ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ -
ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΔΙΟΙΚΗΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Αξιολόγηση επενδύσεων στην ασφάλεια πληροφοριακών συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της/του

ΜΑΥΡΟΥΔΗΣ ΔΗΜΗΤΡΙΟΣ

Επιβλέπων : ΚΟΚΟΛΑΚΗΣ ΣΠΥΡΙΔΩΝ

Μέλη εξεταστικής επιτροπής:ΚΟΚΟΛΑΚΗΣ ΣΠΥΡΙΔΩΝ, ΚΑΡΥΔΑ ΜΑΡΙΑ, ΡΙΖΟΜΥΛΙΩΤΗΣ ΠΑΝΑΓΙΩΤΗΣ

Σάμος, Οκτώβριος 2016

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εντάσσεται στο πεδίο της ασφάλειας των πληροφοριακών συστημάτων, το οποίο αποτελεί σήμερα ένα πρόσφορο ερευνητικό πεδίο ένεκα του μεγάλου όγκου των πληροφοριών που διακινούνται καθημερινά σε παγκόσμιο επίπεδο και των σύστοιχων ζητημάτων ασφαλείας που ανακύπτουν.

Θα ήθελα να ευχαριστήστω τον επιβλέπων καθήγητη μου κύριο Κοκολακη για την ευκαιρία που μου έδωσε να ασχοληθω με το πολύ ενδιαφέρων θεμα.

Την οικογενεια μου τη σύζηγο μου, τους γονεις και τον αδέρφο μου για την αμεριστη κατανόηση και υποστήριξη τους την ώρα που διάβαζα.

Περίληψη

Σε ένα παγκοσμιοποιημένο περιβάλλον, όπου ο όγκος και η ταχύτητα διάδοσης των πληροφοριών λαμβάνουν χώρα με γεωμετρικώς αυξανόμενους ρυθμούς, είναι προφανής η ανάγκη για υιοθέτηση επενδυτικών δράσεων από την πλευρά των επιχειρήσεων και οργανισμών με σκοπό την προστασία των πληροφοριακών τους συστημάτων.

Σκοπός της παρούσας εργασίας ήταν να προβεί σε μια ανάλυση των εννοιών που σχετίζονται με την αξιολόγηση επενδύσεων που αφορούν στην ασφάλεια πληροφοριακών συστημάτων.

Από την ανάλυση που έλαβε χώρα, καταδείχτηκε σαφώς ότι τα μέχρι στιγμής υπάρχοντα μοντέλα για την ανάλυση και αξιολόγηση των επενδύσεων σχετιζομένων με τη ασφάλεια των πληροφοριακών συστημάτων στηρίζουν τις αρχές τους σχεδόν αποκλειστικά στη νεοκλασσική οικονομική θεωρία και υστερούν όσον αφορά στο γεγονός ότι δε λαμβάνουν υπόψη ποιοτικές παραμέτρους.

Υπό αυτό το πρίσμα, οι νέες τάσεις αφορούν στην υιοθέτηση μοντέλων που θα λαμβάνουν υπόψη εκτός των απτών ποσοτικών οικονομικών μεγεθών και ποιοτικές παραμέτρους όπως η συμπεριφορά του ανθρώπινου παράγοντα ή η αύξηση της φήμης του εκάστοτε οργανισμού από την υιοθέτηση εξελιγμένων συστημάτων ασφάλειας των πληροφοριακών του συστημάτων.

Abstract

In a globalized environment where the volume and speed of information dissemination happening with geometrically increasing rate, it is obvious the need for adoption of investment actions from businesses and organizations in order to protect their information systems.

The purpose of this study was to conduct an analysis of the concepts related to the evaluation of investments relating to the security of information systems.

The analysis took place demonstrated clearly that the existing models for the analysis and evaluation of investments linked to the security of information systems based on the principles of neoclassical economic theory and disadvantage with regard to the fact that they do not take into account quality parameters.

Within this framework, new trends come into consideration, related to the adoption of models that take into account not only quantitative financial parameters but also qualitative ones such as the behavior of the human factor or the increase of the reputation of an organization from the adoption of advanced information systems.

Περιεχόμενα

1

Εισαγωγή

1.1 Ασφάλεια πληροφοριακών συστημάτων

Σε ένα περιβάλλον όπου ο όγκος και η ταχύτητα διάδοσης των πληροφοριών λαμβάνουν χώρα με συνεχώς αυξανόμενους ρυθμούς, είναι συνεχής η προσπάθεια των επιχειρήσεων σε παγκόσμιο επίπεδο για υιοθέτηση επενδυτικών δράσεων με σκοπό την αύξηση της ασφάλειας των πληροφοριακών τους συστημάτων.

1.2 Αντικείμενο διπλωματικής

Σκοπός της παρούσας εργασίας είναι να προβεί σε μια ανάλυση των εννοιών που σχετίζονται με την αξιολόγηση επενδύσεων που αφορούν στην ασφάλεια πληροφοριακών συστημάτων.

1.3Η έννοια της πληροφορίας

Η πληροφορία αποτελεί μια αλληλουχία συμβόλων, που είτε καταγράφονται είτε μεταδίδονται, η οποία μπορεί να ερμηνευτεί ως μήνυμα και μπορεί να επηρεάσει ένα δυναμικό σύστημα το οποίο είναι σε θέση να την επεξεργαστεί (Floridi, 2005).

Με βάση τον παραπάνω ορισμό, θα πρέπει αρχικά να προχωρήσουμε σε ένα διαχωρισμό μεταξύ της έννοιας της πληροφορίας και της έννοιας του δεδομένου.

Εκκινώντας, θα πρέπει να σημειώσουμε, ότι τα δεδομένα αναδείχθηκαν, σημασιοδοτήθηκαν και καθιερώθηκαν ως ξεχωριστός όρος σε συνάρτηση με την επεξεργασία δεδομένων και κυρίως με την ανάπτυξη και διάδοση της

αυτοματοποιημένης επεξεργασίας δεδομένων. Η συσχέτιση αυτή αναπόφευκτα τονίζει την έννοια του δεδομένου υπό το πρίσμα του τεχνικού όρου το οποίο αποτελεί μέρος ενός συστήματος επεξεργασίας και οδηγεί στον προσδιορισμό του συνόλου των δεδομένων ως στοιχείων μιας επεξεργασμένης πληροφορίας (Checkland&Scholes, 1990).

Σύμφωνα με την παραπάνω διατύπωση, το δεδομένο συνιστά τη μικρότερη μονάδα πληροφορίας, η οποία συνιστά μία πολλαπλότητα δεδομένων τα οποία αποτελούν την πρώτη ύλη από την οποία προκύπτει η πληροφορία ως ολοκληρωμένο προϊόν.

Σχήμα 1. Συσχέτιση δεδομένου και πληροφορίας (Checkland&Scholes, 1990).

Περαιτέρω, η έννοια της πληροφορίας παραπέμπει αυτόματα στην πληροφοριακή αξία της, ενώ δεν συμβαίνει το ίδιο με τον όρο “δεδομένο”, στο οποίο προσδίδεται μία ουδετερότητα όσον αφορά τον σκοπό του (Checkland&Scholes, 1990).

Οι νέες τεχνολογίες έρχονται σήμερα να μεταβάλλουν εν τέλει τόσο τον ίδιο τον ορισμό όσο και το εννοιολογικό περιεχόμενο της πληροφορίας. Την περίοδο της βιομηχανικής κοινωνίας, η εκμετάλλευση των περισσότερων μορφών πληροφορίας, βρισκόταν σε πλήρη εξάρτηση από τον ανθρώπινο έλεγχο. Η πληροφορία ήταν κλειδωμένη στο μέσο αποθήκευσης με αποτέλεσμα να παραμένει παθητική και μη εξελίξιμη, εκτός και αν κάποιος εξωτερικός παράγοντας εμφανιζόταν προκειμένου να την εκμεταλλευτεί.

Αυτή η κατάσταση έρχεται να αλλάξει ρίζικα ένεκα της αλματώδους τεχνολογικής εξέλιξης. Πλέον, η σημασία και ποιοτική διάσταση της πληροφορίας οφείλεται κατά κύριο λόγο στην υποκείμενη τεχνολογία, ενώ η δύναμη των συστημάτων πληροφορικής και τηλεπικοινωνιών έγκειται ακριβώς στην ικανότητά τους να χειρίζονται γρήγορα, συστηματικά και αποτελεσματικά αυτό που ονομάζουμε

πληροφορία. Υπο αυτό το πρίσμα, η έννοια της πληροφορίας αποκτά μια δυναμική συνιστώσα που αποδίδεται στη δυνατότητα που υπάρχει πλεόν όσον αφορά στην ταχύτητα επεξεργασίας και διάδοσης των πληροφοριών, με τις νέες τεχνολογίες να επιτρέπουν την αποκοπή της πληροφορίας από τον δημιουργό της και το περιβάλλον μέσα στο οποίο γεννιέται αρχικά (Beynon – Davies, 2002).

Όσον αφορά στο περιεχόμενό της, μια πληροφορία μπορεί να διακριθεί σε ‘απλή’ και ‘ευαίσθητη’. Εν γένει, η ποιότητα και η κατάταξη της πληροφορίας σε μια από τις δύο κατηγορίες συναρτάται από το υποκείμενο και το ρόλο του.

Το περιεχόμενο είναι αυτό που σε αρχικό τουλάχιστον στάδιο αποτελεί καθοριστικό παράγοντα για τη διατύπωση του αιτήματος και την παραδοχή της ρύθμισης και κατ΄ επέκταση της προστασίας μιας πληροφορίας,υπό την έννοια ότι το ιδιαίτερο περιεχόμενο μιας πληροφορίας την καθιστά ευαίσθητη και για το λόγο αυτό θα έπρεπε να παρεμποδιστεί ή τουλάχιστον να περιοριστεί η συλλογή, η χρήση ή η κυκλοφορία της (Checkland&Scholes, 1990).

Σε αυτήν την αντίληψη υπάγεται εξάλλου η άποψη ότι υπάρχουν αφενός αβλαβή δεδομένα άνευ σημασίας, ενώ ταυτόχρονα υπάρχουν “ευαίσθητα” δεδομένα που χρήζουν ιδιαίτερης προστασίας και χειρισμού.

1.4 Επιχειρήσεις πληροφοριών

Η έννοια της πληροφορίας δρα και απαντά σήμερα σε ένα πλήθος επιχειρήσεων που σχετίζονται με βασικούς τομείς της ανθρώπινης δραστηριότητας, όπως στις επικοινωνίες, τη βιομηχανία, τις επαγγελματικές επιχειρήσεις, τις δημόσιες υπηρεσίες, την υγεία, την εκπαίδευση, τις επιστήμες και την έρευνα, αλλά και τις τέχνες και την ψυχαγωγία.

Παράκατω καταγράφονται οι σημαντικότερες δράσεις της πληροφορίας σε σχέση με τους παράπανω τομείς (Beynon – Davies, 2002).

Πίνακας 1. Τρόπος συμμετοχής της πληροφορίας στους σημαντικότερους τομείς της ανθρώπινης δραστηριότητας.

Τομέας δράσης	**Αποτύπωση δράσης**
Επικοινωνίες	• Δημοσίευση υλικού. • Διακρατική επικοινωνία. • Συναλλαγές.
Βιομηχανία	• GPS (Συστήματα προσδιορισμού θέσης). • Πολεμική Βιομηχανία. • Εθνική Άμυνα και Ασφάλεια
Επαγγελματικές επιχειρήσεις	• Πληροφοριακά συστήματα • Αυτοματισμοί γραφείου. • Ηλεκτρονικές εκδόσεις.
Δημόσιες υπηρεσίες	• Διάχυση πληροφορίας μεταξύ ηλεκτρονικών μητρώων. • Πληροφοριακά συστήματα. • Τραπεζικές συναλλαγές
Υγεία	• Τηλε-ιατρική • Υπολογιστικές εφαρμογές για την παρακολούθηση της υγείας των

	ασθενών.
Εκπαίδευση	• Εξ’ αποστάσεως εκπαίδευση. • Πολυμεσικές εφαρμογές.
Έρευνα και Ανάπτυξη	• Αποκωδικοποίηση πληροφοριών. • Ταχεία διάδοση ερευνητικής εξέλιξης και εξόρυξη στοιχείων σε πραγματικό χρόνο.
Τέχνες και Ψυχαγωγία	• Αναπαραγωγή πολυμέσων. • Επεξεργασία και σύνθεση ήχου και εικόνας.

1.5Σύστημα πληροφοριών

Με τον όρο σύστημα εννοούμε ένα σύνολο στοιχείων, διαρθρωμένων με συγκεκριμένη οργανωτική δομή, το οποίο επιτελεί ή αναπτύσσει μία σειρά δραστηριοτήτων και επιδιώκει την επίτευξη ενός προκαθορισμένου στόχου. (Longleyetal., 1999).

Κάθε σύστημα επικοινωνεί με το περιβάλλον του δεχόμενο εισροές από αυτό, τις οποίες μετασχηματίζει στο εσωτερικό του και παρέχει με τη σειρά του τα αποτελέσματα του μετασχηματισμού αυτού, στο περιβάλλον

Το σύνολο των εισροών στο σύστημα, αναφέρεται με τον όρο είσοδος - input. Αντίστοιχα, το σύνολο των εκροών από το σύστημα αναφέρεται με τον όρο έξοδος – output. Εκτός από την τυποποιημένη διαδικασία εισόδου → επεξεργασίας → εξόδου, ένα σύστημα, στο βαθμό που αποτελεί μέρος του ευρύτερου συστήματος, δέχεται άτυπες και μη προκαθορισμένες εισροές από το περιβάλλον του. Η διαδικασία του

μετασχηματισμού των εισροών στο εσωτερικό του συστήματος λέγεται επεξεργασία - process.

Ένα Σύστημα Πληροφοριών, αποτελεί υποσύστημα ενός ευρύτερου συνόλου και έχει σαν στόχο να παρέχει πληροφορίες, επεξεργαζόμενο τα διαθέσιμα δεδομένα, με σκοπό να υποστηρίξει κατάλληλες πράξεις και ενέργειες για την αποτελεσματικότερη λήψη αποφάσεων. Οι εισροές ενός Π.Σ. αποτελούν τα δεδομένα - data, ενώ οι εκροές είναι οι πληροφορίες - information.

Ένα Σύστημα Πληροφοριών, βασιζόμενο ή μη σε υπολογιστικά συστήματα, αποτελείται από τα ακόλουθα τέσσερα βασικά στοιχεία (Longleyetal., 1999):

- Συλλογή δεδομένων: Τα δεδομένα αφορούν σε αριθμούς, γεγονότα, πληροφορίες, κ.α.
- Αποθήκευση δεδομένων: Τα δεδομένα είναι δυνατό να αποθηκεύονται σε καρτελοθήκη, σε αρχείο ή σε βάση δεδομένων Η/Υ.
- Επεξεργασία δεδομένων: Η επεξεργασία των δεδομένων περιλαμβάνει κυρίως την ανάλυση, κωδικοποίηση, ταξινόμηση και σύνθεσή τους.
- Παρουσίαση της πληροφορίας: Η παρουσίαση της πληροφορίας στο χρήστη γίνεται στη μορφή που αυτός επιθυμεί και αποτελεί προϊόν που έχει προκαθοριστεί.

Σε ένα τέτοιο πλαίσιο, το Σύστημα Πληροφοριών είναι επομένως ένα σύστημα, το οποίο επεξεργάζεται δεδομένα από το εσωτερικό και εξωτερικό περιβάλλον και παρέχει πληροφορίες, έτσι ώστε να ληφθούν γρήγορα σωστές και έγκυρες αποφάσεις.

1.6Ισχύς πληροφοριών

Με την εξέλιξη της τεχνολογίας και τη διάδοση του διαδικτύου, ο σύγχρονος άνθρωπος έχει στη διάθεση του μια πληθώρα πληροφοριών που μπορεί να χρησιμοποιήσει ανά πάσα ώρα και στιγμή. Οι πληροφορίες αυτές, σε αντίθεση με το παρελθόν, επικαιροποιούνται διαρκώς και περιλαμβάνουν τις εξελίξεις που συντελούνται τη στιγμή που διαδίδονται. Σήμερα υπάρχει η δυνατότητα να

διακινούνται τεράστιες ποσότητες πληροφοριών κάθε στιγμή και με διαδραστική συμμετοχή οποιουδήποτε το επιθυμεί (Jasperson, 2002).

Στην πρόσφατη ιστορία έχουν παρατηρηθεί σημαντικά παραδείγματα που αποδεικνύουν με τον πιο εμφατικό τρόπο την ισχύ της πληροφορίας στο σημερινό γίγνεσθαι[1]. Από τα γεγονότα αυτά διαφαίνεται ξεκάθαρα η τεράστια δύναμη που μέχρι πριν λίγα χρόνια ήταν στα χέρια των ιδιοκτητών των ΜΜΕ και η οποία έχει τώρα πια περάσει σε ολόκληρο τον πληθυσμό αρκεί να υπάρχει πρόσβαση στο internet.

Στο σημείο αυτό θα πρέπει να τονιστεί ότι, ναι μεν η αυξημένη δυναμική της πληροφορίας σήμερα μπορεί να αποτελέσει σημαντικό εφόδιο για τη δημιουργία μιας κατεύθυνσης όπου όλο και περισσότεροι άνθρωποι θα αποφασίζουν και θα διαμορφώνουν πολιτικές για τον ίδιο τον άνθρωπο, από την άλλη όμως, η κακή και χωρίς κριτική σκέψη διαχείριση της ταχέως διαδιδόμενης πληροφορίας ή η απολάβη ευαίσθητων πληροφοριών από λάθος χέρια, μπορεί να προκαλέσει σημαντικές αστοχίες σε ζήτήματα πολύ σημαντικά για τα κράτη και εν γένει για τον πολίτη – άνθρωπο, όπως είναι η Εθνική Ασφάλεια και η διαμόρφωση των Εθνικών Στρατηγικών.

1.7 Ο κύκλος των πληροφοριών

1. Το τελευταίο παράδειγμα είναι η εξέγερση του πληθυσμού στην Αίγυπτο που διοργανώθηκε μέσω των μηνυμάτων στο twitter κυρίως αλλά και του facebook. Ανάλογα παραδείγματα υπήρξαν και στο παρελθόν, στο Ιράν το 2008 και στην Αθήνα με τη δολοφονία του Αλέξη Γρηγορόπουλου. Η κυβέρνηση του Ιράν έβγαλε τα καλώδια από την πρίζα στην κυριολεξία προκειμένου να διακόψει την παροχή του internet σε κάποιες περιοχές της χώρας, άφησε όμως ελεύθερα τα κινητά τηλέφωνα που μετέδιδαν “ζωντανά” τα γεγονότα μέσω των δικτύων κοινωνικής δικτύωσης. Στην περίπτωση της Αιγύπτου, ολόκληρη η χώρα “φιμώθηκε” αφού οι διαδικτυακές υπηρεσίες διακόπηκαν παντού. Βρέθηκε όμως ο τρόπος να μεταδίδονται τα γεγονότα δια της πλαγίας οδού, με τη βοήθεια της Google.

Ως κύκλος πληροφορίας, αναφέρεται η διαδικασία όπου με κατάλληλη επεξεργασία, από απλά μεμονωμένα δεδομένα εξάγεται μια συνολική πληροφορία ως αποτέλεσμα κατάλληλης σύνθεσης αυτών Σε πολλές περιπτώσεις, είναι πιθανό η ίδια η πληροφορία να αποτελέσει αντικείμενο επεξεργασίας το οποίο θα μας οδηγήσει σε νέα δεδομένα. Η διαδικασία όπου μια πληροφορία μετατρέπεται σε αντικείμενο επεξεργασίας ονομάζεται ανατροφοδότηση (Beynon – Davies, 2002).

Σχήμα 2. Ο κύκλος ζωής της πληροφορίας (Beynon – Davies, 2002).

1.8Δομή της διπλωματικής

Για την επίτευξη του σκοπού όπως αυτός καταδείχτηκε προηγουμένως, η παρούσα εργασία απαρτίζεται από τρία κύρια κεφάλαια.

Το πρώτο κεφάλαιο αποτελεί μια προσέγγιση της έννοιας της ασφάλειας των πληροφοριών και των πληροφοριακών συστημάτων. Όσον αφορά στο δεύτερο κεφάλαιο, σε αυτό λαμβάνει χώρα μια περιγραφή των παραγόντων που συνθέτουν το περιγραφικό πλαίσιο της έννοιας των επενδύσεων σχετιζομένων με την ασφάλεια των πληροφοριακών συστημάτων, ενώ τέλος, το τρίτο κεφάλαιο της εργασίας αποτελεί μια προσέγγιση που αφορά στα υπάρχοντα μοντέλα για την ανάλυση και αξιολόγηση επενδύσεων με προσανατολισμό στην ασφάλεια των πληροφοριακών συστημάτων καθώς και στη σχετιζόμενη με αυτά μελλοντική τάση.

2

Ασφάλεια πληροφοριακών συστημάτων

2.1 Η έννοια της ασφάλειας των πληροφοριακών συστημάτων

Η έννοια της ασφάλειας των πληροφοριών που διακινούνται σήμερα μέσω των σύγχρονων πληροφοριακών συστημάτων εμπεριέχεται στις ακόλουθες συνιστώσες (Craig&Ludloff, 2011).

Ασφάλεια των προσωπικών δεδομένων

Η συγκεκριμένη μορφή ιδιωτικότητας σχετίζεται με την εισβολή στα δεδομένα του ατόμου που έχουν να κάνουν με τη φυσική υπόσταση αυτού, τα υπάρχοντά του καθώς και τον προσωπικό του χώρο.

Στις περισσότερες χώρες σήμερα, η νομοθεσία προστατεύει σε μεγάλο βαθμό φαινόμενα όπως, η πραγματοποίηση παράνομων ερευνών στον προσωπικό χώρο των πολιτών, φαινόμενα κατασχέσεων καθώς και δράσεις που προσβάλουν εμφανώς την προσωπική υπόσταση και αξιοπρέπεια των πολιτών.

Ασφάλεια της διάχυσης πληροφοριών σε σχέση με προσωπικά δεδομένα

Ο εν λόγω τύπος ιδιωτικότητας σχετίζεται με την αποτροπή φαινομένων διάχυσης προσωπικών ευαίσθητων πληροφοριών και δεδομένων των ατόμων οι οποίες για διάφορους λόγους, συλλέγονται και αποθηκεύονται σε διάφορες βάσεις

δεδομένων (π.χ. ιατρικά δεδομένα ασθενών στις βάσεις δεδομένων των νοσοκομειακών ιδρυμάτων).

Και σε αυτή την περίπτωση, τα περισσότερα κράτη έχουν μεριμνήσει έτσι ώστε να απαγορεύεται σε σημαντικό βαθμό η διάχυση προσωπικών ευαίσθητων πληροφοριών που σχετίζονται κύρια με οικονομικά και ιατρικά δεδομένα των πολιτών, με σαφή προσανατολισμό την αποτροπή άσκοπης διάχυσης αυτών μέσω του διαδικτύου.

Ιδιωτικότητα των δεδομένων εταιριών και οργανισμών

Σε μια εποχή έντονου ανταγωνισμού στο επιχειρηματικό γίγνεσθαι, είναι προφανές ότι πολλές επιχειρήσεις ανά τον κόσμο θέλουν να κρατούν ενέργειες και πληροφορίες μυστικές από τον ανταγωνισμό, γιατί μπορεί αυτές να τους εξασφαλίζουν ή να δύναται να τους εξασφαλίσουν μελλοντικά ανταγωνιστικό πλεονέκτημα (για παράδειγμα τα χαρακτηριστικά μιας πατέντας ενός καινοτόμου προϊόντος, ή η συνταγή ενός πολύ πετυχημένου προϊόντος, με χαρακτηριστικό παράδειγμα την Coca – Cola).

Σε αυτή την περίπτωση, η νομοθεσία δεν είναι τόσο εκτεταμένη όσο στην περίπτωση της διασφάλισης των προσωπικών δεδομένων, αλλά οι ίδιες οι εταιρίες, έχοντας ισχυρά νομικά τμήματα αλλά και τμήματα επενδύσεων, κινούνται αποδοτικά με ίδιες δράσεις προς την κατεύθυνση της προστασίας των δεδομένων τους.

2.2Πεδία ισχυρής απαίτησης για χρήση συστημάτων ασφάλειας των πληροφοριών

Εν γένει, στη σημερινή ισχυρά ψηφιακή εποχή όπου ο όγκος των διακινούμενων πληροφορίων είναι τεράστιος, απαντώνται 6 κύρια πεδία ισχυρής απαίτησης για χρήση συστημάτων ασφάλειας των πληροφοριών. Τα εν λόγω πεδία αποτελούν τα επόμενα (Zikopoulos, 2012):

- ITloganalytics,
- της ανίχνευσης απάτης,
- των συστημάτων διαχείρισης ρίσκου.

- Διασφάλισης συνομιλιών τηλεφωνικών κέντρων.

ITloganalytics

Το πεδίο των ITloganalytics αποτελεί ένα σημαντικό πεδίο όσον αφορά στη χρήση συστημάτων για την ασφάλεια των πληροφοριών. Σε αυτή την περίπτωση, η αναφορά στην ασφάλεια της διακινούμενης πληροφορίας έχει να κάνει κυρίως με τα δεδομένα που συσσωρεύονται ως ‘ρυποι’ και προκύπτουν μετά την επεξεργασία των δεδομένων κύριου ενδιαφέροντος μέσω των εφαρμογών IT.

Οι εταιρίες εμφανίζουν καθημερινά σημαντική ποσότητα τέτοιου τύπου δεδομένων, με τις περισσότερες εξ’ αυτών να θεωρούν αυτά τα δεδομένα ανάξια χρήσης και να προχωρούν στην άμεση διαγραφή τους, θεωρώντας ότι η περαιτέρω αποθήκευσή τους αποτελεί σπατάλη αποθηκευτικού χώρου χωρίς ιδιαίτερο λόγο, ενώ η προσπάθεια για επεξεργασία τους αποτελεί μια οικονομικά και χρονικά απαιτητική διαδικασία που δε θα αποφέρει καμία σημαντική πληροφοριά.

Ανίχνευση απάτης

Στο σημερινό γίγνεσθαι, είθισται η έννοια της απάτης να συνδέεται συνήθως με συναλλαγές οικονομικού περιεχομένου, αλλά στην πραγματικότητα φαινόμενα απάτης μπορούν να απαντηθούν σε πλήθος τομέων της ανθρώπινης δραστηριότητας όπως στις διαδικτυακές συναλλαγές και δημοπρασίες, σε ασφαλιστικές απαιτήσεις κ.α. Η χρήση εφαρμογών με προσανατολισμό στην ασφάλεια των πληροφοριών μπορούν να μειώσουν αισθητά την ύπαρξη τέτοιων φαινομένων στις διάφορες συναλλαγές και δράσεις.

Μέχρι σήμερα, η προσπάθεια για αντιμετώπιση φαινομένων απάτης στηρίζεται σχεδόν αποκλειστικά σε συμβατικά συστήματα επεξεργασίας δεδομένων τα οποία όμως παρουσιάζουν σημαντικούς περιορισμούς όσον αφορά στη δυνατότητα για αποθήκευση και γρήγορη επεξεργασία δεδομένων, με αποτέλεσμα, τις περισσότερες φορές τα φαινόμενα απάτης να μην γίνονται αντιληπτά ή να γίνονται αντιληπτά με σημαντική καθυστέρηση.

Ενδεικτικά, η πλειοψηφία των παραδοσιακών συστημάτων μπορεί να επεξεργαστεί περίπου το 20% της διακινούμενης πληροφορίας, με αποτέλεσμα, η

διάδοση φαινομένων απάτης να έχει ένα σημαντικό εύρος ‘ανεπεξέργαστης’ πληροφορίας για να κινηθεί.

Με βάση την παραπάνω παρατήρηση, εύκολα αντιλαμβάνεται κανείς, ότι τα παραδοσιακά συστήματα για την αντιμετώπιση της απάτης λειτουργούν περισσότερο δειγματοληπτικά και με συγκεκριμένους αλγόριθμους, με αποτέλεσμα κάποιος κυβερνοεγκληματίας αυξημένων δυνατοτήτων, να μπορεί εύκολα να βρει τρόπους να αποφεύγει αυτές τις ελεγκτικές δράσεις.

Η παραπάνω διαπίστωση καταγράφει με τον πιο περιεκτικό τρόπο την αδυναμία των παραδοσιακών συστημάτων να αντιμετωπίσουν τα φαινόμενα της ηλεκτρονικής απάτης σήμερα και καταδεικνύει με τον πιο εμφανή τρόπο την ανάγκη εισαγωγής των εφαρμογών των Μεγάλων Δεδομένων μέσω επενδυτικών δράσεων για την αντιμετώπιση αυτού του είδους απάτης.

Η χρήση εφαρμογών και συστημάτων Μεγάλων Δεδομένων, μπορεί να βοηθήσει ουσιαστικά προς αυτή την κατεύθυνση, εξαιτίας της αυξημένης δυνατότητας που αυτά παρουσιάζουν σε σχέση με τη συνιστώσα της μοντελοποίησης και επεξεργασίας δεδομένων. Στην περίπτωση αυτών των συστημάτων, μπορεί να επεξεργαστεί ένα ποσοστό κοντά στο 80% των δεδομένων που διακινούνται, ενώ λόγω των συνδυασμένων λειτουργικών δυνατοτήτων που παρουσιάζουν, λαμβάνει χώρα μια πολυδιάστατη – και όχι μονοδιάστατη όπως στη περίπτωση των συμβατικών συστημάτων – διαδικασία για την ανίχνευση της απάτης.

Κατά τη διαδικασία αυτή, δεν αφήνεται κανένα είδος πληροφορίας να ξεφύγει χωρίς έλεγχο, ενώ επιπρόσθετα, δεδομένα και πληροφορίες που εμφανίζονται ως ‘ύποπτες’, μέσω μιας διαδικασίας ανάδρασης επιστρέφουν στο σημείο ελέγχου προκειμένου να ελεγχθούν ξανά. Υπό αυτό το πρίσμα, η πιθανότητα για ανίχνευση πιθανής απάτης αυξάνεται σημαντικά.

Συστήματα διαχείρισης ρίσκου

Η διαχείριση του κινδύνου αποτέλεσε και αποτελεί ένα από τα σημαντικότερα ζητήματα που καλούνται να αντιμετωπίσουν οι ανά τον κόσμο επιχειρήσεις και οργανισμοί. Η υιοθέτηση κατάλληλων συστημάτων και δράσεων στο πεδίο της

διαχείρισης κινδύνου, μπορεί να αποδειχθεί πολλές φορές σημαντική ακόμα και για την ίδια τη βιωσιμότητα μιας εταιρίας σε ένα πλήρως ανταγωνιστικό περιβάλλον.

Όπως αναφέρθηκε και στη περίπτωση της ανίχνευσης απάτης, τα παραδοσιακά σύστηματα επεξεργασίας δεδομένων μπορούν να επεξεργαστούν ένα ποσοστό μέχρι 20% της διακινούμενης πληροφορίας.

Στην περίπτωση της διαχείρισης κινδύνου, που αποτελεί ένα ιδιαίτερα απαιτητικό πεδίο, είναι προφανές ότι τα παραδοσιακά συστήματα δεν μπορούν να λάβουν υπόψη όλους εκείνους τους παράγοντες και συνιστώσες που συνθέτουν ένα σύγχρονο πρόβλημα, και επομένως να προβούν στους απαραίτητους συνδυασμούς, προκειμένου να παράσχουν ικανοποιητικά αποτελέσματα στο πεδίο αυτό.

Με βάση την παραπάνω παρατήρηση, εύκολα αντιλαμβάνεται κανείς ότι η διαχείριση κινδύνου στο πλαίσιο εταιριών και οργανισμών αποτελεί ένα κλασσικό παράδειγμα εφαρμογής σύγχρονων πληροφοριακών συστημάτων, λόγω του πολύ μεγάλου και πολυεπίπεδου όγκου πληροφοριών που πρέπει να ληφθούν υπόψη – για παράδειγμα, ένα οικονομικό γεγονός στην Κίνα, μπορεί να επηρεάσει μια εταιρία στην Ελλάδα, οπότε πρέπει να ληφθεί υπόψη – και της πολυδιάστασης ανάλυσης που πρέπει να λάβει χώρα.

Σε ένα τέτοιο πλαίσιο, είναι προφανής και η συγγενής απαίτηση για ασφάλεια των διακινούμενων πληροφοριών και δεδομένων μείζονος σημασίας για τη στρατηγική του εκάστοτε οργανισμού σε ένα ιδαιτέρως ανταγωνιστικό σύγχρονο επιχειρηματικό περιβάλλον.

Διασφάλιση συνομιλιών μέσω τηλεφωνικών κέντρων

Η χρήση εφαρμογών ασφάλειας πληροφοριών έχει συντελέσει και συνεχίζει να συντελεί στη βελτίωση της αποδοτικότητας και δυνατότητας για ασφαλή διακίνηση πληροφοριών όσον αφορά στην περίπτωση των τηλεφωνικών κέντρων.

Σε μια εποχή όπου συνεχώς και καθημερινά το σύνολο των πολιτών δέχεται κλήσεις από τηλεφωνικά κέντρα διαφόρων εταιριών παροχής υπηρεσιών και προϊόντων, με την ανταλλαγή πληροφοριών να είναι συνεχής και ογκώδης, είναι

συνήθες φαινόμενο να ανακύπτουν φαινόμενα προστασίας των διακινούμενων πληροφοριών και δεδομένων.

Στην πραγματικότητα, η αλματώδης αύξηση της τεχνολογίας με τη δημιουργία συνεχώς εξελισσόμενων συσκευών συνεχούς παρακολούθησης, σε συνδυασμό με τις αμφιλεγόμενες πολιτικές προστασίας του απορρήτου που υπάρχουν σήμερα, οδηγούν στο συμπέρασμα ότι το γεγονός ότι στην πλειοψηφία τους οι επικοινωνίες μεταξύ ατόμων δεν παρακολουθούνται, οφείλεται σε έλλειψη ενδιαφέροντος και όχι στη δυσκολία του εγχειρήματος για μια τέτοια παρακολούθηση.

Σε ένα τέτοιο πλαίσιο, η υιοθέτηση επενδυτικών δράσεων από την πλευρά των εταιριών για την ασφάλεια των πληροφοριακών συστημάτων, αποτελεί τη μόνη ενδεδειγμένη λύση για την εξασφάλιση της όσο το δυνατόν μεγαλύτερης ασφάλειας και προστασίας των διακινούμενων πληροφοριών μεταξύ καταναλωτών και παρόχων υπηρεσιών και προϊόντων.

3

Επένδυση στην ασφάλεια πληροφοριακών συστημάτων

3.1 Χαρακτηριστικά της επένδυσης στην ασφάλεια των πληροφοριακών συστημάτων

Τα χαρακτηριστικά της επένδυσης που σχετίζεται με την ασφάλεια των πληροφοριακών συστημάτων μπορούν να ομαδοποιηθούν σε τρεις κύριες κατηγορίες (Shao, 2015):

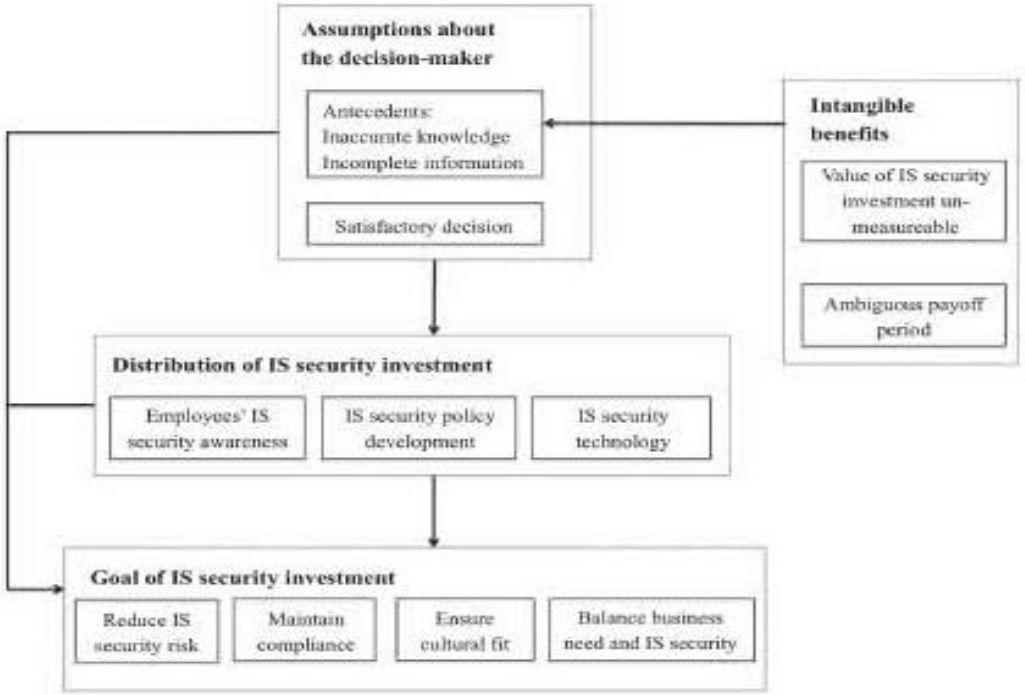
- Διάδοση της ασφάλειας.
- Στόχοι σε σχέση με την ασφάλεια.
- Οφέλη από την αυξανόμενη ασφάλεια.

Ο επόμενος πίνακας αποτυπώνει καθένα από τα παραπάνω χαρακτηριστικά καθώς και τις υπο – συνιστώσεις που καθορίζουν το συνολικό περιεχόμενο αυτών.

Πίνακας 2. Χαρακτηριστικά επένδυσης για την ασφάλεια των πληροφοριακών συστημάτων και υπο – συνιστώσες καθορισμού αυτών.

	Description
Distribution	– IS security training/education to improve employees' security behaviors – IS security policy development – IS security technologies
Goal	– Reduce the risk to an acceptable level – Balance the need to secure information assets against the need to facilitate the business function – Maintain compliance – Ensure cultural fit
Intangible benefits	– Value of IS security investment lies in "preventing something from happening," not in "making something happen" – Payoff period of IS security investment is ambiguous

Εν γένει, το υπάρχον πλαίσιο δράσης, σχετιζόμενο με την επένδυση στην ασφάλεια των πληροφοριακών συστημάτων, απεικονίζεται στο επόμενο σχήμα.



Σχήμα 3. Πλαίσιο δράσης, σχετιζόμενο με την επένδυση στην ασφάλεια των πληροφοριακών συστημάτων(Shao, 2015).

3.2 Περιοχές ενασχόλησης της επένδυσης στην ασφάλεια των πληροφοριακών συστημάτων

Εν γένει, οι περιοχές στις οποίες αποσκοπεί προς βελτίωση η υιοθέτηση επενδυτικών δράσεων με προσανατολισμό στην ασφάλεια των πληροφοριακών συστημάτων είναι (Shao, 2015):

- Οι άνθρωποι.
- Οι διαδικασίες.
- Η τεχνολογία.

Εκκινώντας από την ανθρώπινη συνιστώσα, όπως τονίζουν οι Siponen&Vance (2010), το μεγαλύτερο ποσοστό θεμάτων ασφαλείας που ανακύπτουν σε έναν επιχειρησιακό οργανισμό οφείλεται στο ίδιο το ανθρώπινο δυναμικό του οργανισμού και λαμβάνει χώρα είτε ακούσια ένεκα της ανεπάρκειας αυτού σε συγκεκριμένα ζητήματα, είτε εκκούσια με σκοπό μέρη του ανθρώπινου δυναμικού του οργανισμού να βλάψουν αυτόν.

Σε ένα τέτοιο πλαίσιο, αν το σύνολο του ανθρώπινου δυναμικού εντός ενός οργανισμού δεν εναρμονιστεί με τις απαιτήσεις για ασφάλεια των πληροφοριακών συστημάτων αυτού, οποιαδήποτε υιοθέτηση τεχνολογικών δράσεων προς αυτή την κατεύθυνση, όσο και αν εξελιγμένη είναι, δεν μπορεί να επιτελέσει ολοκληρωτικά το έργο της.

Σε σχέση με τη συνιστώσα των διαδικασίων, αυτή στο πεδίο των επενδύσεων για την ασφάλεια των πληροφοριακών συστημάτων σχετίζεται κύρια με την ανάπτυξη πολιτικών για την ενδυνάμωση της ασφάλειας αυτών.

Η αποκωδικοποίηση εμπιστευτικών e-mail, ή ο ανά τακτά διαστήματα έλεγχος των ΄πληροφοριακών συναλλαγών’ των εργαζομένων εντός του πλαισίου της εταιρίας, αποτελούν δράσεις προς αυτή την κατεύθυνση, οι οποίες όμως όπως τονίζει ο Puhakainen (2006) μπορούν να προκαλέσουν τη σφοδρή αντίδραση των εργαζομένων με αποτέλεσμα τη δημιουργία ενός αρνητικού εργασιακού κλίματος.

Τέλος, το τρίτο και ίσως πιο σημαντικό πεδίο για την υιοθέτηση επενδυτικών δράσεων με προσανατολισμό στην ασφάλεια των πληροφοριακών συστημάτων, αποτελεί αυτό της τεχνολογίας.

Στο σημερινό γίγνεσθαι, καθημερινά σχεδόν το σύνολο των επιχειρήσεων ανά τον κόσμο υιοθετεί δράσεις με σκοπό την προστασία των διακινούμενων πληροφοριών, με απώτερο στόχο την προστασία της ίδιας της στρατηγικής αυτών και εν γένει τη βιωσιμότητα και περαιτέρω ανάπτυξή τους σε ένα πλήρως ανταγωνιστικό περιβάλλον δράσης.

Τις σημαντικότερες δράσεις προς αυτή την κατεύθυνση αποτελούν (Liu&Mookerjee, 2005):

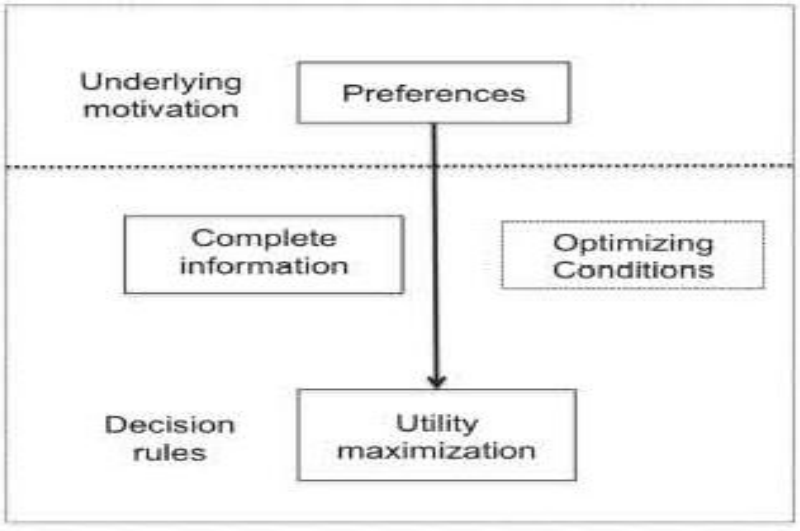
- Η χρήση των ασφαλέστερων δυνατών περιηγητών διαδικτύου.
- Η χρησιμοποίηση φίλτρων για το έλεγχο των διακινούμενων πληροφοριών.
- Η χρήση συστημάτων κινητής πρόσβασης (VPN).
- Η κωδικοποιημένη χρήση των υπολογιστικών συστημάτων.
- Η συνεχής εξέλιξη του ψηφιακού δικτύου διακίνησης πληροφοριών και δεδομένων.
- Η υιοθέτηση των πιο επίκαιρων επιταγών του τεχνολογικού management.

Κλείνοντας, θα πρέπει να καταδειχτεί ότι τα δύο πρώτα πεδία (ανθρώπινο δυναμικό και διαδικασίες) σχετίζονται με την προστασία των εταιριών από εσωτερικές απειλές, ενώ το τρίτο πεδίο (τεχνολογία) έχει να κάνει κύρια με την προστασία των οργανισμών από εξωτερικούς παράγοντες που απειλούν την ασφάλεια των πληροφοριακών συστημάτων αυτών.

4

Μοντέλα ανάλυσης και αξιολόγησης επενδύσεων για την ασφάλεια πληροφοριακών συστημάτων

Τα μέχρι στιγμής υπάρχοντα μοντέλα για την ανάλυση και αξιολόγηση των επενδύσεων σχετιζομένων με τη ασφάλεια των πληροφοριακών συστημάτων στηρίζουν τις αρχές τους σχεδόν αποκλειστικά στη νεοκλασσική οικονομική θεωρία και ΄δρούν’ σύμφωνα με το διάγραμμα του επόμενου σχήματος.



Σχήμα 4. Πλαίσιο δράσης υπαρχόντων μοντέλων για την ανάλυση και αξιολόγηση των επενδύσεων σχετιζομένων με τη ασφάλεια των πληροφοριακών συστημάτων (Simon, 1997).

Τα εν λόγω μοντέλα, ανάλογα με τον τρόπο προσέγγισης που χρησιμοποιούν διακρίνονται σε:

- Μοντέλα στηριζόμενα στις αρχές της λήψης αποφάσεων.
- Μοντέλα στηριζόμενα στη θεωρία των παιγνίων.
- Μοντέλα στηριζόμενα στην κλασσική οικονομική προσέγγιση ανάλυσης των επενδύσεων.

4.1 Μοντέλα στηριζόμενα στις αρχές της λήψης αποφάσεων

Τα συγκεκριμένα μοντέλα συνδυάζουν τις αρχές της νεοκλασσικής οικονομικής θεωρίας και τις αρχές της λήψης αποφάσεων σύμφωνα με τον ακόλουθο πίνακα.

Πίνακας 3. Χαρακτηριστικά μοντέλων στηριζόμενων στις αρχές της λήψης αποφάσεων (Simon, 1997).

	Description
Preferences	Given a set of exhaustive and exclusive options to choose from, an individual can rank the options in terms of his/her preferences, this preference structure is internally consistent, and there should be at least one maximal option. Preferences are often described by utility function or payoff function.
Utility maximization	Individuals maximize utility. Firms maximize profits.
Complete information	People have full and relevant information about exactly what will occur due to any choice made. In game theory, every player knows payoffs and strategies of every other player.
Optimizing condition	Neoclassical optimization are described by a set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.

Σε ένα τέτοιο πλαίσιο, οι Gordon&Loeb (2002) δημιούργησαν ένα μοντέλο προσδιορισμού του ύψους των επενδύσεων που πρέπει να κάνει μια εταιρία για την ασφάλεια των πληροφοριακών της συστημάτων. Το συγκεκριμένο μοντέλο

στηρίζονταν στη σύγκριση των αναμενόμενων ωφελειών από την υιοθέτηση των πιο εξελιγμένων συστημάτων ασφάλειας σε σύγκριση με την υπάρχουσα κατάσταση, ανοιγμένη σε οικονομικές μονάδες μέσω της χρήσης του μοντέλου κόστους - οφέλους. Το μοντέλο εφαρμόστηκε σε 15 εταιρίες ανά τον κόσμο και τα αποτλέσματα κατέδειξαν ότι οι εταιρίες μπορούν να έχουν όφελος ακόμα και αν δεν υιοθετήσουν ότι πιο εξελιγμένο τεχνολογικά για την ασφάλεια των συστημάτων τους, στην περίπτωση που οι διαθέσιμοι πόροι εμφανίζονται περιορισμένοι. Το όφελος ασφαλείας φυσικά είναι πιο μεγάλο όσο πιο εξελιγμένα είναι τα προς υιοθέτηση συστήματα.

Οι Huangetal. (2006) από την άλλη, πρότειναν ένα οικονομικό μοντέλο που ως είσοδο χρησιμοποιούσε εξωτερικές απειλές με διαφορετικά χαρακτηριστικά και ως έξοδο τις βελτιστοποιημένες αντίστοιχες επενδύσεις με βάση την προσέγγιση της βελτιστοποίησης του οφέλους. Τα αποτελέσματα από την εφαρμογή του μοντέλου κατέδειξαν ότι οι εταιρίες θα πρέπει να δίνουν μεγαλύτερη βάση στους τύπους απειλών distributed και targeted, ενώ οι εταιρίες που διαθέτουν μικρότερο budget θα πρέπει να καταναλίσκουν το σημαντικότερο μέρος αυτού στην αντιμετώπιση απειλών τύπου targeted.

Προχωρώντας ένα βήμα πιο πέρα, οι Huang&Goo (2009) δημιούργησαν ένα γενικό μοντέλο για τη διαχείριση των επενδύσεων που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων για την αξιολόγηση του οποίου εφήρμοσαν στη γενική βάση αυτού διαφορετικά σενάρια απωλειών από εξωτερικές επιθέσεις. Τα αποτελέσματα κετέδειξαν ότι το μέγεθος των απωλειών είναι αυτό που καθορίζει στο σημαντικότερο βαθμό το ύψος των επενδύσεων με προσανατολισμό στην ασφάλεια των πληροφοριακών συστημάτων. Επιπρόσθετα, όπως υποστηρίζουν οι δύο συγγραφείς, η ανάγκη για επενδύσεις προς αυτή την κατεύθυνση μειώνεται με την αύξηση της ΄αμυντικής ικανότητας’ του συνολικού πληροφοριακού συστήματος της εκάστοτε εταιρίας και τη διατήρησης αυτού σε ένα συνεχές πλαίσιο ενημέρωσης.

ΟιBojancet. al., (2012) πρότειναν ένα μαθηματικό μοντέλο για την προσέγγιση του βέλτιστου ύψους επένδυσης σε τεχνολογία προστασίας πληροφοριακών συστημάτων. Τα αποτελέσματα κατέδειξαν ότι το βέλτιστο ύψος επένδυσης αποτελεί συνάρτηση της δυνατότητας των εταιριών για αντιμετώπιση των

εξωτερικών απειλών αλλά και ο διατιθέμενος από αυτές τεχνολογικός εξοπλισμός προς αυτή την κατεύθυνση.

Εισάγωντας σθεναρά την έννοια της αβεβαιότητας, οι Kantarcioglouetal., (2011) χρησιμοποιώντας τις συναρτήσης Copulaμέσω του αντίστοιχου στατικού μοντέλου, κατέδειξαν ότι η αβεβαιότητα θα πρέπει να παίζει ρόλο στην απόφαση για υιοθέτηση επενδυτικών δράσεων μόνο στην περίπτωση όπου αυτή ξεπερνά ένα ανώτατο όριο το οποίο εξαρτάται από τη δομή του οργανισμού αλλά και από τις δυνατότητες των ανταγωνιστικών εταιριών του κλάδου. Επιπρόσθετα, η συγκεκριμένη παράμετρος καθορίζει και το χρόνο που αυτές οι επενδύσεις θα πρέπει να λάβουν χώρα με το χρόνο επένδυσης να πρέπει να είναι άμεσος στην περίπτωση μονοπωλιακών καταστάσεων ένεκα του γεγονότος ότι σε αυτή την περίπτωση ο στόχος των απειλών είναι πιο ξεκάθαρος.

ΟιLeeetal, (2011), στο άρθρο τους ασχολήθηκαν περισσότερο με την προστασία των δεδομένων των επιχειρήσεων που σχετίζονται με τους πελάτες αυτών. Σε ένα τέτοιο πλαίσιο, με τη χρήση ενός μοντέλου βελτιστοποίησης του κέρδους που σχετίζεται με την προστασία των προσωπικών δεδομένων των πελατών, κατέδειξε ότι οι εταιρίες θα πρέπει να μετακυλούν ένα μέρος του κόστους για την υιοθέτηση συστημάτων προστασίας των δεδομένων και πληροφοριών στους καταναλωτές προκειμένου να εξασφαλίζουν τη βέλτιστη προστασία αυτών.

4.2 Μοντέλα στηριζόμενα στη θεωρία των παιγνίων

Οι εν λόγω τύποι μοντέλων αξιολόγησης των επενδύσεων σχετιζομένων με τη ασφάλεια των πληροφοριακών συστημάτων στηρίζουν την εφαρμογή τους στη θεωρία των παιγνίων.

Σε ένα πιο συγκεκριμένο πλαίσιο, η προσέγγιση των εν λόγω μοντέλων στηρίζεται στη θεώρηση δύο παικτών, της εκάστοτε εταιρίας και των απειλών αυτής. Το τίμημα της επένδυσης για την εταιρία είναι συνάρτηση του σθένους των απειλών αυτής, ενώ το τίμημα των ατόμων που αποτελούν την απειλή, σχετίζεται με την πιθανότητα αυτοί να εντοπιστούν.

Έστώ ότι ο σχετιζόμενος πίνακας σύμφωνα με τη θεωρία των παιγνίων για το παραπάνω σενάριο είναι ο Πίνακας 4 που ακολουθεί. Τότε:

Αν ο παίκτης Α (εταιρία) επιλέξει τη στρατηγική A_i και ο παίκτης Β (απειλή) επιλέξει τη στρατηγική B_j, τότε παίκτης Α κερδίζει α_{ij} και ο πάικτης Β χάνει α_{ij}.

Πίνακας 4. Τυπικός πίνακας μοντέλων αξιολόγησης των επενδύσεων σχετιζομένων με τη ασφάλεια των πληροφοριακών συστημάτων στηριζόμενων στη θεωρία παιγνίων (Tadelis, 2013).

		Παίκτης Β			
	Στρατηγικές	1	2		n
Παίκτης Α	1	α_{11}	α_{12}	…	α_{1n}
	2	α_{21}	α_{22}	…	α_{2n}
	⋮	⋮	⋮	⋱	⋮
	m	α_{m1}	α_{m2}	…	α_{mn}

Υιοθετώντας ένα τέτοιο μοντέλο, οι Cavusogluetal., (2005), κατέδειξαν στη μελέτη τους ότι η βέλτιστη στρατηγική που πρέπει να ακολουθήσει η εκάστοτε εταιρία για την προστασία των πληροφοριακών της συστημάτων δεν εξαρτάται από τις εσωτερικές οικονομικές παραμέτρους αυτής, αλλά από εξωτερικές παραμέτρους που σχετίζονται με την απειλή. Σε ένα τέτοιο πλαίσιο, όπως καταδεικνύουν οι συγγραφείς θα πρέπει να υπάρξει πρόβλεψη τόσο της συμπεριφοράς όσο και των κινήτρων της απειλής.

Στο ίδιο μήκος κύματος, οι Bohme&Moore (2009) πρότειναν ένα μοντέλο ανάλυσης ενισχύοντας τη δυναμική συνιστώσα μεταξύ εταρίας και απειλής. Σε ένα τέτοιο πλαίσιο, θεωρήθηκε ότι και οι δύο πλευρές μπορούσαν ανά πάσα στιγμή να αναγνωρίσουν το πιο αδύναμο σημείο του αντιπάλου. Η εφαρμογή της έρευνας σε δύο εταιρίες κατέδειξε ότι είναι δυνατή η διαβάθμιση του ύψους της επένδυσης ανάλογα με την εξωτερική απειλή και τις δυνατότητες αυτής, αλλά και ότι το ύψος για επένδυση αναβάθμισης ακόμα και μετά από επιτυχημένη επίθεση της απειλής

μπορεί να θεωρηθεί σχετικά μικρό εφόσον υπάρχει το κατάλληλο προηγούμενο τεχνολογικό και ανθρώπινο ‘υπόστρωμα’.

Προχωρώντας, ο Hausken (2006), μέσω της εφαρμογής των αρχών της θεωρίας των παιγνίων και θεωρώντας σύμφωνα με τα προηγούμενα δύο παίκτες, την εταιρία και την απειλή, απέδειξε ότι οποιαδήποτε επενδυτική δράση με σκοπό την αντιμετώπιση πολύ ισχυρών απειλών που εξελίσσονται συνεχώς είναι ουσιαστικά μη ωφέλιμη. Επιπρόσθετα ο συγγραφέας επισήμανε ότι η επενδυτική δράση των εταιριών με προσανατολισμό στην ασφάλεια των πήροφοριακών συστημάτων είναι άμεση συνάρτηση του επιπέδου του εσόδου που επιτυγχάνει η εταιρία αναφοράς.

Εφαρμόζοντας μια συνδυαστική προσέγγιση, οιCavusoglou&Raghunathan (2004), παρουσίασαν δύο μοντέλα, το ένα στηριζόμενο στην θεωρία της λήψης αποφάσεων και το άλλο στην θεωρία των παιγνίων. Σύμφωνα με τα αποτελέσματα της έρευνας, η προσέγγιση μέσω της θεωρίας των παιγνίων αποδείχτηκε ότι οδηγεί στην υιοθέτηση συστημάτων χαμηλότερου κόστους και επομένως οδηγεί σε μεγαλύτερη οικονομική ωφέλεια για τις εταιρίες.

Τέλος, στο ίδιο μήκος κύματος, οιCavusoglouet. al. (2008), ροχώρησαν ένα βήμα παραπάνω την προηγούμενη έρευνα καταδεικνύοντας ότι η προσέγγιση μέσω της θεωρίας των παιγνίων οδηγεί στην υιοθέτηση συστημάτων οδηγεί σε μεγαλύτερη οικονομική ωφέλεια για τις εταιρίες και μάλιστα αυτή είναι τόσο μεγαλύτερη όσο πιο πολύ προηγείται η εταιρία της απειλής.

4.3 Μοντέλα στηριζόμενα στην κλασσική οικονομική προσέγγιση ανάλυσης των επενδύσεων

Τα συγκεκριμένα μοντέλα στηρίζουν την εφαρμογή τους στον υπολογισμό των κλασσικών οικονομικών μεγεθών για την αξιολόγηση μιας οποιασδήποτε επένδυσης που περιλαμβάνει την οικονομική συνιστώσα. Τα μεγέθη που υπολογίζονται στην πλειονότητα των περιπτώσεων τέτοιων προσεγγίσεων είναι:

- Η επιστροφή της επένδυσης (ROI).
- Η περίοδος επανείσπραξης (Paybackperiod).

- Η καθαρή παρούσα αξία (NPV).
- Ο εσωτερικός βαθμός απόδοσης (IRR).

Η επιστροφή της επένδυσης (ROI)

Η επιστροφή της επένδυσης ουσιαστικά αποτελεί το δείκτη που μας δείχνει την αναλογία των μεικτών κερδών από την επένδυση προς το ποσό που σπαταλήθηκε για αυτή. Ο εν λόγω δείκτης χρησιμοποιείται για τη μέτρηση της αποδοτικότητας και εν γένει για την αξιολόγηση επενδυτικών δράσεων.

$$ROI = \frac{Μεικτά\ κέρδη\ επένδυσης}{Κόστος\ επένδυσης}$$

Η περίοδος επανείσπραξης (Paybackperiod)

Η περίοδος επανείσπραξης ισούται με το πηλίκο του αρχικού κόστους προς την ταμειακή ροή. Δηλαδή:

$$Payback\ period = \frac{Αρχικό\ κόστος\ επένδυσης}{Ταμειακή\ ροή}$$

Η οικονομική λογική της χρήσης της περιόδου επανείσπραξης στην αξιολόγηση επενδυτικών στοιχείων έγκειται στον προσδιορισμό του χρονικού διαστήματος μέσα στο οποίο το επενδυτικό σχέδιο θα αποδώσει το αρχικό του κόστος.

Η καθαρή παρούσα αξία (NPV)

Η καθαρή παρούσα αξία του επενδυτικού σχεδίου ισούται με τη διαφορά της παρούσας αξίας των ταμειακών ροών και του αρχικού κόστους.

Για την αναγωγή των ταμειακών ροών σε παρούσα αξία χρησιμοποιείται ο τύπος:

$$NPV = \frac{F}{(1+IRR)^n}, \text{όπου } n: 1 \dots t$$

Διακρίνονται οι ακόλουθες περιπτώσεις:

- Αν NPV> 0, η επένδυση είναι οικονομικά ωφέλιμη.
- Αν NPV = 0, η επένδυση είναι οικονομικά αδιάφορη.
- Αν NPV< 0, η επένδυση είναι οικονομικά μη ωφέλιμη.

Ο εσωτερικός βαθμός απόδοσης (IRR)

Ο εσωτερικός συντελεστής απόδοσης του σχεδίου, είναι αυτός για τον οποίο η NPV του σχεδίου γίνεται ίση με το 0.

Ο υπολογισμός του IRR λαμβάνει χώρα μέσω του ακόλουθου τύπου:

$$IRR = NPV - Αρχικό\ κόστος$$

Η οικονομική λογική της χρήσης του εσωτερικού συντελεστή απόδοσης, έγκειται στην ανάγκη να είναι γνωστό στην πλευρά των επενδυτών το επιτόκιο για το οποίο η παρούσα αξία των ταμειακών ρόων της επένδυσης ισούται με το αρχικό κόστος.

Οι Ghahremanietal., (2012) ομαδοποίησαν σε έναν πίνακα ερωτήσεων τα πεδία ελλείψεων και κάλυψης των παραπάνω οικονομικών μεγεθών σε σχέση με το πεδίο της αξιολόγησης επενδύσεων σχετιζόμενων με την ασφάλεια πληροφοριακών συστημάτων.

Πίνακας 5. Πεδία ελλείψεων και κάλυψης των σημαντικότερων οικονομικών μεγεθών σε σχέση με το πεδίο της αξιολόγησης επενδύσεων σχετιζόμενων με την ασφάλεια πληροφοριακών συστημάτων (Ghahremanietal., 2012).

Evaluation Criteria	ARR/ROI	PBK	NPV	IRR
1. Does it consider the entire lifetime of the investment?	Yes	No	Yes	Yes
2. Does it consider time value of money?	No	No	Yes	Yes
3. Can risk-level be entered into the feasibility evaluation?	Yes	No	Yes	Yes
4. Can risk-level be entered in the selection of mutually exclusive projects?	No	No	Yes	No
5. Does it consider other department's perspectives except investment department?	No	No	No	No
6. Does it consider non-financial benefits, intangible, or immeasurable factors	No	No	No	No
7. Can several sources of uncertainty be entered into the appraisal process	No	No	No	No
8. Does it consider managerial flexibility to alter the course of a project	No	No	No	No
9. Does it manage the project actively?	No	No	No	No
10. Does it take into account behavioral and organizational biases?	No	No	No	No

Με βάση τα περιεχόμενα του παραπάνω πίνακα, εύκολα αντιλαμβάνεται κανείς ότι τα μοντέλα που στηρίζουν την εφαρμογή τους στον υπολογισμό των κλασσικών οικονομικών μεγεθών, όσον αφορά στο πεδίο της αξιολόγησης επενδύσεων σχετιζόμενων με την ασφάλεια των πληροφοριακών συστημάτων, υστερούν όσον αφορά στο γεγονός ότι δε λαμβάνουν υπόψη ποιοτικές παραμέτρους, όπως για παράδειγμα η συμπεριφορά του ανθρώπινου παράγοντα, αλλά παραμένουν προσηλωμένα στον ποσοτικό υπολογισμό καθαρά οικονομικών μεγεθών.

Προς αυτή την κατεύθυνση, οιBrockeetal., (2007 ασχολήθηκαν με τα οφέλη από την υιοθέτηση επενδυτικών δράσεων από τις εταιρίες για την ασφάλεια των πληροφοριακών τους συστημάτων μέσω του υπολογισμού του δείκτη ReturnonSecurityInvestmentsστη βάση του διατιθέμενου προϋπολογισμού των εταιριών αναφοράς. Τα αποτελέσματα κατέδειξαν ότι υπάρχει θετική συσχέτιση μεταξύ του ύψους της επένδυσης και του οφέλους από αυτή αν και όπως επισημαίνουν οι συγγραφείς, η προσέγγιση μέσω του συγκεκριμένου δείκτη δεν

λαμβάνει υπόψη ποιοτικά χαρακτηριστικά αβεβαιότητας, σύστοιχα με τις επισημάνσεις που έλαβαν χώρα προηγουμένως.

Συνεχίζοντας, οι Bojan&Jerman – Blazic (2012), στο άρθρο τους περιγράφουν ένα μοντέλο για τον προσδιορισμό της βέλτιστης επενδυτικής δράσης με βάση τις συνιστώσες του υπάρχοντος για την εκάστοτε εταιρία ρίσκου και των διατιθέμενων κονδυλίων για ψηφιακές δράσεις. Το μοντέλο υπολογίζει τα μεγέθη ROI, NPVκαι IRRόπως αυτά αναλύθηκαν παραπάνω και όπως τονίζουν χαρακτηριστικά οι συγγραφείς αποτελεί το ενδεδιγμένο μοντέλο για περιπτώσεις όπου το ενδιαφέρον επικεντρώνεται καθαρά σε ποσοτικές συσχετίσεις.

4.4 Νέες τάσεις όσον αφορά στα μοντέλα αξιολόγησης και ανάλυσης επενδύσεων σχετιζόμενων με την ασφάλεια των πληροφοριακών συστημάτων

Όπως καταδείχτηκε στο προηγούμενο χωρίο, τα μοντέλα που στηρίζουν την εφαρμογή τους στον υπολογισμό των κλασσικών οικονομικών μεγεθών, όσον αφορά στο πεδίο της αξιολόγησης επενδύσεων σχετιζόμενων με την ασφάλεια των πληροφοριακών συστημάτων, υστερούν όσον αφορά στο γεγονός ότι δε λαμβάνουν υπόψη ποιοτικές παραμέτρους.

Κάτι ανάλογο ισχύει και για τα μοντέλα που βασίζονται στις προσεγγίσεις της λήψης αποφάσεων και της θεωρίας παιγνίων όπως αυτά περιγράφησαν προηγουμένως και στηρίζονται πλήρως στη νεοκλασσική οικονομική θεωρία.

Σε ένα τέτοιο πλαίσιο, οι νέες τάσεις αφορούν στην υιοθέτηση μοντέλων που θα λαμβάνουν υπόψη εκτός των απτών ποσοτικών οικονομικών μεγεθών και ποιοτικές παραμέτρους όπως η συμπεριφορά του ανθρώπινου παράγοντα ή η αύξηση της φήμης του εκάστοτε οργανισμού από την υιοθέτηση εξελιγμένων συστημάτων ασφάλειας των πληροφοριακών του συστημάτων.

Πίνακας 6. Διαφοροποίησεις μεταξύ υπάρχουσας κατάστασης και τάσεων.

Neoclassical economics	Satisfactory solution assumption
To obtain maximum benefit from IS security investment	To achieve a satisfactory solution
Complete information about decision maker's own preference and the environment (consequences of IS security investment)	Incomplete information about one's own preferences and the environment
Complete knowledge, such that decision maker could accurately predict the value of all consequences	Inaccurate knowledge about the consequences of IS security investment due to limited cognitive ability and the intangible nature of IS security investment benefits

5

Συμπεράσματα

Συμπερασματικά, σε ένα παγκοσμιοποιημένο περιβάλλον όπου ο όγκος και η ταχύτητα διάδοσης των πληροφοριών λαμβάνουν χώρα με γεωμετρικώς αυξανόμενους ρυθμούς, είναι προφανής η ανάγκη για υιοθέτηση επενδυτικών δράσεων από την πλευρά των επιχειρήσεων και οργανισμών με σκοπό την προστασία των πληροφοριακών τους συστημάτων.

Τα μέχρι στιγμής υπάρχοντα μοντέλα για την ανάλυση και αξιολόγηση των επενδύσεων σχετιζομένων με τη ασφάλεια των πληροφοριακών συστημάτων στηρίζουν τις αρχές τους σχεδόν αποκλειστικά στη νεοκλασσική οικονομική θεωρία και ανάλογα με τον τρόπο προσέγγισης που χρησιμοποιούν διακρίνονται σε μοντέλα στηριζόμενα στις αρχές της λήψης αποφάσεων, σε μοντέλα στηριζόμενα στη θεωρία των παιγνίων και σε μοντέλα στηριζόμενα στην κλασσική οικονομική προσέγγιση ανάλυσης των επενδύσεων.

Τα άρθρα που αναλύθηκαν στην παρούσα εργασία κατηγοριοποιημένα σύμφωνα με την παραπάνω επισήμανση παορυσιάζονται στον επόμενο πίνακα

Πίνακας 7. Κατηγοριοποίηση αναλυθέντων άρθρων.

Κατηγορία	**Συγγραφείς**
Άρθρα στηριζόμενα στις αρχές λήψης αποφάσεων.	• Gordon&Loeb (2002). • Huangetal. (2006).

	• Huang&Goo (2009). • Bojancet. al., (2012). • Kantarcioglouetal., (2011). • Leeetal, (2011).
Άρθρα στηριζόμενα στη θεωρία των παιγνίων.	• Cavusogluetal., (2005). • Bohme&Moore (2009). • Hausken (2006). • Cavusoglou&Raghunathan (2004). • Cavusoglouet. al. (2008).
Άρθρα στηριζόμενα στην κλασσική οικονομική προσέγγιση ανάλυσης των επενδύσεων.	• Brockeetal., (2007) . • Bojan&Jerman – Blazic (2012).

Ταυπάρχοντα μοντέλαπου σχετίζονταιμε το πεδίο της αξιολόγησης επενδύσεων σχετιζόμενων με την ασφάλεια των πληροφοριακών συστημάτων, υστερούν όσον αφορά στο γεγονός ότι δε λαμβάνουν υπόψη ποιοτικές παραμέτρους.

Υπό αυτό το πρίσμα, οι νέες τάσεις αφορούν στην υιοθέτηση μοντέλων που θα λαμβάνουν υπόψη εκτός των απτών ποσοτικών οικονομικών μεγεθών και ποιοτικές παραμέτρους όπως η συμπεριφορά του ανθρώπινου παράγοντα ή η αύξηση της φήμης του εκάστοτε οργανισμού από την υιοθέτηση εξελιγμένων συστημάτων ασφάλειας των πληροφοριακών του συστημάτων.

6

Αναφορές

- Beynon - Davies P., (2002), *Information Systems: an introduction to informatics in Organisations.*, Palgrave, Basingstoke, UK.
- Böhme, R. & Moore, T., (2009), *The Iterated Weakest Link--A Model of Adaptive Security Investment*, The Eighth Workshop on the Economics of Information Security, London.
- Bojanc R, Jerman-Blažič B.& Tekavčič. M., (2012), Managing the investment in informationsecurity technology by use of a quantitative modeling,*Information Processing &Management*, 48(6): 1031–1052.
- Bojanc R, & Jerman-Blažič B., (2012), Quantitative Model for Economic Analyses of information Security Investment in an Enterprise Information Organizacija, 45: 276 – 288.
- Brocke, J., Buddendick, C., & Strauch, G., (2007), Return on Security Investments – Design Principles of Measurement Systems Based on Capital Budgeting, AMCIS, 1 – 9.

- Ghahremani, M., Aghaie, A., & Abedzadeh, M., (2012) Captial Budgeting Technique Selection through Four decades: With a great focus on Real Option, *International Journal of Business and Management*, 7(17).
- Cavusoglu, H., Mishra, B. & Raghunathan, S., (2005), The Value of Intrusion Detection Systems in Information Technology Security Architecture, *Information Systems Research*, 16(1): 28 – 46.
- Cavusoglu, H., Raghunathan, S., &Yue, W. T., (2008), Decision – Theoritic and Game – Theoritic Approaches to IT Security Investment,Journal of Management Information Systems, 25(2): 281 – 304.
- Cavusoglu, H.& Raghunathan, S., (2004), Configuration of Detection Software: A Comparisonof Decision and Game Theory Approaches,*Decision Analysis*, 1(3): 131–148.
- Checkland & Scholes, (1990), *Information equals data plus meaning*. London.
- Hausken., K, (2006), Income, interdependence, & substitution effects affecting incentives forsecurity investment,*Journal of Accounting and Public Policy* 25(6): 629–665.
- Huang, C.D., Hu, Q. & Behara, R.S., (2006), *Economics of information security investment in the case of simultaneous attacks*. The Fifth Workshop on the Economics of Information Security.
- Huang, C.D.,& Goo J., (2009),*Investment Decision on Information System Security: AScenario Approach,* American Conference on Information Systems (AMCIS) 2009proceedings.

- Gordon, L.A. & Loeb, M.P., (2002), The economics of information security investment, *ACM Transactions on Information and System Security (TISSEC)*, 5(4): 438 – 457.
- Craig, T., & Ludloff, M., (2011), *Privacy and Big Data*, O’Reilly Media, Sebastopol.
- Jasperson, (2002), Power and Information, Technology Research: A metatriangulation review, *Power and IT Research*, 26(4), 397- 459.
- Kantarcioglou, M., Bensoussan, A., & SingRu(Celine), H., (2011), LNCS, 219 – 238.
- Lee, J. Y., Kauffman, R. J., & Sougstad, R., (2011), Profit – maximizing firm investments in customer information security, Decision Support Systems, 904 – 920.
- Liu D, Ji Y., & Mookerjee, V. (2005), *Information Security Investment with Different Information Types: A Two- Firm Analysis*. AMCIS 2005 Proceedings.
- Longley , P. A., Goodchild, M. F., Maguire, D. J., & Rhind, D. W, (1999), *Geographical Information Systems: Principles, Techniques, Management and Applications*, New York.
- Luciano Floridi, (2005), *Is Information Meaningful Data?, The Standard Definition of Information*, Philosophy and Phenomenological Research, New York.
- Puhakainen, P., (2006), *Design Theory for Information Security Awareness*, University of Oulu.

- Shao, X., (2015), *Understanding Information Systems Security Investments in Organizations*, Acta Universitatis Ouluensis.
- Simon, H., (1997), Rationality in Psychology and Economics, *Journal of Business*, 59(4): 209 – 224.
- Siponen, M. & Vance, A., (2010), Neutralization: New Insight into the Problem of Employee, *Information Systems Security Policy Violations, MIS Quarterly*, 34(3): 487–502.
- Tadelis, S., (2013), *Game Theory: An introduction*, Princeton University Press.
- Zikopoulos, (2012), Understanding Big Data, McGraw Hill, New York.