριότητες περιλαμβάνουν τη μετακίνηση, την αρχειοθέτηση, την απόρριψη, ή την καταστροφή των πληροφοριών και την «απολύμανση» του υλικού και του λογισμικού	Οι δραστηριότητες διαχείρισης επικινδυνότητας διενεργούνται για τα στοιχεία του συστήματος που θα διατεθούν ή θα αντικατασταθεί για να διασφαλίσουν ότι το hardware και το software έχουν σωστά απορριφθεί, τα υπολειμματικά δεδομένα έχουν διαχειριστεί κατάλληλα και ότι το migration του συστήματος γίνεται με ασφαλή τρόπο και συστηματικό

3.12.3 Αρχές και πρακτικές Διαχείρισης Επικινδυνότητας, βασισμένες στον κύκλο ζωής

Δεδομένου ότι η διαχείριση επικινδυνότητας είναι μια συνεχής διαδικασία, ο διευθυντής της ασφάλειας πληροφοριών πρέπει να χειριστεί τη διαχείριση του κινδύνου σαν να έχει έναν κύκλο ζωής. Αυτός ο κύκλος ζωής μπορεί να περιλαμβάνουν τις φάσεις της αξιολόγησης, της μείωσης και της παρακολούθησης. Χρησιμοποιώντας μια προσέγγιση διαχείρισης επικινδυνότητας, βασισμένη στον κύκλο ζωής και την ενσωμάτωση με την αλλαγή διαχείρισης, βελτιώνει το κόστος, δεδομένου ότι μια πλήρης αξιολόγηση του κινδύνου δεν πρέπει να γίνει περιοδικά. Αντ 'αυτού, οι ενημερώσεις μπορούν να γίνουν στην αξιολόγηση του κινδύνου και στις διαδικασίες διαχείρισης επικινδυνότητας σε συνεχόμενη βάση.

3.13 Βασικοί έλεγχοι ασφαλείας

Η διατύπωση βασικών αρχών για τις διαδικασίες ασφάλειας προωθεί την ελαχιστοποίηση των αναγκαίων μέτρων ασφαλείας σε όλη την επιχείρηση. Ο γενικός στόχος των βασικών ελέγχων ασφαλείας δεν πρέπει να επικεντρώνονται αποκλειστικά στην ελαχιστοποίηση της ασφάλειας σε έναν οργανισμό. Ο αρχικός στόχος τους είναι η διαμόρφωση των βασικών αρχών για τον καθορισμό κατευθυντήριων γραμμών, μετρήσεων ή δοκιμών για τους ελέγχους και τη διευκόλυνση αξιολόγησης των επιδόσεων των ελέγχων.

Το τελικό αποτέλεσμα από την εκτέλεση μιας τακτικής αξιολόγησης των ελέγχων είναι η δυνατότητα αξιολόγησης του ελέγχου ενός οργανισμού από ένα υψηλό επίπεδο και ο καθορισμός των ελάχιστων προδιαγραφών, ή των βασικών αρχών. Η ειδική για την ασφάλεια πρέπει να δώσουν, επίσης, προσοχή στην ανάπτυξη των βασικών αρχών, λόγω της δυναμικής φύσης του IT εξοπλισμού, λογισμικού, δικτύων και της ασφάλειας καθώς και των εξωτερικών παραγόντων. Όλα αυτά συνδυάζονται για να δημιουργήσουν συνεχώς μεταβαλλόμενα τρωτά σημεία και παράγοντες επίθεσης.

Μια βασική αρχή ορίζεται στο λεξικό ως "μια σειρά από γνωστά μέτρα ή της θέσεις που χρησιμοποιούνται για τον υπολογισμό ή τον εντοπισμό" ή "ένα αρχικό πακέτο παρατηρήσεων ή δεδομένων που χρησιμοποιούνται για σύγκριση ή έλεγχο." Μπορούμε να δούμε από αυτούς τους ορισμούς ότι, προκειμένου να διατυπωθεί μια βασική αρχή των ελέγχων ασφαλείας, είναι απαραίτητα κάποια μέτρα της αποτελεσματικότητας και της αποδοτικότητας των ελέγχων αυτών. Μια βασική αρχή συνήθως δεν βασίζεται σε ένα ενιαίο τεστ των ελέγχων, αλλά με βάση τη μέση ή την ενδιάμεση τιμή πολλαπλών δοκιμών.

Για τη δημιουργία βασικών αρχών ελέγχου, οι διαχειριστές ασφάλειας μπορεί να αναφερθούν σε πολλά από τα πρότυπα που ενδεχομένως να έχουν εφαρμοστεί εντός του οργανισμού. Με βάση αυτά τα πρότυπα, μια δοκιμασία ελέγχου γίνεται πολλές φορές για να καθορίσει την αξιολόγηση της αποτελεσματικότητας και της αποδοτικότητας του ελέγχου που απαιτείται από το πρότυπο. Για παράδειγμα, οι CobitT references DS5- *Ensure Systems Security* - απαιτεί μια πολιτική προστασίας από ιούς. Για τη δημιουργία μιας βασικής αρχής για τον έλεγχο του IT, ότι αυτό πληρεί τις διαδικασίες προστασίας από ιούς, ένας διαχειριστής ασφαλείας θα πρέπει να συγκεντρώσει τις τακτικές, περιοδικές (εβδομαδιαίες, μηνιαίες) εκθέσεις των μολυσμένων συστημάτων, τις ειδοποιήσεις ιών, τα περιστατικά ιών που αναφέρθηκαν, τις ενημερώσεις αρχείων και άλλες σχετικές πληροφορίες. Με βάση αυτές τις πληροφορίες, είναι δυνατό να αξιολογηθεί η αποτελεσματικότητα του ελέγχου και με βάση κάποιες πρόσθετες πληροφορίες -όπως οι άνθρωπο-ώρες που απαιτούνται, το κόστος του λογισμικού και των λανθανόντων κινδύνων- για την αξιολόγηση της αποτελεσματικότητας της διαδικασίας προστασίας από ιούς, όπως οι IT έλεγχοι.

Το παράδειγμα της διαδικασίας εντοπισμού ιών που παρουσιάζεται παραπάνω είναι ένα παράδειγμα μέτρησης ασφαλείας στο βαθμό που αυτό μπορεί να θεωρηθεί ως μέτρηση. Με βάση την τακτική αξιολόγηση των μετρήσεων, οι διαχειριστές ασφάλειας μπορούν να αναπτύξουν αποτελεσματικές βασικές αρχές έλεγχου. Οι καλές μετρήσεις για την αξιολόγηση των ελέγχων έχουν τα ακόλουθα χαρακτηριστικά:

- Μετρήσεις βασισμένες σε ποσοστά συγκεκριμένων απαιτήσεων.
- Ανέξοδη συγκέντρωση των αναγκαίων πληροφοριών για την εκτέλεση των μετρήσεων αυτών.
- Μετρήσεις με συνέπεια, σύμφωνα με τεκμηριωμένες και αμετάβλητες διαδικασίες μέτρησης για την διασφάλιση συνεπών αποτελεσμάτων.
- Τακτικές μετρήσεις σε συγκεκριμένα και προκαθορισμένα χρονικά διαστήματα.

Καθώς το κόστος για τη συλλογή των μετρήσεων αυξάνει και η ικανότητα για ποσοτικοποίηση των αποτελεσμάτων μειώνεται, η οργανωτική αξία των μετρήσεων μειώνεται. Αν η μέτρηση δεν είναι ποσοτική έτσι ώστε τα αποτελέσματα να είναι αδιαμφισβήτητα, τότε οι χρήστες των δεδομένων θα τείνουν να μειώσουν την αξία των δεδομένων. Εάν το κόστος για τη συλλογή δεδομένων αυξάνεται πάρα πολύ, οι υπεύθυνοι ασφαλείας πρέπει να εξετάσουν τη χρήση άλλων μεθόδων μέτρησης, όπως η έμμεση ανάλυση ή προεκτάσεις που βασίζονται σε άλλες σχετικές μετρήσεις.

Η ρύθμιση των βασικών αρχών ασφαλείας για την λειτουργία ενός οργανισμού έχει μια σειρά από οφέλη. Τυποποιεί το ελάχιστο μέγεθος των μέτρων ασφαλείας που πρέπει να χρησιμοποιούνται σε όλη την επιχείρηση και αυτό οδηγεί σε θετικά οφέλη για τη διαχείριση επικινδυνότητας. Δεύτερον, παρέχει ένα σημείο αναφοράς για τη μέτρηση των αλλαγών στην ασφάλεια και τον προσδιορισμό των αντίστοιχων επιπτώσεων των κίνδυνων.

Δουλεύοντας σε συνεργασία με την ομάδα επιχειρησιακής αρχιτεκτονικής του οργανισμού, μπορούν να αναπτυχθούν οι βασικές αρχές της ασφάλεια πληροφοριών των ελέγχων, που να είναι κατάλληλες για το περιβάλλον λειτουργίας του οργανισμού.

Υπάρχει ένας πλούτος πληροφοριών που διατίθενται από τα NIST, COBIT, ISO / IEC 27001 και τους παρόχους ασφάλειας όσον αφορά τα πρότυπα για τους ελέγχους της ασφάλειας πληροφοριών. Ωστόσο, ο διευθυντής της ασφάλειας πληροφοριών πρέπει να έχει κατά νου ότι κάθε οργανισμός έχει τις δικές του ανάγκες και προτεραιότητές. Ενώ το NIST και οι πάροχοι μπορούν να παρέχουν σημεία εκκίνησης της υποστήριξης για την ανάπτυξη των ελέγχων, πρέπει να γίνεται πάντα ειδική ανάλυση. Κατάλληλοι έλεγχοι για την επιχείρηση θα πρέπει να αναπτυχθούν με βάση μια ποικιλία παραγόντων, όπως η κουλτούρα, η δομή, η ανοχή του κινδύνου, κλπ. Είναι επίσης σημαντικό να έχουμε κατά νου ότι, εκτός από την τεχνολογία στον ορισμό ενός προγράμματος ανάλυσης των κινδύνων, οι άνθρωποι και οι διαδικασίες πρέπει να λαμβάνονται εξίσου υπόψη. Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει επίσης να αναπτύξει βασικές αρχές ασφάλειας για τις διαδικασίες και την σωματική ακεραιότητα. Αυτό θα παρουσιάσει συχνά περισσότερες από μια προκλήσεις, δεδομένου ότι αποτελούν συνήθως περιοχές εκτός των ορίων των ελέγχων του τμήματος ασφαλείας. Τα κατάλληλα πρότυπα, με την έγκριση του διοικητικού συμβουλίου, μπορεί να είναι η πιο αποτελεσματική προσέγγιση για την αντιμετώπιση αυτού του ζητήματος. Ο εσωτερικός έλεγχος και η τακτική αξιολόγηση της ασφάλειας μπορεί να παρέχει την διασφάλιση συμμόρφωσης.

Υπάρχει μια γενική συναίνεση μεταξύ παρόχων, οργανισμών ασφάλειας, ειδικών σε θέματα ασφάλειας πληροφοριών και των ελεγκτών των συστημάτων σχετικά με τις προδιαγραφές των παραμέτρων ασφαλείας που αντιστοιχούν σε ένα αποδεκτό επίπεδο δέουσας προσοχής των συστημάτων. Αυτές οι συνεργατικές προσπάθειες συνεχίζουν να καθορίζουν συναινετικές, ορθές πρακτικές ρυθμίσεων ασφαλείας για διάφορα συστήματα και πλατφόρμες. Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να εξετάσει αυτές τις

προδιαγραφές και, ανάλογα με την περίπτωση, πρέπει να προσαρμόσει και να ενσωματώσει τις βασικές οργανωτικές αρχές ασφάλειας.

Ενώ τα βιομηχανικά πρότυπα είναι σημαντικό να τα γνωρίζει ο διαχειριστής της ασφάλειας πληροφοριών, πρέπει να αξιολογήσει το επίπεδο ασφάλειας που πρέπει να εφαρμοστεί στον οργανισμό. Η συνεύρεση διαφορετικών τεχνολογιών μπορεί να εισάγει συχνά νέους κινδύνους και να μεταβάλει ένα ασφαλές σύστημα ή πλατφόρμα σε ένα σύστημα με πολλά τρωτά σημεία. Μια εξειδικευμένη αξιολόγηση κινδύνων, που αναγνωρίζει αυτές τις αλληλεπιδράσεις και τις εξαρτήσεις, επιτρέπει στο διευθυντή της ασφάλειας πληροφοριών να καθορίσει αν οι διαδικασίες ασφαλείας είναι απαραίτητες για την παροχή επαρκούς ασφάλειας, ανάλογη με τα καθορισμένα επίπεδα αποδεκτού κινδύνου των οργανισμών. Ορισμένες οργανώσεις και βιομηχανίες μπορεί να χρειαστούν ισχυρότερες βασικές αρχές. Η κανονιστική απαίτηση για ορισμένους βιομηχανικούς κλάδους και περιοχές μπορεί να θέσει υψηλότερα επίπεδα. Ένα άλλο θέμα είναι ότι ορισμένες από τις πληροφορίες του οργανισμού χαρακτηρίζονται ως ιδιαίτερα ευαίσθητες και πρέπει να υπάρχουν πάντα μηχανισμοί ελέγχου που να παρέχουν υψηλότερα επίπεδα ασφάλειας.

3.14 Επικοινωνία και Παρακολούθηση Κινδύνων

Η εφαρμογή ενός αποτελεσματικού προγράμματος διαχείρισης κινδύνων απαιτεί παρακολούθηση και επικοινωνία. Η παρακολούθηση της αποτελεσματικότητας των ελέγχων είναι μια συνεχής προσπάθεια που απαιτείται για να διαχειριστεί ο κίνδυνος. Πρέπει να καθιερωθούν κανάλια επικοινωνίας τόσο για την υποβολή εκθέσεων και την διάδοση των πληροφοριών σχετικά με τη διαχείριση των κινδύνων καθώς και για την παροχή στην διαχείριση της ασφάλειας πληροφοριών με πληροφορίες σχετικά με τον κίνδυνο, που σχετίζονται με τις δραστηριότητες σε ολόκληρη την επιχείρηση, συμπεριλαμβανομένων αναφορών με σημαντικές αλλαγές στον κίνδυνο την κατάρτιση και την ενημέρωση.

3.14.1 Υποβολή εκθέσεων σημαντικών αλλαγών των κινδύνων

Η αναφορά των σημαντικών αλλαγών των κινδύνων στα κατάλληλα επίπεδα της διαχείρισης σε περιοδική βάση αποτελεί πρωταρχική ευθύνη της διαχείρισης της ασφάλειας πληροφοριών. Καθώς οι αλλαγές συμβαίνουν μέσα στην οργάνωση, η εκτίμηση κινδύνου πρέπει να ενημερώνεται συνεχώς ώστε να εξασφαλίζεται ότι παραμένει ακριβής. Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να έχει περιοδικές συναντήσεις ενημέρωσης της ανώτερης διοίκησης για την παρουσίαση της κατάστασης σχετικά με το συνολικό πρόγραμμα για την ασφάλεια του οργανισμού. Αυτή η ενημέρωση πρέπει να περιλαμβάνει κάθε σημαντική αλλαγή στο προφίλ κινδύνου του οργανισμού καθώς και την τρέχουσα κατάσταση των μη διευθετημένων κινδύνων.

Επιπλέον, το πρόγραμμα ασφαλείας πρέπει να περιλαμβάνει μια διαδικασία με την οποία κάθε σημαντικό συμβάν παραβίασης της ασφάλειας θα ενεργοποιήσει αναφορά στην ανώτερη διοίκηση. Ο διαχειριστής της ασφάλειας πληροφοριών πρέπει να καθορίσει τις διαδικασίες με τις οποίες αξιολογούνται τα συμβάντα ασφαλείας, με βάση τις επιπτώσεις στην επιχείρηση. Η αξιολόγηση αυτή μπορεί να απαιτεί μια ειδική έκθεση για την ανώτερη διοίκηση για την ενημέρωση τους για την εκδήλωση, τις επιπτώσεις και τα μέτρα που λαμβάνονται για τον περιορισμό του κινδύνου.

Ένα σημαντικό στοιχείο του κύκλου ζωής της διαχείρισης επικινδυνότητας είναι η συνεχής παρακολούθηση, η αξιολόγηση και η εκτίμηση των κινδύνων. Τα αποτελέσματα και το καθεστώς αυτής της συνεχούς ανάλυσης πρέπει να τεκμηριώνονται και να αναφέρονται στα ανώτερα διευθυντικά στελέχη σε τακτική βάση. Για να διευκολυνθεί η υποβολή εκθέσεων, οπτικά βοηθήματα όπως η χρώμα-κωδικοποίηση και η συνοπτική επισκόπηση μπορεί να είναι χρήσιμα.

Η διοίκηση συνήθως δεν θέλει να επιβαρύνεται με τις τεχνικές λεπτομέρειες και είναι πιθανό να θέλουν μια επισκόπηση της τρέχουσας κατάστασης και των δεικτών κάθε άμεσης ή επικείμενης απειλής. Κατά συνέπεια, κόκκινες – πορτοκαλί - πράσινες εκθέσεις, συχνά αναφέρονται ως πίνακες ασφαλείας ή διαγράμματα κι δείχνουν μια συνολική εκτίμηση της κατάστασης ασφάλειας και, ως εκ τούτου, χρησιμοποιούνται συχνά. Ανάλογα με τους παραλήπτες, άλλες μορφές που αντιπροσωπεύουν το καθεστώς ασφαλείας, όπως γραφήματα ή αραχνοειδή διαγράμματα είναι συχνά πιο αποτελεσματικά στο να μεταφέρουν τις τάσεις αυτές. Όποια και αν είναι η μορφή των εκθέσεων, ο διευθυντής της ασφάλειας πληροφοριών είναι υπεύθυνος για τη διαχείριση αυτής της διαδικασίας υποβολής εκθέσεων για να εξασφαλίσει ότι θα υλοποιηθεί και ότι τα αποτελέσματα αναλύονται επαρκώς και θα υλοποιούνται κατάλληλα και έγκαιρα. Αυτό περιλαμβάνει τον προσδιορισμό των τύπων των γεγονότων τα οποία θα προκαλέσουν την υποβολή εκθέσεων ,που απαιτούνται από τους ρυθμιστικούς οργανισμούς και / ή την επιβολή του νόμου και την παροχή συμβουλών διαχείρισης της εν λόγω απαίτησης.

3.15 Κατάρτιση και ενημέρωση

Οι άνθρωποι συνήθως αποτελούν το μεγαλύτερο κίνδυνο σε οποιαδήποτε οργανισμό εν γένει, λόγω ατυχήματος, λάθους ή έλλειψης γνώσης / πληροφόρησης και, περιστασιακά, λόγω κακόβουλων προθέσεων. Η κατάλληλη εκπαίδευση και ενημέρωση του κοινού μπορεί να έχει σημαντική θετική συμβολή στη διαχείριση των κινδύνων. Πολλοί έλεγχοι είναι διαδικαστικού χαρακτήρα και απαιτούν κάποια επιχειρησιακή γνώση και συμμόρφωση. Οι τεχνικές ελέγχου πρέπει να ρυθμιστούν και να λειτουργούν σωστά για να παρέχουν το αναμενόμενο επίπεδο ασφαλείας. Η διασφάλιση ότι οι χρήστες εκπαιδεύονται στις διαδικασίες και κατανοήσουν τις διαδικασίες διαχείρισης επικινδυνότητας είναι η ευθύνη του διαχειριστή της ασφάλειας πληροφοριών και οι κατάλληλες δραστηριότητες κατάρτισης και ενημέρωσης θα πρέπει να περιλαμβάνονται σε οποιοδήποτε πρόγραμμα διαχείρισης επικινδυνότητας.

Το πρόγραμμα εκπαίδευσης και ενημέρωσης πρέπει να απευθύνεται σε διαφορετικά επίπεδα στελέχωσης και ασφάλειας (π.χ. ανώτερα διοικητικά στελέχη, μεσαία στελέχη / το προσωπικό και τους τελικούς χρήστες).

Η εκπαίδευση του τελικού χρήστη σε θέματα ασφάλειας πρέπει να περιλαμβάνει τις εξής συνεδρίες:

- Μετάδοση της σημασίας της κανονιστικής συμμόρφωσης με τις πολιτικές και τις διαδικασίες ασφαλείας της επιχείρησης.
- Ξεκάθαρες πολιτικές γραφείου.
- Αντίδραση σε κατάσταση έκτακτης ανάγκης
- Σημασία της λογικής πρόσβασης σε ένα IT περιβάλλον.
- Προστασία προσωπικών δεδομένων και απορρήτου.
- Την αναγνώριση και την αναφορά περιστατικών ασφάλειας.
- Αναγνώριση και αντιμετώπιση του social engineering.

3.16 Έγγραφα

Για τη σωστή διαχείριση επικινδυνότητας απαιτούνται τα κατάλληλα έγγραφα. Οι αποφάσεις σχετικά με την έκταση των εγγράφων συνεπάγεται κόστος και συναφή οφέλη. Το πρόγραμμα και η πολιτική διαχείρισης επικινδυνότητας καθορίζει το απαιτούμενο documentation. Συγκεκριμένα, κάθε στάδιο της διαδικασίας της τεκμηρίωσης πρέπει να περιλαμβάνονται:

- Οι στόχοι
- Το Κοινό
- Οι πηγές πληροφοριών
- Παραδοχές
- Αποφάσεις

Τα έγγραφα της πολιτικής διαχείρισης επικινδυνότητας περιλαμβάνουν πληροφορίες όπως:

- Στόχοι της πολιτικής και το σκεπτικό για τη διαχείριση επικινδυνότητας.
- Οι σχέσεις μεταξύ της πολιτικής διαχείρισης επικινδυνότητας, της στρατηγικής του οργανισμού και των επιχειρηματικών σχεδίων
- Την έκταση και το εύρος των θεμάτων στα οποία εφαρμόζεται η πολιτική.
- Οδηγίες για το τι μπορεί να θεωρηθεί αποδεκτός κίνδυνος.
- Αρμοδιότητες διαχείρισης επικινδυνότητας.
- Υποστήριξη ειδικών διαθέσιμων να βοηθήσουν τους υπεύθυνους διαχείρισης κινδύνων.
- Απαιτούμενο επίπεδο τεκμηρίωσης.
- Ένα πλάνο για την συμμόρφωση με την πολιτική διαχείρισης επικινδυνότητας.
- Επίπεδα σοβαρότητας Περιστατικών.
- Υποβολή εκθέσεων κινδύνων και κλιμάκωση των διαδικασιών, μορφών και τη συχνότητας αυτών.

Σε ορισμένες περιπτώσεις, η κανονιστική συμμόρφωση μπορεί να χρειαστεί για να διασφαλιστεί ότι οι διαχειριστές αναγνωρίσουν επίσημα την ευθύνη τους για την συμμόρφωσης με τις πολιτικές και διαδικασίες διαχείρισης επικινδυνότητας.

Το τυπικό documentation για τη διαχείριση επικινδυνότητας πρέπει να περιλαμβάνει, τουλάχιστον, τα ακόλουθα:

- Μητρώο Κινδύνων - Για κάθε προσδιορισμένο κίνδυνο, καταγράφονται:
  - Πηγή του κινδύνου
  - Φύση του κινδύνου
  - Οι υπάρχοντες έλεγχοι
  - Οι απαιτούμενοι έλεγχοι που δεν έχουν υλοποιηθεί και οι λόγοι για τους οποίους πρέπει να εφαρμοστούν.

- Επιπτώσεις και πιθανότητα, συμπεριλαμβανομένων:
  - Απώλειας εισοδήματος.
  - Απρόβλεπτη δαπάνη.
  - Νομικός κίνδυνος (συμμόρφωση και οι συμβατικοί).
  - Αλληλένδετες διαδικασίες.
  - Απώλεια της δημόσιας φήμη ή της εμπιστοσύνης του κοινού
- Αρχική εκτίμηση του κινδύνου.
- Ευπάθεια σε εξωτερικούς / εσωτερικούς παράγοντες
- Η απογραφή των τηλεπικοινωνιακών και των IT περιουσιακών στοιχείων που να περιλαμβάνει τουλάχιστον:
  - Περιγραφή των IT περιουσιακών στοιχείων.
  - Τεχνικές προδιαγραφές
  - Αριθμός / ποσότητα
  - Τοποθεσία
  - Ειδικές απαιτήσεις Αδειοδότησης, εάν υπάρχουν
- Μείωση του κινδύνου και σχέδιο δράσης, παρέχοντας:
  - Ποιος έχει την ευθύνη για την εφαρμογή του σχεδίου
  - Πόροι που θα χρησιμοποιηθούν
  - Κατανομή του προϋπολογισμού
  - Χρονοδιάγραμμα για την εφαρμογή
  - Στοιχεία του μηχανισμού / μέτρων ελέγχου
  - Συχνότητα συμμόρφωσης
- Έγγραφα παρακολούθησης και ελέγχου, τα οποία περιλαμβάνουν:
  - Τα αποτελέσματα των ελέγχων / κριτικές και άλλες διαδικασίες παρακολούθησης
  - Παρακολούθηση των συστάσεων της αξιολόγησης και της κατάστασης της υλοποίησης.

Κεφάλαιο 4ο

Μελέτη Περίπτωσης

Διαχείριση Επικινδυνότητας Σε Πάροχο Κινητών Επικοινωνιών.

Όπως αναφέρθηκε και παραπάνω, η διασφάλιση ότι ο εντοπισμός των κινδύνων, η ανάλυση και οι ενέργειες μείωσης αυτών είναι ενσωματωμένες στις διαδικασίες του κύκλου ζωής κάθε συστήματος και αποτελούν ένα σημαντικό καθήκον της διαχείρισης της ασφάλειας πληροφοριών. Δεδομένου ότι οι αλλαγές σε κάθε πηγή πληροφοριών είναι πιθανό να περιέχουν νέα τρωτά σημεία και να αλλάξουν τη συνολική εξίσωση επικινδυνότητας, είναι σημαντικό να έχουμε επίγνωση των προτεινόμενων τροποποιήσεων καθώς η προσέγγιση αυτή επιτρέπει στις δραστηριότητες εντοπισμού, ανάλυσης και μείωσης των κινδύνων να ενσωματωθούν στις διαδικασίες του κύκλου ζωής του οργανισμού.

Όπως ειπώθηκε και προηγουμένως, η αποτελεσματική διαχείριση επικινδυνότητας θα πρέπει να ενσωματωθεί πλήρως στην ανάπτυξη του κύκλου ζωής των συστημάτων (system development life cycle - SDLC). Η SDLC ενός πληροφοριακού συστήματος έχει πέντε φάσεις: **έναρξη, ανάπτυξη ή απόκτηση, την υλοποίηση, τη λειτουργία ή τη συντήρηση και τη διάθεση**. Σε ορισμένες περιπτώσεις, ένα σύστημα πληροφορικής μπορεί να καταλάβει πολλά από τα στάδια αυτά την ίδια στιγμή. ***Ωστόσο, η μεθοδολογία διαχείρισης επικινδυνότητας είναι η ίδια, ανεξάρτητα από τη φάση SDLC για την οποία διεξάγεται η αξιολόγηση.***

Στο κεφάλαιο αυτό λοιπόν, καταγράφονται οι κίνδυνοι – ευπάθειες καθώς και τα τρωτά σημεία που διαπιστώθηκαν στις φάσεις **έναρξης, ανάπτυξης ή απόκτησης, υλοποίησης, λειτουργίας ή συντήρησης και διάθεσης** ενός νέου συστήματος για την εξυπηρέτηση υπηρεσιών προπληρωμένης κινητής τηλεφωνίας σε πάροχο τηλεπικοινωνιών

4.1 Αξιολόγηση Επικινδυνότητας

Στην περίπτωση που θα μελετήσουμε παρακάτω, ο διαχωρισμός και η κατηγοριοποίηση των κινδύνων έγινε με βάσει τους τομείς που επηρεάζονται και εμπεριέχουν **διαφορετικές** φάσεις του κύκλου ζωής ο καθένας τους.

Για την λειτουργία του τρόπου αξιολόγησης των κινδύνων που θα ακολουθήσουν θα πρέπει να επισημάνουμε όμως μερικές, ιδιαιτέρως κρίσιμες παραμέτρους:

1. Αναγνώριση πιθανών απειλών. (βλ. Παράρτημα)

2. Εκτίμηση πιθανότητας των κινδύνων.

Έχοντας εντοπίσει τις απειλές που επηρεάζουν τον οργανισμό, τις αξιολογούμε μέσω υποκειμενικών εκτιμήσεων (πίνακας 4.1).

Επίπεδο	Περιγραφή	Πιθανότητα στα 10 έτη (%)	Πιθανότητα στα 10 έτη.
1	Αμελητέο	> 0,005%	1 στα 20000
2	Σπάνιο	> 0,05%	1 στα 2000
3	Απίθανο	> 0,5%	1 στα 200
4	Δυνατόν	> 5%	1 στα 20
5	Πιθανό	> 50%	1 στα 2
6	Πάρα Πολύ Πιθανό	> 75%	3 στα 4
7	Σχεδόν βέβαιο	> 90%	9 στα 10

Πίνακας 4.1: Κατηγοριοποίηση Πιθανοτήτων

3. Πιθανή επιρροή αυτών (πίνακας 4.2):

Σοβαρότητα Επιρροής					
Επίπεδα	**Απαιτούμενα Επίπεδα Ενημέρωσης**	**Θέματα Υγείας και Ασφάλειας**	**Θέματα Πελατών**	**Θέματα Υπόληψης και ΜΜΕ**	**Προβλήματα Λειτουργίας**
5	Κρισιμη (Ενημέρωση διοικητικού συμβουλίου, θανάσιμα γεγονότα, μαζική καταστροφή, ολική απώλεια συστημάτων.)				
4	Πολύ Σημαντική (Ενημέρωση γενικών διευθύνσεων, Φυσική καταστροφή, τεχνική βλάβη με σοβαρή επιρροή)				
3	Σημαντική (Ενημέρωση διευθύνσεων, Επείγοντα περιστατικά υγείας, σοβαρές βλάβες)				
2	Μικρής Επιρροής (Ενημέρωση υπεύθυνων, βλάβες, ατυχήματα με ιατρική περίθαλψη)				
1	Ασήμαντη (πχ μικρές βλάβες, ατυχήματα, ενημέρωση ομάδας κλπ)				

Πίνακας 4.2 Επίπεδα Επιρροής Κινδύνων

4. Αξιολόγηση των κινδύνων

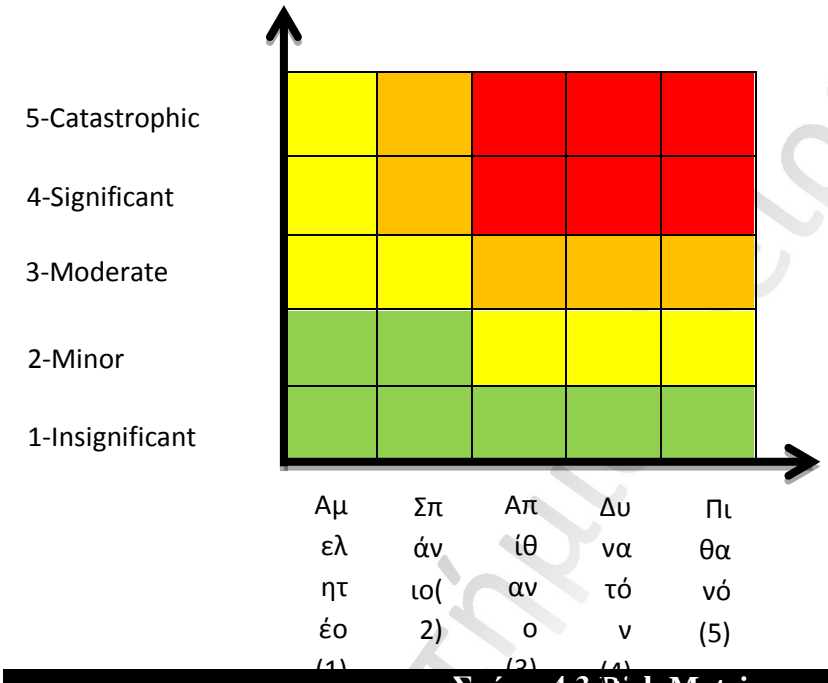
Η συνολική εκτίμηση της επικινδυνότητας επιτυγχάνεται με τον ακόλουθο τρόπο.

Αρχικά υπολογίζουμε την ***έκθεση κινδύνου*** με τον πολλαπλασιασμό της πιθανότητας εμφάνισης επί το επίπεδο επιρροής αυτής. Τα αποτελέσματα καταγράφονται στα αντίστοιχα Φύλλα Κινδύνου και στην συνέχεια αντιστοιχούνται στον Risk Matrix.

Στην συνέχεια, με βάση τα παραπάνω, καταγράφεται η προτεραιότητα του συστήματος, όπως κλιμακώνεται στον πίνακα 4.9 και τέλος, πολλαπλασιάζουμε την έκθεση με την προτεραιότητα για την εύρεση της συνολικής έκθεσης και τα αποτελέσματα αντιστοιχούνται με βάση τον πίνακα 4.10.

5. Προληπτικά και διορθωτικά μέτρα

6. Τοποθέτηση – Αντιστοίχιση κινδύνων στον risk matrix (Σχήμα 4.3).



Σχήμα 4.3 Risk Matrix

Στην συνέχεια, αφού καθορίσουμε πιθανότητα και επιρροή και αντιστοιχήσουμε τα αποτελέσματα στον Risk Matrix, αυτόματα έχουμε ένδειξη για τις ενέργειες που πρέπει να ακολουθήσουμε για την αντιμετώπιση του κινδύνου.

Πιο συγκεκριμένα,

Αποδοχή: Καθορίζεται στα σημεία όπου η πιθανότητα και η επιρροή είναι Μικρή/Αμελητέα. Η διοίκηση αποφασίζει να μην προβεί σε ενέργειες και αποδέχεται τον κίνδυνο.

Πρόληψη: Η πιθανότητα εδώ είναι μικρή αλλά η επιρροή μπορεί να είναι σοβαρή και πρέπει να ληφθεί υπόψη στα πλάνα της διοίκησης.

Διαχείριση: Υψηλή πιθανότητα αλλά η επιρροή μικρή. Η καλύτερη επιλογή εδώ είναι η διαχείριση του κινδύνου.

Αντιμετώπιση: Η πιθανότητα και η επιρροή είναι μεγάλη. Αν δεν είναι εύκολο να ελαχιστοποιηθεί ο κίνδυνος, τότε πιθανότατα να πρέπει να προχωρήσουμε σε παύση των δραστηριοτήτων.

7. Ολοκλήρωση καταγραφής Φύλλων Κινδύνου.

4.2 Ταξινόμηση Συστήματος (Προτεραιότητα)

Η ταξινόμηση των συστημάτων βασίζεται στην αποτίμηση των επιχειρηματικών επιπτώσεων που θα είχε η διακύβευση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας και λαμβάνοντας υπόψη την ταξινόμηση των πληροφοριακών στοιχείων που επεξεργάζεται, αποθηκεύει ή μεταδίδει.

Η ταξινόμηση των συστημάτων είναι αναγκαία για τον υπολογισμό του επιπέδου των κινδύνων που εντοπίζονται σε αυτά, στο πλαίσιο διεξαγωγής της αποτίμησης κινδύνων ασφάλειας συστήματος, βάσει της σχετικής διαδικασίας και μεθοδολογίας, ώστε να λαμβάνονται τα κατάλληλα μέτρα προστασίας τους.

Ως προς την εμπιστευτικότητα, εκτιμώνται οι επιπτώσεις που θα είχε η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών που επεξεργάζεται, αποθηκεύει ή μεταδίδει το σύστημα στις επιχειρησιακές διεργασίες της εταιρίας.

Ως προς την ακεραιότητα, εκτιμώνται οι επιπτώσεις που θα είχε η μη εξουσιοδοτημένη τροποποίηση των πληροφοριών που επεξεργάζεται, αποθηκεύει ή μεταδίδει το σύστημα στις επιχειρησιακές διεργασίες που υποστηρίζονται από το σύστημα.

Ως προς τη διαθεσιμότητα, εκτιμώνται οι επιπτώσεις που θα είχε η μη διαθεσιμότητα του συστήματος και των πληροφοριακών στοιχείων που επεξεργάζεται, αποθηκεύει ή μεταδίδει στις επιχειρησιακές διεργασίες που υποστηρίζονται από το σύστημα.

Πιθανές επιπτώσεις που συνυπολογίζονται στην εκτίμηση των επιχειρηματικών επιπτώσεων είναι:

- Απώλεια εσόδων ή απάτη
- Πρόσθετες δαπάνες
- Απώλεια μεριδίου αγοράς
- Ανταγωνιστικό μειονέκτημα ή απώλεια πλεονεκτήματος
- Παραβίαση νομικού / κανονιστικού πλαισίου
- Ζημιά στην εταιρική εικόνα (κλονισμός εμπιστοσύνης κοινού, πελατών, μετόχων, προμηθευτών)
- Κλονισμός ηθικού εργαζομένων
- Λανθασμένες αποφάσεις / ενέργειες του προσωπικού
- Ανωμαλία στην καθημερινή λειτουργία της εταιρείας

Το Σχήμα Ταξινόμησης των συστημάτων για κάθε παράμετρο ασφάλειας περιγράφεται στη συνέχεια.

4.2.1 Αξιολόγηση Κρισιμότητας Πληροφοριακού Συστήματος

Στο στάδιο αυτό αξιολογείται η κρισιμότητα κάθε συστήματος, ως προς τις συνέπειες που θα είχε η διακύβευση της εμπιστευτικότητας, διαθεσιμότητας ή ακεραιότητας των πληροφοριών, λαμβάνοντας υπόψη και την ταξινόμηση των πληροφοριακών στοιχείων που διαχειρίζεται το σύστημα.

a. Αναγνώριση και Αξιολόγηση Απειλών & Ευπαθειών

Τα πληροφοριακά συστήματα εκτίθενται σε διάφορες απειλές. Μια απειλή εκδηλώνεται όταν μια κατάσταση ή ένα γεγονός εκμεταλλεύονται κάποια ευπάθεια του συστήματος, με αποτέλεσμα την παραβίαση της ασφάλειας του συστήματος και την εκδήλωση ενός περιστατικού. Η εκδήλωση μιας απειλής θα είχε ως αποτέλεσμα ένα περιστατικό ασφάλειας, με συνέπειες για την επιχειρηματική λειτουργία της εταιρίας.

Μια απειλή θα πρέπει να εκμεταλλευτεί κάποια ευπάθεια του συστήματος, ώστε να επιτύχει το σκοπό της, π.χ. τη διαρροή εμπιστευτικών πληροφοριών. Ο στόχος είναι να αναπτυχθεί μία λίστα με ευπάθειες συστήματος, δηλαδή αδυναμίες ή ελλείψεις μηχανισμών προστασίας, η εκμετάλλευση των οποίων θα οδηγούσε στην εκδήλωση ενός περιστατικού ασφάλειας. Μια ευπάθεια μπορεί να γίνει αιτία εκδήλωσης μιας απειλής, είτε χωρίς πρόθεση, είτε από δόλο. Μια πιθανή απειλή δεν αποτελεί κίνδυνο, αν δεν υπάρχουν σχετικές ευπάθειες που θα μπορούσε να εκμεταλλευτεί.

Η αξιολόγηση του συνδυασμού απειλής και ευπάθειας πρέπει να λαμβάνει υπόψη:

a. Τη συχνότητα με την οποία έχουν εκδηλωθεί σχετικά περιστατικά στο παρελθόν, είτε στην εταιρία ή σε άλλους τηλεπικοινωνιακούς φορείς

b. Στατιστικές μελέτες σχετικά με την εκδήλωση περιστατικών ασφάλειας

c. Πιθανά κίνητρα εισβολέων καθώς και τις απαραίτητες γνώσεις, δεξιότητες και πόρους που απαιτούνται από εισβολείς, καθώς επίσης και τη λογική θέση του εισβολέα (εσωτερικός χρήστης / εξωτερικός εισβολέας)

Η κλίμακα που χρησιμοποιείται για τον σκοπό αυτό απεικονίζεται στον παρακάτω πίνακα 4.7:

Επίπεδο Συνδυασμού Απειλής και Ευπάθειας	Περιγραφή
1 - Χαμηλό	Η απειλή έχει χαμηλή πιθανότητα εκδήλωσης ή υπάρχουν υλοποιημένοι μηχανισμοί ελέγχου που μπορούν να αποτρέψουν την εκμετάλλευση της ευπάθειας
2 - Μέτριο	Η απειλή έχει μέτρια πιθανότητα εκδήλωσης ή/και υπάρχουν μερικώς υλοποιημένοι μηχανισμοί ελέγχου που μπορεί να αποτρέψουν την εκμετάλλευση της ευπάθειας
3 - Υψηλό	Η απειλή έχει υψηλή πιθανότητα εκδήλωσης και δεν υπάρχουν επαρκείς μηχανισμοί προστασίας για την ευπάθεια

Πίνακας 4.7: Επίπεδο Συνδυασμού Απειλής και Ευπάθειας

b. Υπολογισμός Επιπέδου Κινδύνου

Το επίπεδο κινδύνου του συστήματος, για κάθε ευπάθεια / απειλή, υπολογίζεται ως συνδυασμός:

- της κρισιμότητας του συστήματος, ως προς την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα
- της πιθανότητας εκδήλωσης μιας απειλής, εκμεταλλευόμενη μια ευπάθεια του συστήματος

Το επίπεδο κινδύνου, υπολογίζεται για καθεμιά παράμετρο ασφάλειας (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) με βάση τον πίνακα 4.8:

Επίπεδο Κινδύνου						
		Επίπεδο Κρισιμότητας Ε/Δ/Α				
		1	2	3	4	5
Επίπεδο Απειλής και Ευπάθειας	1	1	1	2	3	4
	2	1	2	3	4	5
	3	2	3	4	5	5

Πίνακας 4.8: Υπολογισμός Επίπεδου Κινδύνου

Το επίπεδο κινδύνου χρησιμοποιείται ώστε να γίνει επιλογή των κατάλληλων αντιμέτρων για την αντιμετώπιση του.

Η ταξινόμηση του συστήματος για καθεμιά απαίτηση ασφάλειας γίνεται ως εξής:

i. Εμπιστευτικότητα

Επίπεδο Κρισιμότητας	Περιγραφή Επιπέδου ως προς την Εμπιστευτικότητα
5 Πολύ Υψηλό	Το σύστημα επεξεργάζεται άκρως απόρρητα πληροφοριακά στοιχεία ή/ και η αποκάλυψη των πληροφοριακών στοιχείων του συστήματος μπορεί να προκαλέσει πάρα πολύ σοβαρές επιπτώσεις στην λειτουργία της Εταιρίας.
4 Υψηλό	Το σύστημα επεξεργάζεται απόρρητα πληροφοριακά στοιχεία ή/και η αποκάλυψη των πληροφοριακών στοιχείων του συστήματος μπορεί να προκαλέσει πολύ σοβαρές επιπτώσεις στην λειτουργία της Εταιρίας.
3 Μέτριο	Το σύστημα επεξεργάζεται εμπιστευτικά πληροφοριακά στοιχεία ή/και η αποκάλυψη των πληροφοριακών στοιχείων του συστήματος μπορεί να προκαλέσει σημαντικές επιπτώσεις στην λειτουργία της Εταιρίας.
2 Χαμηλό	Το σύστημα επεξεργάζεται πληροφοριακά στοιχεία για εσωτερική χρήση ή/ και η αποκάλυψη των πληροφοριακών στοιχείων του συστήματος μπορεί να προκαλέσει μικρές επιπτώσεις στην λειτουργία της Εταιρίας.
1 Πολύ Χαμηλό	Το σύστημα επεξεργάζεται πληροφοριακά στοιχεία για δημόσια χρήση ή/ και η αποκάλυψη των πληροφοριακών στοιχείων του συστήματος μπορεί να προκαλέσει πολύ μικρές επιπτώσεις στην λειτουργία της Εταιρίας.

Πίνακας 4.4: Επίπεδο Κρισιμότητας ως προς την Εμπιστευτικότητα

i. Ακεραιότητα

Επίπεδο Κρισιμότητας	Περιγραφή Επιπέδου ως προς την Ακεραιότητα
5 Πολύ Υψηλό	Η τροποποίηση των πληροφοριών που επεξεργάζεται το σύστημα θα έχει εξαιρετικά σημαντικές επιπτώσεις στη λειτουργία της Εταιρίας
4 Υψηλό	Η τροποποίηση των πληροφοριών που επεξεργάζεται το σύστημα θα έχει πολύ σημαντικές επιπτώσεις στη λειτουργία της Εταιρίας
3 Μέτριο	Η τροποποίηση των πληροφοριών που επεξεργάζεται το σύστημα θα έχει σημαντικές επιπτώσεις στη λειτουργία της Εταιρίας
2 Χαμηλό	Η τροποποίηση των πληροφοριών που επεξεργάζεται το σύστημα θα έχει μικρές επιπτώσεις στη λειτουργία της Εταιρίας
1 Πολύ Χαμηλό	Η τροποποίηση των πληροφοριών που επεξεργάζεται το σύστημα θα έχει πολύ μικρές επιπτώσεις στη λειτουργία της Εταιρίας

Πίνακας 4.5: Επίπεδο Κρισιμότητας ως προς την Ακεραιότητα

ii. Διαθεσιμότητα

Επίπεδο Κρισιμότητας	Περιγραφή Επιπέδου ως προς τη Διαθεσιμότητα
5 Πολύ Υψηλό	Η μη διαθεσιμότητα του συστήματος θα έχει εξαιρετικά σημαντικές επιπτώσεις στη λειτουργία της Εταιρίας. Το ανεκτό διάστημα μη διαθεσιμότητας του συστήματος είναι λίγα λεπτά.
4 Υψηλό	Η μη διαθεσιμότητα του συστήματος θα έχει πολύ σημαντικές επιπτώσεις στη λειτουργία της Εταιρίας. Το ανεκτό διάστημα μη διαθεσιμότητας του συστήματος είναι 1-2 ώρες.
3 Μέτριο	Η μη διαθεσιμότητα του συστήματος θα έχει σημαντικές επιπτώσεις στη λειτουργία της Εταιρίας. Το ανεκτό διάστημα μη διαθεσιμότητας του συστήματος είναι 1-2 ημέρες.
2 Χαμηλό	Η μη διαθεσιμότητα του συστήματος θα έχει μικρές επιπτώσεις στη λειτουργία της Εταιρίας. Το ανεκτό διάστημα μη διαθεσιμότητας του συστήματος είναι 1 εβδομάδα.
1 Πολύ Χαμηλό	Η μη διαθεσιμότητα του συστήματος θα έχει πολύ μικρές επιπτώσεις στη λειτουργία της Εταιρίας. Το ανεκτό διάστημα μη διαθεσιμότητας του συστήματος είναι ένας μήνας.

Πίνακας 4.6: Επίπεδο Κρισιμότητας ως προς την Διαθεσιμότητα

Για την καλύτερη παρουσίαση των αποτελεσμάτων, οι κίνδυνοι που εντοπίζονται για το σύστημα κατηγοριοποιούνται, βάσει του αθροίσματος του επιπέδου κινδύνου για τις τρεις παραμέτρους ασφάλειας, όπως φαίνεται στον πίνακα 4.9:

Επίπεδο Κινδύνου [Α] + Επίπεδο Κινδύνου [Ε] + Επίπεδο Κινδύνου [Δ]	Χαρακτηρισμός
12-15	Υψηλής Επικινδυνότητας
8-11	Μέτριας Επικινδυνότητας
3-7	Χαμηλής Επικινδυνότητας.

Πίνακας 4.9: Υπολογισμός Προτεραιότητας - Κρισιμότητας

4.3 Συνολική Έκθεση Κινδύνου

Συνολική Έκθεση Κινδύνου	
High	< 325
Moderate	< 250
Low	< 125

Πίνακας 4.10

4.4 Φύλλα Κινδύνου

Α. **Κίνδυνοι Ασφάλειας Πληροφοριών**

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α1</th></tr>
<tr><th colspan="6">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος Ελέγχων Ασφάλειας Πληροφοριών και Δικτύων.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Ο κίνδυνος διασφάλισης της εμπιστευτικότητας (confidentiality), της ακεραιότητας (integrity) και της διαθεσιμότητας (availability) των πληροφοριών και Συστημάτων της εταιρείας, σύμφωνα με την κρισιμότητά τους, είναι ζωτικής σημασίας για την επίτευξη των επιχειρησιακών στόχων αυτής, καθώς και της συμμόρφωσής της με το ισχύον νομοθετικό και ρυθμιστικό πλαίσιο.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση ασφάλειας πληροφοριών</td></tr>
<tr><th colspan="6">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td colspan="2">Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>3 (0.25%)</td><td>5</td><td>15</td><td colspan="2" rowspan="2">15</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>225</td></tr>
<tr><th colspan="6">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Ο κίνδυνος αυτός επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως αλλαγή επιχειρηματικής στρατηγικής ή τακτικής, εκδήλωση σοβαρών περιστατικών ασφάλειας, γνωστοποίηση νέων απειλών και αδυναμιών, κλπ.). Έλεγχοι πραγματοποιούνται είτε σε περιοδική βάση ή εκτάκτως, εφόσον κριθεί αναγκαίο από τη Διεύθυνση Ασφάλειας Πληροφοριών.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Επιπτώσεις στην εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) των πληροφοριών και Συστημάτων της εταιρείας</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Πολιτική Ελέγχου Ασφάλειας Πληροφοριών και Δικτύων</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
</table>

Προληπτικά μέτρα:	Η ασφάλειας πληροφοριών αξιολογεί το πλάνο ελέγχου και αποφασίζει αν ο έλεγχος θα διενεργηθεί εσωτερικά ή θα ανατεθεί σε εξωτερικό συνεργάτη. Στην περίπτωση που ο έλεγχος ασφάλειας διενεργηθεί από εξωτερικό συνεργάτη τα βήματα που ακολουθούν εκτελούνται από αυτόν, με το συντονισμό της ασφάλειας πληροφοριών
Διορθωτικά μέτρα:	Οποιαδήποτε παραβίαση της παρούσας πολιτικής από εργαζόμενο, προμηθευτή, ανάδοχο, ή συνεργάτη επισύρει τις κυρώσεις που προβλέπονται από εσωτερικό κανονισμό της εταιρίας, ή τις σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.
Εναλλακτικό σχέδιο:	
Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Με την ολοκλήρωση των εργασιών του ελέγχου, τα στελέχη της ασφάλειας πληροφοριών συντάσσουν την αναφορά του ελέγχου. Ενδεικτικά, η αναφορά ελέγχου περιλαμβάνει το εύρος και τα είδη των δοκιμών που πραγματοποιήθηκαν καθώς επίσης και τα ευρήματα του ελέγχου, τα συμπεράσματα και τις απαραίτητες συστάσεις, ώστε να μετριαστούν οι κίνδυνοι που απορρέουν.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α2</th></tr>
<tr><td colspan="6">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος καταγραφής και ταξινόμησης πληροφοριακών στοιχείων και συστημάτων</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Κίνδυνος διασφάλισης ότι τα πληροφοριακά στοιχεία και τα συστήματα της εταιρίας καταγράφονται και ταξινομούνται σύμφωνα με τις πολιτικές ασφάλειας</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση ασφάλειας πληροφοριών</td></tr>
<tr><td colspan="6">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>3 (0.30%)</td><td>4</td><td>12</td><td rowspan="2">10</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>120</td></tr>
<tr><td colspan="6">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Η διαδικασία ενεργοποιείται στις ακόλουθες περιπτώσεις:
-Στα πλαίσια διεξαγωγής της αποτίμησης κινδύνων ασφάλειας,
-Περιοδικά, εφόσον προκύψει ανάγκη για επισκόπηση της καταγραφής και ταξινόμησης των πληροφοριακών στοιχείων και συστημάτων.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5"></td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Σύνταξη διαδικασίας καταγραφής και ταξινόμησης πληροφοριακών στοιχείων και συστημάτων</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5"></td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Εάν προκύψει ανάγκη για καταγραφή και ταξινόμηση σε υπάρχον σύστημα, ο Υπεύθυνος Λειτουργίας του Συστήματος,
με τη συμβολή του Συντονιστή Ασφάλειας, επιβεβαιώνει τα Τεχνικά Χαρακτηριστικά του συστήματος. Εφόσον έχουν
προκύψει αλλαγές στα τεχνικά χαρακτηριστικά του συστήματος, αυτά καταγράφονται σύμφωνα με τις προδιαγραφές
που ορίζονται από την διεύθυνση Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5"></td></tr>
</table>

Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Μετά την ολοκλήρωση της καταγραφής και ταξινόμησης των στοιχείων η διεύθυνση Ασφάλειας Πληροφοριών ελέγχει την πληρότητά τους και ενημερώνει το Αρχείο Πληροφοριακών Στοιχείων και Συστημάτων (Asset Inventory) που διατηρεί.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α3</th></tr>
<tr><th colspan="6">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος αποτίμησης κινδύνων ασφαλείας συστημάτων</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5"></td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Ασφάλειας Πληροφοριών</td></tr>
<tr><th colspan="6">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td colspan="2">Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>1 (0.01%)</td><td>4</td><td>4</td><td colspan="2" rowspan="2">12</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>48</td></tr>
<tr><th colspan="6">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Αποτίμηση κινδύνων πραγματοποιείται τουλάχιστον:
- Στη διάρκεια της αρχικής υλοποίησης του Συστήματος,
- στη περίπτωση εμφάνισης νέων απειλών.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Εμφάνιση νέων απειλών</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Σύνταξη διαδικασίας αποτίμησης κινδύνων ασφαλείας συστημάτων</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Η αντίστοιχη ομάδα αποτίμησης κινδύνων ασφάλειας εντοπίζει τις απειλές / ευπάθειες του συστήματος
και αξιολογεί την πιθανότητα εκδήλωσης ενός περιστατικού,
λαμβάνοντας υπόψη την ευκολία εκμετάλλευσης των
ευπαθειών και το επίπεδο υλοποίησης αντίστοιχων μηχανισμών
προστασίας.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Η ομάδα αποτίμησης κινδύνων ασφάλειας εξετάζει τις εναλλακτικές λύσεις (αντίμετρα) για τον περιορισμό
των κινδύνων, οι οποίες μπορεί να περιλαμβάνουν τεχνολογικά μέτρα προστασίας ή / και διοικητικούς μηχανισμούς
ασφάλειας, (όπως π.χ. την ανάπτυξη συγκεκριμένων διαδικασιών) και διαμορφώνει πρόταση για την υλοποίηση
συγκεκριμένων μηχανισμών προστασίας.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5"></td></tr>
</table>

Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Η αποτίμηση κινδύνων ασφάλειας για κάποιο σύστημα επαναλαμβάνεται σε διάστημα δώδεκα (12) μηνών μετά την ολοκλήρωση της πιο πρόσφατης διεξαγωγής της με ευθύνη της διεύθυνσης Ασφάλειας Πληροφοριών.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α4</th></tr>
<tr><td colspan="6">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος απορρήτου και προστασίας δεδομένων επικοινωνίας και προσωπικών δεδομένων χρηστών – πελατών.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Κίνδυνος διασφάλισης του απορρήτου των δεδομένων επικοινωνίας, του περιεχομένου της επικοινωνίας και των προσωπικών δεδομένων των χρηστών-πελατών (στο εξής «χρηστών») που χρησιμοποιούνται για την παροχή, υποστήριξη και βελτίωση των υπηρεσιών της εταιρίας.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Ασφάλειας Πληροφοριών</td></tr>
<tr><td colspan="6">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>1 (0.04%)</td><td>4</td><td>4</td><td rowspan="2">12</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>48</td></tr>
<tr><td colspan="6">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Η Εταιρία εφαρμόζει και συμμορφώνεται με την εκάστοτε ισχύουσα νομοθεσία περί απορρήτου των επικοινωνιών που πραγματοποιούνται μέσω του δικτύου της καθώς και περί απορρήτου των πληροφοριών που απέκτησε από το χρήστη. Απαγορεύεται η ακρόαση, παγίδευση, αποθήκευση, επεξεργασία, ανακοίνωση, δημοσιοποίηση ή άλλου τύπου υποκλοπή ή παρακολούθηση της τηλεπικοινωνίας και των δεδομένων επικοινωνίας από άλλα πρόσωπα χωρίς τη συγκατάθεση των χρηστών που αφορούν, εξαιρουμένων των περιπτώσεων που προβλέπονται στο Σύνταγμα και τους σχετικούς νόμους.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Δημοσιοποίηση ή χρήση στοιχείων χρηστών – πελατών.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Πολιτική Διαφύλαξης του Απορρήτου και της Προστασίας Δεδομένων Επικοινωνίας και Προσωπικών Δεδομένων</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Προληπτικά μέτρα προστασίας που λαμβάνονται είναι:
− Εφαρμογή Πολιτικών Ασφάλειας και Διαδικασιών, σύμφωνα με διεθνή πρότυπα και σε συμμόρφωση με το νομοθετικό πλαίσιο.
− Μέτρα φυσικής ασφάλειας των χώρων εργασίας καθώς και των ευαίσθητων χώρων στέγασης τηλεπικοινωνιακών και πληροφοριακών συστημάτων
− Ελεγχόμενη πρόσβαση σε συστήματα και εφαρμογές, με βάση την</td></tr>
</table>

	αρχή της ‘ανάγκης γνώσης’. − Λήψη και τήρηση αντιγράφων ασφάλειας σε προστατευόμενους χώρους − Μηχανισμοί προστασίας του δικτύου κινητών επικοινωνιών − Υλοποίηση υποδομών ασφάλειας για την προστασία του εταιρικού δικτύου − Χρήση κρυπτογραφίας.
Διορθωτικά μέτρα:	Η Εταιρία πρέπει να διαθέτει καταγεγραμμένη διαδικασία για τη διερεύνηση περιστατικών παραβίασης του απορρήτου, η οποία ενεργοποιείται με εντολή της Διεύθυνσης Συστημάτων Διοίκησης & Ασφάλειας Πληροφοριών. Οι ενέργειες που πραγματοποιούνται στα πλαίσια διερεύνησης περιστατικών πρέπει να καταγράφονται.
Εναλλακτικό σχέδιο:	
Σχέδιο μετάπτωσης:	Η Εταιρία διαφυλάσσει το απόρρητο δεδομένων επικοινωνίας και προσωπικών δεδομένων χρηστών, ακολουθώντας αυστηρές διαδικασίες για την επεξεργασία των δεδομένων και επιτρέποντας την πρόσβαση μόνο σε εξουσιοδοτημένους και κατάλληλα εκπαιδευμένους υπαλλήλους. Το προσωπικό της Εταιρίας δεσμεύεται, μέσω της υπογραφής σχετικών εγκυκλίων, για την διαφύλαξη του απορρήτου των δεδομένων επικοινωνιών και των προσωπικών δεδομένων του χρήστη και υπόκεινται σε πειθαρχικές κυρώσεις, σε περίπτωση παραβίασης της παρούσας πολιτικής. Επίσης, εξωτερικοί συνεργάτες δεσμεύονται, μέσω συμφωνίας εμπιστευτικότητας (Non-Disclosure Agreement), που περιλαμβάνεται στις συμβάσεις, για τη διαφύλαξη του απορρήτου και υπόκεινται σε κυρώσεις, σε περίπτωση παραβίασής της.
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Η πολιτική αυτή επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα ή/ και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως αλλαγή στο νομικό πλαίσιο, κλπ.).
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α5</th></tr>
<tr><td colspan="6">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος Λογικής Πρόσβασης.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Κίνδυνος διασφάλισης ότι μόνο εξουσιοδοτημένοι χρήστες έχουν δυνατότητα πρόσβασης στις πληροφορίες της εταιρίας και στα σχετιζόμενα με αυτές Συστήματα (συμπεριλαμβάνονται όλες οι υποδομές, όπως εφαρμογές, λειτουργικά συστήματα, στοιχεία δικτύου—network elements— και πλατφόρμες)</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση ασφάλειας πληροφοριών</td></tr>
<tr><td colspan="6">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>2 (0.3%)</td><td>4</td><td>8</td><td rowspan="2">15</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>120</td></tr>
<tr><td colspan="6">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Για την παρακολούθηση προσπέλασης και χρήσης των Συστημάτων θα πρέπει τηρούνται αρχεία καταγραφής γεγονότων (audit logs/trails). Η πρόσβαση σε αυτά τα αρχεία πρέπει να γίνεται βάσει αυστηρών διαδικασιών και από κατάλληλα εξουσιοδοτημένο προσωπικό.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5"></td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Πολιτική Διαχείρισης Λογικής Πρόσβασης</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Τα δικαιώματα πρόσβασης που δύναται να αποκτήσει ο κάθε Χρήστης σε Συστήματα της Εταιρίας πρέπει να είναι επακριβώς ορισμένα, και αυστηρά συνδεδεμένα με τις απαιτήσεις της εργασίας του, βάσει του ρόλου του στην μονάδα την οποία ανήκει. Η χορήγηση προνομιακών Δικαιωμάτων Πρόσβασης απαγορεύεται εκ προοιμίου. Εκχωρούνται μόνο σε Υπεύθυνους Συστημάτων με ελεγχόμενο τρόπο και, όπου κριθεί αναγκαίο, για περιορισμένο χρονικό διάστημα. Η παροχή λογικής πρόσβασης των χρηστών στα Συστήματα της Εταιρίας διενεργείται σύμφωνα με τη Διαδικασία «Διαχείριση Πρόσβασης Χρηστών σε Συστήματα». Οι χρησιμοποιούμενοι μηχανισμοί ταυτοποίησης και πιστοποίησης των Χρηστών πρέπει να αξιολογούνται βάσει του επιπέδου ασφάλειας που</td></tr>
</table>

	παρέχουν και σε συνάρτηση με τις απαιτήσεις ασφάλειας και την κρισιμότητα των Συστημάτων.
Διορθωτικά μέτρα:	Οποιαδήποτε παραβίαση της παρούσας πολιτικής από εργαζόμενο, προμηθευτή, ανάδοχο, ή συνεργάτη θα επισύρει τις κυρώσεις που προβλέπονται από τον Εσωτερικό Κανονισμό της Εταιρίας, ή τις σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.
Εναλλακτικό σχέδιο:	
Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Ο κίνδυνος αυτός επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως αλλαγή επιχειρηματικής στρατηγικής ή τακτικής, εκδήλωση σοβαρών περιστατικών ασφάλειας, γνωστοποίηση νέων απειλών και αδυναμιών, κλπ.).
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α6</th></tr>
<tr><th colspan="6">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος απομακρυσμένης πρόσβασης και εργασίας.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Προστασία της ασφάλειας των πληροφοριών και υποδομών της Εταιρίας όταν υπάρχει ανάγκη εργασίας εκτός των χώρων της</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Ασφάλειας Πληροφοριών</td></tr>
<tr><th colspan="6">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td colspan="2">Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>2 (0.15%)</td><td>4</td><td>8</td><td colspan="2" rowspan="2">12</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>96</td></tr>
<tr><th colspan="6">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Οι ενέργειες που γίνονται μέσω απομακρυσμένης πρόσβασης καταγράφονται και επιθεωρούνται ώστε να ελέγχεται το κατά πόσο ταυτίζονται με τους λόγους για τους οποίους δόθηκε η δυνατότητα απομακρυσμένης πρόσβασης.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5"></td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Πολιτική απομακρυσμένης πρόσβασης και εργασίας</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Όλοι οι χρήστες στους οποίους εγκρίνεται η δυνατότητα απομακρυσμένης εργασίας πρέπει να ενημερώνονται σχετικά με τους δυνητικούς κινδύνους για την Εταιρία, καθώς και για τις απαραίτητες προφυλάξεις που πρέπει να παίρνουν.
Τα συστήματα τα οποία παρέχουν δυνατότητα απομακρυσμένης πρόσβασης πρέπει να είναι καταγεγραμμένα και όσο το δυνατόν λιγότερα ώστε ο έλεγχός τους να είναι πιο αποτελεσματικός.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Οποιοδήποτε περιστατικό ασφάλειας πρέπει να αναφέρεται αμέσως στο υπεύθυνο προσωπικό της εταιρίας, όπως ορίζουν οι αντίστοιχες διαδικασίες.
Οποιαδήποτε παραβίαση της παρούσας πολιτικής από εργαζόμενο προμηθευτή, ανάδοχο, ή συνεργάτη θα επισύρει τις κυρώσεις που προβλέπονται από τον εσωτερικό κανονισμό της εταιρίας, ή τις σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.</td></tr>
<tr><td>Εναλλακτικό</td><td colspan="5"></td></tr>
</table>

σχέδιο:	
Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Ο κίνδυνος αυτός επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως αλλαγή επιχειρηματικής στρατηγικής ή τακτικής, εκδήλωση σοβαρών περιστατικών ασφάλειας, γνωστοποίηση νέων απειλών και αδυναμιών, κλπ.)
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α7				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος αποθηκευτικών μέσων και εγγράφων.			
Σύντομη Περιγραφή:	Κίνδυνος που προέρχεται από την χρήση των αποθηκευτικών μέσων και εγγράφων.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Ασφάλειας Πληροφοριών**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση ασφάλειας πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (4%)	4	12	9	
Συνολική Έκθεση:		108		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Βασική αρχή της εταιρίας είναι ότι όλες οι πληροφορίες που περιέχονται σε αποθηκευτικά μέσα (ηλεκτρονικά και έντυπα) πρέπει να προστατεύονται από αλλοίωση, απώλεια, ή γνωστοποίηση σε μη εξουσιοδοτημένα άτομα.			
Προπομπός Κινδύνου:	Δημοσιοποίηση , κοινοποίηση εγγράφων.			
Στρατηγική Αντιμετώπισης:	Πολιτική Διαχείρισης αποθηκευτικών μέσων και εγγράφων.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Όλα τα μέσα αποθήκευσης πληροφορίας, είτε ηλεκτρονικής (ταινίες, σκληροί δίσκοι, CD κλπ) είτε έντυπης μορφής (έγγραφα, βιβλία κλπ), θα υπόκεινται σε διαδικασίες ταξινόμησης βάσει της πολιτικής και των διαδικασιών ταξινόμησης πληροφοριακών στοιχείων. Κατά την αποθήκευση αποθηκευτικών μέσων πρέπει να τηρούνται οι προδιαγραφές του κατασκευαστή σχετικά με τις συνθήκες φύλαξης. Όλα τα συστήματα τα οποία περιέχουν στο εσωτερικό τους ηλεκτρονικά αποθηκευτικά μέσα (σκληροί δίσκοι, μνήμες κλπ) πρέπει να διαθέτουν ειδική σήμανση που θα εξασφαλίζει ότι δεν έχει γίνει μη εξουσιοδοτημένη επέμβαση στο εσωτερικό τους.			
Διορθωτικά μέτρα:	Οποιαδήποτε παραβίαση της παρούσας πολιτικής από εργαζόμενο προμηθευτή, ανάδοχο, ή συνεργάτη θα επισύρει τις κυρώσεις που προβλέπονται από τον Εσωτερικό Κανονισμό της Εταιρίας, ή τις σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.			
Εναλλακτικό				

σχέδιο:	
Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Ο κίνδυνος αυτός επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως αλλαγή επιχειρηματικής στρατηγικής ή τακτικής, εκδήλωση σοβαρών περιστατικών ασφάλειας, γνωστοποίηση νέων απειλών και αδυναμιών, κλπ.)
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="5">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α8</th></tr>
<tr><th colspan="5">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="4">Κίνδυνος μη αποδεκτής χρήσης</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="4">Κίνδυνος εκμετάλλευσης από τους χρήστες της εταιρείας της πρόσβασης που τους παρέχεται(emails, internet), σύμφωνα με τις πολιτικές ασφαλείας, στις πληροφορίες και τα συστήματα της Εταιρείας, προκειμένου να προβούν σε ενέργειες οι οποίες παραβιάζουν τόσο τις εταιρικές πολιτικές ασφαλείας , όσο και το ισχύον νομοθετικό πλαίσιο.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="4">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="4"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="4">Διεύθυνση Ασφάλειας Πληροφοριών</td></tr>
<tr><th colspan="5">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>3 (3%)</td><td>4</td><td>12</td><td rowspan="2">9</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>108</td></tr>
<tr><th colspan="5">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="4"></td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="4">Διαρροή δεδομένων που αφορούν την εταιρεία, τους πελάτες, τις εφαρμογές.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="4">Πολιτική Αποδεκτής χρήσης</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="4"></td></tr>
<tr><td colspan="5">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="4">Ανάλυση και επεξήγηση των ευθυνών κατά την πρόσληψη. Εκπαίδευση και ενημέρωση σχετικά με την ασφάλεια πληροφοριών.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="4">Οποιαδήποτε παραβίαση της παρούσας πολιτικής από εργαζόμενο προμηθευτή, ανάδοχο, ή συνεργάτη θα επισύρει τις κυρώσεις που προβλέπονται από τον Εσωτερικό Κανονισμό της Εταιρίας, ή τις σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="4"></td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="4"></td></tr>
<tr><th colspan="5">Παρακολούθηση Κινδύνου</th></tr>
</table>

Παρακολούθηση:	Ο κίνδυνος αυτός επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως αλλαγή επιχειρηματικής στρατηγικής ή τακτικής, εκδήλωση σοβαρών περιστατικών ασφάλειας, γνωστοποίηση νέων απειλών και αδυναμιών, κλπ.)
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α9</th></tr>
<tr><td colspan="6">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος διαχείρισης περιστατικών ασφαλείας.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Κίνδυνος διαχείρισης περιστατικών ασφαλείας κατά των συστημάτων της εταιρείας (εφαρμογές, λειτουργικά συστήματα, στοιχεία δικτύου και πλατφόρμες.)</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Ασφάλειας Πληροφοριών</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Ασφάλειας Πληροφοριών</td></tr>
<tr><td colspan="6">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td colspan="2">Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>3 (1.5%)</td><td>4</td><td>12</td><td colspan="2" rowspan="2">14</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>168</td></tr>
<tr><td colspan="6">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Η οργανωμένη και αποτελεσματική διαχείριση περιστατικών ασφαλείας απαιτεί την ύπαρξη συγκεκριμένων διαδικασιών και πρακτικών ανίχνευσης, αναφοράς και αντιμετώπισής τους. Η ετοιμότητα όλων των παραπάνω μηχανισμών, καθώς και των εμπλεκόμενων προσώπων θα πρέπει να ελέγχεται σε τακτικά χρονικά διαστήματα, ώστε να διασφαλίζεται η απόδοσή τους.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Πιθανές κακόβουλες ενέργειες.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Πολιτική διαχείρισης περιστατικών ασφαλείας</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Για την πρόληψη εκδήλωσης περιστατικών ασφαλείας πρέπει να αξιοποιούνται συστηματικά και να υλοποιούνται όλοι οι απαιτούμενοι μηχανισμοί ασφαλείας σύμφωνα με τις υφιστάμενες πολιτικές και διαδικασίες, με τελικό στόχο την επίτευξη του επιθυμητού επιπέδου ασφαλείας των συστημάτων.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Αναλόγως με την διαβάθμιση του περιστατικού πρέπει να συμμετέχουν όλες οι αρμόδιες μονάδες καθώς και οι αρμόδιοι εξωτερικοί συνεργάτες, προκειμένου να προβούν σε από κοινού ενέργειες για την αντιμετώπισή του.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5"></td></tr>
</table>

Σχέδιο μετάπτωσης:	Σε περίπτωση που το περιστατικό αφορά μη εξουσιοδοτημένη γνωστοποίηση στοιχείων πελατών, ιδιαίτερα στη περίπτωση που δεν είναι δυνατό να αντιμετωπιστεί με τα υπάρχοντα μέσα, πρέπει επίσης να ενημερώνονται οι εμπλεκόμενοι χρήστες – πελάτες σχετικά με τους υφιστάμενους κινδύνους και τις συνέπειες αυτών και να παρέχονται στοιχεία για την αποτροπή ή αντιμετώπιση τους. Σε αυτές τις περιπτώσεις πρέπει να ενημερώνεται και η ΑΔΑΕ.
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Για κάθε περιστατικό ασφαλείας συντάσσεται πόρισμα και τηρείται αρχείο.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Α10				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Αντιγράφων Ασφαλείας			
Σύντομη Περιγραφή:	Ο κίνδυνος της διασφάλισης ότι σε οποιαδήποτε περίπτωση απώλειας δεδομένων λόγω φυσικής καταστροφής, τεχνικής βλάβης, κακόβουλης ή λανθασμένης ενέργειας, τα δεδομένα μπορούν να ανακτηθούν εντός μιας λογικής χρονικής περιόδου.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Ασφάλειας Πληροφοριών**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση λειτουργίας και συντήρησης. Διεύθυνση ασφάλειας πληροφοριών.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
1 (0.08%)	5	5	15	
Συνολική Έκθεση:		75		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ο κίνδυνος αυτός επανεξετάζεται και αν κριθεί αναγκαίο αναθεωρείται σε τακτά χρονικά διαστήματα και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (αλλαγή επιχειρησιακής στρατηγικής, τακτικής, εκδήλωση σοβαρών περιστατικών ασφαλείας)			
Προπομπός Κινδύνου:	Σοβαρές επιπτώσεις στην διαθεσιμότητα δεδομένων.			
Στρατηγική Αντιμετώπισης:	Πολιτική Αντιγράφων Ασφαλείας			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τα αποθηκευτικά μέσα πρέπει να ελέγχονται περιοδικά και να αποσύρονται βάσει των οδηγιών που δίνει ο κατασκευαστής τους. Η διαδικασία ανάκτησης των δεδομένων πρέπει να εξετάζεται περιοδικά.			
Διορθωτικά μέτρα:	Η ανάκτηση δεδομένων και πρέπει να γίνεται βάσει καταγεγραμμένων διαδικασιών.			
Εναλλακτικό σχέδιο:	Για υψηλής κρισιμότητας πληροφοριακά στοιχεία τα αντίγραφα ασφαλείας πρέπει να αποθηκεύονται σε 2 αντίγραφα, τα οποία θα διατηρούνται σε διαφορετικά κτίρια.			
Σχέδιο μετάπτωσης:	Κυρώσεις από τον εσωτερικό κανονισμό της εταιρείας, σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.			
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Δεδομένα διάρθρωσης δικτυακών διατάξεων αντιγράφονται καθημερινά και διατηρούνται 7 ημέρες. Τα εβδομαδιαία για ένα μήνα και τα μηνιαία για τουλάχιστον 3 μήνες
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Β. **Κίνδυνοι Νομικής και ρυθμιστικής συμμόρφωσης**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Β1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος διαχείρισης απαιτήσεων Sarbanes Oxley			
Σύντομη Περιγραφή:	Κίνδυνος του τρόπου με τον οποίο συντονίζεται το έργο της αναγνώρισης, καταγραφής και πιστοποίησης κατά SOX όλων των κύκλων / διαδικασιών.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Νομικής και ρυθμιστικής συμμόρφωσης**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση εσωτερικού ελέγχου.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
1 (0.015%)	3	3	5	
Συνολική Έκθεση:		15		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Η διεργασία διαχείρισης απαιτήσεων Sarbanes – Oxley, ξεκινά στην κάθε έτος με σκοπό την αξιολόγηση των επιλεγμένων διεργασιών με σημαντική επιρροή στις οικονομικές αναφορές της εταιρείας, για να εξεταστεί η ανάγκη προσθήκης νέων κύκλων ή αλλαγών στις υφιστάμενες καταγραφές.			
Προπομπός Κινδύνου:	Ευρήματα από την ανάλυση και καταγραφή διαδικασιών			
Στρατηγική Αντιμετώπισης:	Πολιτική διαχείρισης απαιτήσεων Sarbanes Oxley			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ο εσωτερικού έλεγχος καθορίζει την στρατηγική ελέγχου, τη δειγματοληψία για κάθε σημείο ελέγχου καθώς και το πλάνο ελέγχου για το σύνολο των καταγεγραμμένων σημείων ελέγχου.			
Διορθωτικά μέτρα:	Ό εκάστοτε υπεύθυνος υλοποιεί τις συμφωνημένες ενέργειες του διορθωτικού πλάνου στα σημεία ελέγχου και ενημερώνει κατάλληλα τον εσωτερικό έλεγχο για την ολοκλήρωση τους.			
Εναλλακτικό σχέδιο:				

Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Στο τέλος του χρόνου, οι υπεύθυνοι επιβεβαιώνουν εγγράφως, μέσω επιστολής προς το εσωτερικό έλεγχο, την ορθή καταγραφή των αρχείων, την τήρηση καθ όλη την διάρκεια του έτους των καταγεγραμμένων στα σημεία ελέγχου και τέλος τη συμφωνία τους για όλες τις ενδεχόμενες διορθωτικές ενέργειες.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Β2</th></tr>
<tr><td colspan="6">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος απορρήτου και προστασίας δεδομένων επικοινωνίας και προσωπικών δεδομένων χρηστών – πελατών.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Κίνδυνος διασφάλισης του απορρήτου των δεδομένων επικοινωνίας, του περιεχομένου της επικοινωνίας και των προσωπικών δεδομένων των χρηστών-πελατών που χρησιμοποιούνται για την παροχή, υποστήριξη και βελτίωση των υπηρεσιών της εταιρίας.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Νομικής και ρυθμιστικής συμμόρφωσης</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Ασφάλειας Πληροφοριών</td></tr>
<tr><td colspan="6">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>2 (0.08%)</td><td>5</td><td>10</td><td rowspan="2">11</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>110</td></tr>
<tr><td colspan="6">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Ο κίνδυνος αυτός επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα ή/ και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως αλλαγή στο νομικό πλαίσιο, κλπ.).</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Η μη τήρηση των αρχών της πολιτικής απορρήτου και προστασίας δεδομένων επικοινωνίας και προσωπικών δεδομένων χρηστών – πελατών.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Πολιτικής απορρήτου και προστασίας δεδομένων επικοινωνίας και προσωπικών δεδομένων χρηστών – πελατών.</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Η Εταιρία λαμβάνει όλα τα δυνατά οργανωτικά και τεχνολογικά μέτρα προστασίας για τη διαφύλαξη του απορρήτου των επικοινωνιών χρηστών.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Η Εταιρία πρέπει να διαθέτει καταγεγραμμένη διαδικασία για τη διερεύνηση περιστατικών παραβίασης του απορρήτου, η οποία ενεργοποιείται με εντολή της Διεύθυνσης Συστημάτων Διοίκησης & Ασφάλειας Πληροφοριών. Οι ενέργειες που πραγματοποιούνται στα πλαίσια διερεύνησης περιστατικών πρέπει να καταγράφονται.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5"></td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="5"></td></tr>
</table>

Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Το χρονικό διάστημα διατήρησης δεδομένων επικοινωνίας και προσωπικών δεδομένων καθορίζεται με βάση τις απαιτήσεις και υποχρεώσεις που επιβάλλει η ελληνική νομοθεσία.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Β3</th></tr>
<tr><th colspan="6">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνοι συμμόρφωσης στο δίκαιο του ελεύθερου ανταγωνισμού.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Κίνδυνος από τους απαγορευτικούς κανόνες του δικαίου του ελεύθερου ανταγωνισμού.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Νομικής και ρυθμιστικής συμμόρφωσης</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Εσωτερικού Ελέγχου.</td></tr>
<tr><th colspan="6">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>1 (0.06%)</td><td>4</td><td>4</td><td rowspan="2">10</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>40</td></tr>
<tr><th colspan="6">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Σύμφωνα με τη νομοθεσία η ελληνική επιτροπή ανταγωνισμού είναι αρμόδια για την τήρηση των διατάξεων κατά την προστασία του ελεύθερου ανταγωνισμού, ενώ η ΕΕΤΤ μεριμνά για την τήρηση της νομοθεσίας περί ηλεκτρονικών επικοινωνιών και εφαρμόζει τις διατάξεις για την προστασία του ελεύθερου ανταγωνισμού.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Συμπράξεις μεταξύ επιχειρήσεων και χειραγώγηση τιμών. Εκμετάλλευση δεσπόζουσας θέσης στην αγορά.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Πολιτική για την συμμόρφωση στο δίκαιο του ελεύθερου ανταγωνισμού.</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Έλεγχος βιβλίων, στοιχείων και λοιπών εγγράφων επιχειρήσεων και ενώσεων επιχειρήσεων. Έρευνες στα γραφεία και τους λοιπούς χώρους των επιχειρήσεων και ενώσεων επιχειρήσεων.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Κυρώσεις έως 10% του συνολικού κύκλου εργασιών κατά το προηγούμενο οικονομικό έτος για παραβάσεις των διατάξεων προστασίας ανταγωνισμού και πρόστιμα έως 1% του συνολικού κύκλου εργασιών κατά το προηγούμενο οικονομικό έτος για ανακριβή στοιχεία ή άρνηση παροχής πληροφοριών.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5"></td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="5"></td></tr>
<tr><th colspan="6">Παρακολούθηση Κινδύνου</th></tr>
</table>

Παρακολούθηση:	Απροειδοποίητοι έλεγχοι από την ελληνική επιτροπή ανταγωνισμού και η ΕΕΤΤ
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Γ. **Κίνδυνος Στρατηγικής**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Γ1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος ανεπαρκούς διαχωρισμού αρμοδιοτήτων			
Σύντομη Περιγραφή:	Κίνδυνος ανεπαρκούς διαχωρισμού αρμοδιοτήτων μεταξύ υπευθύνων σχεδιασμού / υλοποίησης και διαχειριστών συστήματος			
Κατηγορία Κινδύνου:	**Κίνδυνος Στρατηγικής**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση Ασφάλειας Πληροφοριών και Εσωτερικού Ελέγχου.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (1.1%)	4	12	15	
Συνολική Έκθεση:		180		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ο κίνδυνος αυτός επανεξετάζεται και αν κριθεί αναγκαίο, αναθεωρείται σε τακτά χρονικά διαστήματα και όταν το επιβάλουν επιχειρησιακοί ή εξωγενείς παράγοντες (αλλαγή επιχειρηματικής στρατηγικής, εκδήλωση σοβαρών περιστατικών ασφαλείας, γνωστοποίηση νέων απειλών)			
Προπομπός Κινδύνου:	Προβλήματα και επιπτώσεις στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων που απαιτούνται για την καλή και αδιάλειπτη λειτουργία.			
Στρατηγική Αντιμετώπισης:	Θεσμοθέτηση αντίστοιχης πολιτικής ασφαλείας στην σχεδίαση, υλοποίηση, λειτουργία και συντήρηση των συστημάτων.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Για όλα τα συστήματα της εταιρείας πρέπει να υπάρχει γραπτή τεκμηρίωση για κάθε φάση της διαδικασίας ανάπτυξης ή προμήθειας.			
Διορθωτικά μέτρα:	Η μη τήρηση της πολιτικής ασφαλείας και η παραβίαση αυτής από εργαζόμενο, προμηθευτή, ανάδοχο ή συνεργάτη επισύρει τις κυρώσεις που προβλέπονται από τον εσωτερικό κανονισμό της εταιρείας ή της σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.			
Εναλλακτικό σχέδιο:				

Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Η επανεξέταση αυτών των απαιτήσεων ασφαλείας καθώς και των μηχανισμών ελέγχου πραγματοποιείται στο πλαίσιο της Διαρκούς αποτίμησης Κινδύνων της εταιρείας.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Γ2				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλειπής καθορισμός ρόλων			
Σύντομη Περιγραφή:	Ελλειπής καθορισμός ρόλων και αρμοδιοτήτων μεταξύ των εργαζομένων.			
Κατηγορία Κινδύνου:	**Κίνδυνος Στρατηγικής**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Ασφάλεια πληροφοριών και εσωτερικός έλεγχος.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (1.7%)	4	12	14	
Συνολική Έκθεση:		168		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ο κίνδυνος αυτός επανεξετάζεται και αν κριθεί αναγκαίο, αναθεωρείται σε τακτά χρονικά διαστήματα και όταν το επιβάλουν επιχειρησιακοί ή εξωγενείς παράγοντες (αλλαγή επιχειρηματικής στρατηγικής, εκδήλωση σοβαρών περιστατικών ασφαλείας, γνωστοποίηση νέων απειλών)			
Προπομπός Κινδύνου:	Προβλήματα και επιπτώσεις στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων που απαιτούνται για την καλή και αδιάλειπτη λειτουργία.			
Στρατηγική Αντιμετώπισης:	Θεσμοθέτηση αντίστοιχης πολιτικής ασφαλείας στην σχεδίαση, υλοποίηση, λειτουργία και συντήρηση των συστημάτων.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Για όλα τα συστήματα της εταιρείας υπάρχει γραπτή τεκμηρίωση για κάθε φάση της διαδικασίας ανάπτυξης ή προμήθειας.			
Διορθωτικά μέτρα:	Η μη τήρηση της πολιτικής ασφαλείας και η παραβίαση αυτής από εργαζόμενο, προμηθευτή, ανάδοχο ή συνεργάτη επισύρει τις κυρώσεις που προβλέπονται από τον εσωτερικό κανονισμό της εταιρείας ή της σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Η επανεξέταση αυτών των απαιτήσεων ασφαλείας καθώς και των μηχανισμών ελέγχου πραγματοποιείται στο πλαίσιο της Διαρκούς αποτίμησης Κινδύνων της εταιρείας.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Γ3</th></tr>
<tr><th colspan="6">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Ελλειπής απαιτήσεις ασφαλείας τρίτων</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Ελλειπής απαιτήσεις ασφαλείας σε συμβάσεις με τρίτους που έχουν πρόσβαση στο σύστημα.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνος Στρατηγικής</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Ασφάλεια πληροφοριών.</td></tr>
<tr><th colspan="6">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>2 (0.07%)</td><td>4</td><td>8</td><td rowspan="2">12</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>96</td></tr>
<tr><th colspan="6">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Ο κίνδυνος αυτός επανεξετάζεται και αν κριθεί αναγκαίο, αναθεωρείται σε τακτά χρονικά διαστήματα και όταν το επιβάλουν επιχειρησιακοί ή εξωγενείς παράγοντες (αλλαγή επιχειρηματικής στρατηγικής, εκδήλωση σοβαρών περιστατικών ασφαλείας, γνωστοποίηση νέων απειλών)</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Σοβαρές επιπτώσεις στην ομαλή λειτουργία των μονάδων της εταιρείας.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Σχετικές συμβάσεις και συμφωνίες εμπιστευτικότητας.</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Κάθε διασύνδεση και πρόσβαση Τρίτων μερών σε πληροφορίες καθώς και στην πληροφοριακή και τηλεπικοινωνιακή υποδομή της εταιρείας απαγορεύεται εκ προοιμίου, εκτός αν υπαγορεύεται από τις επιχειρησιακές και λειτουργικές ανάγκες της. Οι διασυνδέσεις πρέπει να είναι καταγεγραμμένες και εγκεκριμένες. Μηχανισμοί εποπτείας μέσω αρχείων καταγραφής γεγονότων.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Κυρώσεις Εσωτερικού κανονισμού Εταιρείας και συμβάσεων.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5"></td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="5">Καταγγελία στην ΑΔΑΕ οποιαδήποτε παραβίασης των συμφωνημένων απαιτήσεων ασφαλείας από την πλευρά του Τρίτου Μέρους.</td></tr>
</table>

Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Επανεξέταση σε περιοδική βάση, ώστε να επιβεβαιώνεται ότι εξακολουθεί να ικανοποιεί τις ανάγκες της εταιρείας σχετικά με την ασφάλεια. Περιοδική επισκόπηση συνδέσεων και κατάργηση όσων χρειάζεται. Επανεξέταση των συμφωνιών εμπιστευτικότητας και των απαιτήσεων ασφαλείας.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Γ4				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Ελλειπής απαιτήσεις ασφαλείας outsourcing			
Σύντομη Περιγραφή:	Ελλειπής απαιτήσεις ασφαλείας σε συμβάσεις outsourcing			
Κατηγορία Κινδύνου:	**Κίνδυνος Στρατηγικής**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση Ασφάλειας Πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
1 (0.01%)	4	4	13	
Συνολική Έκθεση:		52		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Έλεγχος ανά τακτά χρονικά διαστήματα του κατά πόσο ο πάροχος εφαρμόζει όσα προβλέπονται.			
Προπομπός Κινδύνου:	Σοβαρές επιπτώσεις στην ομαλή λειτουργία των μονάδων της εταιρείας.			
Στρατηγική Αντιμετώπισης:	Θεσμοθέτηση αντίστοιχης πολιτικής ασφαλείας στην σχεδίαση, υλοποίηση, λειτουργία και συντήρηση των συστημάτων.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τήρηση πολιτικής πρόσβασης και κρυπτογράφησης και κανόνων passwords.			
Διορθωτικά μέτρα:	Ο πάροχος υπηρεσίας οφείλει να ενημερώνει άμεσα τον υπεύθυνο Ασφαλείας της εταιρείας σε σχέση με όλα τα περιστατικά ασφαλείας που αφορούν τα απόρρητα δεδομένα επικοινωνιών. Χρηματικές ποινές, κατάργηση υπηρεσιών.			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:	Καταγγελία στην ΑΔΑΕ οποιαδήποτε παραβίασης των συμφωνημένων απαιτήσεων ασφαλείας από την πλευρά του Παρόχου Υπηρεσιών			
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Ο κίνδυνος αυτός επανεξετάζεται και αν κριθεί αναγκαίο, αναθεωρείται σε τακτά χρονικά διαστήματα και όταν το επιβάλουν επιχειρησιακοί ή εξωγενείς παράγοντες (αλλαγή επιχειρηματικής στρατηγικής, εκδήλωση σοβαρών περιστατικών ασφαλείας,			

	γνωστοποίηση νέων απειλών)
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Δ. **Κίνδυνος Τεχνολογίας**

<table>
<tr><th colspan="5">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Δ1</th></tr>
<tr><td colspan="5">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="4">Κίνδυνος ασφάλειας δικτύων κινητών και ασύρματων επικοινωνιών</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="4">Κίνδυνοι κατά το σχεδιασμό, υλοποίηση και λειτουργίας των δικτύων κινητών και ασύρματων επικοινωνιών, προκειμένου να παρέχονται στους χρήστες ασφαλείς υπηρεσίες.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="4">Κίνδυνος Τεχνολογίας</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="4"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="4">Τεχνική Διεύθυνση</td></tr>
<tr><td colspan="5">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>2 (0.06%)</td><td>4</td><td>8</td><td rowspan="2">12</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>96</td></tr>
<tr><td colspan="5">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="4">Η εταιρεία στα πλαίσια της διαρκούς αποτίμησης κινδύνων πρέπει να επανεξετάζει τους δυνητικούς κινδύνους για την ασφάλεια των επικοινωνιών και να αναπροσαρμόζει κατάλληλα αν χρειάζεται την πολιτική ασφαλείας.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="4">Πρόβλημα σε υποδομές δικτύου επικοινωνιών.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="4">Πολιτική ασφάλειας δικτύων κινητών και ασύρματων επικοινωνιών</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="4"></td></tr>
<tr><td colspan="5">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="4">Ο σχεδιασμός, η υλοποίηση και η λειτουργία των δικτύων κινητών και ασύρματων επικοινωνιών πρέπει να καλύπτουν τις απαιτήσεις ασφαλείας της εταιρείας και ν εξυπηρετούν τις υποχρεώσεις της απέναντι στους χρήστες βάσει του νομικού και ρυθμιστικού πλαισίου.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="4">Για την αντιμετώπιση περιστατικών ασφαλείας υπάρχουν καταγεγραμμένες διαδικασίες, ώστε η αντιμετώπιση τους να είναι άμεση και αποτελεσματική.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="4"></td></tr>
</table>

Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Η πολιτική αυτή επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα ή/ και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως εκδήλωση σοβαρών περιστατικών ασφαλείας, κλπ.).
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Δ2				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος ασφαλείας εταιρικού δικτύου δεδομένων.			
Σύντομη Περιγραφή:	Κίνδυνος που προκύπτει από το σχεδιασμό και την λειτουργία του εταιρικού δικτύου δεδομένων.			
Κατηγορία Κινδύνου:	**Κίνδυνος Τεχνολογίας**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
2 (0.012%)	5	10	15	
Συνολική Έκθεση:		150		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Το δίκτυο δεδομένων πρέπει να μπορεί να προσαρμόζεται στις μεταβαλλόμενες επιχειρησιακές ανάγκες της εταιρείας χωρίς να απαιτούνται συχνοί επανασχεδιασμοί.			
Προπομπός Κινδύνου:	Προσπάθειες παραβίασης firewalls, routers.			
Στρατηγική Αντιμετώπισης:	Πολιτική ασφαλείας εταιρικού δικτύου δεδομένων.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τα συστήματα προστασίας δικτύου πρέπει να παρέχουν μηχανισμούς έγκαιρης ενημέρωσης.			
Διορθωτικά μέτρα:	Τα συστήματα προστασίας δικτύου πρέπει να είναι ενεργοποιημένες οι δυνατότητες καταγραφής και αποθήκευσης ιστορικού ενεργειών ώστε να γίνεται έλεγχος.			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Η πολιτική αυτή επανεξετάζεται, και εάν κριθεί αναγκαίο αναθεωρείται, σε τακτά χρονικά διαστήματα ή/ και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως εκδήλωση σοβαρών περιστατικών ασφαλείας, κλπ.).			

Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Δ3				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Αστοχίας υλικού.			
Σύντομη Περιγραφή:	Κίνδυνος που προκύπτει από προβληματικό hardware.			
Κατηγορία Κινδύνου:	**Κίνδυνος Τεχνολογίας**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
4 (25%)	5	20	15	
Συνολική Έκθεση:		300		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο διαχείρισης δικτύου (24/7)			
Προπομπός Κινδύνου:	Αρχεία καταγραφής, ενδείξεις και alarming.			
Στρατηγική Αντιμετώπισης:	SLAs			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τα συστήματα προστασίας δικτύου πρέπει να παρέχουν μηχανισμούς έγκαιρης ενημέρωσης. Μηχανισμοί παρακολούθησης hardware. Πρέπει να είναι ενεργοποιημένες οι δυνατότητες καταγραφής και αποθήκευσης ιστορικού ενεργειών ώστε να γίνεται έλεγχος.			
Διορθωτικά μέτρα:	Άμεση αντικατάσταση υλικού. Εφεδρικά συστήματα.			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:	Πάροχος υλικού			
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Τα SLAs ανανεώνονται σε τακτά χρονικά διαστήματα ή/ και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως εκδήλωση σοβαρών περιστατικών ασφαλείας, κλπ.).			
Κατάσταση:				

Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Δ4				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Προβληματικής Καλωδίωσης.			
Σύντομη Περιγραφή:	Κίνδυνος που προκύπτει από προβληματικά καλώδια.			
Κατηγορία Κινδύνου:	**Κίνδυνος Τεχνολογίας**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
4 (20%)	5	20	15	
Συνολική Έκθεση:		300		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο διαχείρισης δικτύου (24/7)			
Προπομπός Κινδύνου:	Αρχεία καταγραφής, ενδείξεις και alarming.			
Στρατηγική Αντιμετώπισης:	SLAs			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Τα συστήματα προστασίας δικτύου πρέπει να παρέχουν μηχανισμούς έγκαιρης ενημέρωσης. Μηχανισμοί παρακολούθησης hardware. Πρέπει να είναι ενεργοποιημένες οι δυνατότητες καταγραφής και αποθήκευσης ιστορικού ενεργειών ώστε να γίνεται έλεγχος.			
Διορθωτικά μέτρα:	Άμεση αντικατάσταση υλικού. Εφεδρικά συστήματα.			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:	Πάροχος υλικού			
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Τα SLAs ανανεώνονται σε τακτά χρονικά διαστήματα ή/ και όταν το επιβάλλουν επιχειρησιακοί ή εξωγενείς παράγοντες (όπως εκδήλωση σοβαρών περιστατικών ασφαλείας, κλπ.).			

Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Δ5				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Ηλεκτροδότησης.			
Σύντομη Περιγραφή:	Κίνδυνος που προκύπτει από πρόβλημα κατά την παροχή ηλεκτρικής ενέργειας.			
Κατηγορία Κινδύνου:	**Κίνδυνος Τεχνολογίας**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
4 (20%)	5	20	15	
Συνολική Έκθεση:		300		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο διαχείρισης δικτύου (24/7)			
Προπομπός Κινδύνου:	Αρχεία καταγραφής, ενδείξεις και alarming.			
Στρατηγική Αντιμετώπισης:	Εφεδρικά συστήματα παροχής ηλεκτρικής ενέργειας			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εφεδρικά συστήματα παροχής ηλεκτρικής ενέργειας. Γεννήτριες ηλεκτρικού ρεύματος, φωτοβολταικά			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:	Πάροχος Ηλεκτρικής Ενέργειας.			
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Κέντρο διαχείρισης δικτύου (24/7)			
Κατάσταση:				
Ημερομηνία Κλεισίματος:				

Ε. **Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ε1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Εμπρησμού			
Σύντομη Περιγραφή:	Κίνδυνος εμπρηστικών ενεργειών στους χώρους εργασίας και τεχνολογικού εξοπλισμού.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση και ασφάλεια πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
1 (0.001%)	5	1	14	
Συνολική Έκθεση:		14		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7			
Προπομπός Κινδύνου:	Μηνύματα απειλητικού περιεχομένου. Πολιτική Αστάθεια και Κοινωνική αναταραχή.			
Στρατηγική Αντιμετώπισης:	Πυρανίχνευση, πυροπροστασία, πυρόσβεση. Εφαρμογή σχεδίου άμεσης εκκένωσης των κτιριακών εγκαταστάσεων, κλήση αστυνομικών δυνάμεων			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Φύλαξη κτιριακών εγκαταστάσεων από εταιρία security. Έλεγχος παραβίασης (συναγερμός), έλεγχος και καταγραφή πρόσβασης εισόδου και εξόδου (ACCESS control), παρακολούθηση και καταγραφή μέσω κλειστού κυκλώματος τηλεόρασης. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα.			
Διορθωτικά μέτρα:	Πυρόσβεση. Εφαρμογή σχεδίου άμεσης εκκένωσης των κτιριακών εγκαταστάσεων, κλήση αστυνομικών δυνάμεων			
Εναλλακτικό σχέδιο:				

Σχέδιο μετάπτωσης:	Ασφαλιστικοί οργανισμοί
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Συνεχόμενη παρακολούθηση μέχρι το κλείσιμο του κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ε2				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Τρομοκρατικών Ενεργειών			
Σύντομη Περιγραφή:	Κίνδυνος Τρομοκρατικών ενεργειών στους χώρους εργασίας και τεχνολογικού εξοπλισμού.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση και ασφάλεια πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
1 (0.0015%)	5	5	15	
Συνολική Έκθεση:		75		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7			
Προπομπός Κινδύνου:	Μηνύματα απειλητικού περιεχομένου. Πολιτική Αστάθεια και Κοινωνική αναταραχή.			
Στρατηγική Αντιμετώπισης:	Εφαρμογή σχεδίου άμεσης εκκένωσης των κτιριακών εγκαταστάσεων. Κλήση αστυνομικών δυνάμεων			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Φύλαξη κτιριακών εγκαταστάσεων από εταιρία security. Έλεγχος παραβίασης (συναγερμός), έλεγχος και καταγραφή πρόσβασης εισόδου και εξόδου (ACCESS control), παρακολούθηση και καταγραφή μέσω κλειστού κυκλώματος τηλεόρασης. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα.			
Διορθωτικά μέτρα:	Εφαρμογή σχεδίου άμεσης εκκένωσης των κτιριακών εγκαταστάσεων, κλήση αστυνομικών δυνάμεων			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:	Ασφαλιστικοί οργανισμοί			
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Συνεχόμενη παρακολούθηση μέχρι το κλείσιμο του κινδύνου.			

Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ε3				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Κλοπής (1)			
Σύντομη Περιγραφή:	Κίνδυνος Κλοπής τεχνολογικού εξοπλισμού			
Κατηγορία Κινδύνου:	**Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση και ασφάλεια πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
2 (0.062%)	4	8	12	
Συνολική Έκθεση:		96		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7			
Προπομπός Κινδύνου:	Απόπειρες Κλοπής, Απουσία Φύλαξης.			
Στρατηγική Αντιμετώπισης:	Φύλαξη κτιρίων, alarming.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Φύλαξη κτιριακών εγκαταστάσεων από εταιρία security. Έλεγχος παραβίασης (συναγερμός), έλεγχος και καταγραφή πρόσβασης εισόδου και εξόδου (ACCESS control), παρακολούθηση και καταγραφή μέσω κλειστού κυκλώματος τηλεόρασης. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα.			
Διορθωτικά μέτρα:	Κλήση (emergency) στον προμηθευτή και αποκατάσταση υλικού. Κλήση αστυνομικών δυνάμεων			
Εναλλακτικό σχέδιο:	Χρήση εφεδρικών υλικών.			
Σχέδιο μετάπτωσης:	Εταιρεία φύλαξης και Ασφαλιστικοί οργανισμοί			
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Συνεχόμενη παρακολούθηση μέχρι το κλείσιμο του κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ε4				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Εκβιασμού			
Σύντομη Περιγραφή:	Κίνδυνος Εκβιασμού για την διαφύλαξη της ακεραιότητας του τεχνολογικού εξοπλισμού, των δεδομένων και των εργαζομένων.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση και ασφάλεια πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
1 (0.001%)	5	5	14	
Συνολική Έκθεση:		70		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Συνεχόμενη Παρακολούθηση από την αντίστοιχη διεύθυνση.			
Προπομπός Κινδύνου:	Μηνύματα απειλητικού περιεχομένου.			
Στρατηγική Αντιμετώπισης:	Κλήση αστυνομικών δυνάμεων			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Φύλαξη κτιριακών εγκαταστάσεων από εταιρία security. Έλεγχος παραβίασης (συναγερμός), έλεγχος και καταγραφή πρόσβασης εισόδου και εξόδου (ACCESS control), παρακολούθηση και καταγραφή μέσω κλειστού κυκλώματος τηλεόρασης. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα.			
Διορθωτικά μέτρα:	Κλήση αστυνομικών δυνάμεων			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Συνεχόμενη παρακολούθηση μέχρι το κλείσιμο του κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ε5				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Κλοπής (2)			
Σύντομη Περιγραφή:	Κίνδυνος Κλοπής τεχνολογικού εξοπλισμού από εσκεμμένη αμέλεια			
Κατηγορία Κινδύνου:	**Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση και ασφάλεια πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (0.75%)	4	12	12	
Συνολική Έκθεση:		144		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7			
Προπομπός Κινδύνου:	Απόπειρες Κλοπής, Απουσία Φύλαξης.			
Στρατηγική Αντιμετώπισης:	Φύλαξη κτιρίων, alarming.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Φύλαξη κτιριακών εγκαταστάσεων από εταιρία security. Έλεγχος παραβίασης (συναγερμός), έλεγχος και καταγραφή πρόσβασης εισόδου και εξόδου (ACCESS control), παρακολούθηση και καταγραφή μέσω κλειστού κυκλώματος τηλεόρασης. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα.			
Διορθωτικά μέτρα:	Κλήση αστυνομικών δυνάμεων			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Συνεχόμενη παρακολούθηση μέχρι το κλείσιμο του κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ε6				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Κλοπής (3)			
Σύντομη Περιγραφή:	Κίνδυνος Κλοπής τεχνολογικού εξοπλισμού από βαριά αμέλεια			
Κατηγορία Κινδύνου:	**Κίνδυνοι Παράνομων και Εγκληματικών Πράξεων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνική Διεύθυνση και ασφάλεια πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (0.60%)	4	12	12	
Συνολική Έκθεση:		144		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7			
Προπομπός Κινδύνου:	Απόπειρες Κλοπής, Απουσία Φύλαξης.			
Στρατηγική Αντιμετώπισης:	Φύλαξη κτιρίων, alarming.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Φύλαξη κτιριακών εγκαταστάσεων από εταιρία security. Έλεγχος παραβίασης (συναγερμός), έλεγχος και καταγραφή πρόσβασης εισόδου και εξόδου (ACCESS control), παρακολούθηση και καταγραφή μέσω κλειστού κυκλώματος τηλεόρασης. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα.			
Διορθωτικά μέτρα:	Ενδοδιευθυνσιακή Διαχείριση Κρίσεων.			
Εναλλακτικό σχέδιο:	Κλήση αστυνομικών δυνάμεων			
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Συνεχόμενη παρακολούθηση μέχρι το κλείσιμο του κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Z. **Κίνδυνοι Ελέγχων**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Z1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος εξακρίβωσης οικονομικής απάτης.			
Σύντομη Περιγραφή:	Κίνδυνος κατά την διαχείριση περιπτώσεων οικονομικής απάτης.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Ελέγχων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Ασφάλεια πληροφοριών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (3%)	5	15	7	
Συνολική Έκθεση:		105		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Ετήσιος έλεγχος πολιτικής και αναθεώρηση όποτε κριθεί αναγκαίο.			
Προπομπός Κινδύνου:	Παραποίηση εγγράφων, κλοπή, ληστεία.			
Στρατηγική Αντιμετώπισης:	Σύνταξη πολιτικής για την εξακρίβωσης οικονομικής απάτης			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Αξιολόγηση των υπαρχόντων μηχανισμών για τον εντοπισμό και την πρόληψη απάτης.			
Διορθωτικά μέτρα:	Επιπτώσεις σύμφωνα με το εργατικό δίκαιο, πειθαρχικές επιπτώσεις και ποινικές κυρώσεις.			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Αξιολόγηση κινδύνου ανά τακτά χρονικά διαστήματα και όποτε αυτό κρίνεται απαραίτητο.			

Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Η. **Κίνδυνοι εγκαταστάσεων και περιβάλλοντος εργασίας**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Η1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Πυρκαγιάς			
Σύντομη Περιγραφή:	Κίνδυνος πυρκαγιάς στους χώρους τεχνολογικού εξοπλισμού από αιτίες όπως είναι: υψηλή θερμοκρασία, βραχυκύκλωμα.			
Κατηγορία Κινδύνου:	**Κίνδυνοι εγκαταστάσεων και περιβάλλοντος εργασίας**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση Συντήρησης			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (2%)	4	12	12	
Συνολική Έκθεση:		144		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7			
Προπομπός Κινδύνου:	Ύπαρξη εύφλεκτων υλικών, ανεπαρκής συντήρηση, ενδείξεις θορύβου-καπνού.			
Στρατηγική Αντιμετώπισης:	Πυρανίχνευση, πυροπροστασία, πυρόσβεση.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ανίχνευση-έλεγχος υγρασίας-θερμοκρασίας (κλιματισμός). Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα. Φύλαξη εγκαταστάσεων.			
Διορθωτικά μέτρα:	Πυρόσβεση, μέσω κατάλληλου πυροσβεστικού μέσου.			
Εναλλακτικό σχέδιο:	Εφεδρικές πηγές ενέργειας, εφεδρικά συστήματα πυρόσβεσης, κλήση υπηρεσίας πυρόσβεσης.			
Σχέδιο μετάπτωσης:	Εταιρεία Ασφαλιστικής κάλυψης κτιρίων.			
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Συνεχόμενη παρακολούθηση κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Η2</th></tr>
<tr><th colspan="6">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος εισροής υδάτων / λυμάτων</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Εισροή υδάτων στους χώρους τεχνολογικού εξοπλισμού.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι εγκαταστάσεων και περιβάλλοντος εργασίας</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Συντήρησης</td></tr>
<tr><th colspan="6">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>3 (2%)</td><td>4</td><td>12</td><td rowspan="2">12</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>144</td></tr>
<tr><th colspan="6">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Ενδείξεις υγρασίας, ανεπαρκής συντήρηση.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Συστήματα ανίχνευσης υγρασίας, Συστήματα άντλησης υδάτων, Προγραμματισμένος προληπτικός έλεγχος εγκαταστάσεων.</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Ανίχνευση διαρροών. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα. Φύλαξη κτιριακών εγκαταστάσεων.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Συστήματα άντλησης υδάτων</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5">Εφεδρικές πηγές ενέργειας, εφεδρικά συστήματα άντλησης υδάτων, κλήση υπηρεσίας πυρόσβεσης.</td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="5">Εταιρεία Ασφαλιστικής κάλυψης κτιρίων.</td></tr>
<tr><th colspan="6">Παρακολούθηση Κινδύνου</th></tr>
<tr><td>Παρακολούθηση:</td><td colspan="5">Συνεχόμενη παρακολούθηση κινδύνου.</td></tr>
</table>

Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Θ. **Κίνδυνοι Κλιματολογικοί και καιρικών φαινομένων**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Θ1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Πυρκαγιάς			
Σύντομη Περιγραφή:	Κίνδυνος πυρκαγιάς στους χώρους τεχνολογικού εξοπλισμού από αιτίες όπως είναι: υψηλή θερμοκρασία (καύσωνας), κεραυνός.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Κλιματολογικοί και καιρικών φαινομένων**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση Συντήρησης			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
2 (0.11%)	4	8	12	
Συνολική Έκθεση:		96		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7			
Προπομπός Κινδύνου:	Κλιματολογικές Συνθήκες (Καύσωνας), ύπαρξη εύφλεκτων υλικών, ανεπαρκής συντήρηση.			
Στρατηγική Αντιμετώπισης:	Πυρανίχνευση, πυροπροστασία, πυρόσβεση. Αντικεραυνικά Συστήματα. Συστήματα προστασίας (UPS)			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Ανίχνευση-έλεγχος υγρασίας (κλιματισμός). Αντικεραυνική προστασία. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα. Φύλαξη εγκαταστάσεων.			
Διορθωτικά μέτρα:	Πυρόσβεση, μέσω κατάλληλου πυροσβεστικού μέσου.			
Εναλλακτικό σχέδιο:	Εφεδρικές πηγές ενέργειας, εφεδρικά συστήματα πυρόσβεσης, κλήση υπηρεσίας πυρόσβεσης.			
Σχέδιο μετάπτωσης:	Εταιρεία Ασφαλιστικής κάλυψης κτιρίων.			
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Συνεχόμενη παρακολούθηση κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="6">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Θ2</th></tr>
<tr><th colspan="6">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="5">Κίνδυνος εισροής υδάτων / λυμάτων</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="5">Εισροή υδάτων στους χώρους τεχνολογικού εξοπλισμού από αιτίες όπως είναι: πλημμύρες, καταιγίδες.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="5">Κίνδυνοι Κλιματολογικοί και καιρικών φαινομένων</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="5"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="5">Διεύθυνση Συντήρησης</td></tr>
<tr><th colspan="6">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td colspan="2">Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>2 (0.11%)</td><td>4</td><td>8</td><td rowspan="2">12</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>96</td></tr>
<tr><th colspan="6">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="5">Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="5">Κλιματολογικές Συνθήκες (Έντονες βροχοπτώσεις), ενδείξεις υγρασίας, ανεπαρκής συντήρηση.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="5">Συστήματα ανίχνευσης υγρασίας, Συστήματα άντλησης υδάτων, Προγραμματισμένος προληπτικός έλεγχος εγκαταστάσεων.</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="5"></td></tr>
<tr><td colspan="6">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="5">Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα. Φύλαξη κτιριακών εγκαταστάσεων.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="5">Συστήματα άντλησης υδάτων</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="5">Εφεδρικές πηγές ενέργειας, εφεδρικά συστήματα άντλησης υδάτων, κλήση υπηρεσίας πυρόσβεσης.</td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="5">Εταιρεία Ασφαλιστικής κάλυψης κτιρίων.</td></tr>
<tr><th colspan="6">Παρακολούθηση Κινδύνου</th></tr>
<tr><td>Παρακολούθηση:</td><td colspan="5">Συνεχόμενη παρακολούθηση κινδύνου.</td></tr>
<tr><td>Κατάσταση:</td><td colspan="5"></td></tr>
</table>

Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="5">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Θ3</th></tr>
<tr><th colspan="5">Προσδιορισμός Κινδύνου</th></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="4">Κίνδυνος Σεισμικής Δόνησης</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="4">Σεισμική δόνηση στους χώρους τεχνολογικού εξοπλισμού.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="4">Κίνδυνοι Κλιματολογικοί και καιρικών φαινομένων</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="4"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="4">Διεύθυνση Συντήρησης</td></tr>
<tr><th colspan="5">Ανάλυση Κινδύνου</th></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>4 (30%)</td><td>5</td><td>20</td><td rowspan="2">15</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>300</td></tr>
<tr><th colspan="5">Αντιμετώπιση Κινδύνου</th></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="4">Κέντρο Διαχείρισης Δικτύου και Εγκαταστάσεων - 24/7</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="4"></td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="4">Αντισεισμική προστασία</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="4"></td></tr>
<tr><td colspan="5">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="4">Διαίρεση συνδρομητικής βάσης, με βάση το τελευταίο ψηφίο, σε μονούς(1,3,5,7,9) και ζυγούς(0,2,4,6,8) σε διαφορετικά κτίρια. Οι χώροι και τα συστήματα προστασίας πρέπει να πληρούν τις προδιαγραφές που ορίζει η ισχύουσα Ελληνική ή Διεθνής νομοθεσία – κανονισμοί – διατάγματα. Φύλαξη κτιριακών εγκαταστάσεων.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="4">Εφεδρικές πηγές ενέργειας, Μεταφορά application servers και databases σε τρίτο κτίριο.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="4">Παροχή υπηρεσιών free of charge.</td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="4"></td></tr>
<tr><th colspan="5">Παρακολούθηση Κινδύνου</th></tr>
<tr><td>Παρακολούθηση:</td><td colspan="4">Συνεχόμενη παρακολούθηση κινδύνου.</td></tr>
</table>

Κατάσταση:	
Ημερομηνία Κλεισίματος:	

I. **Γεωπολιτικοί Κίνδυνοι**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ι1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Πολέμου			
Σύντομη Περιγραφή:	Κίνδυνος Πολέμου με άμεσες συνέπειες στον πάροχο τηλεπικοινωνιών			
Κατηγορία Κινδύνου:	**Γεωπολιτικοί Κίνδυνοι**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Υπεύθυνοι σχεδιασμού Β.C.M.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
1 (0.009%)	5	5	15	
Συνολική Έκθεση:		75		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:				
Προπομπός Κινδύνου:	Εθνικές και Διεθνής πολιτικές εξελίξεις.			
Στρατηγική Αντιμετώπισης:	Πλάνο Επιχειρησιακής Συνέχειας (B.C.M.S)			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Περιοδικές εκπαιδεύσεις προσωπικού.			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Συνεχόμενη ενημέρωση από τις εμπλεκόμενες ομάδες του B.C.M.S.			

Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Κ. **Κίνδυνοι Υγείας / Ασφάλειας**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Κ1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Ελέγχων Υγείας και Ασφαλείας			
Σύντομη Περιγραφή:	Κίνδυνοι που απορρέουν από τις συνθήκες εργασίας και την υγεία του προσωπικού.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Υγείας / Ασφάλειας**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Τεχνικός Ασφαλείας και Ιατρός Εργασίας.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
4 (6%)	2	8	5	
Συνολική Έκθεση:		40		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Προγραμματισμένες, ανά τακτά χρονικά διαστήματα, επισκέψεις στους χώρους εργασίας και στις εγκαταστάσεις τις εταιρείας. Πρόγραμμα Επισκέψεων.			
Προπομπός Κινδύνου:	Ενημέρωση για πιθανό πρόβλημα – συμβάν που έχει εντοπιστεί.			
Στρατηγική Αντιμετώπισης:	Διενέργεια επισκέψεων στους χώρους εργασίας και στις εγκαταστάσεις τις εταιρείας. Κατά την διάρκεια των επισκέψεων πραγματοποιούνται έλεγχοι στις εγκαταστάσεις για ελλείψεις σχετικά με τις απαιτήσεις του Συστήματος Υγείας και Ασφάλειας.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Οι διορθωτικές και προληπτικές ενέργειες απορρέουν από τις εσωτερικές επιθεωρήσεις καθώς και από τους ελέγχους που πραγματοποιούν οι υπεύθυνοι. Οι εν λόγω ενέργειες καταγράφονται σε σχετικό έντυπο και συμφωνούνται από όλες τις εμπλεκόμενες μονάδες. Οι διορθωτικές και προληπτικές ενέργειες πρέπει να νε είναι εφικτές και υλοποιήσιμες σε εύλογο χρονικό διάστημα. Τα ευρήματα πρέπει να αντιμετωπιστούν κατόπιν συνεννοήσεως με την εμπλεκόμενη οργανωτική μονάδα.			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				

Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Ο Ιατρός Εργασίας αρχειοθετούν τα παρακάτω: Βιβλίο γραπτών υποδείξεων Ιατρική Βεβαίωση Καταλληλότητας Εργαζομένου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

<table>
<tr><th colspan="5">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Κ2</th></tr>
<tr><td colspan="5">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="4">Κίνδυνοι συστήματος διαχείρισης υγείας και ασφάλειας στην εργασία.</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="4">Αξιολόγηση των κινδύνων από δύναται να υπάρξουν λόγω των δραστηριοτήτων της εταιρείας και παρακολούθηση, μέτρηση, διόρθωση και ανασκόπηση του Συστήματος Υγείας και Ασφάλειας.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="4">Κίνδυνοι Υγείας / Ασφάλειας</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="4"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="4">Εκπρόσωπος Διοίκησης για θέματα Υγείας και Ασφάλειας και Ομάδα Διαχείρισης Υγείας και Ασφαλείας.</td></tr>
<tr><td colspan="5">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>1 (0.006%)</td><td>2</td><td>2</td><td rowspan="2">4</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>8</td></tr>
<tr><td colspan="5">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="4">Επιλογή σε ετήσια βάση κατάλληλων δεικτών για την μέτρηση και επίδοση του συστήματος Διαχείρισης Υγείας και Ασφαλείας με έγκριση από την Ανώτατη Διοίκηση.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="4">Εκτιμήσεις επικινδυνότητας καταστάσεων στο χώρο εργασίας.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="4">Πολιτική και Διεργασίες για την Ασφάλεια και την Υγεία στην εργασία.</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="4"></td></tr>
<tr><td colspan="5">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="4">Ενημέρωση και ευαισθητοποίηση του προσωπικού σχετικά με τους κινδύνους κατά την εκτέλεση εργασίας καθώς και ζητήματα Υγείας και Ασφάλειας. Ενημέρωση Διοίκησης για την εξέλιξη του συστήματος Υγείας και Ασφάλειας. Διαχείριση επισημάνσεων των εργαζομένων σχετικά με ζητήματα Υγείας και Ασφάλειας.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="4">Καταγραφή Αναφοράς Συμβάντων και Ατυχημάτων, στην οποία περιγράφονται οι ενέργειες που ακολουθούνται για την διερεύνηση, την αναφορά και την γνωστοποίηση των εργατικών ατυχημάτων, τόσο στο εσωτερικό της επιχείρησης, όσο και στις αρμόδιες αρχές, καθώς και τα μέτρα που λαμβάνονται για την αποφυγή επανάληψης παρόμοιων ατυχημάτων.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="4"></td></tr>
</table>

Σχέδιο μετάπτωσης:	Κατάλογος Νομοθεσίας για την Υγεία και Ασφάλεια.
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Ανασκόπηση του συστήματος ασφαλείας που καλύπτει την πιθανή ανάγκη για μεταβολές στην πολιτική, τους αντικειμενικούς σκοπούς και όποια άλλα στοιχεία του συστήματος κρίνονται απαραίτητα.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Λ. **Κίνδυνος Υπόληψης**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Λ1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Εκπροσώπησης εταιρείας σε ΜΜΕ και άλλα κρίσιμα κοινά.			
Σύντομη Περιγραφή:	Η εταιρία αναγνωρίζει τη σημασία της ανάπτυξης και εδραίωσης αμφίδρομων σχέσεων επικοινωνίας με κρίσιμα κοινά που βασίζονται στην διαφάνεια, στο σεβασμό και την έγκαιρη ενημέρωση.			
Κατηγορία Κινδύνου:	**Κίνδυνος Υπόληψης**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση Εταιρικών Σχέσεων.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
2 (0.4%)	5	10	6	
Συνολική Έκθεση:		60		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Η στρατηγική εξωτερικής επικοινωνίας καθορίζεται από τον ετήσιο επιχειρησιακό σχεδιασμό της διεύθυνσης εταιρικών σχέσεων (προστασία φήμης, προβολή δραστηριοτήτων) και προβλέπει την αποτελεσματική διάχυση της πληροφόρησης προς τα ΜΜΕ και το εξωτερικό περιβάλλον, περιλαμβάνοντας την άμεση επαφή, την προώθηση και την επικοινωνία.			
Προπομπός Κινδύνου:	Συμβάντα από τον χειρισμό ΜΜΕ που μπορούν να έχουν συνέπειες στη φήμη της εταιρείας.			
Στρατηγική Αντιμετώπισης:	Σύνταξη πολιτικής εκπροσώπησης σε ΜΜΕ και Άλλα κρίσιμα Κοινά, Πολιτική Ενιαίας Μηνυματολογίας.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Έγκαιρος προγραμματισμός ενεργειών προβολής και δημοσιότητας για την βελτιστοποίηση της θετικής προβολής της εταιρείας. Η βέλτιστη, κατάλληλη και έγκαιρη προετοιμασία των στελεχών που καλούνται να εκπροσωπήσουν την εταιρεία. Η καλύτερη ενημέρωση των στελεχών της εταιρείας για τις λεπτομέρειες και ιδιαιτερότητες που διέπουν την επικοινωνία με τα ΜΜΕ και τα άλλα κρίσιμα κοινά καθώς και τους τρόπους που μπορεί η επικοινωνία αυτή να λάβει χώρα.			

Διορθωτικά μέτρα:	Υπό συνθήκες επικοινωνιακής διαχείρισης έκτακτου συμβάντος / κρίσης, η εκπροσώπηση της εταιρείας πραγματοποιείται αυστηρά από τη διεύθυνση εταιρικών σχέσεων
Εναλλακτικό σχέδιο:	
Σχέδιο μετάπτωσης:	
Παρακολούθηση Κινδύνου	
Παρακολούθηση:	
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Μ. **Κίνδυνοι Ηθικής**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Μ1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Περιβαλλοντικής Διαχείρισης			
Σύντομη Περιγραφή:	Ο κίνδυνος αυτός προέρχεται από την διασφάλιση ότι η ανάπτυξη, η παρακολούθηση, η επιθεώρηση, η εσωτερική επικοινωνία και η ανασκόπηση της περιβαλλοντικής διαχείρισης λαμβάνει υπόψη της τις δραστηριότητες καθώς και τα προϊόντα και υπηρεσίες που αλληλεπιδρούν με το περιβάλλον.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Ηθικής**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Υπεύθυνος Περιβαλλοντικής Διαχείρισης.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (1%)	3	9	4	
Συνολική Έκθεση:		36		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Σύνταξη και στη συνέχεια ανασκόπηση καταλόγου Νομοθεσίας 3 φορές το χρόνο			
Προπομπός Κινδύνου:	Επιπτώσεις στο περιβάλλον από δραστηριότητες καθώς και προϊόντα και υπηρεσίες που αλληλεπιδρούν με αυτό.			
Στρατηγική Αντιμετώπισης:	Περιβαλλοντική Πολιτική			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Διεθνή πρότυπα ISO καθώς και υπάρχουσα νομοθεσία.			
Διορθωτικά μέτρα:				
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				

Παρακολούθηση:	Επ αόριστο αρχειοθέτηση Καταλόγου Νομοθεσίας.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Μ2				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος σεξουαλικής παρενόχλησης.			
Σύντομη Περιγραφή:	Η σεξουαλική παρενόχληση μπορεί να λαμβάνει χώρα και στο πλαίσιο της εργασίας και δύναται να προέρχεται και από άνδρες και από γυναίκες, να ασκείται εις βάρος ανδρών και γυναικών και είναι εξίσου μη αποδεκτή. Στις περισσότερες περιπτώσεις υφίσταται σημαντική ανισσοροπία δύναμης/εξουσίας μεταξύ δραστών και θυμάτων και εκμετάλλευση συχνά, ιδίως των σχέσεων ιεραρχικής εξάρτησης.			
Κατηγορία Κινδύνου:	**Κίνδυνοι Ηθικής**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση κανονιστικής συμμόρφωσης.			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (0.06%)	3	9	3	
Συνολική Έκθεση:		27		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:				
Προπομπός Κινδύνου:				
Στρατηγική Αντιμετώπισης:	Πολιτική για την αποτροπή σεξουαλικής παρενόχλησης.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Εσωτερικός κανονισμός λειτουργίας εταιρείας. Ισχύουσα εθνική και κοινοτική νομοθεσία.			
Διορθωτικά μέτρα:	Εκτός από τους φορείς ή αρχές, οι εργαζόμενοι μπορούν να αποταθούν και να καταγγείλουν περιστατικό σεξουαλικής παρενόχλησης στα γραφεία κανονιστικής συμμόρφωσης.			
Εναλλακτικό σχέδιο:				
Σχέδιο μετάπτωσης:	Συμβάσεις εργασίας, Κώδικας Δεοντολογίας.			

Παρακολούθηση Κινδύνου	
Παρακολούθηση:	Επ αόριστο του κινδύνου.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

N. **Κίνδυνοι διαδικασιών και συμπεριφοράς**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ν1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Τήρησης Διαδικασιών			
Σύντομη Περιγραφή:	Κίνδυνος εκτέλεσης των διαδικασιών της εταιρείας εκτός εγκεκριμένων διαδικασιών.			
Κατηγορία Κινδύνου:	**Κίνδυνοι διαδικασιών και συμπεριφοράς**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:				
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (0.6%)	3	9	8	
Συνολική Έκθεση:		72		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Κάθε έτος συντάσσεται το χρονοδιάγραμμα υλοποίησης εσωτερικών επιθεωρήσεων, ώστε κάθε τομέας που έχει καταγραφεί να ελέγχεται ως προς την τήρηση των καταγεγραμμένων διαδικασιών			
Προπομπός Κινδύνου:	Ευρήματα που εντοπίζονται μέσω των εσωτερικών επιθεωρήσεων.			
Στρατηγική Αντιμετώπισης:	Πολιτική Τήρησης Διαδικασιών.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Στους τομείς και στις ημερομηνίες που προβλέπονται από το εγκεκριμένο σχέδιο επιθεώρησης, διενεργείται επιθεώρηση.			
Διορθωτικά μέτρα:	Αποστολή αναφοράς ευρημάτων από το τμήμα διαχείρισης ποιότητας στον υπεύθυνο.			
Εναλλακτικό σχέδιο:	Εάν το τμήμα διαχείρισης ποιότητας δεν συμφωνεί με τον υπεύθυνο γίνεται διερεύνηση εναλλακτικής λύσης.			
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Τα εκτοπισθέντα σημεία βελτίωσης εντάσσονται σε πλάνο παρακολούθησης από το αρμόδιο τμήμα και επικαιροποιείται κάθε			

	εξάμηνο.
Κατάσταση:	Με την ενημέρωση της διεύθυνσης εσωτερικού ελέγχου επικαιροποιείται το πλάνο παρακολούθησης διορθωτικών ενεργειών και χαρακτηρίζονται ως completed όσα ευρήματα βελτίωσης έχουν κλείσει. Όσα μένουν ανοιχτά λαμβάνονται υπόψη στον σχεδιασμό της επόμενης χρονιάς.
Ημερομηνία Κλεισίματος:	

Ξ. **Κίνδυνος Ανθρώπινων Πόρων**

<table>
<tr><th colspan="5">ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ξ1</th></tr>
<tr><td colspan="5">Προσδιορισμός Κινδύνου</td></tr>
<tr><td>Όνομα Κινδύνου:</td><td colspan="4">Κίνδυνος κατά την εξέταση και επιλογή Υποψηφίων Πρόσληψης Ανθρώπινου Δυναμικού</td></tr>
<tr><td>Σύντομη Περιγραφή:</td><td colspan="4">Κίνδυνος που απορρέει από την διαδικασία επιλογής του καταλληλότερου εξωτερικού υποψηφίου για την κάλυψη θέσης εργασίας.</td></tr>
<tr><td>Κατηγορία Κινδύνου:</td><td colspan="4">Κίνδυνος Ανθρώπινων Πόρων</td></tr>
<tr><td>Ημερομηνία Αναγνώρισης:</td><td colspan="4"></td></tr>
<tr><td>Υπεύθυνος:</td><td colspan="4">Γενική διεύθυνση ανθρώπινου δυναμικού.</td></tr>
<tr><td colspan="5">Ανάλυση Κινδύνου</td></tr>
<tr><td>Πιθανότητα Εμφάνισης</td><td>Συνέπεια / Επίπτωση</td><td>Έκθεση</td><td>Προτεραιότητα</td><td>Ημερομηνία Ενημέρωσης</td></tr>
<tr><td>3 (4%)</td><td>3</td><td>9</td><td rowspan="2">8</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Συνολική Έκθεση:</td><td>72</td></tr>
<tr><td colspan="5">Αντιμετώπιση Κινδύνου</td></tr>
<tr><td>Δείκτης Παρακολούθησης:</td><td colspan="4">Κατά την αξιολόγηση αιτήματος κάλυψης νέας θέσης, εάν αποφασίστηκε να γίνει από εξωτερικό υποψήφιο, την ακολουθεί οι ενδιαφερόμενοι εργαζόμενοι.</td></tr>
<tr><td>Προπομπός Κινδύνου:</td><td colspan="4">Δυσαρεστημένοι υπάλληλοι, υπάλληλοι που δεν καλύπτουν τις ανάγκες των τμημάτων τους.</td></tr>
<tr><td>Στρατηγική Αντιμετώπισης:</td><td colspan="4">Σύνταξη και ενημέρωση διαδικασίας εξέτασης και επιλογής Υποψηφίων Πρόσληψης Ανθρώπινου Δυναμικού.</td></tr>
<tr><td>Ημερομηνία Ενημέρωσης</td><td colspan="4"></td></tr>
<tr><td colspan="5">(προαιρετική συμπλήρωση)</td></tr>
<tr><td>Προληπτικά μέτρα:</td><td colspan="4">Επεξεργασία στοιχείων απαντήσεων πρόσληψης νέων υπαλλήλων. Δεύτερη συνέντευξη καθώς και συνέντευξη από τα αρμόδια τμήματα.</td></tr>
<tr><td>Διορθωτικά μέτρα:</td><td colspan="4">Εσωτερική μετακίνηση και αξιοποίηση προσωπικού.</td></tr>
<tr><td>Εναλλακτικό σχέδιο:</td><td colspan="4">Απόλυση</td></tr>
<tr><td>Σχέδιο μετάπτωσης:</td><td colspan="4"></td></tr>
<tr><td colspan="5">Παρακολούθηση Κινδύνου</td></tr>
</table>

Παρακολούθηση:	Τα αρμόδια στελέχη του τμήματος στελέχωσης ανασκοπούν τα σχόλια που καταγράφηκαν κατά την διάρκεια των συνεντεύξεων.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Ο. **Κίνδυνος Προμηθευτών**

ΦΥΛΛΟ ΚΙΝΔΥΝΟΥ Ο1				
Προσδιορισμός Κινδύνου				
Όνομα Κινδύνου:	Κίνδυνος Προμηθειών			
Σύντομη Περιγραφή:	Κίνδυνοι που προκύπτουν από τους όρους και τους κανόνες σύμφωνα με τους οποίους πραγματοποιούνται οι προμήθειες της εταιρείας.			
Κατηγορία Κινδύνου:	**Κίνδυνος Προμηθευτών**			
Ημερομηνία Αναγνώρισης:				
Υπεύθυνος:	Διεύθυνση προμηθειών			
Ανάλυση Κινδύνου				
Πιθανότητα Εμφάνισης	Συνέπεια / Επίπτωση	Έκθεση	Προτεραιότητα	Ημερομηνία Ενημέρωσης
3 (0.6%)	3	9	9	
Συνολική Έκθεση:		81		
Αντιμετώπιση Κινδύνου				
Δείκτης Παρακολούθησης:	Η εκάστοτε διεύθυνση όπου αντιμετωπίζει την ανάγκη για προμήθεια κάποιου είδους συντάσσει αίτηση αγοράς. Η αιτούμενη προμήθεια ελέγχεται ως προς την ύπαρξη προϋπολογισμένου κόστους.			
Προπομπός Κινδύνου:	Μη προϋπολογισμένες δαπάνες, προϋπολογισμός εκτός σχεδιασμού.			
Στρατηγική Αντιμετώπισης:	Σύνταξη αντίστοιχης πολιτικής προμηθειών.			
Ημερομηνία Ενημέρωσης				
(προαιρετική συμπλήρωση)				
Προληπτικά μέτρα:	Έρευνα αγοράς, παρουσιάσεις από προμηθευτές. Αξιολόγηση προτάσεων βάσει κριτηρίων.			
Διορθωτικά μέτρα:	Περιορισμένο ποσό ανάλογα με τα επίπεδα ιεραρχίας.			
Εναλλακτικό σχέδιο:	Διαπραγματεύσεις με προμηθευτές.			
Σχέδιο μετάπτωσης:				
Παρακολούθηση Κινδύνου				
Παρακολούθηση:	Μετά την έγκριση των απαιτούμενων προμηθειών και την υπογραφή των συμβάσεων οι παραγγελίες ακολουθουν εγκριτική ροή σε			

	μηχανογραφικό σύστημα.
Κατάσταση:	
Ημερομηνία Κλεισίματος:	

Κεφάλαιο 5ο

Μελλοντική Έρευνα - Συμπεράσματα

Η παρούσα εργασία, αποδεικνύοντας το γεγονός ότι πάντα υπάρχει ένα ποσοστό επικινδυνότητας που απομένει μετά την ολοκλήρωση του ελέγχου, παρέχει μια καλή βάση πάνω στην οποία μπορεί να στηριχθεί περαιτέρω έρευνα των πεδίων που προκύπτουν από τη συσχέτιση των εννοιών της διαχείρισης επικινδυνότητας στους παρόχους κινητών επικοινωνιών και των ελέγχων που διεξάγονται σε αυτούς.

Πιο συγκεκριμένα, λαμβάνοντας κανείς τους παράγοντες που επηρεάζουν το ποσοστό της εναπομείνασας επικινδυνότητας, έτσι όπως παραθέτονται και αναλύονται στα πλαίσια της εργασίας, θα μπορούσε να κάνει μια προσπάθεια ποσοτικοποίησης τους και ανεύρεσης κατάλληλων μετρικών, ώστε να δοθεί τελικά η δυνατότητα υπολογισμού αυτού του ποσοστού μέσω μαθηματικού τύπου.

Επίσης, θα μπορούσε να πραγματοποιηθεί μοντελοποίηση της επικινδυνότητας στους παρόχους κινητών επικοινωνιών, ενώ παράλληλα ανοίγονται και προοπτικές δημιουργίας αυτοματοποιημένου εργαλείου (software), το οποίο στηριζόμενο και πάλι στους ίδιους παράγοντες, αλλά πιθανόν και σε κάποιους επιπλέον, να παρέχει εκτίμηση του ποσοστού επικινδυνότητας που υπολείπεται μετά το πέρας του ελέγχου. Η δημιουργία ενός τέτοιου εργαλείου, σίγουρα θα προκαλούσε γενικότερο ενδιαφέρον, και ιδιαίτερα αυτό των διαφόρων επιχειρήσεων και οργανισμών που ασχολούνται με τις κινητές επικοινωνίες, αφού η χρήση του θα μπορούσε να αποτελέσει ένα μέσο μείωσης της αβεβαιότητας που αναπόφευκτα ενυπάρχει σε ένα οποιοδήποτε έργο.

Μια άλλη περιοχή στην οποία θα μπορούσε να έχει εφαρμογή με επιτυχία κάτι τέτοιο, είναι αυτή των εταιριών που παρέχουν ασφάλιση που σχετίζεται με τις κινητές επικοινωνίες , μιας και σίγουρα θα ελάττωνε σημαντικά το ποσοστό του ρίσκου που διατίθεται να πάρει ο ασφαλιστής προκειμένου να εξασφαλίσει ένα χρήστη από απώλειες που πιθανόν να συμβούν εξαιτίας μιας αποτυχίας του συστήματος.

Η κατανομή των ρόλων είναι ένα κομμάτι στο οποίο μπορεί να υπάρξει πλούσιο πεδίο για μελλοντική επέκταση. Οργανισμοί και επιχειρήσεις έχουν υποστεί καταστροφικά λάθη εξαιτίας λανθασμένων επιλογών στο κρίσιμο αυτό ζήτημα. Είναι λάθος να στηρίζεται όλο το σύστημα ασφαλείας σε έναν άνθρωπο και η κατανομή των ρόλων πρέπει να προβλέπεται απαραιτήτως στον σχεδιασμό

Είναι επίσης γεγονός ότι στις εταιρίες αυτό που έχει σημασία στο τέλος της ημέρας είναι το κόστος. Θα μπορούσαν λοιπόν στο πρόγραμμα να προστεθεί κάποια σειρά ερωτήσεων, μέσα από τις οποίες στην τελική αναφορά θα προκύπτει κάποιο συμπέρασμα για το οικονομικό

κόστος που θα υπάρξει από μια ενδεχόμενη παραβίαση ασφάλειας. Αυτό είναι ένα επιχείρημα που πείθει τους περισσότερους διοικητικούς στην λήψη των αναγκαίων μέτρων.

Η προσθήκη νέων κατηγοριών και ερωτήσεων ή τροποποίηση αυτών που υπάρχουν ήδη, προκειμένου να επιτευχθεί καλύτερη συλλογή δεδομένων για το διαχειριζόμενο δίκτυο, λόγω του ότι υπάρχει πάντα το ενδεχόμενο να εμφανιστούν νέες και καλύτερες τεχνολογίες, θα ήταν ένα καλό πεδίο για μελλοντική βελτίωση.

Τέλος, αυτό που είναι σημαντικό να επιτευχθεί είναι ένας κατάλληλος ποιοτικός, αλλά κυρίως ποσοτικός συνδυασμός της επικινδυνότητας με τα διάφορα κριτήρια ποιότητας που το χαρακτηρίζουν, όπως είναι για παράδειγμα η αξιοπιστία ή η ασφάλεια, ώστε να παρέχεται στον ενδιαφερόμενο μια πληρέστερη και ακριβέστερη εικόνα.

Κεφάλαιο 6ο

Επίλογος.

Πόσο ασφαλείς μπορούμε να είμαστε τελικά; Αυτό είναι το μεγάλο ζητούμενο. Μπορούμε να είμαστε ασφαλείς σε ικανοποιητικό βαθμό, προφανώς. Η πολιτική ασφάλειας είναι το πρώτο σκαλοπάτι που πρέπει να ανέβει κάποιος πάροχος κινητών επικοινωνιών αν θέλει να «χτίσει» ένα ασφαλές δίκτυο. Η ανάλυση ρίσκου και η αποτίμηση κινδύνων είναι διαδικασίες απαραίτητες στις περιπτώσεις οργανισμών παροχής υπηρεσιών κινητής επικοινωνίας, που πλέον διευκολύνονται σημαντικά και από την ύπαρξη των σχετικών λογισμικών.

Η έννοια της ασφάλειας είναι μια έννοια συνδεδεμένη ούτως ή άλλως στενά με την ανθρώπινη φύση: θέλουμε να νιώθουμε ασφαλής, το επιζητούμε και το ίδιο επιθυμούμε για οτιδήποτε έχουμε δημιουργήσει.

Το δίκτυο μιας εταιρίας ή ενός οργανισμού τηλεπικοινωνιών είναι σήμερα οι πνεύμονές της, αυτό που της δίνει την επικοινωνία με τον έξω κόσμο. Η οικονομία και η στρατηγική της εκάστοτε εταιρίας είναι πλέον ταυτισμένη με το δίκτυό της: εφημερίδες, ξενοδοχεία, κατασκευαστικές εταιρίες, νοσοκομεία, υπουργεία, αλλά και μικρότερης κλίμακας επαγγελματικοί χώροι, όπως δικηγορικά γραφεία και κτηματομεσιτικά γραφεία, δεν μπορούν πια να φανταστούν την λειτουργία τους χωρίς το διαδίκτυο και γενικότερα χωρίς δικτύωση μεταξύ των εργαζομένων. Είναι ζήτημα ουσίας λοιπόν το δίκτυο αυτό να λειτουργεί σωστά, ελλοχεύοντας τους ελάχιστους δυνατούς κινδύνους για τα δεδομένα και του ανθρώπους του.

Είδαμε όμως στην παρούσα διπλωματική εργασία πως αυτοί οι ίδιοι οι άνθρωποι είναι που μπορούν να δημιουργήσουν προβλήματα. Τα εργαλεία αποτίμησης κινδύνων καλούνται να κάνουν μία εξαιρετικά δύσκολη δουλειά. Το να προβλεφθούν οι κίνδυνοι σε οποιαδήποτε ενέργεια της ζωής μας είναι σχεδόν αδύνατο, από την άποψη ότι οι πιθανοί συνδυασμοί ενεργειών που δύνανται να προκαλέσουν πρόβλημα είναι αμέτρητοι. Η κύρια δυσκολία όμως σε μια επιτυχημένη διαδικασία ανάλυσης ρίσκου δεν είναι αυτή. Η κύρια δυσκολία είναι αυτή που αναφέρθηκε και πιο πάνω: η ανθρώπινη φύση που κρύβει εκπλήξεις, ευχάριστες ή - στην προκειμένη περίπτωση - δυσάρεστες.

Από μια άποψη λοιπόν, η πολιτική ασφάλειας και η διαχείριση επικινδυνότητας πιο συγκεκριμένα είναι ο «ψυχολόγος» του πληροφοριακού συστήματος. Λαμβάνοντας υπόψη την εξάρτηση του από τον παράγοντα «άνθρωπο», καλείται να προβλέψει πιθανές ενέργειες και αντιδράσεις, πράγμα εξαιρετικά πολύπλοκο εξαιτίας της ίδιας της πολυπλοκότητας των ανθρώπων.

Συμπερασματικά, οι μηχανισμοί και οι τεχνικές από μόνα τους δεν συνιστούν μέτρα ασφαλείας. Αυτά πρέπει να λειτουργούν κάτω από ένα μοντέλο ασφάλειας.

Βιβλιογραφία

Certified Information Security Manager (ISACA), 2010, 8th edition.

Ασφάλεια πληροφοριακών συστημάτων, κεφάλαιο 10, Προσεγγίσεις Ασφάλειας Πληροφοριακών Συστημάτων, Ευάγγελος Κιουντούζης

Ασφάλεια πληροφοριακών συστημάτων, κεφάλαιο 11, Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας ΠΣ, Σπύρος Κοκολάκης

Ασφάλεια πληροφοριακών συστημάτων, κεφάλαιο 12, Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων, Μαρία Καρύδα

Δικτυακός τόπος Αρχής Προστασίας Προσωπικών Δεδομένων, www.dpa.gr

Νόμος 2472/1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Νόμος 2474/1999, Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.

National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems, NIST 800-53, USA, 2005.

Pironti, John P.; "Information Security Governance: Motivations, Benefits and Outcomes," Information Systems Control Journal, vol. 4, 2006.

Pironti, John P.; "Developing Metrics for Effective Information Security Governance," Information Systems Control Journal, vol. 2, 2007.

Australian Standard, AS/NZS 4360, Risk Management, www.riskmanagement.com.au

IT Governance Institute, IT Governance Implementation Guide: Using CobiT and Val IT, 2nd Edition, USA, 2007

Παράρτημα Α

Λίστα Απειλών

Σκόπιμες Απειλές

Denial of Service

Session Hijacking

Social Engineering

War dialing

Industrial Espionage

Rerouting of Communications (αναδρομολόγηση επικοινωνιών)

Eavesdropping

Bombing/Bomb Threat (Βομβιστική ενέργεια)

Arson (Εμπρησμός)

Vandalism (Βανδαλισμός)

Theft & Fraud (Κλοπή ή/και απάτη)

Malicious Code (Viruses, Worms, Trojan Horses, Logic Bombs, Trap Doors) (Κακόβουλο λογισμικό)

Malicious destruction of data and facilities (Κακόβουλη καταστροφή δεδομένων ή/και υποδομών)

Masquerade (Πλαστοπροσωπία)

Abuse of Access Rights (Κατάχρηση δικαιωμάτων πρόσβασης)

Unauthorized Data Access (Μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά στοιχεία)

Unauthorized Remote Access (Μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση)

Unauthorized Software Changes (Μη εξουσιοδοτημένες αλλαγές στο λογισμικό)

Computer Abuse/Misuse (Εκμετάλλευση πληροφοριακών πόρων)

Τυχαίες Απειλές

Failure of communication services (Αποτυχία επικοινωνιών)

Failure of outsourced operations (Αποτυχία σε outsourced λειτουργίες)

Failure of lines/network equipment (Αποτυχία γραμμών / δικτυακού εξοπλισμού)

Traffic Overloading

Inadequate Communications capacity (ανεπαρκής χωρητικότητα επικοινωνιών)

Non-availability of Key Personnel (Μη διαθεσιμότητα προσωπικού)

Backup unavailability / failure (Αποτυχία / μη διαθεσιμότητα backup)

Operational Staff or User Errors (Ανθρώπινα λάθη)

Software / Programming Errors (Λάθη λογισμικού)

Negligent deletion of data (καταστροφή δεδομένων από αμέλεια)

Uncontrolled disposal of documents (μη ελεγχόμενη καταστροφή εγγράφων)

Technical Failures (Αποτυχία συστήματος)

Transmission Errors (Λάθη μετάδοσης)

Φυσικές Απειλές

Rain/Snow Storm (Έντονα καιρικά φαινόμενα)

High Temperatures (Υψηλές θερμοκρασίες)

Earthquake (Σεισμός)

Flood (Πλημμυρά)

Περιβαλλοντικές Απειλές

Electronic Interference (Ηλεκτρονικές παρεμβολές)

Extremes of Temperature and Humidity (Υψηλές θερμοκρασίας ή/και υψηλά επίπεδα υγρασίας)

Power Supply Failure (Διακοπή ρεύματος)

Fire Damage (Φωτιά)

Unauthorized Access to Site, Building, Room (μη εξουσιοδοτημένη πρόσβαση σε χώρους της εταιρίας)

Λίστα Ευπαθειών

Οργανωτικές

Inadequate Segregation of Duties between developers and operations staff (Ανεπαρκής διαχωρισμός αρμοδιοτήτων μεταξύ υπευθύνων σχεδιασμού/υλοποίησης και διαχειριστών συστήματος)

Not specific assignment of ownership (Ελλειπής καθορισμός ρόλων και αρμοδιοτήτων)

Inadequate security requirements in the contracts of third-parties that have access to the system (Ελλιπείς απαιτήσεις ασφάλειας σε συμβάσεις με τρίτους που έχουν πρόσβαση στο σύστημα)

Inadequate security requirements in outsourcing contract (Ελλιπείς απαιτήσεις ασφάλειας σε συμβάσεις outsourcing)

Inadequate control of externally provided services (ανεπαρκής έλεγχος υπηρεσιών που παρέχονται από τρίτους)

Information Classification

Lack of information classification (Ελλειπής ταξινόμηση των πληροφοριών του συστήματος)

Πρόσβασης Ελέγχου

Lack of identification and authentication mechanisms ('Ελλειψη μηχανισμών προσδιορισμού ταυτότητας και αυθεντικοποίησης)

Inadequate user access procedures for transferred or departing staff (Ανεπαρκής διαδικασία ενημέρωσης δικαιωμάτων πρόσβασης κατά τη μεταφορά ή αποχώρηση υπαλλήλου)

Inadequate allocation of access rights (Ανεπαρκής ανάθεση δικαιωμάτων πρόσβασης)

Inadequate control of visitors / contractors /cleaning maintenance personnel (Ανεπαρκής έλεγχος επισκεπτών / εξωτερικών συνεργατών/ προσωπικού καθαριότητας)

Inadequate review of user profiles and access rights (Ανεπαρκής έλεγχος και αναθεώρηση των προφίλ χρηστών και των αντίστοιχων δικαιωμάτων πρόσβασης)

Inadequate specification of user profiles (Ανεπαρκής ορισμός προφίλ χρηστών)

Uncontrolled provisioning and use of privileged accounts (Μη ελεγχόμενη χορήγηση και χρήση προνομιακών κωδικών χρηστών)

Poor password management (i.e. easily guessable passwords, storing of passwords, insufficient frequency of password change etc.) (Χρήση μη ποιοτικών κωδικών πρόσβασης)

Usage of group accounts (Χρήση group ή shared accounts)

Uncontrolled remote access to the system (i.e. usage of dial-up lines and modems) (Μη ελεγχόμενη απομακρυσμένη πρόσβαση στο σύστημα (π.χ. μέσω της χρήσης modem))

Inadequate restrictions on use / access time (Ανεπαρκείς περιορισμοί στο χρονικό διάστημα χρήσης/πρόσβασης στο σύστημα)

Lack of timeout control (Έλλειψη μηχανισμού timeout)

lack of limitation for number of failed logins (Έλλειψη περιορισμού του αριθμού των δυνατών αποτυχημένων προσπαθειών πρόσβασης στο σύστημα)

Lack of audit logs to detect unauthorized access (Ελλειπής μηχανισμός καταγραφής ενεργειών)

Personnel-related

Inadequate verification checks on permanent staff and/or contractors (Ανεπαρκείς έλεγχοι για το προσωπικό ή εξωτερικούς συνεργάτες)

Inadequate allocation of security responsibilities (Ανεπαρκής ανάθεση αρμοδιοτήτων σχετικά με την ασφάλεια)

Inadequate security training/awareness (Ελλειπής εκπαίδευση / ενημέρωση για θέματα ασφάλειας)

Inadequate procedures for responding to security incidents Αδυναμία αντιμετώπισης περιστατικών ασφάλειας)

Υλικές

Lack of fire prevention and/or suppression mechanisms (Έλλειψη μηχανισμών πυροπροστασίας)

Locating in an area susceptible to flood (Χώρος εκτεθειμένος σε πλημμύρες)

Susceptibility to humidity (χώρος εκτεθειμένος σε υγρασία)

Susceptibility to temperature variations (i.e. malfunctioning of air-conditioning) (Χώρος εκτεθειμένος σε μεταβολές θερμοκρασίες (π.χ. κακή λειτουργία συστήματος κλιματισμού))
Susceptibility to voltage variation (Μεταβολές της τάσης)

Inadequate physical entry controls (Ελλιπείς μηχανισμοί ελέγχου φυσικής πρόσβασης)
Unsupervised work by outside staff, external contractors/consultants (Εργασία εξωτερικών συνεργατών χωρίς εποπτεία από προσωπικό της εταιρίας)

Inadequate clear desk and clear screen policy (Μη εφαρμογή πολιτικής clear desk και clear screen)

Flammable materials such as paper or boxes (Εύφλεκτα υλικά (χαρτί, κουτιά, κλπ))

Inadequate monitoring of environmental conditions (Ελλιπείς μηχανισμοί παρακολούθησης των περιβαλλοντικών συνθηκών)

Unprotected communication lines (μη προστατευμένες γραμμές επικοινωνίας)

Επικοινωνίας και Λειτουργιών

Uncontrolled using and/or downloading of software (Μη ελεγχόμενη χρήση ή/και downloading εφαρμογών)

Uncontrolled hardware installation (e.g. external disks, memory sticks, etc) (Μη ελεγχόμενη εγκατάσταση hardware (πχ. external disks, memory sticks, κλπ))

Inadequate detection and prevention software (i.e. antivirus software) (Ελλείψεις σε λογισμικό προστασίας από κακόβουλο λογισμικό)

Inadequate policy and controls for the use of electronic mail (Ανεπαρκής πολιτική και μηχανισμοί ελέγχου στη χρήση του ηλεκτρονικού ταχυδρομείου)

Inadequate handling and disposal procedures (i.e. shredding important documents, etc.) ('Ελλειψη διαδικασιών διαχείρισης και καταστροφής εγγράφων (π.χ. χρήση shredder για την καταστροφή εμπιστευτικών εγγράφων))

Improper or inappropriate cabling (Ακατάλληλη καλωδίωση)

Improper or inappropriate maintenance of technical facilities (Έλλειψη συντήρησης υποδομών)

Inadequate control of software distribution (μη ελεγχόμενη εγκατάσταση λογισμικού)

Inadequate Firewall Policies (ελλείψεις στις πολιτικές των firewalls)

Inadequate incident handling (αδυναμία αντιμετώπισης περιστατικών)

Inadequate network management (αδυναμίες στη διαχείριση του δικτύου)

Lack of intrusion detection software ('Ελλειψη λογισμικού intrusion detection)

Lack of network capacity through improper planning or maintenance (Ελλείψεις σε network capacity λόγω αδυναμιών στο σχεδιασμό και στη συντήρηση)

Lack of regular update of Antivirus software (Μη τακτική ενημέρωση του λογισμικού προστασίας από κακόβουλο λογισμικό)

Lack of update of Operating System security patches (Έλλειψη ενημέρωσης του συστήματος με security patches)

Lack of back-up copies (έλλειψη αντιγράφων ασφάλειας)

Lack of audit-trail (έλλειψη αρχείων καταγραφής)

Unencrypted communications (Μη κρυπτογραφημένες επικοινωνίες)

Unprotected password tables (Ελλειπής προστασία των password tables)

Unrestricted use of modems (Μη ελεγχόμενη χρήση modems)

Unprotected point of access (Μη προστατευμένα σημεία πρόσβασης)

Ανάπτυξης Συστήματος

Complex user interface (Πολυπλοκότητα user interface)

Inadequate Software Development standards ('Ελλειψη προτύπων για την ανάπτυξη εφαρμογών)

Inadequate system development life cycle procedures (Ανεπαρκείς διαδικασίες ανάπτυξης συστημάτων)

Incorrectly configured / maintained application security features (Ανεπαρκής παραμετροποίηση χαρακτηριστικών ασφάλειας εφαρμογής)

Incorrectly configured / maintained operating system (Ανεπαρκής παραμετροποίηση μηχανισμών ασφάλειας λειτουργικού συστήματος)

Incorrectly configured / maintained security controls (Έλλειψη μηχανισμών ασφάλειας)

Lack of Change Management controls (Έλλειψη μηχανισμών για τη διαχείριση αλλαγών (Change Management))

Lack of documentation (Ελλειπής τεκμηρίωση)

Transmission of unencrypted confidential data (Μεταφορά εμπιστευτικών δεδομένων σε μη κρυπτογραφημένη μορφή)

Unclear or incomplete specifications (Ασαφείς ή μη ολοκληρωμένες προδιαγραφές)

Uncontrolled copying of data and / or software (Μη ελεγχόμενη αντιγραφή δεδομένων ή/και λογισμικού)

Uncontrolled downloading and use of software off the Internet (Μη ελεγχόμενο downloading και χρήση λογισμικού από το Internet)

Inadequate validation controls in application systems (input data validation, output data validation, other validation checks etc) (έλλειψη μηχανισμών ελέγχου και επαλήθευσης δεδομένων)

Πλάνο Επιχειρησιακής Συνέχειας

Lack of business continuity plans and procedures (Έλλειψη Σχεδίων Συνέχειας Λειτουργιών)

Lack of back-up facilities or processes (Ελλείψεις στις διαδικασίες / υποδομές λήψης αντιγράφων ασφάλειας)

Παράρτημα Β Λίστα Μηχανισμών Προστασίας

Οργανωτικοί και Φυσικοί

Safeguard	Safeguard Description	C	I	A
IT Security Management and Policies	This safeguard category contains all those safeguards dealing with the management of IT security, the planning of what should be done, assignment of responsibilities for these processes, and all other relevant activities. The aim of these safeguards is to achieve an appropriate and consistent level of security throughout an organization.			
Corporate IT Security Policy	A written document should be developed which contains rules, directives and practices describing how assets are managed, protected and distributed within an organization.	•	•	•
IT System Security Policy	For each IT system, an IT system security policy should be developed which describes the safeguards which are in place or should be implemented. The procedures to be followed to secure this system, and where possible a summary of the security concerns and/or risks which justify the safeguards	•	•	•
Allocation of Responsibilities	The responsibilities for organization-wide IT security should be clearly documented and allocated according to the corporate IT security policy and IT system security policies.	•	•	•
Organization of IT Security	All business processes which can support IT security (e.g. procurement, co-operation with other organizations) should be organized to provide that support in a secure manner.	•	•	•
Asset Identification and Valuation	All assets within an organization and for each IT system should be identified, and their value to the conduct of business should be assessed.	•	•	•
Approval of IT Systems	Approval of IT systems should take place according to the IT security policy. The approval process should aim at ascertaining that the safeguards implemented provide an appropriate level of protection. It should take into account that an IT system might include networks and underlying communications.	•	•	•

Safeguard	Safeguard	C	I	A
Security Compliance Checking	It is important that compliance is maintained with all required safeguards, and relevant laws, regulations and policies, since any safeguard, regulation or policy can only be working as long as users comply, and systems conform, to them.			
Compliance with IT Security Policies and Safeguards	Regular checks should be conducted to ensure that all safeguards that should be in place, as listed in the corporate IT security policy and the relevant IT system security policy, and other relevant documents, e.g. security operating procedures documents and disaster recovery plans, are implemented correctly, used correctly and effectively and tested, if necessary.	•	•	•
Compliance with Legal and Regulatory Requirements	The compliance checks mentioned above should encompass ensuring that all legal and regulatory requirements related to the country or countries in which the IT system is located, are met. Where this legislation exists, this includes legislation on data protection and privacy, software copying, safeguarding of organizational records, misuse of IT systems or cryptography.	•	•	•
Safeguard	**Safeguard Description**	**C**	**I**	**A**
Incident Handling	Everybody in the organization should be aware of the need to report security incidents, including software malfunctions, and identified weaknesses, as quickly as possible.			
Reporting of Security Incidents	Each employee should be aware of the commitment to report security incidents. Incidents can also be identified and reported by tools. In order to facilitate effective incident handling, a reporting scheme and contact points within the organization should be provided by the organization.	•	•	•
Reporting of Security Weaknesses	If users are noting any security relevant weaknesses, they should report them to the person responsible as soon as possible.	•	•	•
Reporting of Software Malfunctions	If users are noting any security relevant software malfunctions, they should report them to the person responsible as soon as possible.	o	•	•
Incident Management	A management process should be in place that supports the protection against incidents, their detection and reporting, and appropriate reaction to the incident. Information about incidents should be collected and evaluated to avoid incidents in the future and limit the damage, if they occur.	•	•	•

Safeguard	Safeguard Description	C	I	A
Personnel	Safeguards in this category should reduce the security risks resulting from errors or intentional or unintentional breaking of security rules by personnel (permanent or contracted).			
Safeguards for Permanent and Temporary Staff	All employees should be aware of their security roles and responsibilities. All security relevant procedures, which should be followed by the personnel, should be stated in a document. Employees should be subject to recruitment checks before employment, and a confidentiality agreement should be signed if that is necessary.	•	•	•
Safeguards for Contracted Personnel	Contracted personnel (e.g. cleaning or maintenance staff) should be controlled, as well as any other visitor. Contracted, certainly long-term, personnel should sign a confidentiality agreement before having access (physical or logical) to the organization's IT facilities.	•	•	•
Security Awareness and Training	All personnel who use, develop, support and have access to IT equipment should receive regular security awareness briefings and material. This should ensure that the personnel are aware of the importance of the information processed to the business, associated threats, vulnerabilities and risks, and thus understand why safeguards are needed. Users should also be trained to use IT facilities correctly, to avoid errors. For selected personnel, e.g. IT security officers, security administrators, more specific security training might be necessary.	•	•	•
Disciplinary Process	All employees should be aware of the consequences of an (intentional or unintentional) violation of the organization-wide and specific IT system security policies or any other documented security agreement.	•	•	•

Safeguard	Safeguard Description	C	I	A
Operational Issues	Safeguards in this area aim at all procedures maintaining the secure, correct and reliable functioning of the IT equipment and related system(s) used. Operational safeguards are necessary in combination with other, for example, physical and technical, safeguards.			
Configuration and Change Management	Configuration management is the process of keeping track of changes to IT systems. Its primary security goal is to ensure that changes to IT systems do not reduce the effectiveness of safeguards and the overall security provided. Change management can contribute to the identification of new security implications when changes occur to IT systems.		•	o
Capacity Management	Capacity management should be used to avoid failures due to inadequate capacity. Future capacity requirements and current trends should be taken into account when assessing the capacity necessary for an IT system.		o	•
Documentation	All aspects of IT configurations and operations should be documented to ensure continuity and consistency. The security of an IT system also needs to be documented in the IT system security policy, security operating procedures document, and business continuity strategy report(s) and plan(s). The documentation should be current and accessible.		•	o
Maintenance	IT equipment should be correctly maintained to ensure its continued reliability, availability and integrity. All security requirements that have to be met by the maintenance providers should be fully documented in the maintenance contracts. Maintenance should take place in accordance with the supplier's contract, and should only be done by authorized personnel.		o	•
Monitoring Security Relevant Changes	Changes to the impacts, threats, vulnerabilities, and risks and their associated characteristics should be monitored. The monitoring should include both existing and new aspects. The environment within which the system is located should also be monitored.		•	•

Audit Trails and Logging	Auditing and logging capabilities of servers, networks and applications should be utilized to record details of security relevant events. This includes details of readily identifiable unauthorized or error events and details of apparently normal events that may need to be analyzed at a later date. Audit trails and logs should be regularly reviewed to detect unauthorized activities and allow appropriate corrective measures to be taken. Events in logs should also be analyzed for repetition of similar events that may indicate the presence of vulnerabilities or threats for which inadequate safeguards are present. Such analysis may also reveal patterns in apparently unrelated events which may allow identification of people performing unauthorized activity or the root cause of a security problem.	•	o	
Security Testing	Security testing should be used in order to ensure that all IT equipment and all related software components are in a secure manner. Security testing should encompass the security requirements defined in the IT system security policy and test plans, and acceptance criteria should be established to demonstrate that the required level of security is achieved.operating	•	•	•
Assured Storage Deletion	The confidentiality of information previously written to a storage device should be preserved if the information is no longer required. It should be ensured that files containing confidential material are erased and physically overwritten or otherwise destroyed - the activation of delete functions does not always do that. Facilities approved by the responsible personnel should be available for the users to be used for complete and	•		
Segregation of Duties	In order to minimize the risks and the possibilities of misuse of privileges, segregation of duties should be applied where required and possible. In particular duties and functions which, in combination, can lead to the circumvention of safeguards or audits, or to an undue advantage for the employee, should be kept separate.	•	o	
Correct Software Use	It should be ensured that no copyrighted material is copied, and that the license agreements are obeyed for proprietary software.	o	•	o

Software Change Control	Software change control should be applied to maintain the integrity of software when changes are made. Change control procedures for software that manage all changes and ensure that security is maintained throughout the whole process should be established. This includes authorization for changes, security consideration for intermediate solutions, and security checks of the final solution.	o	•	o

Safeguard	Safeguard Description	C	I	A
Business Continuity Planning	In order to protect business, especially critical business processes, from the effects of major failures or disasters and to minimize the damage caused by such events, effective business continuity, including contingency planning/disaster recovery, strategy and plan(s) should be in place.			
Business Continuity Strategy	A business continuity, including contingency planning/disaster recovery, strategy should be^ formulated and documented related to the IT system considered, based on the identified potential adverse business impacts from unavailability, modification and destruction.	o	o	•
Business Continuity Plan	Based on the business continuity strategy, business continuity plan(s), including plans for contingency and disaster recovery, should be developed and documented.	o	o	•
Testing and Updating the Business Continuity Plan	Before being accepted, a business continuity plan should be thoroughly tested to ensure that it is working under 'real life' circumstances, and that it is known to all relevant members of the staff. Since business continuity plans can become out-of-date quickly, it is important that they are updated regularly. The business continuity strategy should also be updated whenever necessary.	o	o	•
Back-ups	Back-ups should be made of all important files and other business data and of important system programs and documentation. The frequency of back-ups should be in line with the importance of the information and the business continuity plan. Back-ups should be stored securely and remotely, and recovery checked regularly for reliability.		•	•

Safeguard	Safeguard Description	C	I	A
Physical Security	Safeguards in this area deal with physical protection. Several of the following items apply to buildings, secure areas, computer rooms and offices. The safeguard selection depends on which part of the building is considered.			
Material Protection	Physical safeguards to protect a building include fences, physical access control, strong walls, doors, and windows. Secure areas within a building should be protected from unauthorized access by physical access controls, guards, etc. Secure areas might be necessary for IT equipment, such as servers, and associated software and data, supporting important business activities. Access to such secure areas should be limited to the minimum number of personnel necessary, and details recorded in a log.	•	o	o
Fire Protection	Equipment and surrounding areas, including access to them, should be protected against the spread of fire from elsewhere in the building or adjacent buildings. Fire hazards in the vicinity of rooms/areas containing equipment should be minimized. There also should be protection against fires starting within and/or affecting all rooms/areas containing key equipment. Safeguards should include fire and smoke detection, alarms and suppression. Care should be taken that the fire protection does not lead to damage of IT systems from water or other extinguishing		o	•
Water/Liquid Protection	Essential facilities should not be sited in any area where serious flooding or water, or other liquid, leakage is likely to occur. Appropriate protection should be provided where a significant threat of flooding exists.		o	•
Natural Disaster Protection	Buildings containing key equipment should be protected against the effects of lightning. Also, the key equipment itself should be protected against the effects of lightning. Protection against other natural disasters can be achieved by avoiding areas where these are likely to happen (if possible) and by having business continuity strategy and planning in place.		o	•
Protection against Theft	To achieve stock control, all items of equipment should be uniquely identifiable and an inventory maintained. Security guards/receptionists should be encouraged to check for equipment or media leaving rooms/areas or the building without authorization. Sensitive information and proprietary software held on portable media (e.g. floppy discs) should be protected	•	o	•

Power and Air conditioning	All IT equipment should be protected from power failures, if necessary. A suitable power supply should be provided, and an uninterruptible power supply should be introduced, if necessary. Another aim of protection should be to ensure admissible temperature and humidity		o	•
Cabling	Power and communication cabling carrying data or supporting IT services should be protected from interception, damage and overloading. Cabling should be physically protected against accidental or deliberate damage, and selected and laid appropriate for its purpose; careful planning taking into account future developments can avoid a lot of problems. Wherever justified and possible, cables should be protected against wiretapping	•	o	•

Ασφαλείας Συστημάτων IT

Safeguard	Safeguard Description	C	I	A
Identification and Authentication (I&A)	Identification is the means by which a user provides a claimed identity to a system. Authentication is the means of establishing the validity of this claim. The following ways are examples of how to achieve I&A (other ways of classifying I&A mechanisms are possible).			
I&A Based on Something the User Knows	Passwords are the most typical way to provide I&A based on something the user knows linked with a user identification process. The allocation of passwords and their regular change should be controlled. If users are choosing the passwords themselves, they should be aware of the common rules for password design and handling. Software can be used to support this, for example by limiting the use of common passwords or patterns and characters. I&A based on something the user knows can also make use of cryptographic means and authentication protocols. This type of identification and authentication can also be used for remote I&A.			
I&A Based on Something the User Possesses	Objects that users possess for the purpose of I&A can be memory tokens and smart tokens. A common application of memory tokens is the magnetic material on the back of a credit card. Authentication is provided based on something the user possesses (the card) and something the user knows (the PIN). Typical examples of smart tokens are smart cards.			
I&A Based on Something the User Is	Biometric authentication technologies use the unique characteristics or attributes of an individual to authenticate the person's identity. This could be fingerprints, hand geometry, retina pattern, as well as voice patterns or handwritten signatures. Relevant details can be securely stored on smart cards, or a system.			

Safeguard	Safeguard Description	C	I	A
Logical Access Control and Audit	Safeguards in this area are implemented to restrict access to information, computers, networks, applications, system resources, files and programs and record details of error and user actions in audit trails and analyze the details recorded, in order to detect and handle security breaches in an appropriate manner.			
Access Control Policy	For each user or group of users, there should be a clearly defined access control policy. This policy should grant access rights according to the business requirements, such as availability, productivity and the 'need to know' principle.	•	•	
User Access to Computers	Access control to computers is applied to prevent any unauthorized access to a computer. It should be possible to identify and verify the identity of each authorized user, with both successful and unsuccessful attempts logged. Computer access control can be aided by passwords, or by any other I&A method.	•	•	
User Access to Data, Services and Applications	Access control should be applied to protect the data and services on a computer or within a network from unauthorized access. This can be done with the appropriate interfaces between networked services, and the configuration of the network which ensures that only authorized access to IT services can take place. To prevent unauthorized access to applications, role-based access control that allows access according to the business functions of the users should be introduced.	•	•	
Reviewing and Updating Access Rights	All access rights given to users should be reviewed regularly and updated if the security or business needs for access have changed. Privileged access rights should be reviewed more frequently to ensure that they are not misused. Access rights should be withdrawn immediately if they are no longer necessary	•	•	
Audit Logs	All work done with IT support should be logged and these logs should be inspected regularly; this includes successful and unsuccessful attempts to log into a system, logging of access to data, functions of the system used, etc. Faults should also be logged, and these logs should be reviewed regularly. These data should be used in accordance with data protection and privacy legislation.	•	•	

Safeguard	Safeguard Description	C	I	A
Protection against Malicious Code	Malicious code may not be detected before damage is done unless suitable safeguards are implemented. Malicious code may result in compromise of security safeguards (e.g. capture and disclosure of passwords), unintended disclosure of information, unintended changes to information, loss of system integrity, destruction of information, and/or unauthorized use of system resources. Malicious code can be viruses, worms, and Trojan horses. Malicious code carriers are: executable software, data files (containing executable macros, e.g. word processing documents or spreadsheets), active contents of World Wide Web pages. Malicious code can propagate via: floppy discs, other removable media, electronic mail, networks, downloads.			
Scanners	Different forms of malicious code can be detected and removed by special scanning software and integrity checkers. Scanners can work in off-line or on-line modes. On-line operation of a scanner provides active protection, i.e. detection (and possible removal) of malicious code before any infection takes place and damage is done to the IT system. Scanners are available for stand-alone computers, workstations, file servers, electronic mail servers and firewalls. However, users and administrators should be made aware that scanners cannot be relied upon to detect all malicious code because new forms of malicious code are continually arising.	o	•	o
Integrity Checkers	Typically, other forms of safeguard are required to augment the protection provided by scanners. For example, checksums can be used to check whether a program has been modified. Integrity checking software should be an integral part of technical safeguards providing protection against malicious code. This technique can only be used for data files and programs that do not keep status information for further use.		•	
Removable Media Circulation Control	Uncontrolled circulation of media (especially usb sticks, CD's etc.) can lead to an increased risk of introducing malicious code to an organization's IT systems. Control of circulation of media can be achieved by the use of: special software, procedural safeguards.	•	o	

Procedural Safeguards	Guidelines for users and administrators should be developed outlining procedures and practices to minimize the possibility for introducing malicious code. Independent reviews of source or executable code should be made when necessary. Security awareness training and disciplinary actions and related procedures should be in place for not following the documented malicious code prevention procedures and practices.	•	•	o

Safeguard	Safeguard Description	C	I	A
Network Management	This area includes topics of planning, operation and administration of networks. The proper configuration and administration of networks is an effective means to reduce risks.			
Operational Procedures	The establishment of operational procedures and responsibilities is necessary to ensure the correct and secure operation of networks. This includes the documentation of the operating procedures and the establishment of procedures to react to security relevant incidents	o		•
System Planning	In order to ensure reliable functioning and adequate network capacity, advanced planning and preparation, and monitoring (including of loading statistics) is necessary. Acceptance criteria for new systems should be applied and changes should be controlled and reacted to	o	o	•
Network Configuration	An appropriate network configuration is essential for its reliable functioning. This includes a standardized approach for the configuration of servers throughout the organization, and, very important, good documentation. Furthermore, it should be ensured that servers used for special purposes are only used for these purposes (e.g. no other tasks should run on a firewall), and that sufficient protection from failure is in place.	o	o	•
Network Segregation	In order to minimize the risks and the possibilities of misuse in a network in operation, business areas dealing with critical business issues and information should be kept separate, logically or physically. As well, development facilities should be separated from operational facilities.	•	o	o
Network Monitoring	Network monitoring should be used to identify the weaknesses within the existing network configuration. It allows for reconfiguration caused by traffic analysis and helps to identify attackers.	o	o	o
Intrusion Detection	Attempts to gain entry to systems or networks and successful unauthorized entry should be detected so that the organization can respond in an appropriate and effective manner.	•	•	

Safeguard	Safeguard Description	C	I	A
Cryptography	Cryptography can help to provide confidentiality and/or integrity of data, non-repudiation, and advanced I&A methods. When applying cryptography, care should be taken to comply with all laws and regulations in this area. One of the most important aspects of cryptography is an adequate key management system.			
Data Confidentiality Protection	In circumstances where preservation of confidentiality is important, e.g. where the information is particularly sensitive, safeguards should be considered to encrypt information for storage or communication over networks. The decision to use encryption safeguards should take account of: -relevant government laws and regulations, -the requirements of key management and the difficulties that need to be overcome to ensure that real security improvements are achieved without creating new vulnerabilities, and -the suitability of the encryption mechanisms used for the deployment situation and the degree of protection required.	•		
Data Integrity Protection	In circumstances where preservation of integrity of stored or processed data is important, hash functions, digital signatures and/or integrity safeguards should be considered to protect stored or communicated information. Integrity safeguards provide protection against accidental or deliberate alteration, addition or deletion of information. Digital signature safeguards can provide similar protection to safeguard message integrity, but also have properties that allow them to enable non-repudiation. The decision to use digital signature or other integrity safeguards should take account of: -relevant government laws and regulations, -relevant public key infrastructures, -the requirements for key management and the difficulties that need to be overcome to ensure that real security improvements are achieved without creating new vulnerabilities.		•	

Non-Repudiation	Cryptographic techniques (e.g. based on the use of digital signatures) can be used to prove or otherwise the sending, transmission, submission, delivery, receipt notification, etc. of messages, communications and transactions.	•	•	
Data Authenticity	In situations where the authenticity of data is important a digital signature can be used to attest to the validity of the data. Digital signatures can also be used to attest the fact that data is originating from a specific person.	o	•	
Key Management	Key management includes technical, organizational and procedural aspects that are necessary to support the use of any cryptographic mechanism. The objective of key management is the secure administration and management of cryptographic keys and related information. Key management includes the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material. Key management procedures depend on the algorithm used, the intended use of the key and the security policy	•	o	

C: Confidentiality	**( ) Not Covered**
I: Integrity	**• : Fully Covered**
A: Availability	**o:Partially covered**