ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων»

Διαχείριση του Ανθρώπινου Παράγοντα στην Απειλή της Βιομηχανικής Κατασκοπείας σύμφωνα με το ISO 31000:2009

Μεταπτυχιακή Διπλωματική Εργασία

Κωνσταντίνος **Λατζανάκης**

Τριμελής Επιτροπή:
Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος
Αναπληρωτής Καθηγητής Ν. Σ. Κουτσούκης
Διδάκτορας Π. Χουντάλας

Τελική έκδοση

Κόρινθος, 2017

UNIVERSITY OF THE PELOPONNESE
SCHOOL OF SOCIAL AND POLITICAL SCIENCES
DEPARTMENT OF POLITICAL SCIENCES & INTERNATIONAL RELATIONS

Master of Arts in
"Global Risks and Analytics"

Managing Human Factor in the Threat of Industrial Espionage according to ISO 31000:2009

Master's Dissertation

Konstantinos **Latzanakis**

Supervisors:
Assistant Professor I. Konstantopoulos
Associate Professor N. S. Koutsoukis
Doctor P. Chountalas

Final Version

Corinth, 2017

Φύλλο αξιολόγησης

Η διπλωματική εργασία με τίτλο «Διαχείριση του Ανθρώπινου Παράγοντα στην Απειλή της Βιομηχανικής Κατασκοπείας σύμφωνα με το ISO 31000:2009» του Κωνσταντίνου Λατζανάκη αξιολογήθηκε από την τριμελή επιτροπή, τόσο ως προς την ποιότητα του κειμένου, όσο και ως προς την ποιότητα της προφορικής παρουσίασης και υπεράσπισης της διπλωματικής εργασίας ενώπιον ακροατηρίου.

Η διαδικασία αξιολόγησης της διπλωματικής εργασίας ολοκληρώθηκε την 09/11/2017 με γενική επίδοση: 9,03

☐ Καλώς

☐ Λίαν Καλώς

☐ Άριστα

Τα μέλη της τριμελούς επιτροπής

Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος

Αναπληρωτής Καθηγητής Ν. Σ. Κουτσούκης

Διδάκτορας Π. Χουντάλας

Περίληψη

Σε έναν κόσμο που χαρακτηρίζεται από ραγδαία τεχνολογική και οικονομική ανάπτυξη, η ανάγκη για οικονομική κυριαρχία αποτελεί το βασικό στοιχείο που καθορίζει την επιβίωση μίας επιχείρησης. Αποτέλεσμα αυτού του έντονα ανταγωνιστικού περιβάλλοντος αποτελεί το φαινόμενο άσκησης βιομηχανικής κατασκοπείας μέσω της οποίας οι επιχειρήσεις υποκλέπτουν πληροφορίες από τους ανταγωνιστές τους ώστε να εκμεταλλευτούν το συγκριτικό πλεονέκτημα που μπορεί να έχουν σε κάποιο τομέα. Ως αποτέλεσμα, καμία επιχείρηση δεν μπορεί πλέον να αγνοήσει τις προφυλάξεις που πρέπει να λάβει ώστε να μην βρεθεί αντιμέτωπη με την απώλεια των στοιχείων αξίας της.

Στην παρούσα εργασία χρησιμοποιείται το πρότυπο ISO 31000:2009 με βάση το οποίο προσδιορίζεται ο κίνδυνος της βιομηχανικής κατασκοπείας. Τα μέσα τα οποία δύναται να χρησιμοποιηθούν είναι ποικίλα, ωστόσο σκοπός της εργασίας αυτής είναι η ανάλυση της επίδρασης του ανθρώπινου παράγοντα και τα φαινόμενα υποκλοπής εταιρικών μυστικών είτε από εσωτερικούς είτε από εξωτερικούς δρώντες οι οποίοι επιθυμούν να επωφεληθούν από τις διαβαθμισμένες πληροφορίες της επιχείρησης.

Τέλος, στο πλαίσιο διαχείρισης του κινδύνου της βιομηχανικής κατασκοπείας χρησιμοποιείται η Διαδικασία Αναλυτικής Ιεράρχησης (AHP) ως μέθοδος ταξινόμησης των εργαζομένων της επιχείρησης ανάλογα με τα προσωπικά τους χαρακτηριστικά όσον αφορά την πιθανότητα υποκλοπής ή αποκάλυψης διαβαθμισμένων πληροφοριών και προτείνεται μία λίστα ελέγχου και αυτοαξιολόγησης των διαδικασιών χειρισμού του κινδύνου.

Όροι κλειδιά: Βιομηχανική Κατασκοπεία, Στοιχεία αξίας, Διαχείριση Κινδύνου, Ασφάλεια

Abstract

In a world characterized by rapid technological and economic development, the need for economic sovereignty is the key factor determining the existence of a business. The result of this highly competitive environment is the industrial espionage phenomenon through which businesses seize information from their competitors in order to profit from the comparative advantage they may have in a certain sector. As a result, no business can ignore any more the precautions it has to take so as not to be confronted with the loss of its value.

This work uses the ISO 31000: 2009 standard to identify the threat of industrial espionage. The means that can be used are varied, but the purpose of this work is to analyze the impact of human factor and the phenomena of corporate secret intrusion by internal or external actors wishing to take advantage of the classified information of the company.

Finally, as part of industrial espionage risk management, the Analytical Hierarchy Process (AHP) is used as a method of classifying the employees of a company according to their personal characteristics with regard to the probability of spying or revealing classified information and also is proposed a self-evaluation checklist of risk management procedures.

Keywords: Industrial Espionage, Values, Risk Management, Security

Ευχαριστίες

Θεωρώντας την παρούσα διπλωματική εργασία το απόγειο των μεταπτυχιακών μου σπουδών στο Τμήμα Πολιτικών Επιστημών και Διεθνών Σχέσεων του Πανεπιστημίου Πελοποννήσου αισθάνομαι την ανάγκη να ευχαριστήσω όλους όσους συνέβαλαν στην ολοκλήρωσή της.

Αρχικά, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή της εργασίας, Επίκουρο Καθηγητή Ιωάννη Κωνσταντόπουλο για τον χρόνο που διέθεσε και την άμεση και ουσιαστική υποστήριξη την οποία παρείχε καθ' όλη τη διάρκεια της έρευνας και της συγγραφής της με τις πολύτιμες συμβουλές, τις εύστοχες παρατηρήσεις και το άριστο κλίμα συνεργασίας μας.

Επιπλέον, θα ήθελα να ευχαριστήσω τα υπόλοιπα μέλη της τριμελούς επιτροπής για την συμβολή τους στην περάτωση της παρούσης διπλωματικής εργασίας και για τις πολύτιμες γνώσεις τις οποίες μου μεταλαμπάδευσαν κατά τη διάρκεια των σπουδών μου.

Τέλος, οφείλω ένα μεγάλο ευχαριστώ στην οικογένειά μου για τη στήριξη και τη διαχρονική συμπαράστασή τους σε κάθε στάδιο της ζωής μου.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Γραφημάτων – Διαγραμμάτων-Εικόνων

1. Εισαγωγή

Η βιομηχανική κατασκοπεία αποτελεί έναν κίνδυνο τον οποίο βιώνουν καθημερινά, εν αγνοία τους ή μη, όλες οι επιχειρήσεις και οι οργανισμοί. Τα περιστατικά που αποκαλύπτονται αποδεικνύουν πως τα κίνητρα, οι μέθοδοι και τα αποτελέσματα αυτής της παράνομης δραστηριότητας ποικίλλουν και είναι όλο και δυσκολότερος ο έγκαιρος εντοπισμός τους.

Παρόλο που η εξέλιξη της τεχνολογίας παρέχει τη δυνατότητα υποκλοπής επιχειρηματικών μυστικών μέσω κυβερνο-επιθέσεων στα συστήματα ασφαλείας, από τα περιστατικά που έρχονται στο φως, είναι προφανές πως οι «φυσικές» επιθέσεις οι οποίες πραγματοποιούνται από εσωτερικούς και εξωτερικούς δρώντες μίας επιχείρησης είναι αναρίθμητες. Άλλωστε, και για την διεξαγωγή μίας κυβερνο-επίθεσης ο ανθρώπινος παράγοντας αποτελεί τον κινητήριο μοχλό καθώς και τον αποδέκτη του οφέλους από την εκμετάλλευση των κεκτημένων μυστικών.

Η συλλογή των στοιχείων τα οποία χρησιμοποιήθηκαν έγινε βάσει της υφιστάμενης ελληνόγλωσσης και ξενόγλωσσης βιβλιογραφίας η οποία περιλαμβάνει βιβλία, άρθρα σε έντυπο και ηλεκτρονικό τύπο και παλαιότερες σχετικές εκθέσεις και έρευνες. Παρότι ο κίνδυνος της βιομηχανικής κατασκοπείας υπήρχε ανέκαθεν και έχει μελετηθεί τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο στο παρελθόν, όλα τα σχέδια χειρισμού και αντιμετώπισής του αφορούν την «παθητική» ασφάλεια των επιχειρήσεων. Τα σχέδια αυτά περιλαμβάνουν ενέργειες πρόληψης και διαδικασίες με στόχο την προστασία των πολύτιμων αγαθών και πληροφοριών μίας επιχείρησης.

Σκοπός της παρούσας διπλωματικής εργασίας είναι η ανάδειξη επιπλέον μεθόδων «ενεργητικής» ασφάλειας, οι οποίες περιλαμβάνουν τρόπους εντοπισμού πιθανών μελλοντικών κατασκόπων και πρακτικών άσκησης βιομηχανικής κατασκοπείας για την καλύτερη προετοιμασία και τη μείωση όσο το δυνατόν περισσότερο των επιπτώσεων και των χαμένων στοιχείων αξίας. Η παρούσα διπλωματική εργασία βασίζεται στο πρότυπο διαχείρισης κινδύνου ISO 31000:2009, με τίτλο "Risk management – Principles and guidelines", το οποίο χρησιμοποιείται ως οδηγός για τον κατάλληλο χειρισμό του κινδύνου της βιομηχανικής κατασκοπείας με στόχο τη δημιουργία ενός πλαισίου αναγνώρισης και πρόληψης των ενδεχόμενων περιστατικών.

Το δεύτερο κεφάλαιο περιλαμβάνει μία σύντομη παρουσίαση του προτύπου ISO 31000:2009 το οποίο παρέχει τις αρχές, το πλαίσιο και τη διαδικασία που μπορεί να ακολουθήσει μία επιχείρηση για την οργανωμένη διαχείριση κινδύνων. Με βάση το ISO 31000:2009

διαρθρώνεται η δομή της παρούσης διπλωματικής εργασίας στην οποία μελετάται η επίδραση του ανθρώπινου παράγοντα στον κίνδυνο της βιομηχανικής κατασκοπείας.

Στο τρίτο κεφάλαιο γίνεται ο προσδιορισμός του κινδύνου της βιομηχανικής κατασκοπείας και εξετάζεται η σχέση του με παρεμφερείς όρους με τους οποίους συχνά συγχέεται. Επίσης, εκτελείται η αναγνώρισή του και παρουσιάζονται οι εμπλεκόμενοι δρώντες, τα κίνητρα και οι παράγοντες που συμβάλλουν στην επιδείνωσή του.

Το τέταρτο κεφάλαιο περιλαμβάνει την ανάλυση και την εκτίμηση του κινδύνου. Όσον αφορά την ανάλυση, αναφέρονται οι κύριες πρακτικές άσκησης κατασκοπείας, και τα είδη των απειλών που την απαρτίζουν. Οι απειλές αυτές είναι οι εξωτερικοί δρώντες, δηλαδή κατάσκοποι εκτός της επιχείρησης, οι εσωτερικοί δρώντες, δηλαδή εργαζόμενοι και συνεργάτες της επιχείρησης, αλλά και η απειλή της μεθόδου της κοινωνικής μηχανικής με την οποία οι εξωτερικοί δρώντες εκμεταλλεύονται τους εσωτερικούς για την απόκτηση σημαντικών επουσιωδών πληροφοριών. Στο στάδιο της εκτίμησης του κινδύνου, παρουσιάζονται αφενός στοιχεία από μελέτες σχετικά με την οικονομική ζημία που επιφέρει η βιομηχανική κατασκοπεία στις επιχειρήσεις και τα κράτη και αφετέρου προτείνονται δύο μαθηματικές σχέσεις με τις οποίες είναι δυνατή η ταξινόμηση του βαθμού των κινδύνων που διατρέχει κάθε επιχείρηση αναλόγως των μεθόδων που χρησιμοποιούνται, της συχνότητας/πιθανότητας εμφάνισής τους και του αντίκτυπού τους.

Στο πέμπτο κεφάλαιο, περιέχονται οι απαραίτητες ενέργειες χειρισμού που πρέπει να εκτελέσει κάθε επιχείρηση για να μειώσει την πιθανότητα άσκησης βιομηχανικής κατασκοπείας εις βάρος της. Οι ενέργειες αυτές περιλαμβάνουν την θέσπιση του κατάλληλου κατά περίπτωση σχεδίου με προγράμματα εκπαίδευσης, τυποποιημένες διαδικασίες ασφαλείας και εναλλακτικούς τρόπους αποτροπής της κατασκοπείας με βάση το υπάρχον νομικό πλαίσιο.

Το έκτο κεφάλαιο αναφέρεται στην παρακολούθηση της διαδικασίας και την επικοινωνία μεταξύ των στελεχών μίας επιχείρησης σε όλα τα στάδια της διαχείρισης κινδύνων αδιάκοπα και καθολικά. Για το λόγο αυτό, παρουσιάζεται ένας πίνακας με προκαθορισμένους δείκτες ανάλυσης επιθέσεων οι οποίοι στοχεύουν στην πρόβλεψη και την αναγνώριση μίας πιθανής εσωτερικής απειλής. Επιπρόσθετα, χρησιμοποιείται η Διαδικασία Αναλυτικής Ιεράρχησης ως μέθοδος εντοπισμού ενός εν δυνάμει κατασκόπου αναλόγως των προσωπικών και επαγγελματικών χαρακτηριστικών των εργαζομένων και των συνεργατών μίας επιχείρησης. Τέλος, στο πλαίσιο της επικοινωνίας του κινδύνου της βιομηχανικής κατασκοπείας, παρέχονται δύο πίνακες αυτοαξιολόγησης όσον αφορά την ανάπτυξη, την ωριμότητα, την ενσωμάτωση και την εφαρμογή των προτύπων διαχείρισης κινδύνων στο σύνολο μίας επιχείρησης.

Εν κατακλείδι στο έβδομο κεφάλαιο, περιλαμβάνονται τα συμπεράσματα που εξήχθησαν από τη μελέτη της επίδρασης του ανθρώπινου παράγοντα στο φαινόμενο της βιομηχανικής κατασκοπείας και οι προοπτικές περαιτέρω διερεύνησης των μεθόδων ανάλυσης και διαχείρισής της.

2. Το Πρότυπο ISO 31000:2009

Η διαχείριση κινδύνου αποτελείται από δύο βασικές έννοιες:

- Τον κίνδυνο, δηλαδή την κατάσταση στην οποία ένα άτομο βρίσκεται εκτεθειμένο στην πιθανότητα μίας κακής έκβασης.

- Τη διαχείριση (του) κινδύνου, δηλαδή την ανάληψη ηθελημένης δράσης προκειμένου να μεταβληθούν οι πιθανότητες προς όφελος του -αυξάνοντας τις πιθανότητες καλών εκβάσεων και μειώνοντας τις πιθανότητες κακών εκβάσεων.

Παρότι όλοι οι οργανισμοί διαχειρίζονται τον κίνδυνο έως ένα βαθμό, το Διεθνές Πρότυπο ISO 31000:2009 καθορίζει ένα σύνολο από αρχές που πρέπει να λαμβάνονται υπόψη ώστε να καταστεί αποτελεσματική η διαχείριση του κινδύνου. Πιο συγκεκριμένα η διαχείριση κινδύνου: (International Organization for Standardization, 2009, σσ. 7-8)

- Δημιουργεί και προστατεύει τα στοιχεία αξίας, διότι συμβάλλει στην αποδεδειγμένη επίτευξη των στόχων του.

- Αποτελεί αναπόσπαστο κομμάτι όλων των διαδικασιών οργάνωσης και δεν είναι μία αυτόνομη δραστηριότητα, ξεχωριστή από τις κύριες δραστηριότητες και τις διαδικασίες του οργανισμού.

- Αποτελεί μέρος της διαδικασίας λήψης αποφάσεων, καθώς βοηθά τους αρμόδιους να κάνουν ενημερωμένες επιλογές, να δίνουν προτεραιότητα σε δράσεις και να κάνουν διάκριση μεταξύ των εναλλακτικών τρόπων δράσης.

- Αντιμετωπίζει ρητά την αβεβαιότητα, τη φύση της και τον τρόπο με τον οποίο μπορεί να αντιμετωπιστεί.

- Είναι συστημική, δομημένη και έγκαιρη και έτσι συμβάλλει στην αποτελεσματικότητα και σε συνεπή, συγκρίσιμα και αξιόπιστα αποτελέσματα.

- Βασίζεται στις βέλτιστες διατιθέμενες πληροφορίες.

- Είναι προσαρμοσμένη και ευθυγραμμίζεται με το εξωτερικό και το εσωτερικό πλαίσιο του οργανισμού και το προφίλ κάθε κινδύνου.

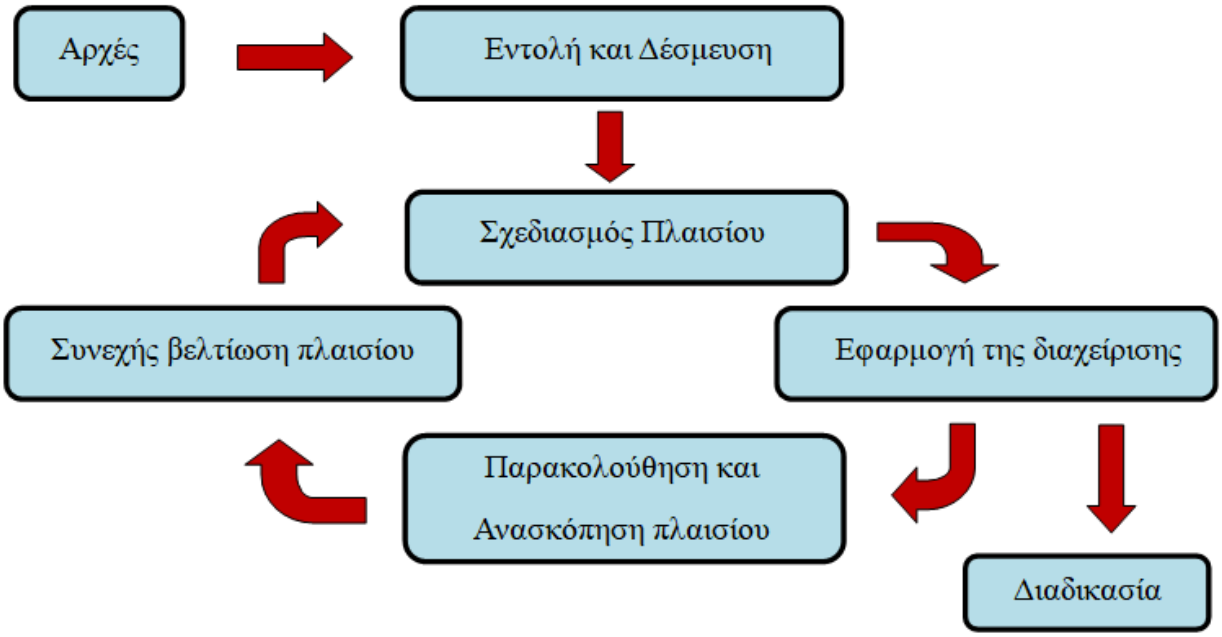
- Λαμβάνει υπόψη τους ανθρώπινους και πολιτισμικούς παράγοντες, καθώς αναγνωρίζει τις δυνατότητες, τις αντιλήψεις και τις προθέσεις των εξωτερικών και εσωτερικών ανθρώπων που μπορούν να διευκολύνουν ή να παρεμποδίσουν την επίτευξη των στόχων του οργανισμού.

- Είναι διαφανής και χωρίς αποκλεισμούς.

- Είναι δυναμική, επαναληπτική και ανταποκρίνεται στην αλλαγή.

- Διευκολύνει τη συνεχή βελτίωση του οργανισμού.

Το πρότυπο ISO 31000:2009 συστήνει στους οργανισμούς να αναπτύξουν, να εφαρμόσουν και να βελτιώνουν συνεχώς ένα πλαίσιο του οποίου ο στόχος είναι να ενσωματωθεί η διαδικασία διαχείρισης κινδύνου στη γενική διακυβέρνηση, στη στρατηγική, στο σχεδιασμό, στη διαχείριση, στις διαδικασίες αναφοράς, στις πολιτικές, στις αξίες και στον πολιτισμό τους. Η διαχείριση κινδύνων μπορεί να εφαρμοστεί σε ολόκληρο τον οργανισμό, σε πολλούς τομείς και επίπεδα, ανά πάσα στιγμή, καθώς και σε συγκεκριμένες λειτουργίες, έργα και δραστηριότητες. Το πλαίσιο αυτό περιλαμβάνει:

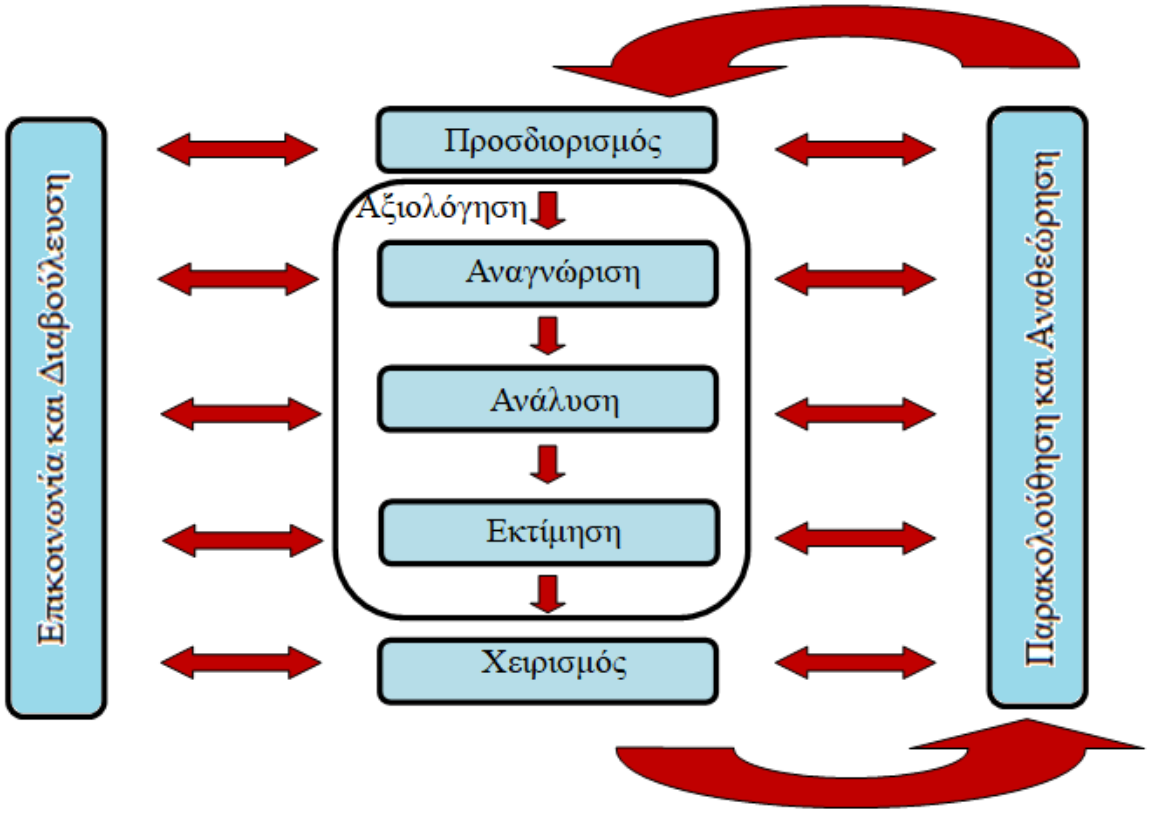


Διάγραμμα 1. Πλαίσιο Διαχείρισης Κινδύνων ISO 31000:2009 (Πηγή ISO, 2009:9)

Η εισαγωγή της διαχείρισης κινδύνων και η εξασφάλιση της διαρκούς αποτελεσματικότητάς της απαιτεί ισχυρή και συνεχή δέσμευση από τη διοίκηση του οργανισμού καθώς και αυστηρό στρατηγικό σχεδιασμό για την επίτευξή της σε όλα τα επίπεδα. Πριν ξεκινήσει ο σχεδιασμός και η εφαρμογή του πλαισίου διαχείρισης κινδύνων, είναι σημαντικό να αξιολογηθεί και να κατανοηθεί τόσο το εξωτερικό όσο και το εσωτερικό περιεχόμενο του οργανισμού, καθώς μπορεί να επηρεάσουν σημαντικά το σχεδιασμό του. Η πολιτική διαχείρισης των κινδύνων

πρέπει να αναφέρει σαφώς τους στόχους του οργανισμού και τη δέσμευσή του. Ο οργανισμός πρέπει να διασφαλίζει ότι υπάρχει υπευθυνότητα, εξουσία και κατάλληλη ικανότητα διαχείρισης της επικινδυνότητας, συμπεριλαμβανομένης της εφαρμογής και διατήρησης της διαδικασίας διαχείρισης κινδύνων και της διασφάλισης της επάρκειας, της αποτελεσματικότητας και της απόδοσης των ελέγχων. Με βάση τα αποτελέσματα της παρακολούθησης και της ανασκόπησης, πρέπει να λαμβάνονται αποφάσεις σχετικά με τον τρόπο βελτίωσης του πλαισίου, της πολιτικής και του σχεδίου διαχείρισης του κινδύνων. Αυτές οι αποφάσεις θα πρέπει να οδηγούν σε βελτιώσεις στην κουλτούρα και στη διαχείριση των κινδύνων από τον οργανισμό. (International Organization for Standardization, 2009, σσ. 9-13)

Με βάση το ανωτέρω πλαίσιο καθορίζεται η διαδικασία διαχείρισης κινδύνων η οποία περιλαμβάνει τα ακόλουθα επίπεδα:



Διάγραμμα 2. Διαδικασία Διαχείρισης Κινδύνων ISO 31000:2009 (Πηγή ISO, 2009:14)

Μακροπρόθεσμα, η μόνη εναλλακτική στη διαχείριση κινδύνων είναι η διαχείριση κρίσεων και η διαχείριση κρίσεων απαιτεί περισσότερα χρήματα, περισσότερο χρόνο και είναι πιο ντροπιαστική. (Lam, 2014, p. 3) Σε ένα κόσμο γεμάτο με συνεχείς αλλαγές, ο ρόλος της διαχείρισης κινδύνων είναι πιο σημαντικός από ποτέ. Και όταν πρόκειται για τη διαχείριση ενός κινδύνου που απειλεί την ύπαρξη μίας επιχείρησης, είναι αυτονόητο ότι πρέπει να είμαστε όσο το δυνατό καλύτερα προετοιμασμένοι. (Miller, 2017)

3. Προσδιορισμός και Αναγνώριση Κινδύνου Βιομηχανικής Κατασκοπείας

3.1 Προσδιορισμός Κινδύνου Βιομηχανικής Κατασκοπείας

Προσδιορίζοντας τους κινδύνους, ο οργανισμός καθορίζει τους στόχους του, τις στρατηγικές του, το πεδίο εφαρμογής και τις παραμέτρους των δραστηριοτήτων του. Η διαχείριση του κινδύνου πρέπει να γίνεται λαμβάνοντας πλήρως υπόψη την ανάγκη να δικαιολογούνται οι πόροι και να διευκρινιστούν οι ευθύνες, οι αρχές και τα αρχεία που πρέπει να τηρούνται. Το πλαίσιο της διαδικασίας διαχείρισης κινδύνων ποικίλει ανάλογα με τις ανάγκες ενός οργανισμού. Αν και τα όπλα και τα χρήματα θεωρούνται σημαντικοί παράγοντες για τη λειτουργία ενός σύγχρονου κόσμου, στο τέλος της ημέρας, αυτό που έχει πραγματική σημασία είναι ο έλεγχος και η αξιοποίηση των πληροφοριών για να αποκτηθεί πολιτικό, στρατιωτικό, οικονομικό και εμπορικό πλεονέκτημα. (Gupta & Sharma, 2009, σ. 18) Παρακολουθώντας την ανθρώπινη ιστορία είναι εύκολη η διαπίστωση πως η οικονομία είναι μια μορφή πολέμου, διότι όταν η αναζήτηση πόρων δεν παράγει ένοπλη βία, λαμβάνει άλλες μορφές, λιγότερο εμφανείς ή μετρήσιμες, πάντως εξίσου αποτελεσματικές. Μπορεί το οπλοστάσιο του οικονομικού πολέμου να μην περιλαμβάνει όλμους και τεθωρακισμένα και να μην πεθαίνουν με άμεσο τρόπο άνθρωποι, αλλά θύματα υπάρχουν: επιχειρήσεις καταστρέφονται, αυξάνεται η ανεργία και η φτώχεια και η κοινωνική συνοχή διαρρηγνύεται. Στην προσπάθεια ελέγχου των πλουτοπαραγωγικών πηγών κάθε μορφής, χρησιμοποιούνται άλλα μέσα: τεχνολογία, παραγωγικότητα, αλλά και η πληροφορία, η κατοχή και διαχείριση της οποίας είναι ουσιώδους σημασίας για την τελική επικράτηση. Στο πεδίο της οικονομίας οι όροι εχθρός και φίλος δεν έχουν αντίκρισμα: υπάρχουν ανταγωνιστές και στόχοι προς επίτευξη, αλλά και συμμαχίες λόγω αμοιβαίων συμφερόντων. Η ισχύς ανήκει σε αυτόν που, την κατάλληλη στιγμή, επιτυγχάνει να αποκτήσει, να αναλύσει και να ανασυνθέσει με τη μεγαλύτερη ταχύτητα δεδομένα και πληροφορίες που είναι διαθέσιμα στο ανταγωνιστικό περιβάλλον. Και η πληροφορία επιδιώκεται να αποκτηθεί με κάθε μέσο, θεμιτό και αθέμιτο. (Κάτσουρα, 2017)

3.1.1 Ορισμός Βιομηχανικής Κατασκοπείας

Ως κατασκοπεία ορίζεται η απόκτηση διαβαθμισμένων (απορρήτων ή εμπιστευτικών) πληροφοριών από μία κυβέρνηση, μία επιχείρηση, ένα ή περισσότερα φυσικά πρόσωπα, χωρίς την άδεια του κατόχου τους. Για την αποτελεσματική ενασχόληση με το φαινόμενο της

κατασκοπείας στον επιχειρηματικό κόσμο, είναι σημαντική η κατανόηση της σχετικής ορολογίας. Υπάρχουν πέντε όροι οι οποίοι χρησιμοποιούνται για να περιγράψουν την ίδια γενική επιχειρηματική απειλή αλλά έχουν σαφείς διαφορές μεταξύ τους.

- Επιχειρηματική κατασκοπεία
- Εταιρική κατασκοπεία
- Βιομηχανική κατασκοπεία
- Εμπορική κατασκοπεία
- Οικονομική κατασκοπεία

Οι όροι της εταιρικής και βιομηχανικής κατασκοπείας χρησιμοποιούνται πιο συχνά για κατασκοπεία μεταξύ ανταγωνιστικών επιχειρήσεων ενός κράτους. Ο όρος της οικονομικής κατασκοπείας χρησιμοποιείται για τη διάκριση της κυβερνητικής/ στρατιωτικής κατασκοπείας μέσω των κρατικών Υπηρεσιών Πληροφοριών. Ωστόσο, σε μια όλο και πιο παγκόσμια οικονομία η διάκριση μεταξύ εσωτερικού και εξωτερικού εμπορίου είναι δύσκολη και επειδή οι επιχειρηματικές τεχνολογίες μπορεί να έχουν και στρατιωτικές εφαρμογές ή επειδή κάποιες κυβερνήσεις κατέχουν ή ελέγχουν επιχειρήσεις, η διάκριση δεν είναι πάντα σαφής. Για το λόγο αυτό χρησιμοποιείται συχνά ο όρος επιχειρηματική κατασκοπεία ο οποίος μπορεί να περιλαμβάνει όλους τους ανωτέρω. (Wimmer, 2015, σ. xiv) Γενικότερα, ο όρος βιομηχανική κατασκοπεία έχει επικρατήσει έναντι του όρου εταιρική κατασκοπεία διότι ασκείται κυρίως στον κλάδο της βαριάς βιομηχανίας και της βιομηχανίας υψηλής τεχνολογίας όπως εταιρίες που έχουν ως αντικείμενο τα λογισμικά και υλικά ηλεκτρονικών υπολογιστών, τη βιοτεχνολογία, τις τηλεπικοινωνίες, την ενέργεια, την τεχνολογία υλικών, οχημάτων και ειδικών εργαλείων.

Πιο συγκεκριμένα η βιομηχανική κατασκοπεία αφορά την αναζήτηση, απόκτηση και μετάδοση μέσω μυστικών μέσων ή ψευδών προσχημάτων βιομηχανικών ή εμπορικών πληροφοριών για βιομηχανικούς, εμπορικούς, πολιτικούς ή ανατρεπτικούς σκοπούς. (Heims, 1982, σ. 4)

Η βιομηχανική κατασκοπεία ορίζεται ως η παράνομη κλοπή/απόκτηση πνευματικής ιδιοκτησίας, όπως σημαντικά εμπορικά μυστικά, πληροφορίες για ευρεσιτεχνίες καθώς και βιομηχανικές τεχνικές, διαδικασίες, ιδέες και τύπους. Ή μπορεί να περιλαμβάνει τη δέσμευση ιδιοκτησιακών ή επιχειρησιακών πληροφοριών, όπως δεδομένα σχετικά με τα στοιχεία πελατών, πωλήσεων, τιμολογίων, έρευνας και ανάπτυξης, πολιτικών, προοπτικών προσφορών, στρατηγικών σχεδιασμού ή μάρκετινγκ ή μεταβαλλόμενων συνθέσεων προσωπικού και θέσεων παραγωγής. Βασικά, μπορεί να περιλαμβάνει οτιδήποτε δίνει στην επιχείρησή ένα πλεονέκτημα στην αγορά και που την κάνει επιτυχημένη. (Dodge, 2014)

Για τους σκοπούς αυτής της εργασίας θα χρησιμοποιείται ο όρος βιομηχανική κατασκοπεία καθώς η έρευνα η οποία πραγματοποιήθηκε αφορά τη διαχείριση του κινδύνου της υποκλοπής εμπορικών μυστικών από ανταγωνιστικές επιχειρήσεις και την επίδραση του ανθρώπινου παράγοντα σε αυτή.

3.1.2 Βιομηχανική Κατασκοπεία και Ανταγωνιστική Ευφυΐα

Το 90% των πληροφοριών είναι ελεύθερο για όλους: στις βάσεις δεδομένων, στα ΜΜΕ, στα εξειδικευμένα έντυπα κάθε κατηγορίας, σε επιμελητήρια και, φυσικά, στο διαδίκτυο. Ωστόσο, το σημαντικό υπόλοιπο 10%, τα ευαίσθητα και εξαιρετικής σπουδαιότητας δεδομένα, το κρατούν πηγές στις οποίες η πρόσβαση είναι πολύ δύσκολη και για την απόκτησή τους μπορεί να απαιτηθούν μέσα ανήθικα, ακόμη και παράνομα. (Κάτσουρα, 2017)

Είναι απαραίτητο να μην γίνεται σύγχυση μεταξύ των εννοιών της επιχειρηματικής ευφυΐας και της βιομηχανικής κατασκοπείας. Η διαφορά μεταξύ τους είναι πως η πρώτη αφορά την ανάλυση, οργάνωση και διανομή νόμιμων και διαθέσιμων πληροφοριών που είναι χρήσιμες στους υπευθύνους για την χάραξη πολιτικής μίας εταιρίας. Αντιθέτως, η βιομηχανική κατασκοπεία αφορά την κλοπή μυστικών. (Samli & Jacobs, 2003, σ. 97)

Ο ανταγωνισμός μεταξύ ανθρώπων που ασκούν το ίδιο επάγγελμα είναι απαραίτητος, αναπόφευκτος και καθ' όλα νόμιμος. Συνεπώς, η προσπάθεια για να παραμείνουν ενημερωμένοι όσον αφορά τις τεχνολογικές και οργανωτικές καινοτομίες αποτελεί ίσως το σημαντικότερο μέσο για την επιβίωσή τους. Η προσπάθεια αυτή αφορά την ανταγωνιστική ευφυΐα (ή ανταγωνιστική πληροφόρηση) και περιλαμβάνει τη συλλογή και την κατάλληλη ερμηνεία δεδομένων και πληροφοριών από διάφορες «ανοικτές» πηγές. Υπάρχουν αμέτρητες πηγές νόμιμων πληροφοριών διαθέσιμων σε επιχειρήσεις που επιθυμούν να παραμείνουν ενημερωμένες σχετικά με τις μεταβαλλόμενες κοινωνικές τάσεις, τις εξελίξεις στις αγορές, τους νόμους, τις εθνικές και πολιτικές αλλαγές, τις εργασιακές συνθήκες και τις εταιρικές συμφωνίες που επηρεάζουν το έργο τους και τις σχέσεις τους με τους εργαζομένους. (Heims, 1982, σ. 14)

Η ανταγωνιστική ευφυΐα είναι ένα συστηματικό και ηθικό πρόγραμμα για τη συλλογή, ανάλυση και διαχείριση πληροφοριών που μπορούν να επηρεάσουν τα σχέδια, τις αποφάσεις και τις λειτουργίες μιας επιχείρησης. Μετά τη συλλογή και ανάλυση αυτών των πληροφοριών, είναι εφικτή η κατανόηση ενός ανταγωνιστή, του περιβάλλοντος, των στρατηγικών, των δυνατοτήτων, των λειτουργιών, καθώς και των μακροπρόθεσμων στόχων του. Η ανταγωνιστική ευφυΐα αποτελείται από δύο όψεις. Η πρώτη είναι η χρήση δημόσιων πηγών για την ανάπτυξη δεδομένων σχετικά με τον ανταγωνισμό, τους ανταγωνιστές και το περιβάλλον της αγοράς. Η δεύτερη είναι η μετατροπή αυτών των δεδομένων σε πληροφορίες για την υποστήριξη των επιχειρησιακών αποφάσεων. (Nasheri, 2005, σ. 73)

Η ανταγωνιστική ευφυΐα συνδέεται στενά με τη στρατηγική διαδικασία λήψης αποφάσεων, υποστηρίζοντας μια βιώσιμη εξέλιξη της εταιρείας σε ένα μεταβαλλόμενο επιχειρηματικό περιβάλλον και δημιουργεί προστιθέμενη αξία χρησιμοποιώντας τη συλλογή άυλων περιουσιακών στοιχείων. Αντίθετα, η βιομηχανική κατασκοπεία ορίζεται ως μια ανήθικη και συνεχής αναζήτηση οποιωνδήποτε στοιχείων που μπορούν να χρησιμοποιηθούν είτε για να συνθέσουν μια μεγαλύτερη εικόνα για έναν ανταγωνιστή είτε για εκβιαστικούς σκοπούς. Η απόκτηση και διατήρηση ενός πλεονεκτήματος σε σχέση με τον ανταγωνισμό είναι ο κοινός στόχος που έχουν τόσο η κατασκοπεία όσο και η ανταγωνιστική ευφυΐα. Ωστόσο, μέσω των μεθόδων ανάλυσης, η δεύτερη είναι σε θέση να δημιουργήσει ένα σταθερό περιβάλλον για τη

διαδικασία λήψης αποφάσεων. Η κατασκοπεία, ακόμη και αν παρέχει χρήσιμες πληροφορίες, δεν βοηθά την εταιρεία να δημιουργήσει γνώσεις, είναι χρήσιμη μόνο βραχυπρόθεσμα. (Colibasanu, 2009)

Το φάσμα των δραστηριοτήτων που αναφέρονται ως κατασκοπεία είναι ευρύ. Κυμαίνεται από τη χρήση των ματιών και των αυτιών του ατόμου ενώ ασχολείται με ανοικτές και νόμιμες δραστηριότητες έως και κλασικές κρυφές επιχειρήσεις κατασκοπείας που διεξάγονται με παράνομα μέσα. Η νόμιμη μορφή κατασκοπείας έχει προκαλέσει επιτάχυνση της επιχειρηματικής ευφυΐας. Περιλαμβάνει την εξέταση διαθέσιμων στο κοινό πληροφοριών, όπως δικαστικών αρχείων, ετήσιων εταιρικών εκθέσεων, κυβερνητικών εγγράφων, εκθέσεων αγοράς, εμπορικών εκθέσεων, ομιλιών εταιρικών στελεχών και εκθέσεων εκπροσώπων πωλήσεων. Αντιθέτως, οι δραστηριότητες βιομηχανικής κατασκοπείας είναι ανήθικες και συχνά παράνομες. Αυτές οι δραστηριότητες περιλαμβάνουν τη δωροδοκία ανταγωνιστών για μυστικές τεχνικές λειτουργίες, την πρόσληψη υπαλλήλων για την απόκτηση ανταγωνιστικών πληροφοριών όπως διαδικασίες ή πληροφορίες μάρκετινγκ, την υποκλοπή επικοινωνιών και τους εκβιασμούς πολύτιμων υπαλλήλων. (Samli & Jacobs, 2003, σ. 97)

3.2 Αναγνώριση Κινδύνου Βιομηχανικής Κατασκοπείας

Ως αξιολόγηση κινδύνου ορίζεται η συνολική διαδικασία αναγνώρισης, ανάλυσης και εκτίμησής του. Η αναγνώριση κινδύνου περιλαμβάνει τον καθορισμό των πηγών κινδύνου, των σημείων των επιπτώσεων, τα γεγονότα (συμπεριλαμβανομένων των αλλαγών των περιστάσεων), τις αιτίες και τις ενδεχόμενες συνέπειές τους. Στόχος αυτού του βήματος είναι η δημιουργία ενός εκτενή καταλόγου των κινδύνων βασισμένο στα γεγονότα που ενδέχεται να δημιουργήσουν, να ενισχύσουν, να αποτρέψουν, να υποβαθμίσουν, να επιταχύνουν ή να καθυστερήσουν την επίτευξη των στόχων της επιχείρησης. (International Organization for Standardization, 2009, σ. 17).

Το βήμα αυτό είναι πολύ σημαντικό καθώς σε περίπτωση που ένας κίνδυνος δεν ληφθεί υπόψη, δεν θα περιλαμβάνεται και στην ακόλουθη ανάλυσή του. Για το λόγο αυτό, κάθε επιχείρηση πρέπει να χρησιμοποιεί τα κατάλληλα εργαλεία και τις αποτελεσματικότερες τακτικές εντοπισμού των ενδεχόμενων κινδύνων που να ανταποκρίνονται στους στόχους και στις ικανότητες της. Η αναγνώριση πρέπει να περιλαμβάνει κινδύνους ανεξάρτητα από το εάν η πηγή τους βρίσκεται υπό τον έλεγχο της επιχείρησης ή ενδέχεται να μην είναι εμφανής.

Υπάρχουν γενικά δύο είδη ευαίσθητων επιχειρηματικών πληροφοριών. Το ένα είναι η πνευματική ιδιοκτησία, η οποία αποτελείται από ιδέες, έννοιες και εφευρέσεις, συμπεριλαμβανομένων των συνταγών ή τύπων των προϊόντων. Το δεύτερο είναι οι πληροφορίες λειτουργίας, όπως τα λεπτομερή στοιχεία παραγωγής και εμπορίας, συμπεριλαμβανομένων στοιχείων όπως ο όγκος παραγωγής μιας συγκεκριμένης μονάδας παραγωγής, το μερίδιο αγοράς της, οι μεταβαλλόμενες συνθέσεις και οι θέσεις παραγωγής της. (Nasheri, 2005, σ. 73)

3.2.1 Εμπλεκόμενοι Δρώντες

Τα άτομα τα οποία προβαίνουν σε ενέργειες βιομηχανικής κατασκοπείας ανήκουν ως επί το πλείστον σε δύο βασικές κατηγορίες οι οποίες είναι και οι πηγές του κινδύνου. Ο διαχωρισμός στις κατηγορίες αυτές γίνεται λαμβάνοντας υπόψη τη σχέση που τα συνδέει με την επιχείρηση, της οποίας τα μυστικά επιθυμούν να υποκλέψουν και την αρχική πρόθεση που έχουν πριν προβούν στις ενέργειες αυτές. Οι δύο αυτές κατηγορίες είναι οι εσωτερικοί κατάσκοποι και οι εξωτερικοί κατάσκοποι. Ως εσωτερικοί ορίζονται οι κατάσκοποι οι οποίοι εργάζονται ή αποτελούν γενικότερα μέρος της επιχείρησης και καταλήγουν να υποκλέπτουν τα μυστικά της ανεξαρτήτως των κινήτρων τους. Αντίθετα, ως εξωτερικοί κατάσκοποι ορίζονται τα άτομα τα οποία υποκλέπτουν μία επιχείρηση χωρίς να αποτελούν μέρος αυτής ή να έχουν άμεση πρόσβαση στα μυστικά της. Είναι σημαντικό για τις επιχειρήσεις να κατανοούν τις πιθανές απειλές και το πώς μπορεί να προσπαθούν να διεξάγουν κατασκοπεία εναντίον τους. Οι απειλές αυτές είναι οι παρακάτω:

Πίνακας 1. Κατηγορίες και απειλές βιομηχανικής κατασκοπείας (Βασισμένο στο Dodge, 2014)

Κατηγορία	**Απειλή**
Εξωτερική	Εμπορικοί Ανταγωνιστές
	Εγκληματικές Οργανώσεις
	Κρατικές Υπηρεσίες Πληροφοριών
Εσωτερική	Εσωτερικοί δρώντες με πρόσβαση
	Ακούσια Αποκάλυψη

3.2.2 Κίνητρα Άσκησης Βιομηχανικής Κατασκοπείας

Σε κάθε περιστατικό βιομηχανικής κατασκοπείας οι παράγοντες οι οποίοι συμβάλλουν στην επιτυχή επίτευξη της είναι: (Benny, 2014, σσ. 8-10)

- Κίνητρο : Προκειμένου να αντιμετωπιστεί με επιτυχία η βιομηχανική κατασκοπεία, είναι σημαντικό να κατανοήσουμε τα κίνητρα των ατόμων που συμμετέχουν σε μία τέτοια παραπλανητική και εγκληματική δραστηριότητα.

- Ευκαιρία : Ως ευκαιρία θεωρείται η κατάσταση στην οποία ένα άτομο έχει πρόσβαση σε προστατευμένες πληροφορίες και αισθάνεται ότι υπάρχει η δυνατότητα να τις υποκλέψει ή να τις αναπαράγει χωρίς να γίνει αντιληπτό και χωρίς συνέπειες.

- Ορθολογισμός : Ο ορθολογισμός είναι η ικανότητα του δράστη να δικαιολογεί στον εαυτό του ότι η βιομηχανική κατασκοπεία δεν είναι λανθασμένη. Αυτή η δικαιολόγηση μπορεί να τον οδηγήσει στο συμπέρασμα ότι είναι για ένα καλό σκοπό

επειδή υποστηρίζει τις πολιτικές ή ιδεολογικές του απόψεις.

- Ικανότητα : Αφορά την ικανότητα του δράστη να ξεπεράσει τις αναστολές του και να βάλει στην άκρη τις ηθικές του αξίες, την εμπιστοσύνη και το φόβο μήπως αποκαλυφθεί.

- Έναυσμα : Ως έναυσμα θεωρείται η βαθύτερη αιτία για την οποία ένα άτομο διαπράττει βιομηχανική κατασκοπεία, όπως η ανάγκη για ένα ακριβό τρόπο ζωής, ο εθισμός στα ναρκωτικά, η πίεση λόγω εκβιασμού ή συμμετοχής σε εγκληματική οργάνωση.

Είναι προφανές πως το πνευματικό κεφάλαιο μίας επιχείρησης αποτελεί το στοιχεί-κλειδί για την ενίσχυση του ανταγωνιστικού πλεονεκτήματός της. Ωστόσο, η σταθερά αυξανόμενη αξία των εμπορικών μυστικών και η διάδοση της τεχνολογίας σε ολόκληρο τον πλανήτη συμβάλλουν σημαντικά στην αύξηση τόσο των ευκαιριών όσο και των κινήτρων για την άσκηση βιομηχανικής κατασκοπείας. (Samli & Jacobs, 2003)

Τα κίνητρα στα οποία οφείλεται το φαινόμενο της βιομηχανικής κατασκοπείας διαφέρουν ανά περίπτωση και μπορεί να είναι είτε προσωπικά, με την έννοια της απόκτησης προσωπικού οφέλους από ένα συγκεκριμένο άτομο, είτε επαγγελματικά με την έννοια της απόκτησης ή της αποκάλυψης του πλεονεκτήματος που προσδίδουν τα στοιχεία αξίας μίας επιχείρησης, είτε ιδεολογικά με την έννοια της διαφοροποίησης στις πολιτικές, στις πεποιθήσεις και στον τρόπο λειτουργίας της.

Πίνακας 2. Κίνητρα άσκησης βιομηχανικής κατασκοπείας

Κατηγορία	**Είδος Κινήτρου**	**Στόχος**
Προσωπικά	Προσωπικό Οικονομικό Όφελος	Οικονομικό κέρδος από την αποκάλυψη μυστικών σε ανταγωνιστές
	Εκδίκηση	Πλήγμα απέναντι σε συγκεκριμένο στέλεχος ή όλη την επιχείρηση
	Προσωπική ανέλιξη	Απόκτηση μίας νέας θέσης στην επιχείρηση που δέχεται τις κλεμμένες πληροφορίες
	Εγωισμός	Αίσθημα αύξησης της προσωπικής ισχύος
	Ψυχολογία	Φόβος λόγω εκβιασμού – Ερωτική αποπλάνηση
Επαγγελματικά	Οικονομική Ζημία στην Επιχείρηση	Ζημία λόγω της αναίρεσης του ανταγωνιστικού πλεονεκτήματος της επιχείρησης
	Παρενόχληση	Προσπάθεια αποπροσανατολισμού και δημιουργίας προβλημάτων στην επιχείρηση που υποκλέπτεται
	Δυσφήμηση	Αποκάλυψη επιχειρηματικών μηχανισμών και αδυναμίας της επιχείρησης να τα προστατεύσει
Πολιτικά	Ιδεολογία	Εναντίωση με την ιδεολογία και τον τρόπο λειτουργίας της επιχείρησης

Η βιομηχανική κατασκοπεία μεγαλώνει σε σκοπό, σε ποικιλομορφία θέματος και σε πολυπλοκότητα των μεθόδων και του εξοπλισμού που χρησιμοποιείται. (Heims, 1982, σ. 18). Καμία επιχείρηση δεν είναι απολύτως θωρακισμένη από τον κίνδυνο της βιομηχανικής κατασκοπείας. Αντιθέτως, γίνονται όλο και περισσότερο ευάλωτες για πολλούς λόγους. Στη σημερινή εποχή παρατηρείται επιδείνωση του προβλήματος της βιομηχανικής κατασκοπείας η οποία οφείλεται στους κάτωθι παράγοντες: (Androulidakis & Kioupakis, 2016, σ. 4)

Πίνακας 3. Παράγοντες επιδείνωσης βιομηχανικής κατασκοπείας (Βασισμένο στο Androulidakis & Kioupakis, 2016:4)

A/A	Παράγοντες
1	Υπάρχουν τεράστια ποσά που διακυβεύονται, ενώ οι μισθοί των εμπλεκόμενων ατόμων μπορεί να είναι το ίδιο υψηλοί. Σε περιόδους οικονομικής κρίσης που, μεταξύ άλλων, συμβαίνουν συγχωνεύσεις και εξαγορές, η αξία των πληροφοριών καθίσταται ακόμα πιο σημαντική.
2	Οι υπάλληλοι (και ιδιαίτερα οι διαχειριστές) των τμημάτων Πληροφορικής έχουν πρόσβαση σε συστήματα και servers που φιλοξενούν ευαίσθητες πληροφορίες, πηγαίο κώδικα, στοιχεία πιστωτικών καρτών, σχέδια κ.α.
3	Ακόμα χειρότερα, σε πολλές περιπτώσεις, οι εργαζόμενοι δεν ενημερώνονται για την κρισιμότητα των πληροφοριών που χειρίζονται, με αποτέλεσμα την ανεπαρκή προστασία του.
4	Υπάρχουν δεκάδες τρόποι με τους οποίος μπορεί να προκύψει διαρροή δεδομένων με τη χρήση αποθηκευτικών μέσων και υπηρεσιών δικτύου.
5	Η έλλειψη ασφάλειας σίγουρα καθιστά την κατάσταση χειρότερη, αλλά από την άλλη πλευρά, τα τεχνικά μέσα ασφαλείας μπορούν να χρησιμοποιηθούν υπερβολικά δημιουργώντας μία ψεύτικη αίσθηση ασφάλειας που με τη σειρά της μπορεί να οδηγήσει σε υπερβολική χαλάρωση.
6	Ταυτόχρονα, οι περιορισμοί που οφείλονται σε πολιτικές ασφαλείας παρεμποδίζουν την καθημερινή λειτουργία των εργαζομένων και για το λόγο αυτό είναι συνήθης πρακτική η μη τήρηση ή η υπέρβαση αυτών των περιορισμών.
7	Υπάρχουν επίσης περιπτώσεις ακούσιας αποκάλυψης ευαίσθητων πληροφοριών. Οι επιστήμονες κατά τις ομιλίες τους αποκαλύπτουν συχνά ευαίσθητες πληροφορίες λόγω του ενθουσιασμού τους, χωρίς πρόθεση να βλάψουν την επιχείρηση. Ακόμα και η ίδια η επιχείρηση μπορεί να κάνει παρόμοια λάθη προσπαθώντας να διαφημίσει ένα προϊόν με τον καλύτερο δυνατό τρόπο.
8	Το σύγχρονο επιχειρηματικό περιβάλλον υπαγορεύει τον περιορισμό του κόστους σε όλα τα επίπεδα. Οι πληροφορίες πρέπει να διαβιβάζονται γρήγορα μεταξύ των εταιριών και των εταίρων τους εντός και εκτός των κρατών, ευθυγραμμιζόμενες με τους γρήγορους ρυθμούς με τους οποίους λειτουργούν. Συνεπώς, η ασφαλής ανταλλαγή πληροφοριών έχει γίνει μία πολύ δύσκολη διαδικασία.
9	Παρομοίως, η ανάθεση συμβάσεων σε άλλες εταιρίες ειδικά εκτός Ευρώπης και ΗΠΑ δημιουργούν νέες απειλές.
10	Τα νέα προϊόντα και οι νέες τεχνολογίες δημιουργούν νέες απειλές. Οι μικρές επιχειρήσεις έρευνας και ανάπτυξης με υψηλό βαθμό καινοτομίας επικεντρώνονται κυρίως στην έρευνα, αγνοώντας ή μη προστατεύοντας την πνευματική τους ιδιοκτησία.

Η υποκλοπή των στοιχείων αξίας μίας επιχείρησης από μία άλλη ανταγωνιστική της, ισοσκελίζει το συγκριτικό πλεονέκτημα που έχει όσον αφορά αποκλειστικότητα της γνώσης. Συνεπώς, η επιχείρηση-αποδέκτης πληροφοριών βιομηχανικής κατασκοπείας, αποκτά έτοιμη τεχνογνωσία, εξοικονομώντας χρήματα έρευνας και ανάπτυξης νέων δικών της προϊόντων αλλά και το χρόνο που θα διέθετε.

4. Ανάλυση και Εκτίμηση Κινδύνου Βιομηχανικής Κατασκοπείας

Η διαδικασία ανάλυσης κινδύνων περιλαμβάνει την ανάπτυξη της κατανόησης των κινδύνων. Η ανάλυση παρέχει στοιχεία για την εκτίμηση των κινδύνων, για τις αποφάσεις σχετικά με την ανάγκη αντιμετώπισής τους και για τις κατάλληλες στρατηγικές και μεθόδους αντιμετώπισης. Η ανάλυση των κινδύνων μπορεί επίσης να συμβάλλει στη λήψη αποφάσεων όταν πρέπει να γίνουν επιλογές που περιλαμβάνουν διάφορους επιπλέον τύπους και επίπεδα κινδύνου. Η ανάλυση κινδύνων περιλαμβάνει την εξέταση των αιτιών και των πηγών κάθε κινδύνου, των θετικών και αρνητικών συνεπειών τους και την πιθανότητα να προκύψουν αυτές οι συνέπειες. Οι παράγοντες που επηρεάζουν τις συνέπειες και την πιθανότητα τους πρέπει να προσδιορίζονται. Κάθε κίνδυνος αναλύεται καθορίζοντας τις συνέπειες και την πιθανότητα του, και άλλα χαρακτηριστικά του. Ένα συμβάν μπορεί να έχει πολλαπλές συνέπειες και μπορεί να επηρεάσει πολλαπλούς στόχους. Επίσης, πρέπει να λαμβάνονται υπόψη οι δυνατότητες ελέγχου και η αποτελεσματικότητά τους. (International Organization for Standardization, 2009, σ. 18)

Ο 21^{ος} αιώνας έχει χαρακτηριστεί ως η εποχή της πληροφορίας. Η συνεχής ανάπτυξη της παγκόσμιας αγοράς έχει συμβάλλει στην είσοδο νέων πολιτισμών και οικονομιών στο παγκόσμιο ανταγωνιστικό σύστημα. Λόγω της διαθεσιμότητας υποδομών και της ανάπτυξης του τομέα των τηλεπικοινωνιών και των ηλεκτρονικών υπολογιστών, είναι δυνατός ο ανταγωνισμός σε επίπεδο ιδιωτών, επιχειρήσεων και κρατών σε ισότιμους όρους ανταγωνισμού ακόμα και από τα πιο απομακρυσμένα μέρη του κόσμου. Ωστόσο, η ανάπτυξη αυτή έχει δημιουργήσει ευνοϊκές συνθήκες για την εμφάνιση φαινομένων κλοπής πληροφοριών και βιομηχανικής κατασκοπείας.

Η κλοπή πληροφοριών είναι μία από τις παλαιότερες μορφές απόκτησης στρατηγικού και ανταγωνιστικού πλεονεκτήματος. Η κατασκοπεία συνέβαινε στο παρελθόν, συμβαίνει σήμερα και θα συμβαίνει και στο μέλλον. Το μόνο που αλλάζει είναι οι τεχνικές που εφαρμόζονται. (Podszywalow, 2012)

Οι περισσότερο παραδοσιακές μέθοδοι απόκτησης των μυστικών μίας επιχείρησης είναι η κρυφή είσοδος στις εγκαταστάσεις της επιχείρησης και η παρακολούθηση των εργαζομένων της όταν βρίσκονται εκτός αυτής. (Long, 2008)

Ωστόσο, οι δέκα κύριες πρακτικές διεθνούς κατασκοπείας της σύγχρονης εποχής φαίνονται στον κάτωθι Πίνακα 3: (Samli & Jacobs, 2003, σ. 102)

Πίνακας 4. Κύριες πρακτικές κατασκοπείας (Βασισμένο στο Samli & Jacobs, 2003:102)

Α/Α	ΕΝΕΡΓΕΙΑ	ΜΕΘΟΔΟΣ	ΑΠΟΤΕΛΕΣΜΑ
1	Έρευνα Απορριμμάτων	Αναζήτηση σε εταιρικά απορρίμματα για πληροφορίες	Απόκτηση πολλών εταιρικών τεχνικών μυστικών της επιχείρησης
2	Εξαγωγή	Συμμετοχή σε επιστημονικά σεμινάρια, εμπορικές εκθέσεις, τηλεφωνικές κλήσεις	Απόκτηση τμημάτων πληροφοριών σχετικά με νέες εξελίξεις
3	Ηλεκτρονική παρεμβολή	Εκτέλεση τηλεφωνικών παρεμβολών ή εισβολές σε υπολογιστές	Απόκτηση λεπτομερών πληροφοριών και μυστικών σχεδίων
4	Προδοσία εκ των έσω	Πράξεις κατασκοπείας από προσωπικό της επιχείρησης	Απόκτηση λεπτομερών πληροφοριών και μυστικών σχεδίων
5	Ανακοίνωση Προϊόντων	Ανίχνευση τεχνικών χαρακτηριστικών και διαθεσιμότητας νέων εξελίξεων	Αντιστάθμιση των καινοτομιών του ανταγωνιστή και προβάδισμα στην ανάπτυξη των προϊόντων
6	Αντίστροφη Μηχανική	Απόκτηση ενός δείγματος του προϊόντος, αποσυναρμολόγηση του και ανακατασκευή	Καθορισμός χαρακτηριστικών προϊόντος και παραγωγής
7	Επιχειρηματική Ευφυΐα	Χρήση πληροφοριών όπως θέσεις εργασίας, προμηθευτές, υπεργολάβους, τιμές, συγχωνεύσεις και οικονομικά αποτελέσματα.	Κατανόηση προθέσεων του ανταγωνιστή και ανίχνευση δυνατών σημείων και αδυναμιών
8	Πρόσληψη πληροφοριών-κλειδιά	Πρόσληψη ανώτερων στελεχών ανταγωνιστικών επιχειρήσεων	Μάθηση από πρώτο χέρι πώς ο ανταγωνιστής διαχειρίζεται την επιχείρηση
9	Αγωγές	Αγωγές που αφορούν προϊόντα και πατέντες	Απόκτηση πληροφοριών σχετικά με τα τεχνικά προϊόντα και τις εξελίξεις τους
10	Κατασκοπεία με Κυβερνητική Υποστήριξη	Χρήση κυβερνητικών οργανισμών για βιομηχανική κατασκοπεία	Πολύτιμες μυστικές πληροφορίες μπορούν να αποκτηθούν από ειδικά εκπαιδευμένα άτομα

4.1 Συνήθεις Απειλές

Το βασικό στοιχείο που αποτελεί οδηγό στην ανάλυση του κινδύνου της βιομηχανικής κατασκοπείας είναι η κατανόηση της διαφοροποίησης μεταξύ των πηγών της και των στόχων της. Οι δύο βασικές πηγές όπως αναφέρθηκε και ανωτέρω είναι οι εσωτερικοί και οι εξωτερικοί κατάσκοποι.

4.1.1 Εξωτερική Απειλή

Οι εξωτερικοί κατάσκοποι είναι άτομα τα οποία δεν αποτελούν μέρος της επιχείρησης και είτε με τη χρήση της τεχνολογίας είτε με μεθόδους παραπλάνησης των εργαζομένων της παραβιάζουν ή υποκλέπτουν τις δομές και τα συστήματά της.

Οι εξωτερικοί κατάσκοποι ακολουθούν συνήθως μία διαδικασία πέντε σταδίων ώστε να διεισδύσουν σε έναν οργανισμό. (Cole E., 2013)

1. Αναγνώριση : η εύρεση συνήθως δημόσιων πληροφοριών για την καλύτερη κατανόηση του τρόπου λειτουργίας ενός οργανισμού και τον εντοπισμό ανθρώπων ή ευάλωτων σημείων που μπορούν να χρησιμοποιηθούν για την επιτυχή εκμετάλλευσή τους.

2. Σάρωση : η ανίχνευση επιπλέον αδυναμιών που μπορεί να χρησιμοποιηθούν.

3. Εκμετάλλευση : η διαδικασία υποκλοπής πληροφοριών.

4. Δημιουργία σημείου πρόσβασης : η δημιουργία ενός σημείου εύκολης εισόδου και εξόδου από το σύστημα.

5. Κάλυψη των ιχνών : η απόκρυψη της υποκλοπής με σκοπό τη μακροχρόνια πρόσβαση.

Η εξωτερική απειλή προσβάλει κυρίως τα λειτουργικά κομμάτια μίας επιχείρησης ανακαλύπτοντας τις αδυναμίες τους. Πολλοί θεωρούν πως τα φαινόμενα κατασκοπείας από εξωτερικούς δρώντες είναι πιο συχνά σε σχέση με τα αντίστοιχα από τους εργαζομένους της επιχείρησης. Ωστόσο, με βάση τα περιστατικά που έχουν παρουσιαστεί αποδεικνύεται πως η κλοπή πληροφοριών από εξωτερικούς δρώντες δεν θα ήταν εφικτή εάν δεν υπήρχε, είτε εκούσια είτε ακούσια, βοήθεια από τα άτομα εντός της επιχείρησης. Η μεγαλύτερη ανησυχία στις μέρες μας αφορά την ακούσια παροχή πρόσβασης σε κατασκόπους. Πολλά άτομα δεν επιδιώκουν σκοπίμως να προκαλέσουν βλάβη και σε πολλές περιπτώσεις δεν το συνειδητοποιούν, αλλά με τις πράξεις ή την απροσεξία τους, αποτελούν απειλή για την επιχείρηση. Είναι τα άτομα αυτά που πραγματικά πιστεύουν, για παράδειγμα, πως βοηθάνε έναν πελάτη ενώ στην πραγματικότητα αποκαλύπτουν εταιρικά μυστικά. Ή τα άτομα που κρατάνε την πόρτα ανοιχτή για κάποιο που νομίζουν ότι είναι συνάδελφος, ενώ είναι μεταμφιεσμένος ανταγωνιστής.

4.1.2 Εσωτερική Απειλή

Η εσωτερική απειλή είναι μία από τις πιο συνήθεις και δυνητικά πιο σοβαρές απειλές της βιομηχανικής κατασκοπείας. Η εσωτερική απειλή περιλαμβάνει ένα κακόβουλο στέλεχος το οποίο υποκλέπτει ευαίσθητα περιουσιακά στοιχεία ή μειώνει με άλλο τρόπο την ακεραιότητα της επιχείρησης. (Sood & Enbody, 2014)

Εσωτερική απειλή είναι η πιθανότητα ένας υφιστάμενος ή πρώην υπάλληλος, εργολάβος ή επιχειρηματικός εταίρος να χρησιμοποιήσει κατά λάθος ή κακόβουλα τη διαβαθμισμένη πρόσβασή του για να βλάψει τους υπαλλήλους, τους πελάτες, τα περιουσιακά στοιχεία, τη φήμη ή τα συμφέροντα της επιχείρησης. (DIB & ITS, 2015, σ. 3)

Μία επιλογή κατασκοπείας με μεγάλο χρονικό ορίζοντα δράσης αποτελεί η τοποθέτηση ενός υπαλλήλου στην ανταγωνίστρια εταιρεία. Μπορεί να προσληφθεί σε οποιοδήποτε επιχειρησιακό επίπεδο της εταιρείας, παρέχοντας πολύτιμες πληροφορίες από οποιαδήποτε πιθανή θέση. Ακόμη και στη χαμηλότερη δυνατή θέση, όπως ένας υπάλληλος ή ένας υπάλληλος για εξωτερικές εργασίες, μπορεί να αποδειχθεί πολύτιμος για τη συλλογή ευαίσθητων πληροφοριών. Σε ορισμένες περιπτώσεις, αυτό το εσωτερικό σημείο «επαφής» μπορεί να βρεθεί στο πρόσωπο ενός δυσαρεστημένου εργαζομένου που επιθυμεί να εκδικηθεί την εταιρεία στην οποία εργάζεται (και κυρίως εναντίον του/της επιβλέποντος). Ένας τέτοιος υπάλληλος θα ήταν ευτυχής να παράσχει πληροφορίες στην αντίπαλη εταιρεία προκειμένου να βλάψει την εταιρεία που τον «πρόδωσε».

Συχνά, οι κατάσκοποι προσπαθούν να αντλήσουν πληροφορίες από συγκεκριμένο προσωπικό που έχει πρόσβαση σε αυτές, χρησιμοποιώντας ένα είδος κόλπου. Ωστόσο, αυτό μπορεί να συμβεί και με πιο άμεσο τρόπο. Η απλούστερη μέθοδος είναι η προσπάθεια δωροδοκίας του εξουσιοδοτημένου άτομου, ειδικά σε περίπτωση που το άτομο είναι γνωστό ότι αντιμετωπίζει οικονομικά προβλήματα. Αυτό υπογραμμίζει τη σημασία των ελέγχων ιστορικού που εκτελούν οι κατάσκοποι για να επιλέξουν τον στόχο τους.

Ένας πιο επιθετικός τρόπος είναι ο εκβιασμός, ο οποίος μπορεί επίσης να είναι πολύ αποτελεσματικός, αφού στη πραγματικότητα οι εργαζόμενοι είναι απλοί άνθρωποι. Το «θύμα» μπορεί επίσης να πλαισιώνεται από τους δράστες και τα αποδεικτικά στοιχεία μπορεί να είναι αποτέλεσμα των δράσεων που οργανώνονται εκ των προτέρων.

Με βάση τα προηγούμενα, η εσωτερική απειλή που μπορεί να παρουσιαστεί σε μία επιχείρηση διακρίνεται σε τρεις κατηγορίες. Παρόλο που κάθε υπόθεση είναι μοναδική, οι βασικές κατηγορίες ανθρώπων οι οποίοι ανήκουν στο εσωτερικό περιβάλλον και μπορεί να προκαλέσουν ζημία είναι: (Cole & Ring, 2005, σ. 321)

- Αυτό-παρακινούμενοι (Με προσωπικό κίνητρο)
- Στρατολογημένοι
- Τοποθετημένοι (Κατάσκοποι)

Στον κάτωθι πίνακα φαίνονται οι τύποι επιθέσεων που μπορούν να πραγματοποιηθούν από

εσωτερικούς δρώντες σε μία επιχείρηση.

Πίνακας 5. Εσωτερική Απειλή και Είδη Επίθεσης (Πηγή DIB & ITS, 2015:8)

		Είδη Εσωτερικών Πρακτόρων												
Πρόθεση ->		Μη Εχθρικοί			Πολλαπλοί		Εχθρικοί							
		Απερίσκεπτο Άτομο	Ανεκπαίδευτο/Αφυρημένο Άτομο	Συμπαθές / Εξωστρεφές Άτομο	Προμηθευτής	Συνεργάτης	Παράλογο Άτομο	Κλέφτης	Δυσαρεστημένο Άτομο	Ακτιβιστής	Τρομοκράτης	Οργανωμένο Έγκλημα	Ανταγωνιστής	Κράτος
Είδη Επιθέσεων	Τυχαία Διαρροή	X	X	X	X	X	X		X					
	Κατασκοπεία				X	X		X	X	X		X	X	X
	Οικονομική Απάτη				X	X		X	X			X		
	Κατάχρηση	X	X	X	X	X	X		X	X				
	Ευκαιριακή Κλοπή Δεδομένων				X	X		X	X	X		X	X	X
	Φυσική Κλοπή						X	X	X		X	X		
	Μετατροπή Προιόντος	X	X		X	X			X	X		X	X	X
	Δολιοφθορά						X		X	X	X		X	X
	Βιαιότητα						X		X		X			

Πολλά από τα οικονομικά εγκλήματα διαπράττονται από τους ίδιους τους εργαζόμενους της επιχείρησης, υποστηρίζει ο Στέφεν Σάλβενμοζερ. «Θα λέγαμε ότι σχεδόν το 50% των εγκληματικών αυτών πράξεων αποδίδεται στα ίδια τα στελέχη των επιχειρήσεων. Συνήθως δεν υποπτεύεσαι έναν άνθρωπο με τον οποίο συναναστρέφεσαι καθημερινά, οπότε του δείχνεις ιδιαίτερη εμπιστοσύνη και μοιράζεσαι μαζί του πολλές πληροφορίες», τονίζει ο συνεργάτης της Pricewaterhouse Coopers. (DealNews, 2013) Στις εταιρίες συχνά δεν αρέσει να σκέφτονται το ενδεχόμενο της εσωτερικής απειλής, επειδή τους κάνει να είναι καχύποπτοι για τους ίδιους τους υπαλλήλους της και υπονομεύεται η εμπιστοσύνη μεταξύ τους. Αλλά η αλήθεια είναι πως θα πρέπει να είναι έστω και λίγο, επειδή μπορεί να προκαλέσουν καταστροφική ζημία στην επιχείρηση. Υπάρχουν πράγματα που μπορεί να κάνει μία επιχείρηση για να μειώσει τις πιθανότητες εσωτερικών απειλών κατασκοπείας αλλά πάντα είναι πιθανές. (Wimmer, 2015, σ. 96)

4.2 Κοινωνική Μηχανική

Παρόλο που τα άτομα που επιθυμούν να υποκλέψουν ιδέες και πληροφορίες συχνά πρέπει να

καταφύγουν στη χρήση ειδικών συσκευών, κανείς νοήμων άνθρωπος δεν θα ασχοληθεί με αυτές εάν μπορεί να πετύχει το σκοπό του με τρόπους που είναι απλούστεροι σε εφαρμογή και αποφεύγοντας το ρίσκο και τις φυσικές δυσκολίες της τοποθέτησής τους. (Heims, 1982, σ. 77) Ταυτόχρονα, οι ειδικοί στην υποκλοπή πληροφοριών (χρησιμοποιώντας νόμιμα ή παράνομα μέσα) εκμεταλλεύονται κάθε δημόσια πηγή πληροφοριών καθώς και υπαλλήλους που είναι περισσότερο «ομιλητικοί» από όσο θα έπρεπε, προσποιούμενοι ότι είναι κάποιος άλλος, προκειμένου να αντλήσουν πληροφορίες και να πείσουν τους άλλους να κάνουν κάτι που δεν θα κάνουν υπό κανονικές συνθήκες. (Androulidakis & Kioupakis, 2016, σ. 19). Συνεπώς, επιπλέον των ανωτέρω παραδοσιακών μεθόδων απόκτησης πρόσβασης στα μυστικά μίας επιχείρησης, υπάρχει μία ακόμη μέθοδος η οποία χρησιμοποιείται σε σημαντικό βαθμό και στοχεύει απευθείας στις αδυναμίες του ανθρώπινου παράγοντα. Η μέθοδος αυτή ονομάζεται κοινωνική μηχανική. Ως κοινωνική μηχανική ορίζεται η μέθοδος χειραγώγησης ατόμων με σκοπό την εξαπάτησή τους και την απόσπαση διαβαθμισμένων πληροφοριών.

Η κοινωνική μηχανική είναι μία μέθοδος απόκτησης πρόσβασης σε συστήματα, δεδομένα, κτίρια μέσω της εκμετάλλευσης της ανθρώπινης ψυχολογίας. Αντί να χρησιμοποιούνται τεχνικές μέθοδοι ή παραβιάσεις, η κοινωνική μηχανική περιλαμβάνει μη τεχνικές μεθόδους που χρησιμοποιούν οι επιτιθέμενοι. (Reynolds, 2015, σ. 11)

Ενώ η κοινωνική μηχανική είναι σαφώς μία εξωτερική απειλή για την επιχείρηση, στοχεύει άμεσα στο προσωπικό που συνδέεται με αυτό, το οποίο άθελα του μετατρέπεται σε εκούσια εσωτερική απειλή. Η ακούσια αυτή απειλή είναι ένας υφιστάμενος ή πρώην εργαζόμενος, ένας εργολάβος ή επιχειρηματικός εταίρος ο οποίος έχει ή είχε εξουσιοδοτηθεί να έχει πρόσβαση στο δίκτυο της επιχείρησης ή κατέχει δεδομένα και ο οποίος μέσω δράσης ή και αδράνειας χωρίς κακόβουλη πρόθεση, προξενεί βλάβη ή αυξάνει σημαντικά την πιθανότητα μελλοντικής σοβαρής ζημίας στην εμπιστευτικότητα, την ακεραιότητα ή την διαθεσιμότητα της επιχείρησης. (Mundie, 2014) Η κοινωνική μηχανική περιλαμβάνει ένα ευρύ φάσμα κακόβουλων δραστηριοτήτων, οι οποίες εκτελούνται με διάφορους τρόπους, όπως η δημιουργία προσχημάτων για την απόσπαση πληροφοριών, το ηλεκτρονικό «ψάρεμα» μέσω ψευδών ιστοσελίδων και η αντιστάθμιση με την έννοια της υπόσχεσης ενός προνομίου σε αντάλλαγμα με κάποια συγκεκριμένη πληροφορία. (Reynolds, 2015)

Όλες οι τεχνικές κοινωνικής μηχανικής βασίζονται σε συγκεκριμένες ιδιότητες της ανθρώπινης λήψης αποφάσεων που είναι γνωστές ως γνωστικές προκαταλήψεις. Οι τεχνικές της κοινωνικής μηχανικής βασίζονται στον εκμετάλλευση της ανθρώπινης φύσης καθώς ο ανθρώπινος παράγοντας αποτελεί το πιο ευάλωτο στοιχείο ενός συστήματος και αυτό διότι οι δυνατότητες και οι αδυναμίες των υπολοίπων μερών του συστήματος είναι σε μεγάλο βαθμό δεδομένες και προκαθορισμένες. Αντίθετα, ο ανθρώπινος παράγοντας επηρεάζεται από τις συνθήκες εργασίας και από την ψυχοσύνθεσή του και οδηγείται στην παραπλάνηση.

Επιπλέον αυτών των βασικών ψυχολογικών τακτικών, υπάρχουν και άλλες που χρησιμοποιούνται στην κοινωνική μηχανική. Οι τακτικές αυτές περιλαμβάνουν την επιρροή και την πειθώ. Η τέχνη της επιρροής και της πειθούς είναι μία διαδικασία κατά την οποία κάνουμε κάποιον άλλο να σκέφτεται, να πράττει, να αντιδρά και να πιστεύει με τον τρόπο που

άλλοι θέλουν. (Reynolds, 2015, σ. 47) Στις περισσότερες περιπτώσεις, οι επιτυχημένοι κοινωνικοί μηχανικοί έχουν ισχυρές διαπροσωπικές δεξιότητες. Είναι γοητευτικοί, ευγενικοί και ευχάριστοι, τα οποία είναι κοινωνικά χαρακτηριστικά που απαιτούνται για τη δημιουργία γρήγορης σχέσης και εμπιστοσύνης. Ένας έμπειρος κοινωνικός μηχανικός είναι σε θέση να αποκτήσει πρόσβαση σε σχεδόν οποιαδήποτε στοχευόμενη πληροφορία χρησιμοποιώντας τις στρατηγικές και τις τακτικές του. (Mitnick & Simon, 2002, σ. 8)

Οι λόγοι που καθιστούν τόσο ευάλωτους τους ανθρώπους είναι ψυχολογικοί αλλά και επαγγελματικοί. Όσον αφορά το ψυχολογικό κομμάτι, οι άνθρωποι (στην προκειμένη περίπτωση οι εργαζόμενοι) δεν σκέφτονται πάντα ορθολογικά αλλά επηρεάζονται από τα συναισθήματά τους και αυτό τους κάνει ευκολότερους στόχους. Επίσης, η ενασχόληση με πολλαπλά καθήκοντα και οι πολλαπλές απαιτήσεις και υποχρεώσεις τους οδηγούν στο να λειτουργούν «μηχανικά» και να χρησιμοποιούν όσο το δυνατό λιγότερο τη διανοητική τους ενέργεια για κριτική ανάλυση.

4.3 Εκτίμηση Κινδύνου Βιομηχανικής Κατασκοπείας

Το στάδιο της εκτίμησης κινδύνων έχει ως στόχο να βοηθήσει στη διαδικασία λήψης αποφάσεων, με βάση τα αποτελέσματα της ανάλυσης κινδύνου σχετικά με το ποιοι κίνδυνοι χρειάζονται ιδιαίτερο χειρισμό και την προτεραιότητα για την εφαρμογή του. Η εκτίμηση κινδύνου περιλαμβάνει τη σύγκριση του επιπέδου των κινδύνων που βρέθηκαν κατά το στάδιο της ανάλυσης κινδύνου με τα κριτήρια τα οποία καθορίστηκαν κατά τον προσδιορισμό του κινδύνου. Βάσει αυτής της σύγκρισης, μπορεί να εξετασθεί η ανάγκη για χειρισμό αντιμετώπισης. (International Organization for Standardization, 2009, σ. 18)

4.3.1 Οικονομικά και Στατιστικά Στοιχεία

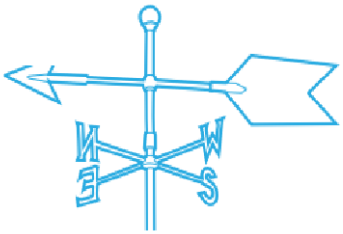
Η επακριβής οικονομική ζημία που προκαλεί η βιομηχανική κατασκοπεία δεν είναι δυνατόν να υπολογισθεί λόγω της έλλειψης στοιχείων, της άγνοιας εκδήλωσης τυχόν επιθέσεων αλλά και της απόκρυψης αυτών από επιχειρήσεις οι οποίες δεν θέλουν να δυσφημιστούν. Ωστόσο, το Διεθνές Εμπορικό Επιμελητήριο εκτιμά πως οι παγκόσμιες δημοσιονομικές απώλειες είναι περισσότερες από 600 δισεκατομμύρια δολάρια ετησίως. (Burgess & Power, 2011, σ. xvii)

Σύμφωνα με το FBI, η βιομηχανική κατασκοπεία κοστίζει στις αμερικανικές επιχειρήσεις περισσότερα από 300 δισεκατομμύρια δολάρια ετησίως. Ειδικότερα, η κλοπή πνευματικής ιδιοκτησίας εκτιμάται ότι αγγίζει τα 250 δισεκατομμύρια δολάρια ετησίως και στοιχίζει στις Η.Π.Α. περίπου 750.000 θέσεις εργασίας. Επίσης από το 1990, το Υπουργείο Δικαιοσύνης των Η.Π.Α. έχει ασκήσει δίωξη για 50 υποθέσεις οι οποίες σχετίζονται με οικονομική κατασκοπεία.

Σύμφωνα με την μελέτη της εταιρίας CEB, η οποία παρέχει υπηρεσίες πληροφόρησης σε επιχειρήσεις παγκοσμίως, για το $1^{ο}$ τρίμηνο του 2017 η προστασία προσωπικών δεδομένων είναι ο $3^{ος}$ σημαντικότερος αναδυόμενος κίνδυνος για τις επιχειρήσεις, ενώ για το $2^{ο}$ τρίμηνο κατέχει τη $2^{η}$ θέση και μαζί με την κυβερνο-ασφάλεια είναι οι ταχύτερα αναδυόμενοι. (CEB Risk Management Leadership Council, 2017)

Πίνακας 6. Δέκα σημαντικότεροι αναδυόμενοι κίνδυνοι Α' και Β' Τριμήνου 2017 (Πηγή CEB Risk Management Leadership Council, 2017)

Δέκα Σημαντικότεροι Αναδυόμενοι Κίνδυνοι για το 1ο και το 2ο Τρίμηνο 2017



Ταχύτητα Κινδύνου

Οι κίνδυνοι αυτοί ταξινομούνται ως οι κίνδυνοι με τη μεγαλύτερη ταχύτητα.

Οι επιχειρήσεις κάθε μεγέθους πρέπει να είναι προσεκτικές με αυτούς, καθώς μπορούν να παρακωλύσουν την οργάνωσή τους γρήγορα σε περίπτωση που πραγματοποιηθούν.

Τίτλος Κινδύνου	Ορισμός	1ο Τρίμηνο 2017	2ο Τρίμηνο 2017
Κόπωση λόγω της Αλλαγής	Ο κίνδυνος ότι η συχνότητα και ο όγκος των πρωτοβουλιών αλλαγής στην οργάνωση θα αυξήσει την κόπωση των εργαζομένων και θα μειώσει την παραγωγικότητά τους.	1	1
Ιδιωτικότητα Δεδομένων	Ο κίνδυνος ότι οι οργανισμοί δεν έχουν επαρκή ικανότητα να προστατεύσουν το απόρρητο των δεδομένων των περουσιακών τους στοιχείων, των υπαλλήλων και των πελατών τους.	3	2
Περιστατικά στον Κυβερνοχώρο με εμπλοκή Ανθρώπων	ο κίνδυνος ότι μια εκμετάλλευση ή η κακόβουλη πρόθεση ενός υπαλλήλου ή ενός εργολάβου θα οδηγήσει σε απώλεια ζωτικών, εμπιστευτικών πληροφοριών.	-	3
Αναλύσεις Μεγάλων Δεδομένων	Ο κίνδυνος η ποσότητα των δεδομένων να καταστεί συντριπτική, ενδεχομένως να οδηγήσει σε λανθασμένα συμπεράσματα λόγω ανακριβούς ανάλυσης ή απώλειας πληροφοριών εξαιτίας της έλλειψης πόρων για την ανάλυση των δεδομένων.	4	4
Διατήρηση της Γνώσης	Ο κίνδυνος ότι ένας οργανισμός δεν εντοπίζει και διατηρεί τις γνώσεις που είναι απαραίτητες για τις δραστηριότητές του.	10	5
Νέο Πολιτικό Τοπίο των Η.Π.Α.	Ο κίνδυνος ότι τα αποτελέσματα των εκλογών του 2016 και η κυβέρνηση Trump θα οδηγήσουν σε αυξημένη αβεβαιότητα και αστάθεια στις παγκόσμιες αγορές.	5	6
Εταιρική Κουλτούρα	Ο κίνδυνος ότι η κουλτούρα ενός οργανισμού θα μπορούσε να ενθαρρύνει ή τουλάχιστον να μην αποθαρρύνει την ανάρμοστη συμπεριφορά που μπορεί να οδηγήσει σε πιθανή ζημία νομικής φύσεως ή φήμης.	7	7
Παγκόσμια Οικονομική Επιβράδυνση	Ο κίνδυνος ότι η επιβράδυνσης της παγκόσμιας οικονομικής ανάπτυξης με αρνητικά ή σχεδόν μηδενικά επιτόκια θα επηρεάσει αρνητικά την ανάπτυξη των οργανισμών.	6	8
Αποκάλυψη στον Κυβερνοχώρο	Ο κίνδυνος ότι οι οδηγίες για την αποκάλυψη παραβιάσεων στον κυβερνοχώρο θα είναι σαφέστερες, με αποτέλεσμα οι οργανισμοί να κυκλοφορήσουν αυτές τις πληροφορίες ταχύτερα από ό, τι στο παρελθόν - ενδεχομένως οδηγώντας σε αυξημένο αντίκτυπο στην φήμη και τα οικονομικά τους.	-	9
Προκλήσεις Διαδοχής	Ο κίνδυνος ότι η αδυναμία εξεύρεσης νέων ηγετών θα επηρεάσει αρνητικά τον τρόπο λειτουργίας των οργανισμών.	9	10
Αβεβαιώτητες Εξωτερικού Περιβάλλοντος	Ο κίνδυνος ότι οι εξωτερικοί παράγοντες (όπως το Brexit, η αστάθεια των τιμών του πετρελαίου, η επιβράδυνση των αναδυόμενων αγορών, η νέα αμερικανική κυβέρνηση) θα οδηγήσουν σε δυσμενείς επιχειρηματικές αποφάσεις.	2	-
Οργανωτική Ανάπτυξη	Ο κίνδυνος ότι οι οργανώσεις δεν γνωρίζουν πώς να προωθήσουν αποτελεσματικά την αύξηση του ενεργητικού τους και την ανάπτυξη των επιχειρηματικών μοντέλων τους.	8	-

Επιπρόσθετα, σύμφωνα με την αμερικανική επιχείρηση παροχής ασφάλειας "SECURITAS", ο κίνδυνος της βιομηχανικής κατασκοπείας κατατάσσεται εντός των 20 κορυφαίων κινδύνων ασφάλειας από το 2000 έως και σήμερα και η απειλή από εσωτερικούς δρώντες στους 5

κορυφαίους, ενώ το 2016 κατείχε την 7η θέση. (SECURITAS Inc, 2016)

Πίνακας 7. Κύριες Απειλές Ασφάλειας από το 2000 έως το 2016 (Πηγή: SECURITAS Inc., 2016:9)

Κύριες Απειλές Ασφάλειας - Κατάταξη 2000 - 2016*									
Απειλές Ασφάλειας	2000	2001	2002	2003	2008	2010	2012	2014	2016
Κυβερνοασφάλεια/Ασφάλεια Επικοινωνιών: Internet (1)	2 (ισοβ)	2	4	3	3	1	1	1	1
Πρόληψη Βίας στο Χώρο Εργασίας	1	1	1	1	1	2	2	3	2
Αυτονομιστές	-	-	-	-	-	-	-	-	3
Σχεδιασμός Συνέχειας Επιχειρησιακής Δραστηριότητας/Οργανωτική Ανθεκτικότητα	2 (ισοβ)	5	2	2	2	3	3	2	4
Κυβερνοασφάλεια/Ασφάλεια Επικοινωνιών: Κινητή Τηλεφωνία (2)	-	-	-	-	-	-	-	-	5
Διαχείριση Κρίσεων: Φυσικές Καταστροφές (2)	-	-	-	-	-	-	-	-	6
Επιλογή και Έλεγχος Εργαζομένων (Συμπεριλ. των Εσωτερικών Απειλών) (3)	5	3	5	5	4	4	4	4	7
Διαχείριση Κρίσεων: Εσωτερική Τρομοκρατία/Μοναχικοί Λύκοι (4)	16	17	3	4	7	12	15	8	8
Εγκλήματα Ιδιοκτησίας (κλοπές,βανδαλισμοί)	12	10	9	12 (ισοβ)	5 (ισοβ)	7	5	6	9
Περιβαλλοντικά/Κοινωνικά: Θέματα Ιδιοκτησίας	-	-	-	-	-	-	-	5	10
Κλοπή Εργαζομένων	6	6	8	7	5 (ισοβ)	8	6	7	11
Κλοπή Ταυτότητας	-	16	14 (ισοβ)	10	12	11	10	9	12
Δικαστικά: Ανεπαρκής Ασφάλεια	13 (ισοβ)	13	11 (ισοβ)	18	19 (ισοβ)	16	9	13	13
Ανήθικη Επιχειρηματική Συμπεριφορά	7	9	7	8	9	5	8	10	14
Προστασία Στελεχών/Υπαλλήλων (Συμπεριλ. της ασφάλειας πτήσεων) (5)	-	-	-	-	22 (ισοβ)	13	18	21	15
Δικαστικά: Αμελής Πρόσληψη/Επιτήρηση	13 (ισοβ)	14	18			23	17	15 (ισοβ)	16
Κατάχρηση ουσιών (ναρκωτικά/αλκοόλ στον εργασιακό χώρο)	9	8	10			17	13	15 (ισοβ)	17
Απάτη/Οικονομικό Έγκλημα	4	4	6	6	8	10	12	14	18
Οργανωτική Κατασκοπεία/Κλοπή Εμπορικών Μυστικών (6)	11	12	19	16	15 (ισοβ)	15	16	17	19
Πνευματική Ιδιοκτησία/Προστασία Εμπορικού Σήματος/Παραποίηση Προϊόντων	-	-	-	-	21	14	11	19	20
Βομβιστικές Επιθέσεις/ Αυτοσχέδιοι Εκρηκτικοί Μηχανισμοί (7)	-	-	-	-	14	24	19	24	21
Διαχείριση Κρίσεων: Πολιτικές Αναταραχές/Δημόσιες Διαδηλώσεις (8)	17	20	14 (ισοβ)	11	10	6	7	12	22
Περιβαλλοντικά/Κοινωνικά: Ληστίες	-	-	-	-	27 (ισοβ)	19	14	18	23
Περιβαλλοντικά/Κοινωνικά: Ασθένειες/Ιοί (9)	-	-	-	-	17	18	22	11	24
Παγκόσμια Ασφάλεια Αλυσίδας Εφοδιασμού	19	18	22	21	27 (ισοβ)	22	20	20	25
Ασφάλεια/Απάτη Αποζημίωσης Εργαζομένων	15	15	17	17	26	25	21	22	26
Διαχείριση Κρίσεων: Διεθνής Τρομοκρατία	-	-	-	-	-	-	-	23	27
Εργατική αναταραχή	-	-	-	-	29	26	23	25	28
Διαχείριση Κρίσεων: Απαγωγή/Εκβιασμός	18	19	20	19	33	27	24	26	29
* Οι κατατάξεις για την περίοδο 2000-2016 δεν περιλαμβάνουν όλες τις επιλογές απειλών, καθώς ορισμένες αντικαταστάθηκαν από νέες επιλογές σε πιο πρόσφατες έρευνες									
(1) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Κυβερνοασφάλεια/Ασφάλεια Επικοινωνιών (Internet, Intranet)									
(2) Νέα απειλή το 2016									
(3) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Επιλογή/ Εξέταση Εργαζομένων									
(4) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Διαχείριση Κρίσεων: Εσωτερική Τρομοκρατία									
(5) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Προστασία Στελεχών (Συμπεριλαμβανομένων των ταξιδιών και της ασφάλειας)									
(6) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Επιχειρηματική Κατασκοπεία/Κλοπή Εμπορικών Μυστικών									
(7) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Βομβιστικές Επιθέσεις									
(8) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Διαχείριση Κρίσεων: Πολιτικές Αναταραχές/Περιφερειακή Αστάθεια/Εθνικές Κατασκτροφές									
(9) Πριν το 2016, αυτή η απειλή ήταν κοινώς γνωστή ως: Διαχείριση Κρίσεων: Περιβαλλοντικά/Κοινωνικά: Πναδημίες									

Τέλος, σύμφωνα με την τελευταία διαθέσιμη ετήσια έκθεση της Εθνικής Υπηρεσίας Αντικατασκοπείας των Η.Π.Α. προς το Κογκρέσο σχετικά με τις εξελίξεις στη συλλογή οικονομικών πληροφοριών και τη βιομηχανική κατασκοπεία για το έτος 2008, το F.B.I. άνοιξε 55 νέες υποθέσεις και συνέχισε 88 εκκρεμείς. Μέσα σε ένα έτος πραγματοποιήθηκαν 158

συλλήψεις και 187 καταγγελίες που οδήγησαν σε 143 καταδίκες για εγκληματικές παραβάσεις και υποβλήθηκαν πειθαρχικά πρόστιμα 2.700.000 δολαρίων, πάνω από 800.000 δολάρια σε κατασχέσεις και 3.600.000 δολάρια σε διοικητικές κυρώσεις (NCIX, 2009)

4.3.2 Εκτίμηση Επιμέρους Πρακτικών και Κινήτρων

Σε επίπεδο οργανισμών και επιχειρήσεων, υπάρχουν 5 λογικά βήματα για την εκτίμηση του κινδύνου: (Burgess & Power, 2011)

- Αναγνώριση κρίσιμων πληροφοριών
- Ανάλυση των απειλών
- Ανάλυση της τρωτότητας
- Εκτίμηση του κινδύνου
- Εφαρμογή των κατάλληλων αντιμέτρων

Γενικότερα, για να προσδιοριστεί το επίπεδο διακινδύνευσης και να ταξινομηθούν οι κίνδυνοι που διατρέχει μία επιχείρηση, πρέπει να ληφθούν υπόψη οι τέσσερις μεταβλητές με τις οποίες ορίζεται. Οι μεταβλητές αυτές είναι:

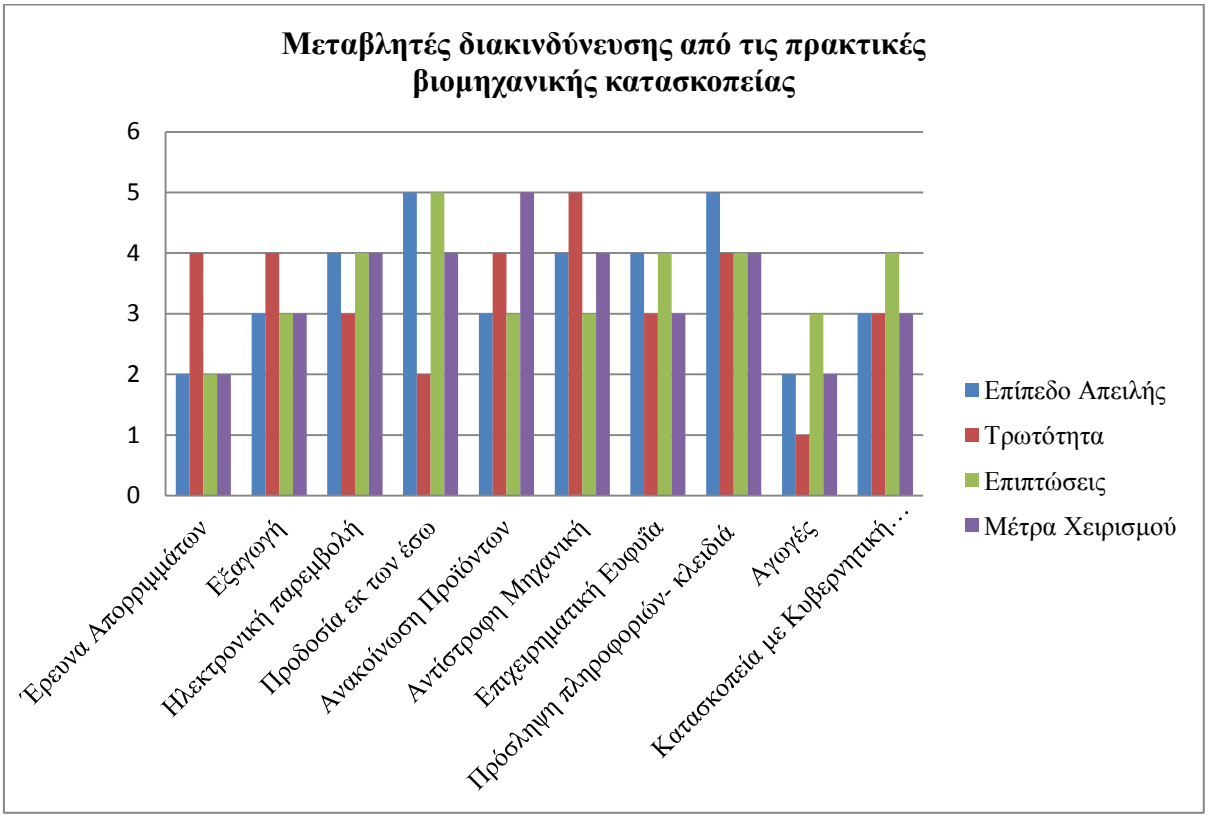
- Το επίπεδο της απειλής
- Η τρωτότητα
- Οι επιπτώσεις
- Τα μέτρα χειρισμού

Όταν εφαρμόζεται η διαδικασία διαχείρισης διακινδύνευσης, ο μαθηματικός τύπος που συνδέει τις παραπάνω μεταβλητές μπορεί να εκφραστεί ως: (Wimmer, 2015)

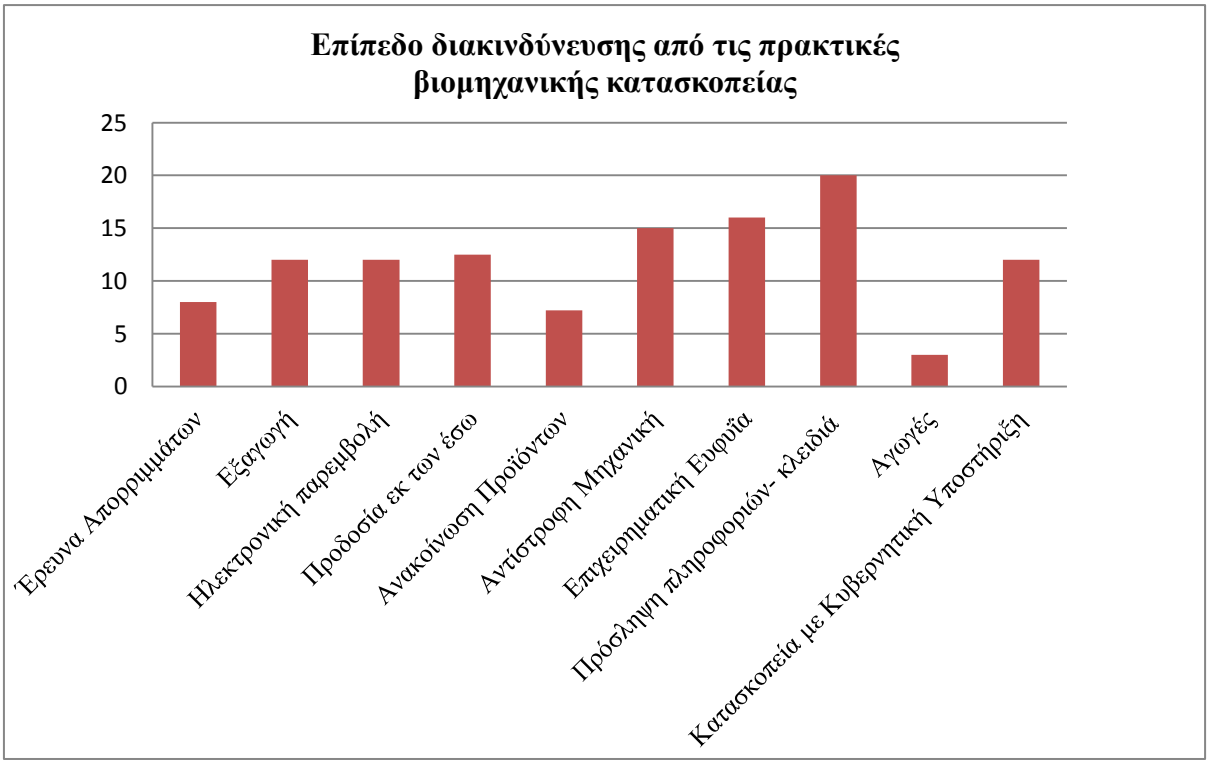
$$Κίνδυνος = \frac{Επίπεδο\ Απειλής\ *\ Τρωτότητα\ *\ Επιπτώσεις}{Μέτρα\ Χειρισμού} \qquad \{4.3.2\text{-}1\}$$

Με την κατανόηση και τον υπολογισμό του κινδύνου, αντιλαμβανόμαστε καλύτερα τα σημεία έκθεσης στον κίνδυνο. Συνεπώς, όσον αφορά τον κίνδυνο της βιομηχανικής κατασκοπείας κάθε επιχείρηση ανεξάρτητα από το μέγεθος της πρέπει να μπορεί να προσδώσει κάποιες ενδεικτικές τιμές σε αυτές τις μεταβλητές, έτσι ώστε να μπορεί να κατατάξει τους ενδεχόμενους κινδύνους και να θέσει τις προτεραιότητες αντιμετώπισής τους. Οι κίνδυνοι που παρουσιάζονται στο κάτωθι διάγραμμα αφορούν τις πρακτικές της βιομηχανικής κατασκοπείας όπως παρουσιάστηκαν στον Πίνακα 3 και έχουν τοποθετηθεί τιμές για κάθε μεταβλητή με

κλίμακα από 1 έως 5 με βάση τα περιστατικά που μελετήθηκαν.



Γράφημα 1. Μεταβλητές διακινδύνευσης από τις πρακτικές βιομηχανικής κατασκοπείας



Γράφημα 2. Επίπεδο διακινδύνευσης από τις πρακτικές βιομηχανικής κατασκοπείας

Ένας απλούστερος μαθηματικός τύπος με τον οποίο μπορεί να εκφραστεί ο κίνδυνος είναι: (Cole & Ring, 2005)

$$\text{Κίνδυνος} = \text{Απειλές} * \text{Τρωτότητα} \qquad \{4.3.2\text{-}2\}$$

Προσδιορίζοντας το επίπεδο των κινδύνων με βάση τον ανωτέρω μαθηματικό τύπο είναι δυνατή η εκτίμηση των κινδύνων που διατρέχει μία επιχείρηση από το φαινόμενο της βιομηχανική κατασκοπείας και η κατασκευή ενός Risk Matrix λαμβάνοντας υπόψη την πιθανότητα/ συχνότητα εμφάνισής τους, και τον αντίκτυπό τους στην επιχείρηση.

Πίνακας 8. Risk Matrix πρακτικών βιομηχανικής κατασκοπείας

	ΕΚΤΙΜΩΜΕΝΟΣ ΑΝΤΙΚΤΥΠΟΣ				
ΣΥΧΝΟΤΗΤΑ ΕΜΦΑΝΙΣΗΣ	ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΙΟΝΤΩΝ		ΠΡΟΣΛΗΨΗ ΠΛΗΡΟΦΟΡΙΩΝ-ΚΛΕΙΔΙΑ		
	ΕΞΑΓΩΓΗ	ΜΕ ΚΥΒΕΡΝΗΤΙΚΗ ΥΠΟΣΤΗΡΙΞΗ		ΑΝΤΙΣΤΡΟΦΗ ΜΗΧΑΝΙΚΗ	ΠΡΟΔΩΣΙΑ ΕΚ ΤΩΝ ΕΣΩ
			ΗΛΕΚΤΡΟΝΙΚΗ ΠΑΡΕΜΒΟΛΗ	ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΕΥΦΥΙΑ	
			ΑΓΩΓΕΣ		
		ΈΡΕΥΝΑ ΑΠΟΡΡΙΜΜΑΤΩΝ			

Η εκτίμηση των θέσεων των πρακτικών βιομηχανικής κατασκοπείας είναι προσωπική, βασίζεται στα περιστατικά που μελετήθηκαν και ενδέχεται να τροποποιηθεί αναλόγως των ιδιαίτερων χαρακτηριστικών κάθε επιχείρησης.

5. Χειρισμός Κινδύνου Βιομηχανικής Κατασκοπείας

Ο χειρισμός των κινδύνων και η επιλογή του καταλληλότερου τρόπου αντιμετώπισης περιλαμβάνει την εξισορρόπηση του κόστους και των προσπαθειών υλοποίησης με τα οφέλη που προκύπτουν, όσον αφορά τις νομικές, κανονιστικές και άλλες απαιτήσεις όπως η κοινωνική ευθύνη και η προστασία του φυσικού περιβάλλοντος. Οι αποφάσεις θα πρέπει επίσης να λαμβάνουν υπόψη τους κινδύνους που μπορούν να δικαιολογήσουν την αντιμετώπισή τους ακόμα και αν δεν δικαιολογείται για οικονομικούς λόγους, π.χ. σοβαροί (με πολύ αρνητικές συνέπειες) αλλά σπάνιοι (χαμηλής πιθανότητας) κίνδυνοι. Ορισμένες επιλογές χειρισμού δύναται να εξεταστούν και να εφαρμοστούν είτε μεμονωμένα είτε σε συνδυασμό, η υιοθέτηση των οποίων μπορεί να προσφέρει μεγαλύτερα οφέλη στον οργανισμό. Κατά την επιλογή τους, ο οργανισμός θα πρέπει να εξετάζει τις αξίες και τις αντιλήψεις των ενδιαφερομένων και τους καταλληλότερους τρόπους επικοινωνίας μαζί τους. Όταν οι τρόποι αντιμετώπισης κινδύνων μπορεί να επηρεάσουν ένα άλλο κομμάτι της οργάνωσης ή τα ενδιαφερόμενα μέρη, αυτά πρέπει να συμμετέχουν στη διαδικασία λήψης της απόφασης.

5.1 Πλαίσιο Χειρισμού κινδύνου

Είναι εύκολο να ισχυριστεί κάποιος ότι είναι ασφαλής, αλλά στην πραγματικότητα είναι πολύ δύσκολο να υπολογίσει και να επικυρώσει ότι έχει εφαρμόσει το κατάλληλο πλάνο ώστε να επιτύχει το επιθυμητό επίπεδο ασφάλειας. Για τη δημιουργία μίας ασφαλούς επιχείρησης υπάρχουν τρία (3) βασικά βήματα που πρέπει να γίνουν: (Podszywalow, 2012)

1. Το πρώτο βήμα για μια καλύτερη άμυνα είναι να προσδιοριστούν οι πληροφορίες που, αν χαθούν, θα την βλάψουν σημαντικά και η αξία αυτών των πληροφοριών για την επιχείρηση και τους ανταγωνιστές της. Αυτά είναι τα πολύτιμα «κοσμήματά» της και απαιτούν τις καλύτερες εγγυήσεις. Οι διαχειριστές ασφάλειας πληροφοριών πρέπει να είναι σε θέση να προσδιορίσουν την πνευματική ιδιοκτησία της εταιρείας, τη θέση της και την αξία της. Μόνο τότε μπορούν να προστατεύσουν και να ελέγξουν ποιος έχει πρόσβαση σε αυτές τις πληροφορίες. Στη συνέχεια, θα πρέπει να γίνει εκτίμηση κινδύνου για τον εντοπισμό των υφιστάμενων τρωτών σημείων ασφαλείας σε αυτά τα πολύτιμα «κοσμήματα».

2. Μόλις οχυρωθούν τα πολύτιμα «κοσμήματα», πρέπει να καθοριστεί ο τρόπος προστασίας από τις επιθέσεις χαμηλής τεχνολογίας. Ένας τρόπος για να γίνει αυτό

είναι μέσω ενός μελετημένου προγράμματος ευαισθητοποίησης σχετικά με την ασφάλεια, το οποίο θα περιλαμβάνει τακτικές δοκιμές ασφάλειας σε ολόκληρη την επιχείρηση.

3. Το τελευταίο βήμα είναι να προσομοιωθεί μια πραγματική επίθεση, η οποία συχνά εμφανίζεται ως μια πολλαπλή απειλή στις δομές ασφάλειας της επιχείρησης. Αυτή η άσκηση θα πρέπει να επικεντρώνεται σε όλους τους τύπους πληροφοριών ανεξάρτητα από τη μορφή τους.

Το βασικό στοιχείο ενός επιτυχημένου προγράμματος κατά της βιομηχανικής κατασκοπείας είναι η ύπαρξη ενός σχεδίου διαχείρισης κινδύνου που να καλύπτει τους ακόλουθους τομείς: (Dodge, 2014)

Πίνακας 9. Τομείς σχεδίου χειρισμού βιομηχανικής κατασκοπείας (Βασισμένο στο Dodge, 2014)

Α/Α	**Τομέας**	**Στόχος**
1	Ασφάλεια Προσωπικού	Εφαρμογή ενός ολοκληρωμένου σχεδίου για τον έλεγχο του ιστορικού των νέων υπαλλήλων και τις διαδικασίες τερματισμού της εργασίας των νυν.
2	Νομική Υποστήριξη	Νόμιμη προστασία της πνευματικής ιδιοκτησίας και καταπολέμηση των επιθέσεων κατασκοπείας
3	Εκπαίδευση και Ευαισθητοποίηση	Παροχή εξειδικευμένης και προσαρμοσμένης εκπαίδευσης με έμφαση στις τεχνικές και τακτικές συλλογής πληροφοριών
4	Φυσική Ασφάλεια	Ελεγχόμενη και εξουσιοδοτημένη πρόσβαση προσωπικού
5	Πληροφόρηση	Συνεχής ενημέρωση σχετικά με τις τάσεις στο τομέα των υποκλοπών και κατανόηση λειτουργικών και στρατηγικών στόχων της επιχείρησης
6	Σύσφιξη σχέσεων με ανταγωνιστές και κράτη	Ανάπτυξη ισχυρών σχέσεων με τις Υπηρεσίες Πληροφοριών και αμοιβαίων σχέσεων συνεργασίας με τους ανταγωνιστές ενάντια στην βιομηχανική κατασκοπεία
7	Ασφάλεια Πληροφοριών	Όλα τα επίπεδα της τεχνολογίας πληροφοριών και του δικτύου πρέπει να είναι προστατευμένα
8	Συγκεντρωμένη Δομή	Εξάλειψη κενών μεταξύ των τομέων της επιχείρησης και συγκεντρωτική αντιμετώπιση της απειλής

5.2 Χειρισμός Φαινομένων Κοινωνικής Μηχανικής

Οι περισσότεροι άνθρωποι υποθέτουν ότι δεν θα εξαπατηθούν από άλλους, βασισμένοι στην πεποίθηση ότι η πιθανότητα να εξαπατηθούν είναι πολύ χαμηλή. Ο επιτιθέμενος, κατανοώντας αυτή την κοινή πεποίθηση, κάνει το αίτημά του να ακούγεται τόσο λογικό ώστε δεν εγείρει καμιά υποψία, εκμεταλλευόμενος παράλληλα την εμπιστοσύνη του θύματος. (Mitnick & Simon, 2002, σ. 8) Σε γενικές γραμμές, οι άνθρωποι δεν είναι πρόθυμοι να παραδεχτούν ότι τείνουν να ξεγελαστούν ή να εξαπατηθούν από επιθέσεις κοινωνικής μηχανικής. Στην πραγματικότητα, οι περισσότεροι άνθρωποι το αρνούνται εξαιτίας του φόβου των επιπτώσεων που μπορεί να έχουν στην εργασία τους καθώς και λόγω ντροπής. Ωστόσο, οι συσκευές καταγραφής αποδεικνύουν την ύπαρξη τέτοιων περιστατικών. (Reynolds, 2015, σ. 64)

Την ίδια λανθασμένη εντύπωση έχουν και τα στελέχη κάποιων επιχειρήσεων θεωρώντας πως είναι ανθεκτικές στον κίνδυνο της βιομηχανικής κατασκοπείας μέσω της κοινωνικής μηχανικής. Στην πραγματικότητα, δεν υφίσταται κανένα σύστημα το οποίο να μην είναι ευάλωτο απέναντι σε τέτοιες επιθέσεις και για το λόγο αυτό είναι αναγκαία η εκπαίδευση των εργαζομένων και γενικότερα όλων των συμμετεχόντων ώστε να αποτρέπει ή έστω να μειωθεί η απειλή. Η κάθε επιχείρηση έχει την ευθύνη να ενημερώνει τους υπαλλήλους για το πώς μπορεί να προκύψει σοβαρό λάθος από την κακή χρήση των μη δημόσιων πληροφοριών της. Μια καλά σχεδιασμένη πολιτική ασφάλειας πληροφοριών, σε συνδυασμό με την κατάλληλη εκπαίδευση και κατάρτιση, μπορεί να αυξήσει δραματικά την ευαισθητοποίηση των εργαζομένων σχετικά με τον σωστό χειρισμό των επιχειρηματικών πληροφοριών. Μια πολιτική ιεράρχησης δεδομένων μπορεί επίσης να βοηθήσει στην εφαρμογή κατάλληλων ελέγχων όσον αφορά την αποκάλυψη πληροφοριών. Χωρίς πολιτική ιεράρχησης δεδομένων, όλες οι εσωτερικές πληροφορίες πρέπει να θεωρούνται εμπιστευτικές, εκτός αν ορίζεται διαφορετικά. (Mitnick & Simon, 2002, σ. 27)

Η εκπαίδευση αυτή πρέπει να περιλαμβάνει τις ακόλουθες διαδικασίες: (Reynolds, 2015)

- Αναγνώριση επίθεσης : Πριν οποιαδήποτε επιχείρηση είναι σε θέση να προλαμβάνει και να μετριάζει τις επιπτώσεις της κοινωνικής μηχανικής, το πρώτο βήμα είναι να μάθει πώς να διακρίνει εάν υφίσταται κάποια επίθεση ή όχι.

- Αύξηση της επαγρύπνησης του προσωπικού : Σε οποιαδήποτε επιχείρηση, η ύπαρξη μίας νοοτροπίας βασισμένη στην ασφάλεια είναι απαραίτητη εφόσον καθίσταται ως πρότυπο λειτουργίας κάθε μέλους της.

- Ασφάλεια Τελικού Χρήστη : Αν και η τεχνολογία συνεχίζει να αλλάζει και να εξελίσσεται, ο τελικός χρήστης παραμένει ο ίδιος. Σύμφωνα με τον Winn Schwartau, ο οποίος είναι ο ιδρυτής της Εταιρίας Ασφάλειας Πληροφοριών, το άτομο στο πληκτρολόγιο ήταν πάντα ο ασθενέστερος σύνδεσμος όσον αφορά την ασφάλεια και η κοινωνική μηχανική έχει προσθέσει νέες μορφές παραπλάνησης, παρόλο που οι βασικές τεχνικές είναι οι ίδιες. Έτσι, οι τελικοί χρήστες δεν θα πρέπει ποτέ να αποκαλύπτουν προσωπικές πληροφορίες σε κανέναν και να λαμβάνουν υπόψη ότι εάν κάποιος ζητήσει τα διαπιστευτήριά τους, τότε μάλλον δεν είναι αξιόπιστος.

- Ενημέρωση Λογισμικών : Είναι σημαντικό για οποιαδήποτε επιχείρηση, να ενημερώνει συνεχώς το λειτουργικό της σύστημα. Τις περισσότερες φορές, οι νεότερες εκδόσεις λογισμικού έχουν ήδη αντιμετωπίσει τα κενά ασφάλειας που μπορεί να είχαν οι προηγούμενες εκδόσεις.

- Ανάπτυξη Σεναρίων : Η ανάπτυξη σεναρίων για την καλύτερη προετοιμασία των υπαλλήλων, ειδικά όταν η κατάσταση απαιτεί κριτική σκέψη, είναι ένας από τους πιο επωφελής τρόπους για την πρόληψη και την μείωση των επιθέσεων κοινωνικής μηχανικής. Τα σενάρια αυτά μπορεί να είναι και απλά περιγράμματα με οδηγίες ώστε να αντιδράσουν σωστά σε συγκεκριμένες περιπτώσεις.

- Προσομοίωση : Η προσομοίωση περιλαμβάνει την επίθεση με μεθόδους κοινωνικής μηχανικής από έναν επαγγελματία σε θέματα ασφάλειας τον οποίο η επιχείρηση προσλαμβάνει ώστε να ελέγξει τις πολιτικές, την φυσική ασφάλεια και το προσωπικό της επιχείρησης.

5.3 Βασικές Διαδικασίες Ασφαλείας

Για την αντιμετώπιση της απειλής της βιομηχανικής κατασκοπείας από εξωτερικούς δρώντες υπάρχουν βασικές πρακτικές οι οποίες μπορούν να εφαρμοστούν με ελάχιστο ή μηδενικό κόστος και αποτελούνται από απλά βήματα τα οποία μπορούν να εφαρμοστούν από όλα τα στελέχη μίας επιχείρησης. (Samli & Jacobs, 2003, σσ. 105-107)

- Απομάκρυνση όλων των Η/Υ, εκτυπωτών και FAX από κοινόχρηστους χώρους και περιοχές έρευνας και ανάπτυξης.

- Δεν πρέπει να αφήνονται έγγραφα εκτεθειμένα πάνω σε τραπέζια, ειδικότερα σε χώρους εργαστηρίων και πωλήσεων.

- Όλα τα τερματικά θα πρέπει να έχουν προφυλάξεις οθόνης προστατευμένες με κωδικούς πρόσβασης.

- Οι συσκευασίες θα πρέπει να επισημαίνονται με τη χρήση χρωματισμένων σημάτων αναγνώρισης και όλα τα μεγάλα πακέτα που βγαίνουν από την επιχείρηση πρέπει να επιθεωρούνται.

- Όλα τα FAX και τα e-mails πρέπει να προστατεύονται.

- Όλα τα παλιά έγγραφα που αφορούν σε έρευνα και ανάπτυξη και άλλα ευαίσθητα έγγραφα πρέπει να καταστρέφονται.

- Οι υπάλληλοι πρέπει να είναι εκπαιδευμένοι να αναγνωρίζουν τη διαφορά μεταξύ εμπορικών μυστικών και γενικών γνώσεων.

- Νομικά έγγραφα τήρησης απορρήτου πρέπει να υπογράφονται πριν από τη διάθεση οποιονδήποτε εμπιστευτικών δεδομένων σε συζητήσεις σχετικά με τη χορήγηση αδειών, την κοινοπραξία ή την συνεργατική έρευνα.

- Οι πρώην υπάλληλοι της εταιρίας δεν πρέπει να έχουν πρόσβαση σε εταιρικά μυστικά.

- Τα εγκαταστημένα συστήματα φυσικής προστασίας πρέπει να είναι σε καλή κατάσταση και οι φύλακες να είναι καλά εκπαιδευμένοι.

5.4 Εναλλακτικές Μέθοδοι Χειρισμού

Επιπλέον, των ανωτέρω διαδικασιών χειρισμού υπάρχουν κάποιες εναλλακτικές μέθοδοι με τις οποίες μπορεί μία επιχείρηση, αν όχι να τις αποτρέψει, αλλά να αμβλύνει τις πιθανότητες εκδήλωσης επιθέσεων.

Μία διαδικασία ασφαλείας για την αποφυγή επιθέσεων βιομηχανικής κατασκοπείας από εσωτερικούς δρώντες είναι η σύναψη συμφωνητικών εμπιστευτικότητας και εχεμύθειας κατά την πρόσληψη και γενικότερα την έναρξη της συνεργασίας της επιχείρησης με κάποιο νέο στέλεχος. Κατά την σύναψη των συμφωνητικών αυτών το νέο στέλεχος της επιχείρησης δεσμεύεται ότι δεν θα χρησιμοποιήσει ή θα αποκαλύψει διαβαθμισμένες πληροφορίες ή θα ανακοινώσει προφορικά ή θα διαρρεύσει εγγράφως ή με οποιονδήποτε άλλο τρόπο θα διαβιβάσει ή θα γνωστοποιήσει προς τρίτους εμπορικές πληροφορίες, φόρμουλες, προγράμματα λογισμικού, αποτελέσματα ελέγχων, μελέτες, υποδείγματα, σχέδια, φωτογραφίες, σκίτσα, προδιαγραφές ή άλλα επαγγελματικά μυστικά, τεχνογνωσία ή ευρήματα επιχειρηματικών ιδεών, για οποιονδήποτε λόγο ή σκοπό, πέραν του σκοπού εκπλήρωσης των σχετικών υποχρεώσεών του.

Σε περίπτωση παραβίασης των ανωτέρω προϋποθέσεων και αθέτησης της συμφωνίας, προβλέπονται κυρώσεις όπως η καταβολή χρηματικής αποζημίωσης η οποία είτε είναι προκαθορισμένη και αναγραφόμενη στο συμφωνητικό είτε σχετίζεται με την αξία των πληροφοριών οι οποίες αποκαλύφθηκαν και με την ζημία που προκλήθηκε στην επιχείρηση. Οι περισσότερες περιπτώσεις κλοπής πνευματικής ιδιοκτησίας από εργαζομένους συμβαίνουν κατά τον τελευταίο μήνα εργασίας τους και γι’ αυτό θα είναι σημαντικό η αναχώρησή τους να είναι όσο το δυνατό πιο ομαλή και ανώδυνη. (Hagon, 2012)

Επίσης, μία ακόμη μέθοδος για την αποτελεσματικότερη ασφάλεια των επιχειρήσεων είναι η προσαρμοσμένη πρόσβαση. Σύμφωνα με τη μέθοδο αυτή δεν είναι δεδομένη η πρόσβαση σε ευαίσθητους χώρους και πληροφορίες για όλο το προσωπικό της επιχείρησης αλλά χρησιμοποιούνται βαθμοί πρόσβασης. Όταν ένας υπάλληλος παρουσιάζει «καλή» συμπεριφορά, του παρέχεται περισσότερη πρόσβαση στους πόρους και όταν παρουσιάζει «κακή» συμπεριφορά, η πρόσβαση της μειώνεται. Αυτό που είναι ενδιαφέρον σε αυτή την προσέγγιση είναι ότι αλλάζει το πρότυπο. Η παραδοσιακή ασφάλεια συχνά βλάπτει τον χρήστη και επιδρά στην δυνατότητα του να εκτελέσει τη δουλειά του. Αυτή η νέα προσέγγιση βλάπτει τον εισβολέα. Εάν ένα σύστημα έχει υποστεί βλάβη από κακόβουλο λογισμικό και ο χρήστης

δεν γνωρίζει ότι το σύστημα έχει υποστεί βλάβη, εξακολουθεί να χρησιμοποιεί το σύστημα για νόμιμους σκοπούς. Με αυτήν την προσέγγιση, καθώς το κακόβουλο λογισμικό προσπαθεί να κάνει κακόβουλα πράγματα στο ίδιο σύστημα με το νόμιμο χρήστη, θα μειωθεί ο βαθμός πρόσβασης που έχει στο σύστημα. Στις περισσότερες περιπτώσεις, η πρόσβαση που μειώνεται σχετίζεται με την κακόβουλη συμπεριφορά και όχι με τον χρήστη. Ως εκ τούτου, το κακόβουλο λογισμικό εμποδίζεται, αλλά ο χρήστης μπορεί ακόμα να εκτελέσει τη δουλεία του. (Cole E., 2013, σ. 31)

5.5 Νομικό Πλαίσιο

Η σημερινή εποχή της πληροφόρησης απαιτεί από τις επιχειρήσεις να ανταγωνίζονται σε παγκόσμια βάση, να μοιράζονται ευαίσθητες πληροφορίες με τα κατάλληλα μέρη, ενώ παράλληλα να προστατεύουν αυτές τις πληροφορίες έναντι ανταγωνιστών. Οι νομοθέτες προσφεύγουν όλο και περισσότερο σε ποινικούς κώδικες για τη θέσπιση οικονομικών και κοινωνικών πολιτικών σχετικά με τη χρήση και τη διάδοση της τεχνολογίας. Πολλοί φοβούνται ότι οι τεχνολογικές εξελίξεις καθιστούν την βιομηχανική κατασκοπεία και την κλοπή του «πνευματικού κεφαλαίου» ευκολότερη και φθηνότερη. (Nasheri, 2005, p. 1)

Σύμφωνα με το Ινστιτούτο Brookings, το 65% των περισσότερων επιχειρηματικών στοιχείων αξίας, πηγές εσόδων, βιωσιμότητας και ανάπτυξης βρίσκονται σε πληροφοριακά περιουσιακά στοιχεία, πνευματική ιδιοκτησία και ιδιόκτητα ανταγωνιστικά πλεονεκτήματα. Είναι σημαντικό να αναγνωρίσουμε ότι στον 21^{ο} αιώνα ο βασικός κίνδυνος για τις επιχειρήσεις είναι η προστασία αυτών των περιουσιακών στοιχείων από την απειλή της βιομηχανικής κατασκοπείας. (Dodge, 2014) Η κλοπή πνευματικής ιδιοκτησίας είναι αχαλίνωτη, αλλά σε μεγάλο βαθμό σιωπηρή, τόσο οι επιχειρήσεις όσο και οι νομοθέτες δυσκολεύονται να εκτιμήσουν τον τεράστιο αντίκτυπό της στην κερδοφορία. Επειδή οι παραβιάσεις των δικαιωμάτων πνευματικής ιδιοκτησίας συχνά δεν συνεπάγονται απώλεια χειροπιαστών περιουσιακών στοιχείων και πολλές φορές δεν απαιτούν καν άμεση επαφή με τον κάτοχο των δικαιωμάτων, ο κάτοχος των δικαιωμάτων συχνά δεν γνωρίζει ότι είναι θύμα, μέχρις ότου οι δραστηριότητες βιομηχανικής κατασκοπείας αποκαλυφθούν. (Nasheri, 2005, p. 2)

Το νομικό πλαίσιο το οποίο συνδέεται με την άσκηση βιομηχανικής κατασκοπείας αφορά αφενός διεθνείς συνθήκες κα συμβάσεις σχετικά με την παραβίαση του προσωπικού απορρήτου και του δικαιώματος της ιδιοκτησίας και αφετέρου νομοθεσίες κρατών όπου αναλύονται επακριβώς οι επιπτώσεις στα εμπλεκόμενα άτομα και επιχειρήσεις.

Συμβάσεις-Συμφωνίες

Σύμφωνα με το άρθρο 17 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου η οποία υιοθετήθηκε στις 10 Δεκεμβρίου 1948 από τα μέλη του Οργανισμού Ηνωμένων Εθνών :

«1. Κάθε άτομο μόνο του ή μαζί με άλλους έχει δικαίωμα στην ιδιοκτησία. 2. Κανείς δεν μπορεί να στερηθεί αυθαίρετα την ιδιοκτησία του.» (Διεθνής Αμνηστία, 1948)

Σύμφωνα με το άρθρο 1 του Πρωτοκόλλου υπ' αριθμόν 1 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου η οποία τέθηκε σε ισχύ στις 03 Σεπτεμβρίου 1953 από τα μέλη του Συμβουλίου της Ευρώπης :

«Κάθε φυσικό ή νομικό πρόσωπο δικαιούται να απολαμβάνει ειρηνικά τα υπάρχοντά του. Ο όρος «υπάρχοντα» περιλαμβάνει μετοχές, διπλώματα ευρεσιτεχνίας, άδειες, μισθωτήρια συμβόλαια και επιδόματα πρόνοιας (υπό την προϋπόθεση ότι αυτά έχουν χορηγηθεί με βάση νόμιμο δικαίωμα και όχι ως αποτέλεσμα ασκήσεως διακριτικής ευχέρειας). Ο όρος «ειρηνικά» περιλαμβάνει το δικαίωμα πρόσβασης στην ιδιοκτησία. Μπορεί να υπάρξουν θετικές υποχρεώσεις για το Κράτος να προστατεύει το δικαίωμα απόλαυσης ης ιδιοκτησίας. Πρώτος ειδικός κανόνας: Η στέρηση ιδιοκτησίας επιτρέπεται μόνον εφόσον είναι νόμιμη, εξυπηρετεί το δημόσιο συμφέρον, είναι σύμφωνη με τις γενικές αρχές του διεθνούς δικαίου, είναι εύλογα αναλογική.» (European Court of Human Rights, 1950)

Στις 20 Μαρτίου 1883 υπογράφθηκε η Σύμβαση των Παρισίων με την οποία δημιουργήθηκε μία Ένωση για την προστασία της βιομηχανικής ιδιοκτησίας. Σύμφωνα με το άρθρο 2 :

«Οι υπήκοοι οποιασδήποτε χώρας της Ένωσης απολαύουν, σε ό, τι αφορά την προστασία της βιομηχανικής ιδιοκτησίας, σε όλες τις άλλες χώρες της Ένωσης τα πλεονεκτήματα που χορηγούν σήμερα ή μπορούν να χορηγήσουν στους υπηκόους τους οι αντίστοιχες νομοθεσίες τους. Κατά συνέπεια, θα έχουν την ίδια προστασία με την τελευταία και την ίδια ένδικη προστασία έναντι τυχόν παραβίασης των δικαιωμάτων τους, υπό την προϋπόθεση ότι τηρούνται οι όροι και οι διατυπώσεις που επιβάλλονται στους υπηκόους.» (Paris Convention for the Protection of Industrial Property, 1979)

Επίσης, κατά την διάρκεια του Γύρου της Ουρουγουάης και κατά τις διαπραγματεύσεις της Γενικής Συμφωνίας Δασμών και Εμπορίου υπογράφθηκε από τα μέλη του Παγκόσμιου Οργανισμού Εμπορίου η διεθνής νομική Συμφωνία για τα Δικαιώματα Πνευματικής Ιδιοκτησίας στον τομέα του εμπορίου (TRIPS) με την οποία θεσπίστηκαν τα ελάχιστα διεθνή πρότυπα για την προστασία και την επιβολή σχεδόν όλων των μορφών δικαιωμάτων πνευματικής ιδιοκτησίας. Σύμφωνα με το άρθρο 61 :

«Τα μέλη πρέπει να προβλέπουν την εφαρμογή ποινικών διαδικασιών και κυρώσεων τουλάχιστον σε περιπτώσεις πλαστογράφησης πλαστών εμπορικών σημάτων ή πειρατείας πνευματικών δικαιωμάτων σε εμπορική κλίμακα. Τα διαθέσιμα διορθωτικά μέτρα περιλαμβάνουν φυλάκιση ή / και χρηματικά πρόστιμα που επαρκούν για την αποτροπή, σε συνάρτηση με το επίπεδο των κυρώσεων που επιβάλλονται για εγκλήματα αντίστοιχης βαρύτητας. Στις κατάλληλες περιπτώσεις, τα διαθέσιμα διορθωτικά μέτρα περιλαμβάνουν επίσης την κατάσχεση, κατάπτωση και καταστροφή των παραβιασθέντων αγαθών και οποιουδήποτε υλικού η κυρίαρχη χρήση του οποίου υπήρξε στη διάπραξη του αδικήματος. Τα μέλη μπορούν να προβλέπουν την εφαρμογή ποινικών διαδικασιών και κυρώσεων σε άλλες περιπτώσεις παραβίασης των δικαιωμάτων πνευματικής ιδιοκτησίας, ιδίως όταν διαπράττονται εκούσια και σε εμπορική κλίμακα. (Agreement on Trade-Related Aspects of Intellectual Property Rights, 1995)

Νομοθεσία Η.Π.Α.

Όσον αφορά τις Ηνωμένες Πολιτείες Αμερικής σύμφωνα με το άρθρο 1832 του Αμερικανικού Ποινικού Κώδικα (Νόμος Περί Κατασκοπείας του 1996) καθορίζονται τα ακόλουθα :

«Σε όποιον με πρόθεση να εκμεταλλευτεί ένα εμπορικό μυστικό, που σχετίζεται με ένα προϊόν ή υπηρεσία που χρησιμοποιείται ή προορίζεται για χρήση στο εσωτερικό ή εξωτερικό εμπόριο, προς οικονομικό όφελος οποιουδήποτε άλλου από τον ιδιοκτήτη του και προτίθεται ή γνωρίζει ότι το αδίκημα θα βλάψει τον ιδιοκτήτη αυτού του εμπορικού μυστικού και εν γνώση του:

- Κλέβοντας ή χωρίς εξουσιοδότηση λαμβάνοντας, μεταφέροντας, αποκρύπτοντας ή εξαπατώντας, αποκτά τέτοιου είδους πληροφορίες.

- Χωρίς άδεια αντιγράφει, σχεδιάζει, φωτογραφίζει, μεταφορτώνει, τροποποιεί, καταστρέφει, αναπαράγει, εκπέμπει, παραδίδει, αποστέλλει, κοινοποιεί ή διαβιβάζει τέτοιου είδους πληροφορίες.

- Λαμβάνει, αγοράζει ή κατέχει τέτοιου είδους πληροφορίες, γνωρίζοντας ότι έχουν κλαπεί ή αποκτηθεί ή μετατραπεί χωρίς εξουσιοδότηση.

- Επιχειρεί να διαπράξει οποιοδήποτε αδίκημα που περιγράφεται στις παραγράφους 1 έως 3.

- Συνωμοτεί με ένα ή περισσότερα άλλα πρόσωπα για να διαπράξουν οποιοδήποτε αδίκημα που περιγράφεται στις παραγράφους 1 έως 3 και ένα ή περισσότερα από αυτά τα πρόσωπα εκτελούν οποιαδήποτε πράξη για την πραγματοποίηση του σκοπού της συνωμοσίας, εκτός από τις περιπτώσεις που προβλέπονται στο παρακάτω εδάφιο,

επιβάλλεται πρόστιμο ή ποινή φυλάκισης έως 10 έτη ή και τα δύο.

Σε έναν οργανισμό που διαπράττει κάποιο από τα αδικήματα που περιγράφονται στο ανωτέρω εδάφιο, επιβάλλεται πρόστιμο έως 5.000.000 δολαρίων ή 3 φορές την αξία του κλεμμένου εμπορικού μυστικού, συμπεριλαμβανομένων των δαπανών για έρευνα και ανάπτυξη και άλλες δαπάνες που η οργάνωση έχει δαπανήσει για να αποφύγει την κλοπή του εμπορικού μυστικού.» (U.S.Code, 2017)

Οδηγία Ευρωπαϊκής Ένωσης

Σύμφωνα με το άρθρο 4 περί «Παράνομης απόκτησης, χρήσης και αποκάλυψης εμπορικών μυστικών» της Οδηγίας υπ' αριθμόν 943/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης «Περί προστασίας της τεχνογνωσίας και των επιχειρηματικών πληροφοριών που δεν έχουν αποκαλυφθεί (εμπορικό απόρρητο) από την παράνομη απόκτηση, χρήση και αποκάλυψή τους» : «Τα κράτη μέλη διασφαλίζουν ότι οι κάτοχοι εμπορικού απορρήτου δικαιούνται να ζητήσουν τα μέτρα, τις διαδικασίες και τα μέσα ένδικης προστασίας που προβλέπονται στην παρούσα οδηγία, προκειμένου να αποτρέψουν την παράνομη απόκτηση, χρήση ή αποκάλυψη οικείου εμπορικού απορρήτου ή να εξασφαλίσουν

έννομη προστασία. Η απόκτηση εμπορικού απορρήτου χωρίς τη συγκατάθεση του κατόχου του θεωρείται παράνομη όποτε διενεργείται με

- Μη επιτρεπόμενη πρόσβαση, ιδιοποίηση ή αντιγραφή εγγράφων, αντικειμένων, υλικών, ουσιών ή ηλεκτρονικών αρχείων που νομίμως βρίσκονται υπό τον έλεγχο του κατόχου του εμπορικού απορρήτου, τα οποία περιέχουν το εμπορικό απόρρητο ή από τα οποία μπορεί να εξαχθεί το εμπορικό απόρρητο.

- Οποιαδήποτε άλλη συμπεριφορά η οποία, υπό τις περιστάσεις αυτές, θεωρείται αντικείμενη στα χρηστά συναλλακτικά ήθη.

Η χρήση ή η αποκάλυψη εμπορικού απορρήτου θεωρείται παράνομη όποτε πραγματοποιείται χωρίς τη συγκατάθεση του κατόχου του εμπορικού απορρήτου από πρόσωπο που αποδεδειγμένα πληροί οποιαδήποτε από τις ακόλουθες προϋποθέσεις :

- Έχει αποκτήσει το εμπορικό απόρρητο παρανόμως.

- Έχει παραβιάσει συμφωνία εμπιστευτικότητας ή άλλη υποχρέωση μη αποκάλυψης του εμπορικού απορρήτου.

- Έχει παραβιάσει συμβατική ή άλλη υποχρέωση να περιορίζει τη χρήση του εμπορικού απορρήτου.

Η απόκτηση, η χρήση ή η αποκάλυψη εμπορικού απορρήτου θεωρείται επίσης παράνομη όταν ένα πρόσωπο, κατά τη στιγμή της απόκτησης, της χρήσης ή της αποκάλυψης, γνώριζε ή όφειλε, υπό τις περιστάσεις, να γνωρίζει ότι το εμπορικό απόρρητο αποκτήθηκε άμεσα ή έμμεσα από άλλο πρόσωπο το οποίο χρησιμοποιούσε ή αποκάλυπτε το εμπορικό απόρρητο παρανόμως. Η παραγωγή, προσφορά ή διάθεση στην αγορά παράνομων εμπορευμάτων, ή η εισαγωγή, εξαγωγή ή αποθήκευση παράνομων εμπορευμάτων για τους σκοπούς αυτούς, θεωρείται επίσης παράνομη χρήση εμπορικού απορρήτου όταν το πρόσωπο που ασκεί αυτές τις δραστηριότητες γνώριζε ή όφειλε, υπό τις περιστάσεις, να γνωρίζει ότι το εμπορικό απόρρητο χρησιμοποιήθηκε παρανόμως.

Επίσης σύμφωνα με το άρθρο 9 περί «Προστασίας του εμπιστευτικού χαρακτήρα των εμπορικών απορρήτων κατά τις δικαστικές διαδικασίες» :

«Τα κράτη μέλη διασφαλίζουν ότι οι αντίδικοι, οι δικηγόροι ή άλλοι εκπρόσωποί τους, τα μέλη του δικαστηρίου, οι μάρτυρες, οι πραγματογνώμονες και κάθε άλλο πρόσωπο που συμμετέχει στη δικαστική διαδικασία που αφορά την παράνομη απόκτηση, χρήση ή αποκάλυψη εμπορικού απορρήτου, ή που έχει πρόσβαση σε έγγραφα τα οποία αποτελούν μέρος των εν λόγω δικαστικών διαδικασιών, απαγορεύεται να χρησιμοποιούν ή να αποκαλύπτουν οποιοδήποτε εμπορικό απόρρητο ή θεωρούμενο εμπορικό απόρρητο, εις χείρας των αρμόδιων δικαστικών αρχών, μετά από δεόντως αιτιολογημένη αίτηση κάποιου ενδιαφερομένου, το οποίο έχει χαρακτηρισθεί εμπιστευτικό και περιήλθε σε γνώση τους λόγω αυτής της συμμετοχής ή πρόσβασης. Τα κράτη μέλη διασφαλίζουν επίσης ότι οι αρμόδιες δικαστικές αρχές δύνανται, βάσει δεόντως αιτιολογημένης αίτησης αντίδικου, να λαμβάνουν ειδικά μέτρα που είναι

αναγκαία προκειμένου να προστατευθεί η εμπιστευτικότητα κάθε εμπορικού απορρήτου ή θεωρούμενου εμπορικού απορρήτου το οποίο χρησιμοποιείται ή αναφέρεται κατά την εξέλιξη της δικαστικής διαδικασίας που αφορά την παράνομη απόκτηση, χρήση ή αποκάλυψη εμπορικού απορρήτου. (European Council, 2016)

Ελληνική Νομοθεσία

Όσον αφορά την ελληνική νομοθεσία, σύμφωνα με το άρθρο 372 του Ποινικού Κώδικα περί «Περί εγκλημάτων κατά της ιδιοκτησίας» :

«Όποιος αφαιρεί ξένο (ολικά ή εν μέρει) κινητό πράγμα από την κατοχή άλλου με σκοπό να το ιδιοποιηθεί παράνομα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών και αν το αντικείμενο της κλοπής είναι ιδιαίτερα μεγάλης αξίας με φυλάκιση τουλάχιστον δύο ετών.

Επιπρόσθετα, σύμφωνα με τα άρθρα 16 έως 18 του νόμου 146/1914 «Περί αθέμιτου ανταγωνισμού» :

«Άρθρο 16: Με φυλάκισιν μέχρις εξ μηνών και με χρηματικήν ποινήν (μέχρι τριών χιλιάδων δραχμών) ή με μίαν των ποινών τούτων τιμωρείται όστις, ως υπάλληλος, εργάτης ή μαθητευόμενος παρά τινι εμπορικώ ή βιομηχανικώ καταστήματι ή επιχειρήσει, ανακοινώνει άνευ δικαιώματος εις τρίτους, κατά το χρονικόν διάστημα της υπηρεσίας του, απόρρητα του καταστήματος ή της επιχειρήσεως εμπεπιστευμένα αυτώ ως εκ της υπηρεσίας του, ή άλλως περιελθόντα εις την αντίληψίν του, προς τον σκοπόν ανταγωνισμού ή επί τη προθέσει βλάβης του κυρίου του καταστήματος ή της επιχειρήσεως. Με την αυτήν ποινήν τιμωρείται και ο χρησιμοποιών ή ανακοινών εις τρίτους άνευ δικαιώματος, προς τον σκοπόν ανταγωνισμού, τα τοιαύτα απόρρητα, ων έλαβε γνώσιν διά τινός των εν τω προηγουμένω εδαφίω ανακοινώσεων ή δι' ιδίας αυτού πράξεως αντικειμένης εις τους νόμους ή τα χρηστά ήθη.

Άρθρο 17: Με την ποινήν του προηγουμένου άρθρου τιμωρείται ο άνευ διακαιώματος χρησιμοποιών ή ανακοινών εις τρίτους τα εμπιστευθέντα αυτώ κατά τας συναλλαγάς σχέδια ή κανόνες τεχνικής φύσεως, ιδία δε σχεδιάσματα, πρότυπα, τύπους, υποδείγματα, οδηγίας.

Άρθρο 18: Αι παραβάσεις των διατάξεων των άρθρων 16 και 17 γεννώσι προς τούτοις και υποχρέωσιν προς αποκατάστασιν της προξενηθείσης ζημίας. Με τας εν τω άρθρω 16 ποινάς, ηλαττωμένας εις το ήμισυ, τιμωρείται και όστις επιχειρεί επί σκοπώ ανταγωνισμού να εξωθήση άλλον εις πράξιν αντικειμένην εις τας διατάξεις του άρθρου 16 εδ.1 και άρθρου 17»

6. Επικοινωνία και Παρακολούθηση Κινδύνου Βιομηχανικής Κατασκοπείας

Οι ενέργειες επικοινωνίας και διαβούλευσης μεταξύ εσωτερικών και εξωτερικών ενδιαφερόμενων πρέπει να πραγματοποιούνται σε κάθε στάδιο της διαδικασίας διαχείρισης κινδύνου και είναι σημαντικές καθώς κρίνουν με βάση της αντιλήψεις τους σχετικά με τον κίνδυνο. Αυτές οι αντιλήψεις μπορεί να ποικίλουν λόγω διαφορών στις αξίες, στις ανάγκες, στις παραδοχές και στις ανησυχίες των ενδιαφερόμενων. Δεδομένου ότι οι απόψεις τους μπορούν να έχουν σημαντικό αντίκτυπο στις αποφάσεις που λαμβάνουν, οι αντιλήψεις τους θα πρέπει να εντοπίζονται, να καταγράφονται και να λαμβάνονται υπόψη στη διαδικασία λήψης αποφάσεων. (International Organization for Standardization, 2009, σσ. 14-15)

Οι προφανείς ενδιαφερόμενοι είναι οι εργαζόμενοι, οι πελάτες, οι προμηθευτές, οι επιχειρηματικοί εταίροι, οι επενδυτές, οι αναλυτές μετοχών, αποθεμάτων και άλλες ομάδες ειδικών συμφερόντων. Οι ρυθμιστικές αρχές θα πρέπει επίσης να συμπεριλαμβάνονται στα ενδιαφερόμενα μέρη μίας επιχείρησης ή ενός οργανισμού εάν οι εγκρίσεις και οι εξετάσεις από αυτές είναι κρίσιμες για την επιχειρηματική της επιτυχία. (Lam, 2014)

Τα περισσότερα προγράμματα αντικατασκοπείας δεν αντιμετωπίζουν επαρκώς τις ανθρώπινες αδυναμίες του εργατικού τους δυναμικού και αυτή η αποτυχία κοστίζει στον οργανισμό σημαντική απώλεια εσόδων, απώλεια ανθρώπινων ωρών έρευνας και ανάπτυξης και απώλεια εμπιστοσύνης των επενδυτών. Ενώ τα ισχυρά τεχνικά αντίμετρα παρέχουν ένα ασφαλές περιβάλλον λειτουργίας, μπορούν να καταστρατηγηθούν από έναν εργαζόμενο που έχει τα κίνητρα και την ικανότητα να το κάνει. Ένα ενισχυμένο εταιρικό πρόγραμμα καταπολέμησης της βιομηχανικής κατασκοπείας αξιοποιεί εξειδικευμένες πρακτικές ανίχνευσης, μεθοδολογίες και στρατηγικές απόκρισης για την αποτροπή, εκμετάλλευση και αντιμετώπιση των πιο σοβαρών απειλών. (OptimalRisk, 2014)

6.1. Δείκτες Συστήματος Ανάλυσης Επιθέσεων

Για να είναι αποτελεσματική η διαχείριση κινδύνου εντός ενός οργανισμού, θα πρέπει να είναι βέβαιο πως τα στελέχη καταλαβαίνουν ότι ενώ οι επιθέσεις πρόκειται να συμβούν, υπάρχουν ενέργειες οι οποίες μπορεί να γίνουν και να έχουν ένα θετικό αντίκτυπο.

Χρησιμοποιώντας συγκεκριμένους δείκτες ανάλυσης είναι δυνατό για μία οργανωμένη

επιχείρηση να εντοπίσει ενδεχόμενες παραβιάσεις και επιθέσεις οι οποίες σχετίζονται με την απειλή της βιομηχανικής κατασκοπείας. Στον κάτωθι Πίνακα 8 παρουσιάζονται περιεκτικές πληροφορίες σχετικά με τις κατηγορίες, τους πιθανούς δείκτες και τους τύπους επιθέσεων που μπορεί να υποδεικνύουν. Οι δείκτες ανάλυσης με τον αριθμό «1» στο κελί δείχνουν πρωτογενείς δείκτες που είναι πιθανότερο να συσχετιστούν με τη δραστηριότητα, τα κελιά με τον αριθμό «2» θεωρούνται δείκτες στήριξης και τα κελιά που δεν περιέχουν αριθμό μπορούν να παρέχουν χρήσιμες πληροφορίες στην επιχείρηση.

Η ανάλυση που δύναται να πραγματοποιηθεί αφορά την συμπεριφορά των εργαζομένων, την ικανοποίηση τους και άλλου είδους συμπεράσματα τα οποία μπορεί να προκύψουν εξ' επαγωγής από την εν γένει εικόνα τους.

Πίνακας 10. Δείκτες Ανάλυσης για τον εντοπισμό επιθέσεων (Πηγή DIB & ITS, 2015:29)

Κατηγορία Δείκτη Ανάλυσης	Δείκτης Ανάλυσης	Είδη Επιθέσεων								
		Τυχαία Διαρροή	Κατασκοπεία	Οικονομική Απάτη	Κατάχρηση	Ευκαιριακή Κλοπή Δεδομένων	Φυσική Κλοπή	Μετατροπή Προϊόντος	Δολιοφθορά	Βιαιότητα
Ανάλυση με Βάση τη Δραστηριότητα										
Σύστημα	Αποτυχία Επαλήθευσης Ταυτότητας και Εξουσιοδότησης		1	1	1	1		1	1	
	Αλλαγές στα Μοτίβα Πρόσβασης σε Δεδομένα		1	1	1	1		1	1	
	Πρόσβαση μη Συμβατή με την Κατηγορία Χρήστη		1	1	1	1		1	1	
	Αλλαγές στα Μοτίβα Δικτύου	2	2	1		1			2	
	Μοτίβα Δικτύου μη Συμβατά με την Κατηγορία Χρήστη	1	1			1				
	Εξαγωγή Δεδομένων	1	2	2		1			2	
	Μη Εγκεκριμένες Μέθοδοι Πρόσβασης σε Δεδομένα	1	1		1	1				
	Αλλαγή Δικαιωμάτων		1	2	1	1		2		2
	Εσφαλμένες Αλλαγές Αμυντικής Στάσης	2			1	1		2		
	Ακατάλληλη Χρήση Εντολών	2								
	Πρόσβαση Γνώσης		1	2	1	1				
	Τροποποίηση Αρχείου Ελέγχου		2	1	1			1	1	
Εγκαταστάσεις	Αλλαγές στα Μοτίβα Χρόνων Πρόσβασης		2	2		2	1	1	1	1
	Αλλαγές στα Μοτίβα Τοποθεσιών Πρόσβασης		2	2		2	1	2	1	1
Επιχειρηματικές Δυνατότητες	Αποτυχημένη Συσχέτιση				2			1	1	2
	Ανάπτυξη Κακόβουλου Λογισμικού		1		1				1	2
	Διαγραφή ή Τροποποίηση Δεδομένων ή Υποδομής			1	1	2		1	2	
	Ανάλυση Ανταγωνιστών		1		1					
	Ανάλυση Μέσων Μαζικής Ενημέρωσης	2	1		1		1			
	Αποτίμηση Δημοσιοποίησης	1	1		1		1			
	Ανάκτηση	2		2	2	1				

Πίνακας 10. Δείκτες Ανάλυσης για τον εντοπισμό επιθέσεων (Πηγή DIB & ITS, 2015:30) (Συνέχεια)

Κατηγορία Δείκτη Ανάλυσης	Δείκτης Ανάλυσης	Είδη Επιθέσεων								
		Τυχαία Διαρροή	Κατασκοπεία	Οικονομική Απάτη	Κατάχρηση	Ευκαιριακή Κλοπή Δεδομένων	Φυσική Κλοπή	Μετατροπή Προϊόντος	Δολιοφθορά	Βιαιότητα
Ανάλυση με Βάση την Ικανοποίηση										
Κοινωνικά	Αδιαφορία	2			1	1	1	2		1
	Προσωπική Ανελαστικότητα	2	2	2	2	2		2	2	2
	Ασυνήθιστα Επαγγελματικά Ταξίδια		1				2	1		2
	Ασυνήθιστα Προσωπικά Ταξίδια		1			2	2	1		2
	Μη Εξουσιοδοτημένες ή Ακατάλληλες Σχέσεις		1			2	2	1		2
	Στέρηση					2	1	2	2	1
	Περιστατικά στο Χώρο Εργασίας		2		2	2	1	2	2	1
	Ικανοποίηση στο Χώρο Εργασίας			2		2	1	1	1	1
Υγεία	Πνευματική Αστάθεια				2			2	1	1
	Έλεγχος Καρδιακών Παλμών			1		1	1			
Ανθρώπινο Δυναμικό	Σημαντικό Γεγονός στη Ζωή			1			1	1	1	1
	Παράπονα Εναντίον του Χρήστη								2	2
	Αρνητικές Κριτικές		2	1	1	2	1	2	1	1
Επαγωγική Ανάλυση										
Οικονομικά	Παρατηρούμενη Ξαφνική Αλλαγή Μέσων		1	1			1	1	1	2
	Παρατηρούμμενη Αλλαγή Μέσων σε Σχέση με τους Ομοίους		1	1			1	1	1	2
	Οικονομικές Αναφορές		1	1				1	1	2
Ασφάλεια	Αλλαγή στα Μοτίβα Παραβίασης		2	2	2		1	2	1	2
	Διάρκεια και Τακτικότητα Περιστατικών Ασφαλείας	1		2	2		1	2	1	2
	Μη εξουσιοδοτημένη ή Ακατάλληλη Χρήση Εργαλείων							2		
Ποινικά	Περιοριστικά Μέτρα				2					1
	Κατασχέσεις			1						
	Βία εκτός του Χώρου Εργασίας				2				1	2
	Πρόσφατη Αύξηση Ποινικών Συμβάντων						1	2		

6.2 Διαδικασία Εντοπισμού εν Δυνάμει Κατασκόπου

Οι επιχειρήσεις πρέπει να προσπαθούν να αναγνωρίσουν κάθε πιθανό παράγοντα που μπορεί να καταστήσει ένα στέλεχός τους περισσότερο επιρρεπή στην αποκάλυψη πληροφοριών. Επίσης, πρέπει να διεξάγουν περιοδικές εκτιμήσεις ασφάλειας του προσωπικού ακόμα και αν έχει αρχικώς ελεγχθεί. (Hagon, 2012) Σε αντίθεση με άλλους τύπους προγραμμάτων ασφάλειας υπολογιστών, τα οποία συνήθως στοχεύουν σε απειλές κακόβουλου λογισμικού ή εσωτερικά συστήματα υπολογιστών, τα προγράμματα απειλών εσωτερικών προσώπων επικεντρώνονται

σε άτομα, τα οποία μπορούν να δημιουργήσουν μια σειρά πολιτικών, ιδιωτικών και ηθικών ανησυχιών. Ένα αποτελεσματικό πρόγραμμα εσωτερικής απειλής πρέπει να εξισορροπήσει διάφορα συμφέροντα, συμπεριλαμβανομένης της προστασίας των ιδιοκτησιακών, ευαίσθητων και διαβαθμισμένων περιουσιακών στοιχείων ενός οργανισμού, καθώς και τη διατήρηση της ιδιωτικής ζωής των πελατών και των εργαζομένων και των πολιτικών ελευθεριών. Ενώ η προστασία των δεδομένων και των στοιχείων ενεργητικού ενός οργανισμού αποτελεί κεντρικό στόχο ενός προγράμματος αθέμιτης εμπιστοσύνης, ένας οργανισμός που δεν προστατεύει επαρκώς τα δεδομένα των εργαζομένων ή τα χρησιμοποιεί με τρόπους που δεν έχουν εγκρίνει οι εργαζόμενοι, κινδυνεύει να χάσει την εμπιστοσύνη των εργαζομένων ή να αντιμετωπίσει τις επιπτώσεις. Η σχέση μεταξύ ενός οργανισμού και των υπαλλήλων του πρέπει να περιλαμβάνει διαφάνεια σχετικά με τις επιχειρηματικές πρακτικές που έχουν ως αποτέλεσμα τη χρήση και τη γνωστοποίηση των πληροφοριών των εργαζομένων. Οποιεσδήποτε βελτιώσεις σε ένα πρόγραμμα εμπιστευτικών πληροφοριών πρέπει να γίνονται με τρόπο που να διατηρεί την εμπιστοσύνη μεταξύ εργαζομένων και εργοδότη, μεταξύ του οργανισμού και των πελατών του, καθώς και μεταξύ του οργανισμού και του κοινού. (DIB & ITS, 2015, σ. 5)

Μία από τις καλύτερες μεθόδους για την πρόληψη και τον εντοπισμό των φαινομένων βιομηχανικής κατασκοπείας είναι η χρήση των στοιχείων που διαθέτει το Τμήμα Ανθρωπίνου Δυναμικού για τους εργαζόμενους της επιχείρησης. Λαμβάνοντας υπόψη τα στοιχεία αυτά, που αφορούν κυρίως στο ιστορικό και στο χαρακτήρα του κάθε υπαλλήλου, είναι δυνατή η συνολική ταξινόμηση σύμφωνα με κάποια προκαθορισμένα κριτήρια.

Το Τμήμα Ανθρώπινου Δυναμικού, συχνά σε συνεργασία με το Τμήμα Ασφαλείας, διεξάγει ελέγχους και έρευνα του ιστορικού όλων των αιτούντων εργασία. Αυτή η έρευνα μπορεί να χρησιμοποιηθεί για την απόρριψη ενός αιτούντος που μπορεί να αποσκοπεί σε κλοπές ή βιομηχανική κατασκοπεία. Μια έρευνα του επαγγελματικού παρελθόντος μπορεί να καθορίσει εάν ένα άτομο αποτελεί μια πιθανή μελλοντική απειλή και να εκθέσει έναν υποψήφιο που προσπαθεί να αποκτήσει μια θέση στον οργανισμό αποκλειστικά με σκοπό τη διεξαγωγή βιομηχανικής κατασκοπείας. Το βάθος της έρευνας εξαρτάται από τον αιτούντα, την πιθανή θέση του στην επιχείρηση και το επίπεδο απειλής. (Benny, 2014, σ. 138)

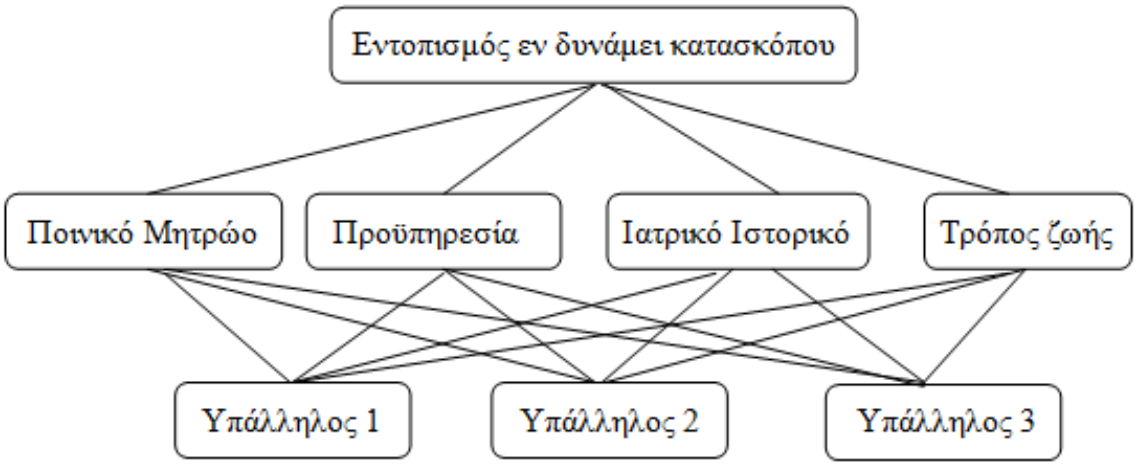
Τα στοιχεία του παρελθόντος που δύναται να χρησιμοποιήσει μία επιχείρηση για τον εντοπισμό ενός πιθανού ή εν δυνάμει κατασκόπου είναι τα ακόλουθα:

- Ποινικό Μητρώο
- Μητρώο Οδήγησης
- Επαγγελματική Προϋπηρεσία
- Επαγγελματικές Άδειες και Πιστοποιήσεις
- Εκπαίδευση
- Συμμετοχή σε Οργανώσεις-Λέσχες

- Ιστορικό Οικονομικής Κατάστασης
- Στρατιωτική Θητεία
- Τόπος διαμονής
- Οικογενειακή Κατάσταση
- Τρόπος ζωής
- Ιατρικό Ιστορικό

Χρησιμοποιώντας τη Διαδικασία Αναλυτικής Ιεράρχησης και τα στοιχεία του προσωπικού είναι δυνατή η δημιουργία μίας ενδεικτικής λίστας αναλόγως της εκτιμώμενης πιθανότητας να διαπράξουν ενέργειες βιομηχανικής κατασκοπείας. Η Διαδικασία Αναλυτικής Ιεράρχησης είναι μία μέθοδος που αποσκοπεί στην ποσοτικοποίηση των διαχειριστικών αποφάσεων με βάση την σχετική σημαντικότητα πολλαπλών αντικρουόμενων κριτηρίων. (Saaty, 2008)

Αρχικά, γίνεται ο προσδιορισμός του προβλήματος, ο οποίος περιλαμβάνει τον καθορισμό του στόχου της διαδικασίας, τα κριτήρια για την επίτευξή του και τις δυνατές επιλογές. Στη συγκεκριμένη περίπτωση ο στόχος της διαδικασίας είναι η ταξινόμηση του προσωπικού, τα κριτήρια είναι τα στοιχεία που διαθέτει η επιχείρηση και οι δυνατές επιλογές είναι οι εργαζόμενοι. Για τους σκοπούς της εργασίας θα παρουσιαστεί η διαδικασία για τρεις υποτιθέμενους εργαζόμενους με βάση τέσσερα κριτήρια. Παρομοίως μπορεί να εκτελεστεί για όλο το προσωπικό της επιχείρησης και περισσότερα κριτήρια αναλόγως των απαιτήσεων. Οι πράξεις υπολογισμού των τιμών παρουσιάζονται αναλυτικά στο Παράρτημα «Β».



Διάγραμμα 3. Προσδιορισμός Προβλήματος Διαδικασίας Αναλυτικής Ιεράρχησης

Το επόμενο βήμα είναι ο σχηματισμός πινάκων σύγκρισης ανά ζεύγη στοιχείων $\mathbf{a_{ij}}$ των εναλλακτικών επιλογών i και j. Πιο συγκεκριμένα, συγκρίνονται τα ζεύγη κριτηρίων με το στόχο και τα ζεύγη εναλλακτικών λύσεων με κάθε ένα από τα κριτήρια και έτσι προκύπτουν

αριθμητικές κλίμακες μέτρησης. Η βαρύτητα της i-οστής επιλογής εκφράζεται ως w_i βάσει του κάθε κριτηρίου σε κλίμακα αντίστροφου λόγου, δηλαδή:

$$a_{ij} = \frac{1}{a_{ij}} \text{ για κάθε i, j, με } a_{ij} \neq \infty \qquad \{6.2\text{-}1\}$$

Έπειτα, εκτελείται ο υπολογισμός των προτεραιοτήτων μεταξύ των στοιχείων της ιεραρχίας που δημιουργεί μια σειρά αποφάσεων. Οι προτεραιότητες είναι αριθμοί που αντιπροσωπεύουν τα σχετικά βάρη των κόμβων σε κάθε ομάδα και κυμαίνονται από 0 έως 1. Τα στοιχεία α_{ij} υπολογίζονται ως ο λόγος βαρύτητας των επιλογών i και j όπου **w** η βαρύτητα των i και j αντίστοιχα.

$$a_{ij} = w_i / w_j \qquad \{6.2\text{-}2\}$$

Έτσι, για n εναλλακτικές δυνατότητες έχουμε:

$$a_{i1}w_1 + a_{i2}w_2 + ... + a_{in}w_n = nw_i \text{ i=1,…, n} \qquad \{6.2\text{-}3\}$$

Επομένως, σύμφωνα με τον πίνακα συγκρίσεων προκύπτει:

$$Aw = nw\text{, όπου A ο πίνακας συγκρίσεων} \qquad \{6.2\text{-}4\}$$

Ο απαραίτητος αριθμός συγκρίσεων που απαιτούνται για τη συμπλήρωση του πίνακα είναι: $(n^2- n)/ 2$. Στη σύγκριση κάθε ζεύγους διακρίνεται ο πιο σημαντικός παράγοντας και ο βαθμός σημαντικότητάς του σύμφωνα με την κλίμακα του Saaty από 1 έως 9. Αφού γίνει αυτό, ο ανωτέρω τύπος (1) μετατρέπεται σε:

$$Aw = \lambda_{max} w \qquad \{6.2\text{-}5\}$$

Όπου λ_{max} η τιμή της πρωτεύουσας ιδιοτιμής που υπολογίζεται από τον τύπο:

$$\lambda_{max} = 1/n \sum_{i=1}^{n} \lambda_i \qquad \{6.2\text{-}6\}$$

Η βαρύτητα w υπολογίζεται ως εξής:

$$w_i = u_i / \sum_{k=1}^{n} u_k \text{, για i= 1,…,n.} \qquad \{6.2\text{-}7\}$$

Έπειτα, γίνεται ο έλεγχος της συνέπειας των αποφάσεων. Ο δείκτης συνέπειας Consistency Index (**C.I.)** δείχνει την απόκλιση της συνέπειας. Ο τύπος του είναι ο εξής: (Saaty & Sodenkamp, 2010)

$$C.I. = (\lambda_{max} - n)/(n-1) \qquad \{6.2\text{-}8\}$$

Επιπλέον, ο τυχαίος δείκτης συνέπειας Random Index (R.I.) υπολογίζεται από ένα θετικά ορισμένο πίνακα συγκρίσεων με τυχαία δεδομένα εισόδου.

Πίνακας 11. Τιμές Random Index (R.I.)

Αριθμός Επιλογών	3	4	5	6	7	8
RI	0,58	0,90	1,12	1,24	1,32	1,41

Ο τελευταίος δείκτης που ολοκληρώνει τη διαδικασία του ελέγχου συνέπειας των αποτελεσμάτων είναι ο λόγος συνέπειας Consistency Ratio (C.R.) και ορίζεται ως:

$$C.R. = C.I./R.I. \qquad \{6.2\text{-}9\}$$

Όταν ο λόγος συνέπειας $C.R. \geq 0{,}1$ είναι ασυνεπής και πρέπει να αναθεωρηθούν τα δεδομένα εισόδου του πίνακα. Όταν ο λόγος συνέπειας $C.R. \geq 0{,}1$ είναι συνεπής και φυσικά η ιδανική τιμή συνέπειας του δείκτη είναι το 0. (Brunelli, 2015)

Τέλος, η συνολική προτεραιότητα κατατάσσει τις εναλλακτικές λύσεις σε σχέση με όλα τα κριτήρια και υπολογίζεται για κάθε εναλλακτική λύση, πολλαπλασιάζοντας την προτεραιότητα του κάθε κριτηρίου με την αντίστοιχη τοπική προτεραιότητα και αθροίζοντάς τες. Ο γενικός τύπος υπολογισμού των παγκόσμιων προτεραιοτήτων είναι:

$\mathrm{wi}^{\mathrm{l}} = \sum_{j=1}^{n_{i-1}} w_{ij}^{j} w_{j}^{I-1}$, όπου **l** το επίπεδο της κάθε εναλλακτικής λύσης. {6.2-10}

Πίνακας 12. Συνολικό Διάγραμμα Προτεραιοτήτων Διαδικασίας Αναλυτικής Ιεράρχησης

Υπάλληλοι	**Κριτήριο 1ο** (0,565)	**Κριτήριο 2ο** (0,201)	**Κριτήριο 3ο** (0,071)	**Κριτήριο 4ο** (0,162)	**Αποτέλεσμα**
Υπάλληλος 1	0,298	0,471	0,571	0,324	0,356
Υπάλληλος 2	0,632	0,059	0,278	0,587	0,484
Υπάλληλος 3	0,069	0,471	0,151	0,089	0,158

Από τα ανωτέρω αποτελέσματα φαίνεται πως ο Υπάλληλος 2 έχεις τις περισσότερες πιθανότητες να προτίθεται ή να καταλήξει να διαπράττει ενέργειες οι οποίες σχετίζονται με τη βιομηχανική κατασκοπεία ενώ ο Υπάλληλος 3 τις λιγότερες.

Με τη μέθοδο της Διαδικασίας Αναλυτικής Ιεράρχησης μπορεί μία επιχείρηση να ταξινομήσει τους υπαλλήλους της σύμφωνα με οποιοδήποτε κριτήριο και να διαμορφώσει μία αντικειμενική άποψη σχετικά με το ποιους να προσλάβει και ποιους να υποπτεύεται περισσότερο.

6.3 Αυτοαξιολόγηση και Απόδοση Χειρισμού

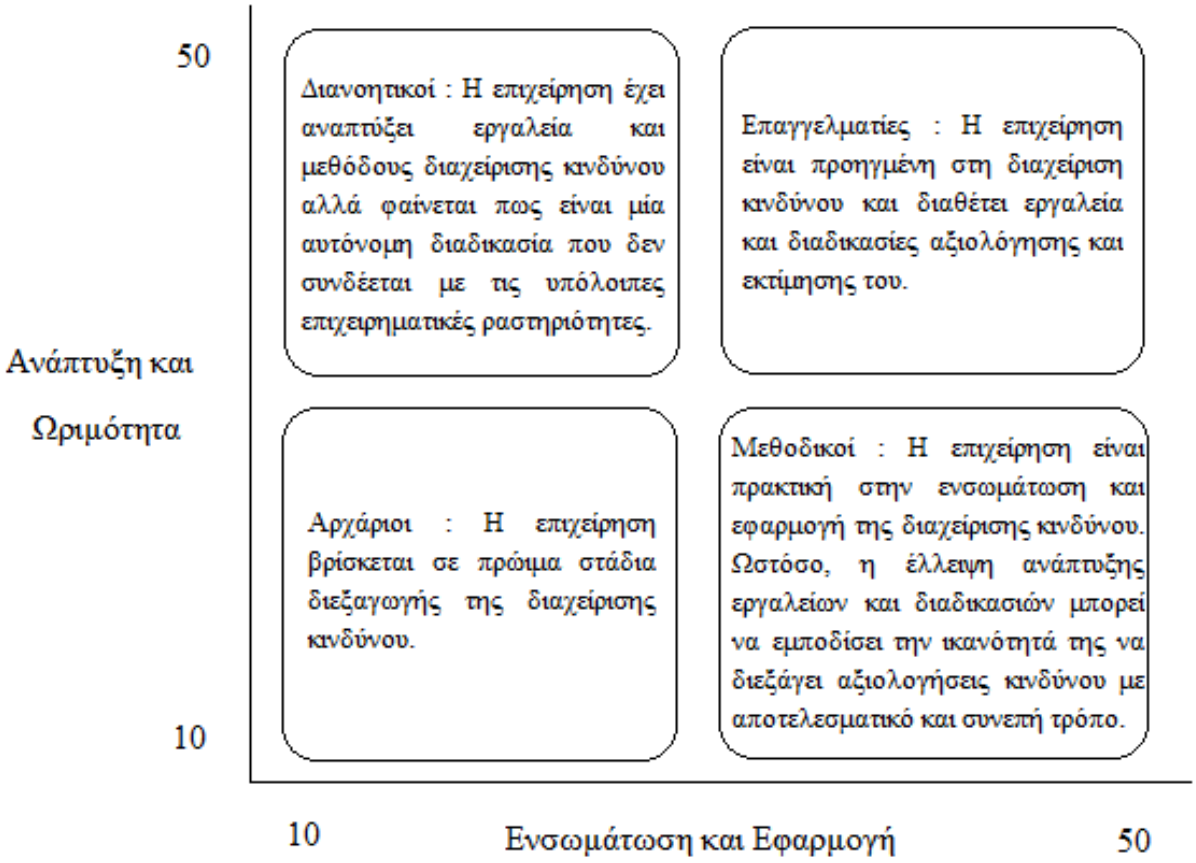
Η διαδικασία διαχείρισης κινδύνων όπως αυτή περιγράφεται στο πρότυπο ISO 31000:2009 περιλαμβάνει σε όλα της τα στάδια την παρακολούθηση και αναθεώρηση των ενεργειών που εκτελούνται. Μία μέθοδος που δύναται να συνδράμει στην επιτυχή αυτοαξιολόγηση και την απόδοση των ενεργειών χειρισμού των κινδύνων είναι η δημιουργία μίας λίστας ελέγχου.

Καθώς οι επιχειρήσεις αξιολογούν τις τρέχουσες διαδικασίες διαχείρισης κινδύνων έναντι των βέλτιστων δυνατών πρακτικών, η ακόλουθη λίστα ελέγχου μπορεί να χρησιμεύσει ως ένα πλαίσιο προτύπων και προτάσεων για τη μετάβαση από το ένα στάδιο στο άλλο. Με βάση τις βαθμολογίες αυτοαξιολόγησης, μία επιχείρηση μπορεί να εντοπίσει κρίσιμα κενά και καθορίσει συγκεκριμένους τομείς βελτίωσης. (Lam, 2014, σ. 415)

Στην περίπτωση της βιομηχανικής κατασκοπείας, κατόπιν της σχετικής εκπαίδευσης οι οποία θα έχει προηγηθεί ως μέσο χειρισμού και πρόληψής της όπως αναφέρθηκε και στο Κεφάλαιο 5, μία λίστα ελέγχου και αυτοαξιολόγησης θα αποτελέσει βασικό μέσο καθορισμού του επιπέδου και της κατάστασης που βρίσκεται μία επιχείρηση και το κατά πόσο το έργο διαχείρισης του κινδύνου της βιομηχανικής κατασκοπείας που επιτελείται είναι επαρκές.

Η αυτοαξιολόγηση μίας επιχείρησης βασίζεται σε δύο διαστάσεις όσον αφορά τη διαχείριση κινδύνων. Η μία διάσταση είναι η ανάπτυξη και ωριμότητα των προτύπων διαχείρισης κινδύνων, δηλαδή το επίπεδο στο οποίο η επιχείρηση έχει αναπτύξει μία ισχυρή και ώριμη διαδικασία διαχείρισης κινδύνων και η δεύτερη διάσταση την ενσωμάτωση και εφαρμογή των αποτελεσμάτων διαχείρισης κινδύνων, δηλαδή σε ποιο επίπεδο η επιχείρηση είναι αποτελεσματική στην ενσωμάτωση της διαχείρισης κινδύνων εντός των διαδικασιών της και στην εφαρμογή των αποτελεσμάτων για την καλύτερη λήψη αποφάσεων.

Η διαδικασία αυτοαξιολόγησης περιλαμβάνει τη βαθμολογία των διαδικασιών διαχείρισης κινδύνου από 1 έως 5 και το άθροισμα των συνολικών βαθμών για την ανάπτυξη/ωριμότητα και ενσωμάτωση/εφαρμογή αντίστοιχα. Για κάθε άθροισμα, η ελάχιστη βαθμολογία είναι 10 βαθμοί και η μέγιστη είναι 50 βαθμοί, με μία βαθμολογία μέσης τάξης τους 30 βαθμούς. Οι πίνακες με τα υπό αξιολόγηση κριτήρια για την ανάπτυξη/ωριμότητα των προτύπων διαχείρισης κινδύνων και την ενσωμάτωση/εφαρμογή των εξαχθέντων αποτελεσμάτων παρουσιάζονται αναλυτικά στο Παράρτημα «Γ».



Διάγραμμα 4. Διάγραμμα Αυτοαξιολόγησης (Βασισμένο στο Lam, 2014:420)

Με βάση τα δύο αθροίσματα, προσδιορίζεται το τεταρτημόριο στο οποίο ανήκει η επιχείρηση και εν συνεχεία γίνεται η αξιολόγηση των αποτελεσμάτων και η δημιουργία ενός πλάνου για την περαιτέρω ανάπτυξη, ενσωμάτωση και εφαρμογή της διαχείρισης κινδύνων στην επιχείρηση.

7. Συμπεράσματα

Στην παρούσα διπλωματική εργασία πραγματοποιήθηκε μία συνοπτική παρουσίαση του φαινομένου της βιομηχανικής κατασκοπείας και αναλύθηκαν οι τακτικές, τα κίνητρα-αίτια και οι παράμετροι οι οποίες οδηγούν στην άσκησή της από εσωτερικούς και εξωτερικούς δρώντες εναντίον επιχειρήσεων. Ακολούθως, προτάθηκαν ενέργειες χειρισμού οι οποίες έχουν σαν στόχο τη θωράκιση του οργανισμού όσον αφορά την «παθητική» του ασφάλεια (προληπτικές), αλλά και μέθοδοι εντοπισμού και εκτίμησης πιθανών μελλοντικών απειλών, ως μέσα για τη δημιουργία ενός προγράμματος «ενεργητικής» ασφάλειας (κατασταλτικές). Η δομή της εργασίας βασίστηκε στο πρότυπο ISO 31000:2009 με τίτλο "Risk management – Principles and guidelines" το οποίο παρέχει ένα συγκεκριμένο πλάνο και μία βηματική διαδικασία για την διαχείριση κινδύνων.

Κατά την διάρκεια της έρευνας για την εκπόνηση της εργασίας, παρατηρήθηκε πως στη βιβλιογραφία γίνεται συχνά σύγχυση μεταξύ των όρων της βιομηχανικής και της οικονομικής κατασκοπείας. Αν και ο ορισμός των δύο αυτών όρων είναι ξεκάθαρος και αναδεικνύει τη διαφορά τους, η σύγχυση αυτή εκτιμάται πως οφείλεται στην έντονη σχέση που έχουν πλέον τα κράτη με τις μεγάλες επιχειρήσεις που δραστηριοποιούνται σε αυτά και επηρεάζουν σε μεγάλο βαθμό την πορεία της οικονομίας τους.

Αναζητώντας τα βαθύτερα αίτια του φαινομένου της βιομηχανικής κατασκοπείας φαίνεται πως οι κυριότεροι λόγοι εμφάνισης και αύξησής του είναι δύο. Από τη μία πλευρά, η αυξανόμενη τάση των ανθρώπων για ικανοποίηση των ατομικών συμφερόντων και η απληστία που επιδεικνύουν για την απόκτηση χρημάτων, τους οδηγούν στην παρανομία και την προδοσία της επιχείρησης στην οποία εργάζονται. Από την άλλη πλευρά, ο δεύτερος λόγος αύξησης των περιστατικών βιομηχανικής κατασκοπείας είναι η τάση για απομάκρυνση της νοοτροπίας των επιχειρήσεων από την απόκτηση ανταγωνιστικού πλεονεκτήματος σε σχέση με τις υπόλοιπες επιχειρήσεις και η προσήλωση στην απόκτηση συγκριτικού πλεονεκτήματος.

Μία επιχείρηση θεωρείται ότι έχει ανταγωνιστικό πλεονέκτημα έναντι των ανταγωνιστών της, όταν η διατήρηση των αποδόσεων ξεπερνά το μέσο όρο του κλάδου της και για να το αποκτήσει θα πρέπει μέσω της έρευνας και της ανάπτυξης νέων προϊόντων και υπηρεσιών να προσφέρει κάτι καινοτόμο το οποίο δεν υπήρχε πριν. Οι εταιρίες που δεν διαθέτουν αυτή την ικανότητα καταφεύγουν στη κατασκοπεία ώστε να αποκτήσουν συγκριτικό πλεονέκτημα, το οποίο αφορά την βραχυπρόθεσμη ικανότητα να προσφέρουν ένα προϊόν, το οποίο έχουν υποκλέψει, σε χαμηλότερη τιμή σε σύγκριση με τους νόμιμους ιδιοκτήτες του. Στην

πραγματικότητα, δίχως να καταφύγουν στην κατασκοπεία, ορισμένες εταιρίες δεν μπορούν να ανταγωνιστούν τις υπόλοιπες και ως εκ τούτου δεν μπορούν να επιβιώσουν.

Η επίδραση της βιομηχανικής κατασκοπείας στην έρευνα και ανάπτυξη και στην καινοτομία είναι μία συνέπεια έμμεση αλλά πολύ σημαντική. Η καινοτομία θεωρείται το σημαντικότερο κλειδί για την συνεχή βελτίωση των προσφερόμενων προϊόντων και υπηρεσιών και την απόκτηση ανταγωνιστικού πλεονεκτήματος. Ωστόσο, συχνά παραγκωνίζεται από το φόβο της απώλειας οικονομικών πόρων αλλά και της υποκλοπής από ανταγωνιστές με αποτέλεσμα την μείωση της αξίας της.

Καθώς οι πληροφορίες αποτελούν πλέον το σημαντικότερο στοιχείο πλούτου, οι επιχειρήσεις θα βρίσκονται υπό αυξανόμενη πίεση για να τις αποκτήσουν εντός ενός όλο και περισσότερο ανταγωνιστικού περιβάλλοντος. Ταυτόχρονα, απαιτείται να προστατεύουν τις κρίσιμες τεχνολογίες και καινοτομίες που έχουν αναπτύξει δεδομένου ότι αποτελούν τη βάση αυτού του νέου πλούτου και καθίστανται στόχοι της βιομηχανικής κατασκοπείας.

Για να είναι επιτυχής αυτή η προσπάθεια είναι απαραίτητη η ανάπτυξη και ενσωμάτωση στο σύνολο των τομέων και των διαδικασιών μίας επιχείρησης ενός σχεδίου κατάλληλα διαμορφωμένου συμφώνως των δυνατοτήτων της και προσαρμοσμένου στα στοιχεία αξίας τα οποία πρέπει να προστατεύσει. Το σχέδιο αυτό πρέπει να περιλαμβάνει ενέργειες πρόληψης, εντοπισμού αλλά και μεθόδους πρόβλεψης της πιθανότητας και των επιπτώσεων έκθεσης στον κίνδυνο της βιομηχανικής κατασκοπείας.

Είναι δεδομένο πως οι επιχειρήσεις θα πρέπει να αντιμετωπίζουν συνεχώς απειλές που θα θέτουν σε κίνδυνο την επιβίωση τους. Παρόλο που είναι αδύνατο να θωρακίσουν πλήρως τα στοιχεία αξίας που συμβάλλουν στην απόκτηση και διατήρηση του ανταγωνιστικού τους πλεονεκτήματος, θα πρέπει να είναι διαθέσιμες να πάρουν υπολογισμένα ρίσκα δίχως ο φόβος της υποκλοπής τους ή ακόμα και της αποτυχίας να γίνεται εμπόδιο στην πραγματοποίηση των στόχων τους.

Βιβλιογραφία

Agreement on Trade-Related Aspects of Intellectual Property Rights. (1995, 1 1). *World Trade Organization*. Ανάκτηση Σεπτέμβριος 4, 2017, από TRIPS Agreement: https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm

Androulidakis, I., & Kioupakis, F.-E. (2016). *Industrial espionage and technical surveillance counter measurers.* Cham: Springer.

Benny, D. J. (2014). *Industrial espionage,developing a counterespionage program.* Florida: CRC Press.

Brunelli, M. (2015). *Introduction to the analytic hierarchy process.* Aalto: Springer.

Burgess, C., & Power, R. (2011). *Secrets Stolen, fortunes lost: preventing intellectual property theft and economic espionage in the 21st century.* Burlington: Syngress.

CEB Risk Management Leadership Council. (2017, Σεπτέμβριος 4). *CEB.* Ανάκτηση από Top 10 Emerging Risks You Should Be Monitor: https://www.cebglobal.com/risk-audit/risk-management/emerging-risks.html

Cole E. (2013). *Advanced persistent threat: understanding the danger and how to protect your organization.* Waltham: Syngress.

Cole, E., & Ring, S. (2005). *Insider threat: Protecting the enterprise from sabotage, spying, and theft.* Massachusetts: Syngress.

Colibasanu, A. (2009, 4 15). *Between intelligence and espionage in the contemporary business environment.* Ανάκτηση Σεπτέμβριος 4, 2017, από SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1381009

DealNews. (2013, 11 12). *Deal News*. Ανάκτηση Σεπτέμβριος 4, 2017, από Περιορίζεται η οικονομική κατασκοπεία στην Γερμανία: http://www.dealnews.gr/leaders/item/91258-Περιορίζεται-η-οικονομική-κατασκοπεία-στην-Γερμανία?tmpl=component&print=1#.WUaIeFTyjIW

DIB, & ITS. (2015). *Analytic aproaches to detect insider threats.* Pittsburgh: Software

Engineering Institute.

Dodge, R. (2014, 12 1). *Security Magazine*. Ανάκτηση Σεπτέμβριος 4, 2017, από Addressing corporate espionage in the 21st century: http://www.securitymagazine.com/articles/85958-addressing-corporate-espionage-in-the-21st-century

European Council. (2016, 6 8). *EUR-lex*. Ανάκτηση Σεπτέμβριος 4, 2017, από Οδηγία (ΕΕ) 2016/943: http://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32016L0943

European Court of Human Rights. (1950, 11 4). *Council of Europe*. Ανάκτηση Σεπτέμβριος 4, 2017, από The European Convention on Human Rights: http://www.echr.coe.int/pages/home.aspx?p=basictexts

Gupta, J., & Sharma, S. (2009). *Information security and assurance.* New York: Information Science Reference.

Hagon, C. (2012, 9 29). *Incident Management Group*. Ανάκτηση από 10 strategies for preventing corporate espionage: http://www.imgsecurity.net/10-strategies-for-preventing-corporate-espionage/

Heims, P. A. (1982). *Countering industrial espionage.* Surrey: 20th Century Security Education Ltd.

International Organization for Standardization. (2009). *ISO 31000:2009, Risk management-principles and guidelines.* Geneva: ISO Copyright Office.

Lam, J. (2014). *Enterprise risk management, from incentives to controls.* New Jersey: Wiley.

Long, J. (2008). *No tech hacking:a guide to social engineering, dumpster diving, and shoulder surfing.* Burlington: Syngress.

Miller, D. (2017, 4 28). *Innovation Enterprise*. Ανάκτηση 8 19, 2017, από Risk Visualization and Predictive Analytics in Risk Management: https://channels.theinnovationenterprise.com/articles/risk-visualisation-and-predictive-analytics-in-risk-management

Mitnick, K., & Simon, W. (2002). *The art of deception, controlling the human element of security.* Indianapolis: Wiley.

Mundie, D. (2014, 3 31). *Software Engineering Institute*. Ανάκτηση από Unintentional insider threat and social engineering: https://insights.sei.cmu.edu/sei_blog/2014/03/unintentional-insider-threat-and-social-engineering.html?wt.ac=hpBlog

Nasheri, H. (2005). *Economic espionage and industrial spying.* New York: Cambridge

University Press.

NCIX. (2009, 7 23). *Homeland Security DIgital Library*. Ανάκτηση Σεπτέμβριος 4, 2017, από Annual Reports to Congress on Foreign Economic Collection and Industrial Espionage: https://www.hsdl.org/?lists&id=1980

OptimalRisk. (2014, 2 27). *Optimal Risk*. Ανάκτηση από A counter-espionage approach to corporate security management: http://www.optimalrisk.com/Counter-Espionage/Blog/Counter-Espionage-Blog/February-2014/A-Counter-Espionage-Approach-to-Corporate-Security

Paris Convention for the Protection of Industrial Property. (1979, 9 28). *WIPO*. Retrieved Σεπτέμβριος 4, 2017, from Paris Convention for the Protection of Industrial Property: http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=287556

Podszywalow, M. (2012, 3 1). *Risk Management Magazine*. Retrieved 6 18, 2017, from Preventing corporate espionage: http://www.rmmagazine.com/2012/03/01/preventing-corporate-espionage/

Reynolds, V. (2015). *Social engineering, the art of psychological warfare, human hacking, persuasion and deception.* CreateSpace Independent.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, σσ. 91-166.

Saaty, T. L., & Sodenkamp, M. (2010, Απρίλιος 21). The analytic hierarchy and analytic network measurement processes: the measurement of intangibles. *Applied Optimization*, σσ. 91-166.

Samli, C., & Jacobs, L. (2003). *Countering global industrial espionage: a damage control strategy.* Malden: Balckwell.

SECURITAS Inc. (2016). *SECURITAS INC*. Ανάκτηση Αύγουστος 30, 2017, από Top Security Threats and Management Issues Facing Corporate America: http://www.securitasinc.com/en/stand-alone/top-security-threats/

Sood, A. K., & Enbody, R. (2014, 12 19). *Georgetown Journal*. Ανάκτηση Σεπτέμβριος 4, 2017, από US military defense systems: the anatomy of cyber espionage by chinese hackers: http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/

U.S.Code. (2017, Σεπτέμβριος 4). *Cornell Law School*. Ανάκτηση από https://www.law.cornell.edu/uscode/text/18/1832

Wimmer, B. (2015). *Business Espionage, Risks, Threats and Countermeasures.* Oxford:

Elsevier.

Διεθνής Αμνηστία. (1948, 12 10). *Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου*. Ανάκτηση Σεπτέμβριος 4, 2017, από https://www.amnesty.gr/universal-declaration-of-human-rights

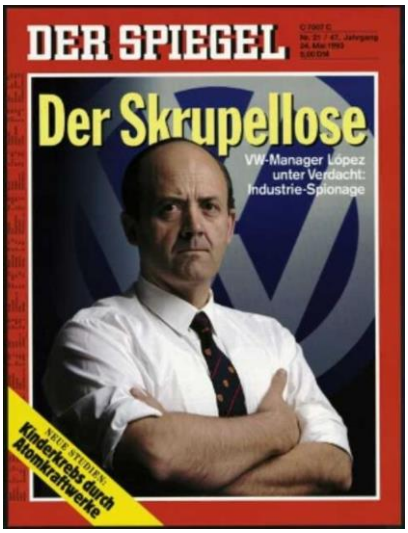
Κάτσουρα, Α. (2017, 3 12). *Efsyn*. Ανάκτηση Σεπτέμβριος 4, 2017, από Οικονομική κατασκοπία-ένας αόρατος πόλεμος: http://www.efsyn.gr/arthro/oikonomiki-kataskopia-enas-aoratos-polemos

Παραρτήματα

Α. Υποθέσεις Βιομηχανικής Κατασκοπείας

Υπόθεση 1η General Motors κατά Volkswagen

Κίνητρο : Προσωπική Ανέλιξη



Εικόνα Α.1. Υπόθεση Volkswagen-General Motors

Μεγάλο σκάνδαλο που ταλάνισε την αυτοκινητοβιομηχανία ήταν αυτό της μετεγγραφής στη γερμανική Volkswagen, το 1993, του Jose Ignacio Lopez de Arriortua, υψηλόβαθμου στελέχους της αμερικανικής General Motors και γενικού διευθυντή της θυγατρικής της Opel στις ΗΠΑ. Ο Jose Ignacio Lopez de Arriortua, ήταν γνωστός και με το όνομα «Σούπερ Lopez», διότι κατόρθωσε να περιορίσει τις δαπάνες της GM και να βελτιώσει τη γραμμή παραγωγής.

Δεν θα υπήρχε τίποτα το μεμπτό στη μετεγγραφή του μεγαλοστελέχους, που επ' ουδενί δεν θύμιζε Τζέιμς Μποντ, αν δεν προέκυπταν εις βάρος του υποψίες ότι, αλλάζοντας εργοδότη, μετέφερε στη Volkswagen μυστικά βιομηχανικά σχέδια και έγγραφα της GM, ενώ στέρησε από

την εταιρεία σειρά από συνεργάτες της.

Εκτός από την GM, εναντίον του Lopez στράφηκε και το FBI, ενώ εις βάρος του σχηματίστηκε δικογραφία για απάτη, εμπορική κατασκοπία και κατάχρηση εμπιστοσύνης, κατηγορίες που επισύρουν ποινές πενταετούς φυλάκισης και πολύ υψηλά πρόστιμα.

Ο Lopez υποστήριξε ότι είχε καταστρέψει όλα τα στοιχεία για την GM που είχε στα χέρια του πριν αναχωρήσει για τη VW, που τον στήριξε στην υπόθεση. Οι έρευνες των αμερικανικών αρχών όμως έφτασαν στα σπίτια συγγενών του, σε ένα εκ των οποίων βρέθηκε κουτί με βιομηχανικά έγγραφα και σχέδια της εταιρείας.

Εκτός από το πλήγμα στην εικόνα της VW, η υπόθεση λίγο έλειψε να δημιουργήσει διπλωματικό επεισόδιο μεταξύ Γερμανίας και ΗΠΑ, ενώ στη διευθέτησή της ενεπλάκησαν ο τότε καγκελάριος Χέλμουτ Κολ και ο πρόεδρος των ΗΠΑ, Μπιλ Κλίντον.

Το ζήτημα λύθηκε εξωδικαστικά μεταξύ των εταιρειών, αφού ο Lopez αναγκάστηκε να παραιτηθεί, να πληρώσει στο γερμανικό Δημόσιο πρόστιμο 400.000 ευρώ και να καταφύγει στην Ισπανία -παρά το αμερικανικό ένταλμα, δεν εκδόθηκε στις ΗΠΑ- με τη συμφωνία ότι η VW θα πλήρωνε στην GM 100 εκατ. δολάρια ως αποζημίωση, ενώ θα αγόραζε από την αμερικανική εταιρεία ανταλλακτικά συνολικής αξίας 1 δισ. δολαρίων.

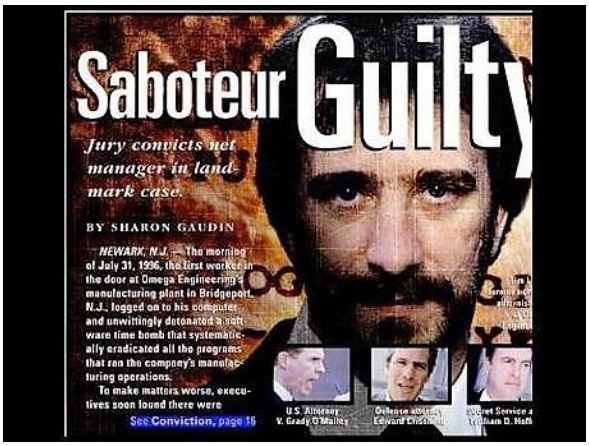
Υπόθεση 2η Cisco Systems κατά Osowski και Tang

Κίνητρο : Προσωπικό Οικονομικό Όφελος

Ο Geoffrey Osowski ήταν οικονομικός αναλυτής και ο Wilson Tang ήταν υπεύθυνος λογιστικής για τη Cisco Systems. Ως εργαζόμενοι γνώριζαν πλήρως το σύστημα ηλεκτρονικών υπολογιστών Sabrina που χρησιμοποιούσε για τη διαχείριση δικαιωμάτων προαίρεσης αγοράς μετοχών για την εταιρεία. Οι δυο τους τελικά χρησιμοποίησαν αυτές τις γνώσεις με κακόβουλο τρόπο και μεταβίβασαν παράνομα 7,8 εκατομμύρια δολάρια από το εταιρικό απόθεμα στους προσωπικούς τους λογαριασμούς. Έπειτα πούλησαν αυτό το παράνομα αγορασμένο απόθεμα και αγόρασαν πλούσια αντικείμενα όπως μια νέα Mercedes 320 για $ 52.000 και ένα δαχτυλίδι διαμαντιών για $ 44.000 και ένα ρολόι Rolex για $ 20.000.16 Σύμφωνα με την ανακοίνωση καταδίκης : "... την πρώτη φορά που το έκαναν αυτό, τον Δεκέμβριο του 2000, 97.750 μετοχές της Cisco τοποθετήθηκαν σε δύο ξεχωριστούς λογαριασμούς της Merrill Lynch, 58.250 μετοχές κατατέθηκαν σε λογαριασμό που ορίστηκε από τον Osowski και 39500 μετοχές σε λογαριασμό του Tang. Τον Φεβρουάριο του 2001 εκτέλεσαν δύο επιπλέον μεταφορές μετοχών, ύψους 67.500 μετοχών και 65.300 μετοχών, οι οποίες μεταβιβάστηκαν σε λογαριασμούς χρηματιστηριακών εταιρειών στο όνομά τους. Στις 20 Αυγούστου 2001, κηρύχθηκαν ένοχο και καταδικάστηκαν σε 34 μήνες φυλάκισης, τρία έτη ελεγχόμενης απελευθέρωσης και $ 7.868.637,50 αποζημίωση.

Υπόθεση 3η Wilmington Delaware κατά Lloyd

Κίνητρο : Εκδίκηση



Εικόνα Α.2. Υπόθεση Omega

Ο Timothy Allen Lloyd, της Wilmington, Delaware, ξεκίνησε ως μηχανικός της Omega Engineering Corporation. Αναρριχήθηκε στην εταιρική ιεραρχία και έγινε προγραμματιστής δικτύου υπολογιστών ο οποίος ήταν υπεύθυνος για τη διαμόρφωση και τη διατήρηση μέρους της υποδομής του Novell NetWare στην εταιρεία. Συνολικά, ο Lloyd πέρασε 11 χρόνια στην Omega. Σύμφωνα με δημοσιεύματα, αυτά τα χρόνια δεν ήταν πάντα θετικά και παραγωγικά. Καθώς η εταιρεία μεγάλωσε, το ίδιο έκανε και το δίκτυό τους. Ο Lloyd διαπίστωσε ότι πολλές από τις ευθύνες του μεταβιβάστηκαν σε άλλους και τα αρχεία του δικαστηρίου δείχνουν ότι το αντιλήφθηκε αυτό ως υποβιβασμό. Αφού η Omega αποφάσισε να απολύσει τον Lloyd, ο επιβλέπων του ζήτησε να εκπαιδεύσει και να δώσει πρόσβαση στον διακομιστή αρχείων στον εαυτό του και σε άλλους δύο υπαλλήλους. Ο Lloyd δεν το έκανε ποτέ αυτό. Μετά από μια σειρά προβλημάτων απόδοσης και συμπεριφοράς, ο Lloyd απολύθηκε στις 10 Ιουλίου 1996. Είκοσι μία ημέρες αργότερα, το πρωί της 31ης Ιουλίου 1996, ένα πρόγραμμα που ο Lloyd είχε εγκαταστήσει στους διακομιστές πριν από την αναχώρησή του και διέγραψε περίπου 1200 κρίσιμα προγράμματα. Παρά τις προσπάθειες για επανεκκίνηση του διακομιστή, δεν λειτουργούσε και οι μηχανές κατασκευής που βασίζονταν σε προγράμματα εργαλείων από το διακομιστή δεν μπορούσαν να λειτουργήσουν σωστά. Ο Jim Ferguson ήταν ο διευθυντής της εγκατάστασης εκείνη την εποχή και η άμεση απόφαση του ήταν να ανοικοδομήσει το διακομιστή από εφεδρικές ταινίες όσο το δυνατόν γρηγορότερα. Ωστόσο, οι εφεδρικές ταινίες δεν βρέθηκαν πουθενά. Στη συνέχεια προσπάθησε να ανακτήσει αντίγραφα των προγραμμάτων από μεμονωμένους σταθμούς εργασίας, αλλά είχαν επίσης διαγραφεί. Ο Lloyd είπε στον Ferguson ότι δεν είχε τις κασέτες και ότι έμειναν στο συρτάρι του στο γραφείο του. Γνωρίζοντας ότι το γραφείο του ήταν τελείως άδειο, ο Ferguson πήγε στο σπίτι του Lloyd και τον παρακάλεσε αυτοπροσώπως. Ακόμα, ο Lloyd έδειξε ότι δεν είχε την κατοχή των ταινιών. Αρκετές διαφορετικές εταιρείες ανάκτησης δεδομένων προσλήφθηκαν για να προσπαθήσουν

να ανακτήσουν τα διαγραμμένα προγράμματα, αλλά κάθε ένας δήλωσε στον Ferguson ότι ήταν αδύνατο. Ο Ferguson έκλεισε τα μηχανήματα, έκανε ανακατανομές στους εργαζόμενους σε άλλα τμήματα και προσέλαβε μια ομάδα προγραμματιστών για να ξαναγράψουν τα προγράμματα. Μία από τις εταιρείες ανάκτησης δεδομένων, η Ontrack Data International, έκανε ένα αντίγραφο του σκληρού δίσκου της Omega και το ανέλυσε. Ο Greg Olson αναγνώρισε την παρουσία ενός λογαριασμού χρήστη με την επωνυμία "12345" με πρόσβαση εποπτεύοντος, αλλά χωρίς κωδικό πρόσβασης. Δεύτερον βρήκε ένα πρόγραμμα που περιείχε έξι γραμμές κώδικα που φαινόταν να είναι η αιτία της βλάβης. Ο Olsen κατέληξε ότι το πρόγραμμα αυτό ενεργοποίησε για πρώτη φορά ένα πρόγραμμα με το όνομα "FIX.EXE" και το καθάρισε το δίσκο. Στην ανάλυσή του FIX.EXE διαπίστωσε ότι ήταν στην πραγματικότητα ένα αντίγραφο του DELTREE.EXE, ενός προγράμματος DOS που χρησιμοποιείται για τη διαγραφή καταλόγων αρχείων από λειτουργικά συστήματα Windows. Εν τω μεταξύ, τα στελέχη της Omega ανέφεραν την υπόθεση στη Μυστική Υπηρεσία των ΗΠΑ και ο Ειδικός Αντιπρόσωπος William Hoffman ήρθε στην Omega South για να ερευνήσει . Επειδή ο Lloyd ήταν το μόνο άτομο που είχε την απαραίτητη πρόσβαση για να προκαλέσει αυτή τη ζημιά και ήταν ο τελευταίος που γνώρισε τις εφεδρικές ταινίες την 1η Ιουλίου, εκδόθηκε ένταλμα έρευνας για το σπίτι του. Στις 12 Αυγούστου 1996, ερευνήθηκε το σπίτι του και κατασχέθηκαν περίπου 700 αποδεικτικά στοιχεία. Ο Lloyd κατηγορήθηκε στις 28 Ιανουαρίου 1998 από μια μεγάλη ομοσπονδιακή κριτική επιτροπή του Camden. Ισχυρίστηκαν ότι «προκάλεσε ανεπανόρθωτη ζημιά» στα συστήματα ηλεκτρονικών υπολογιστών της Omega και μετέφερε εξοπλισμό ηλεκτρονικών υπολογιστών κλεμμένο από το διαμετακομιστικό Omega στο σπίτι του στο Delaware. Η δίκη διήρκεσε τέσσερις εβδομάδες και η εισαγγελική αρχή ισχυρίστηκε ότι ο Lloyd ζήλευε και φερόταν άσχημα στους συναδέλφους του. Όπως αναφέρουν τα αρχεία του δικαστηρίου, οι μάρτυρες ισχυρίστηκαν ότι ο Lloyd «επανειλημμένα ακουμπούσε, έσπρωχνε και χτυπούσε τους συναδέλφους στους διαδρόμους και ότι έγινε λεκτικά καταχρηστικός». Μετά από τριήμερη συνάντηση της κριτικής επιτροπής, ο Lloyd καταδικάστηκε για τέλεση σαμποτάζ στον υπολογιστή και καταδικάστηκε σε ποινή φυλάκισης τριών ετών και πάνω από 2 εκατομμύρια δολάρια αποζημίωσης.

Υπόθεση 4η IBM κατά Hitachi

Κίνητρο : Οικονομική Ζημία στην Επιχείρηση

Η Hitachi Ltd. και δύο από τους υπαλλήλους της παραδέχθηκαν ότι συνωμοτούσαν για να κλέψουν εμπιστευτικές πληροφορίες υπολογιστών από τη International Business Machines Corporation και να τις μεταφέρουν στην Ιαπωνία. Σε αντάλλαγμα για την ενοχή για τη συνωμοσία, η κυβέρνηση συμφώνησε να μην απαγγελθούν περαιτέρω κατηγορίες εναντίον της Hitachi και των δύο υπαλλήλων και επιβλήθηκε πρόστιμο ύψους 10.000 $. Οι δύο υπάλληλοι που παραδέχθηκαν την ενοχή τους ήταν ο Kenji Hayashi, ανώτερος μηχανικός, και ο Isao Ohnishi, διευθυντής τμήματος λογισμικού. Στον κ. Hayashi επιβλήθηκε πρόστιμο ύψους 10.000 δολαρίων και στον κ. Ohnishi επιβλήθηκε πρόστιμο ύψους 4.000 δολαρίων, και οι δύο τέθηκαν υπό δικαστική επιτήρηση.

Ο Peter Fleming, δικηγόρος της Hitachi, δήλωσε ότι το διοικητικό συμβούλιο της ιαπωνικής εταιρίας πληροφορικής είχε εγκρίνει τις ενοχές πράξεις, παρόλο που η εταιρεία εξακολούθησε να ισχυρίζεται ότι δεν γνώριζε για τη συνωμοσία.

Οι κατηγορίες απαγγέλθηκαν μετά από επτάμηνη έρευνα από F.B.I. Κατά τη διάρκεια της έρευνας, πράκτορες του F.B.I. προσποιήθηκαν ότι είναι ειδικοί σύμβουλοι ηλεκτρονικών υπολογιστών με πρόσβαση σε μυστική τεχνολογία υπολογιστών στην I.B.M., και πούλησαν μερικές από τις πληροφορίες στους Ιάπωνες.

Η απόκτηση πρόσβασης σε τέτοια εμπορικά μυστικά, όπως υποστήριξε το υπουργείο Δικαιοσύνης, θα είχε βοηθήσει τη Hitachi και τη Mitsubishi να δημιουργήσουν υπολογιστές που θα μπορούσαν να χρησιμοποιηθούν εναλλακτικά με τα προϊόντα I.B.M. Οι εταιρείες στο πεδίο των υπολογιστή συχνά προσπαθούν να κάνουν τον εξοπλισμό τους εναλλάξιμο με τους υπολογιστές I.B.M προκειμένου να αυξήσουν τις πωλήσεις τους.

Μετά την εμφάνιση των κατηγοριών, η Hitachi ομολόγησε ότι είχε εγκρίνει την πληρωμή των 540.000 δολαρίων για εμπιστευτικές πληροφορίες ηλεκτρονικών υπολογιστών που ανήκαν στην I.B.M., αλλά επέμεινε ότι δεν γνώριζε ότι το υλικό είχε κλαπεί.

Υπόθεση 5η Unilever κατά Procter & Gamble

Κίνητρο : Οικονομική Ζημία στην Επιχείρηση

Η Procter & Gamble θα κατέβαλε στην Unilever περίπου 10 εκατομμύρια δολάρια και συμφώνησε σε έναν ασυνήθιστο έλεγχο τρίτων για να διευθετήσει μια διαμάχη που προέκυψε αφού η P. & G. αναγνώρισε ότι είχε λάβει έγγραφα από δοχεία απορριμμάτων έξω από τα γραφεία της Unilever στο Σικάγο. Οι υπάλληλοι και των δύο εταιρειών αρνήθηκαν να αποκαλύψουν τους όρους του διακανονισμού. Ωστόσο, ένα άτομο που ενημερώθηκε για τα αποτελέσματα των διαπραγματεύσεων δήλωσε ότι η Procter & Gamble, συμφώνησε με την πληρωμή και τον έλεγχο.

Η Unilever, είχε ζητήσει να εξασφαλιστεί ότι η Procter & Gamble δεν θα αλλάξει τα σχέδια μάρκετινγκ ή ανάπτυξης προϊόντων της, αφού εξέτασε περίπου 80 σελίδες εμπιστευτικών σχεδίων της Unilever. Παρόλο που οι εξωτερικοί ελεγκτές διορίζονται συνήθως για να διασφαλίσουν ότι οι ανάδοχοι μιας εταιρείας συμμορφώνονται με τα πρότυπα της εταιρικής εργασίας, είναι ασυνήθιστο να έχει κάποιος διορισθεί σε περίπτωση εταιρικής κατασκοπείας για να παρακολουθεί την ανάπτυξη προϊόντων ή την εμπορία άλλου.

Η Procter & Gamble, η οποία εδρεύει στο Cincinnati, δήλωσε ότι οι πράκτορες που εργάζονταν για λογαριασμό της δεν παραβίασαν τον νόμο, αλλά παραβίασαν τις πολιτικές δεοντολογίας της εταιρείας, οι οποίες απαγορεύουν τη συλλογή απορριμμάτων για να αποκτήσουν πληροφορίες σχετικά με τους ανταγωνιστές τους. Η εταιρεία ενημέρωσε την Unilever ότι οι πράκτορες που εργάζονταν για αυτήν είχαν αποκτήσει κακώς έγγραφα της Unilever και τα έδωσαν στους υπαλλήλους της εταιρείας.

Β. Υπολογιστικά Βήματα Διαδικασίας Αναλυτικής Ιεράρχησης

Η κατασκευή του Πινάκα Συγκρίσεων για κάθε κριτήριο περιλαμβάνει τις επιλογές και συμπληρώνονται οι σχετικές βαρύτητες μεταξύ τους με βάση την κλίμακα του Πίνακα Β.1.

Πίνακας Β.1. Κλίμακα Συγκρίσεων Επιλογών Διαδικασίας Αναλυτικής Ιεράρχησης

Τιμή	**Ορισμός**	**Εξήγηση**
1	Ίση σπουδαιότητα	Και οι δύο παράγοντες συμβάλλουν εξίσου στον στόχο ή το κριτήριο.
3	Μικρή σπουδαιότητα ενός σε σχέση με άλλον	Η πείρα και η κρίση ευνοούν ελαφρώς τον έναν παράγοντα σε σχέση με τον άλλον.
5	Βασική ή μεγάλη σπουδαιότητα	Η πείρα και η κρίση ευνοούν σαφώς τον έναν παράγοντα σε σχέση με τον άλλον.
7	Πολύ ισχυρή ή αποδεδειγμένη σπουδαιότητα	Ένας παράγοντας ευνοείται ιδιαίτερα σε σχέση με έναν άλλον. Η κυριαρχία του αποδεικνύεται στην πράξη.
9	Απόλυτη σπουδαιότητα σε σχέση με άλλον	Τα στοιχεία που ευνοούν έναν παράγοντα είναι αδιαμφισβήτητα.
2,4,6,8	Ενδιάμεσες τιμές	Χρησιμοποιούνται όταν απαιτείται συμβιβασμός.
0	Καμία σχέση	Ο παράγοντας δεν συμβάλλει στον στόχο.

Πίνακας Β.2. Πίνακας Συγκρίσεων Υπαλλήλων

Ποινικό Μητρώο					**Τρόπος ζωής**			
	Υπ. 1	Υπ. 2	Υπ. 3			Υπ. 1	Υπ. 2	Υπ. 3
Υπ. 1	1	1/3	6		Υπ. 1	1	8	1
Υπ. 2	3	1	7		Υπ. 2	1/8	1	1/8
Υπ.3	1/6	1/7	1		Υπ. 3	1	8	1

Πίνακας Β.2. Πίνακας Συγκρίσεων Υπαλλήλων (Συνέχεια)

Ιατρικό Ιστορικό					**Προϋπηρεσία**			
	Υπ. 1	Υπ. 2	Υπ. 3			Υπ. 1	Υπ. 2	Υπ. 3
Υπ. 1	1	7	2		Υπ. 1	1	1/2	4
Υπ. 2	1/7	1	5		Υπ. 2	2	1	6
Υπ. 3	1/2	1/5	1		Υπ. 3	¼	1/6	1

Η κατασκευή του Κανονικοποιημένου Πίνακα προκύπτει από τη διαίρεση κάθε τιμής του Πίνακα Συγκρίσεων με το άθροισμα της αντίστοιχης στήλης.

Πίνακας Β.3. Κανονικοποιημένος Πίνακας Συγκρίσεων Υπαλλήλων

Ποινικό Μητρώο					**Τρόπος ζωής**			
	Υπ. 1	Υπ. 2	Υπ. 3			Υπ. 1	Υπ. 2	Υπ. 3
Υπ. 1	6/25	7/31	6/14		Υπ. 1	8/17	8/17	8/17
Υπ. 2	18/25	21/31	7/14		Υπ. 2	1/17	1/17	1/17
Υπ.3	1/25	3/31	1/14		Υπ. 3	8/17	8/17	8/17
Ιατρικό Ιστορικό					**Προϋπηρεσία**			
	Υπ. 1	Υπ. 2	Υπ. 3			Υπ. 1	Υπ. 2	Υπ. 3
Υπ. 1	14/23	35/41	2/8		Υπ. 1	4/13	3/10	4/11
Υπ. 2	2/23	5/41	5/8		Υπ. 2	8/13	6/10	6/11
Υπ. 3	7/23	1/41	1/8		Υπ. 3	1/13	1/10	1/11

Η κατασκευή Διανύσματος Προτεραιότητας προκύπτει από το μέσο όρο κάθε γραμμής του Κανονικοποιημένου Πίνακα.

Πίνακας Β.4. Διάνυσμα Προτεραιότητας Υπαλλήλων

Ποινικό Μητρώο		**Τρόπος ζωής**		**Ιατρικό Ιστορικό**		**Προϋπηρεσία**	
Υπ. 1	0,298	Υπ. 1	0,471	Υπ. 1	0,571	Υπ. 1	0,324
Υπ. 2	0,632	Υπ. 2	0,059	Υπ. 2	0,278	Υπ. 2	0.587
Υπ. 3	0,069	Υπ. 3	0,471	Υπ. 3	0,151	Υπ. 3	0,089

Ο Υπολογισμός του Βαθμού Συνέπειας CR προκύπτει από τον πολλαπλασιασμό κάθε στήλης του Πίνακα Συγκρίσεων με την αντίστοιχη προτεραιότητα και κατόπιν τη διαίρεση του αποτελέσματος με την αντίστοιχη προτεραιότητα. Έπειτα, με το μέσο όρο των αποτελεσμάτων, υπολογίζεται ο Δείκτης Συνέπειας CI και ο Βαθμός Συνέπειας.

Πίνακας Β.5. Υπολογισμός Βαθμού Συνέπειας Στοιχείων Υπαλλήλων

Ποινικό Μητρώο								
0,298 *	1	+ 0,632 *	1/3	+ 0,069 *	6	= 0,923	/ 0,298	= 3,097
	3		1		7	= 2.009	/ 0,632	= 3,179
	1/6		1/7		1	= 0, 209	/ 0,069	= 3,029
Τρόπος ζωής								
0,471 *	1	+ 0.059 *	8	+ 0.471 *	1	= 1,414	/ 0,471	= 3,002
	1/8		1		1/8	= 0,177	/ 0,059	= 2,996
	1		8		1	= 1,414	/ 0,471	= 3,002
Ιατρικό Ιστορικό								
0,571 *	1	+ 0.278 *	7	+ 0.151 *	2	= 2,248	/ 0,571	= 3,937
	1/7		1		5	= 1,115	/ 0.278	= 4,010
	1/2		1/5		1	= 0,492	/ 0,151	= 3,258

Πίνακας Β.5. Υπολογισμός Βαθμού Συνέπειας Στοιχείων Υπαλλήλων (Συνέχεια)

Προϋπηρεσία								
0,324 *	1	+ 0,587 *	1/2	+ 0,089 *	4	= 0,974	/ 0,324	= 3,006
	2		1		6	= 1,769	/ 0,587	= 3,014
	1/4		1/6		1	= 0,268	/ 0,089	= 3,011

Ποινικό Μητρώο

Μέσος Όρος (3,097+3,179+3,029) / 3 = 3,102

Δείκτης Συνέπειας CI = (M.O. – n) / (n-1) = (3,102-3) / 2 = 0,051

Βαθμός Συνέπειας CR = CI / RI = 0,051 / 0,58 = 0,088 < 0,10 (εντός των αποδεκτών ορίων συνέπειας)

Ομοίως

Τρόπος ζωής : CR = 0

Ιατρικό Ιστορικό : CR = 0,063

Προϋπηρεσία : CR = 0,009

Έπειτα γίνεται η κατασκευή Πίνακα Συγκρίσεων, Κανονικοποιημένου Πίνακα Συγκρίσεων, Διανύσματος Προτεραιοτήτων και Έλεγχος Βαθμού Συνέπειας για τα κριτήρια ομοίως με ανωτέρω.

Πίνακας Β.6. Πίνακας Συγκρίσεων Κριτηρίων

	Ποινικό Μητρώο	**Τρόπος ζωής**	**Ιατρικό Ιστορικό**	**Προϋπηρεσία**
Ποινικό Μητρώο	1	7	3	8
Τρόπος ζωής	1/7	1	7	3
Ιατρικό Ιστορικό	1/3	1/7	1	1/9
Προϋπηρεσία	1/8	1/3	9	1

Πίνακας Β.7. Κανονικοποιημένος Πίνακας Συγκρίσεων Κριτηρίων

	Ποινικό Μητρώο	**Τρόπος ζωής**	**Ιατρικό Ιστορικό**	**Προϋπηρεσία**
Ποινικό Μητρώο	168/269	147/178	3/20	72/109
Τρόπος ζωής	24/269	21/178	7/20	27/109
Ιατρικό Ιστορικό	56/269	3/178	1/20	1/109
Προϋπηρεσία	21/269	7/178	9/20	9/109

Ποινικό Μητρώο

Μέσος Όρος κάθε γραμμής (168/269+147/178+3/20+72/109) / 4 = 0,565

Τρόπος ζωής

Μέσος Όρος κάθε γραμμής (24/269+21/178+7/20+27/109) / 4 = 0,201

Ιατρικό Ιστορικό

Μέσος Όρος κάθε γραμμής (56/269+3/178+1/20+1/109) / 4 = 0,071

Προϋπηρεσία

Μέσος Όρος κάθε γραμμής (21/269+7/178+9/20+9/109) / 4 = 0,162

Πίνακας Β.8. Υπολογισμός Βαθμού Συνέπειας Κριτηρίων

0,565*	1	+0,201*	7	+0,071*	3	+0,162*	8	=3,481	/0,565	=6,161
	1/7		1		7		3	=1,265	/0,201	=6,294
	1/3		1/7		1		1/9	=0,306	/0,071	=4,310
	1/8		1/3		9		1	=0,939	/0,162	=5,796

Δείκτης Συνέπειας CI = (M.O. – n) / (n-1) = 6,187

Βαθμός Συνέπειας CR = CI / RI = 0,06

Γ. Υπολογιστικά Βήματα Διαδικασίας Αναλυτικής Ιεράρχησης

Πίνακας Γ.1. Αξιολόγηση ανάπτυξης και ωριμότητας των προτύπων διαχείρισης κινδύνων (Πηγή Lam, 2014:416)

Κριτήριο Κινδύνου	**Διαφωνώ Απόλυτα (1)**	**Διαφωνώ (2)**	**Ούτε Συμφωνώ-Ούτε Διαφωνώ (3)**	**Συμφωνώ (4)**	**Συμφωνώ Απόλυτα (5)**
Οργανωτική ευθυγράμμιση και υποστήριξη. Η διαδικασία αξιολόγησης των κινδύνων υποστηρίζεται πλήρως από το διοικητικό συμβούλιο και την ανώτερη διοίκηση, καθώς και από τις επιχειρησιακές μονάδες. Οι συμμετέχοντες συμμετέχουν σε ανοικτές συζητήσεις και παρέχουν ειλικρινή συμβολή στους κινδύνους και τους ελέγχους.					
Σχεδιασμός και πόροι. Έχουμε ένα καλά καθορισμένο σχέδιο για την εκτίμηση κινδύνων. Συγκεκριμένοι ρόλοι είναι σαφώς καθορισμένοι και διαθέτουμε τους κατάλληλους πόρους για τη διεξαγωγή του σχεδίου.					
Ταξινόμηση κινδύνων. Έχουμε δημιουργήσει μια ταξινόμηση κινδύνων με βασικές κατηγορίες και ορισμούς για τους κινδύνους. Οι συμμετέχοντες χρησιμοποιούν μια κοινή γλώσσα όταν συζητούν θέματα διακινδύνευσης και ελέγχου.					
Εργαλεία αξιολόγησης κινδύνου. Διαθέτουμε ένα ισχυρό σύνολο εργαλείων για την υποστήριξη της εκτίμησης κινδύνων, συμπεριλαμβανομένων τυποποιημένων ερωτηματολογίων, προτύπων και λογισμικού και εργαλείων συγκέντρωσης.					

Πίνακας Γ.1. Αξιολόγηση ανάπτυξης και ωριμότητας των προτύπων διαχείρισης κινδύνων (Πηγή Lam, 2014:416) (Συνέχεια)

Κριτήριο Κινδύνου	Διαφωνώ Απόλυτα (1)	Διαφωνώ (2)	Ούτε Συμφωνώ-Ούτε Διαφωνώ (3)	Συμφωνώ (4)	Συμφωνώ Απόλυτα (5)
Εξάσκηση και ανάπτυξη. Παρέχουμε προγράμματα κατάρτισης και ανάπτυξης σχετικά με την εκτίμηση κινδύνων. Αυτά τα προγράμματα είναι διαθέσιμα σε νέους συμμετέχοντες.					
Σύνδεση με επιχειρησιακούς στόχους. Η διαδικασία αξιολόγησης των κινδύνων συνδέεται ρητά με τους επιχειρηματικούς στόχους τόσο σε επίπεδο εταιρικών όσο και επιχειρηματικών μονάδων.					
Σύνδεση με κανονιστικές και πολιτικές απαιτήσεις. Η διαδικασία αξιολόγησης των κινδύνων ενσωματώνει τις βασικές ρυθμιστικές και πολιτικές απαιτήσεις για την επιχείρησή μας.					
Ποιότητα εισόδου. Κατά τη διάρκεια συνεντεύξεων, οι συζητήσεις αξιολόγησης των κινδύνων είναι εξαιρετικά αποτελεσματικές.					
Ποιότητα Εξόδου. Οι εκθέσεις αξιολόγησης κινδύνων και οι χάρτες επικινδυνότητας είναι ιδιαίτερα αποτελεσματικές. Έχουμε ένα σαφές προφίλ κινδύνου τόσο σε επίπεδο εταιρικών όσο και επιχειρηματικών μονάδων.					
Προσδιορισμός κινδύνου. Έχουμε θεσπίσει μια συστηματική μεθοδολογία για τον εντοπισμό των κυριότερων κινδύνων. Διεξάγονται αναλύσεις για την απόκτηση λεπτομερέστερων πληροφοριών.					

Συνολική βαθμολογίας ανάπτυξης και ωριμότητας προτύπων διαχείρισης κινδύνων : …….

Πίνακας Γ.2. Αξιολόγηση ενσωμάτωσης και εφαρμογής των αποτελεσμάτων (Πηγή Lam, 2014:418)

Κριτήριο Κινδύνου	Διαφωνώ Απόλυτα (1)	Διαφωνώ (2)	Ούτε Συμφωνώ-Ούτε Διαφωνώ (3)	Συμφωνώ (4)	Συμφωνώ Απόλυτα (5)
Βασικοί δείκτες κινδύνου. Έχουμε ενσωματώσει τις αξιολογήσεις κινδύνων και τους Β.Δ.Κ. Οι αξιολογήσεις κινδύνων προσφέρουν στοιχεία σχετικά με το σχεδιασμό των Β.Δ.Κ. και μας βοηθούν να παρακολουθούμε τις εκθέσεις και τις τάσεις κινδύνων.					
Επίπεδα ανοχής κινδύνων. Έχουμε θεσπίσει επίπεδα ανοχής κινδύνων για τους κύριους κινδύνους μας για να διασφαλίσουμε ότι τα πραγματικά μας εκθέματα είναι εντός αποδεκτών επιπέδων.					
Διαχείριση κινδύνων. Για τους βασικούς μας κινδύνους, αναπτύσσουμε σχέδια διαχείρισης κινδύνων και δράσεων, με σαφή ευθύνη για την αποφυγή, μετριασμό, μεταφορά ή αποδοχή των κινδύνων.					
Συστήματα έγκαιρης προειδοποίησης. Έχουμε δημιουργήσει συστήματα έγκαιρης προειδοποίησης που περιλαμβάνουν τους κύριους δείκτες κινδύνων και τα σχέδια δράσης έκτακτης ανάγκης.					
Στρατηγικός Σχεδιασμός και Ανασκοπήσεις. Η διαδικασία αξιολόγησης των κινδύνων ενσωματώνεται στον στρατηγικό σχεδιασμό, καθώς και σε συνεχιζόμενες στρατηγικές και επιχειρηματικές αναθεωρήσεις.					

Πίνακας Γ.2. Αξιολόγηση ενσωμάτωσης και εφαρμογής των αποτελεσμάτων (Πηγή Lam, 2014:418) (Συνέχεια)

Κριτήριο Κινδύνου	Διαφωνώ Απόλυτα (1)	Διαφωνώ (2)	Ούτε Συμφωνώ-Ούτε Διαφωνώ (3)	Συμφωνώ (4)	Συμφωνώ Απόλυτα (5)
Επιχειρηματικές διεργασίες και λειτουργίες. Εφαρμόζουμε τα αποτελέσματα αξιολόγησης κινδύνων στις επιχειρηματικές μας διαδικασίες.					
Ανάλυση σεναρίων και δοκιμές πίεσης. Εκτός από τους μεμονωμένους κινδύνους και τους ελέγχους, διεξάγουμε σεναρίων ανάλυσης και προσομοιώσεις ακραίων καταστάσεων συμβάντων κινδύνου και/ή αποτυχίας πολλαπλών βασικών ελέγχων.					
Πίνακες Αναφορών. Έχουμε εφαρμόσει πίνακες αναφορών στη διοίκηση οι οποίοι παρέχουν ολοκληρωμένη απόδοση και αναφορά κινδύνων.					
Βάση Δεδομένων/Συμβάντων. Έχουμε δημιουργήσει μία βάση δεδομένων που περιέχει τις υλικές απώλειες και τα συμβάντα. Αυτή η βάση δεδομένων υποστηρίζει την ανάλυση, παρακολούθηση και αντιμετώπιση των κινδύνων και τη συνεχή βελτίωση της αξιολόγησής τους.					
Πολιτική κλιμάκωσης κινδύνου. Για τη συμπλήρωση της αξιολόγησης των κινδύνων, έχουμε εφαρμόσει μια πολιτική κλιμάκωσης κινδύνων με συγκεκριμένες «ειδοποιήσεις» για απώλειες υλικών ή συμβάντα. Αυτή η πολιτική διασφαλίζει ότι κοινωνούνται σε όλο τον οργανισμό.					

Συνολική βαθμολογίας ενσωμάτωσης και εφαρμογής των αποτελεσμάτων διαχείρισης κινδύνων : …….

Γλωσσάρι

- Κίνδυνος (Risk): Επίδραση της αβεβαιότητας στους αντικειμενικούς στόχους.
- Απειλή (Threat): Ακούσιο ή Εκούσιο αίτιο ανεπιθύμητου περιστατικού το οποίο μπορεί να έχει αρνητικό αντίκτυπο.
- Διαχείριση κινδύνου (Risk management): Συντονισμένες δράσεις καθοδήγησης και ελέγχου ενός οργανισμού όσον αφορά τον κίνδυνο.
- Ενδιαφερόμενα μέρη (Stakeholders): Πρόσωπο ή οργανισμός που μπορεί να επηρεάσει, να επηρεαστεί ή να αντιληφθεί ότι επηρεάζεται από μία απόφαση ή δραστηριότητα.
- Ασφάλεια: Η προστασία από τον κίνδυνο ή την απώλεια.
- Κατασκοπεία: Απόκτηση διαβαθμισμένων (απορρήτων ή εμπιστευτικών) πληροφοριών από μία κυβέρνηση, μία επιχείρηση, ένα ή περισσότερα φυσικά πρόσωπα, χωρίς την άδεια του κατόχου τους.
- Βιομηχανική Κατασκοπεία (Industrial Espionage): Η συνειδητή και ηθελημένη υπεξαίρεση των εμπορικών μυστικών που σχετίζονται ή περιλαμβάνονται σε ένα προϊόν που παράγεται ή διατίθεται στο εμπόριο για οικονομικό όφελος οποιουδήποτε άλλου από τον ιδιοκτήτη.
- Εμπορικά μυστικά (Trade secrets): Πληροφορίες οι οποίες έχουν ανεξάρτητη οικονομική, πραγματική ή δυνητική οικονομική αξία λόγω της αποκλειστικότητας χρήσης τους από τον ιδιοκτήτη.
- Ανταγωνισμός (Competition): Προσπάθεια επικράτησης έναντι ενός αντιπάλου.