Διαχείριση κρίσεων στο ηλεκτρονικό εμπόριο

Η εργασία υποβάλλεται για τη μερική κάλυψη των απαιτήσεων με στόχο την απόκτηση του διπλώματος

Μεταπτυχιακό Δίπλωμα Σπουδών στην

«Οικονομική και Επιχειρησιακή Στρατηγική»

M.Sc. – Master of Science in Economic and Business Strategy

από

ΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ευτυχία Ηλιοπούλου

Τμήμα Οικονομικής Επιστήμης, 2006

Αφιερώνεται

Στους γονείς μου για την αμέριστη συμπαράσταση

ΠΕΡΙΕΧΟΜΕΝΑ

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στο Διδάκτορα κ. Ιωάννη Σμυρλή που ως επιβλέπων της παρούσας εργασίας, μου παρείχε την αμέριστη βοήθειά του, καθώς και πολύτιμες συμβουλές και κατευθύνσεις για τη σωστή συγγραφή της.

Επίσης, επιθυμώ να ευχαριστήσω τους αρμόδιους εκπροσώπους του δικτυακού τόπου papasotiriou.gr καθώς και την Προϊσταμένη Τεχνικών Ασφαλειών της Interamerican που διέθεσαν τον πολύτιμο χρόνο τους να συζητήσουν μαζί μου και συνέβαλαν σημαντικά στην υλοποίηση της διπλωματικής αυτής εργασίας.

ΚΑΤΑΣΤΑΣΗ ΠΙΝΑΚΩΝ Σελ.

ΚΑΤΑΣΤΑΣΗ ΣΧΗΜΑΤΩΝ Σελ.

ΚΑΤΑΣΤΑΣΗ ΓΡΑΦΗΜΑΤΩΝ Σελ.

Μέρος Α

ΚΕΦΑΛΑΙΟ 1ο : ΕΙΣΑΓΩΓΗ

Κυρίαρχο χαρακτηριστικό της τελευταίας δεκαετίας του 20ου αιώνα αποτέλεσε το ξεκίνημα ενός νέου μετασχηματισμού της οικονομίας και της κοινωνίας. Οι αλλαγές που δρομολόγησαν η οικονομία της γνώσης και της πληροφορίας, η νέα οικονομία, είναι εντυπωσιακές. Οι αλλαγές αυτές που διαδραματίζονται, πολλές φορές αθόρυβα, συγκρίνονται ήδη με τις αλλαγές που προξένησε στο παρελθόν ο μετασχηματισμός των αγροτικών οικονομιών σε βιομηχανικές.

Στο παρελθόν, η οργάνωση της βιομηχανικής κοινωνίας αντανακλούσε τον ανταγωνισμό των δύο συντελεστών παραγωγής, της εργασίας και του κεφαλαίου. Σήμερα, υπεισέρχεται και ένας τρίτος συντελεστής παραγωγής, με σημαίνουσα βαρύτητα στην προστιθέμενη αξία των παραγόμενων αγαθών και υπηρεσιών, η γνώση. Σήμερα, γίνεται λόγος για Οικονομία της Γνώσης επειδή η ταχύτητα με την οποία η γνώση ενσωματώνεται στο φυσικό και το ανθρώπινο κεφάλαιο έχει αυξηθεί σημαντικά. Ορισμένοι αναλυτές ισχυρίζονται ότι οι τεχνολογικές καινοτομίες, σε λιγότερο από 20 χρόνια από σήμερα, θα έχουν συμβάλει στην αλλαγή της δομής της οικονομίας πολύ περισσότερο από ότι συνέβαλαν σωρευτικά τα προηγούμενα 200 χρόνια (Γεωργόπουλος, 2001).

Πολλοί υποστηρίζουν ότι διανύεται η αρχή μιας εποχής που μπορεί να περιγραφεί ως Πληροφορική Επανάσταση και η οποία θα αλλάξει ριζικά τη δομή της Μετα-Βιομηχανικής Κοινωνίας, οδηγώντας προς την Κοινωνία των Πληροφοριών (Information Society).

Η Πληροφορική Επανάσταση δημιουργεί μια καινούρια προοπτική αναζήτησης και διαχείρισης πληροφοριών. Δημιουργεί μια Κοινωνία Πληροφοριών όπου η πρόσβαση σε εκατοντάδες χιλιάδες πληροφορίες γίνεται ταχύτατα, με ελάχιστο

κόστος και σε ελάχιστο χρόνο από όλους τους πολίτες. Σήμερα οι πληροφορίες που παρέχονται διπλασιάζονται σε όγκο κάθε 2.5 χρόνια. Το 2020 υπολογίζεται ότι ο όγκος των πληροφοριών θα διπλασιάζεται κάθε 73 ημέρες (Καλεμικεράκη, 2003). Οι επιδράσεις αυτών των εξελίξεων είναι καθοριστικές και πολυδιάστατες για το κοινωνικό και οικονομικό γίγνεσθαι παγκοσμίως. Δημιουργούνται οι απαραίτητες προϋποθέσεις για τη μετάβαση της κοινωνίας σε μια νέα μορφή οργάνωσης και λειτουργίας που χαρακτηρίζεται από μια σειρά πρωτόγνωρων δυνατοτήτων και ευκαιριών για όλους τους πολίτες. Ίσως η Πληροφορική Επανάσταση αλλάζει δραματικά τον τρόπο που αντιλαμβάνεται κανείς τον κόσμο (Καλεμικεράκη, 2003).

Η μεγαλύτερη αλλαγή όμως διαδραματίζεται στον επιχειρηματικό κόσμο. Νέες τεχνολογίες, νέα προϊόντα και υπηρεσίες, νέες επιχειρηματικές πρακτικές προβάλουν ως σημαντικά όπλα στα χέρια των επιχειρήσεων προκειμένου να ανταποκριθούν στο νέο ανταγωνιστικό περιβάλλον του 21ου αιώνα και να επιβιώσουν (Ε.Α.Σ.Ε., 2001).

Ενδεικτικά ορισμένες τεχνολογικές εξελίξεις που σηματοδοτούν τη νέα εποχή και δείχνουν το βαθμό διείσδυσης της νέας τεχνολογίας στο σύγχρονο περιβάλλον είναι οι ακόλουθες:

- *Απόκτηση πληροφοριών*. Η κυριότερη και ευρύτερα χρησιμοποιούμενη δυνατότητα που παρέχει ο παγκόσμιος ιστός είναι η απόκτηση πληροφοριών. Δυνατότητα που παρέχεται σε κάθε πολίτη ανεξάρτητα από την ιδιότητά του, ακόμα και από γεωγραφικά απομακρυσμένες περιοχές. Οι οργανωμένες βάσεις δεδομένων και οι μηχανές αναζήτησης πληροφοριών επιτρέπουν την ανάκτηση οποιωνδήποτε πληροφοριών σε πραγματικό χρόνο, ενώ η χρήση υπερσυνδέσμων (hyperlinks) επιτρέπει τη μεταφορά του χρήστη μεταξύ λογικά συνδεδεμένων δικτυακών τόπων.

- *Ηλεκτρονική επικοινωνία*. Άλλη μία εντυπωσιακή τεχνολογική εξέλιξη είναι η επικοινωνία μέσω του ηλεκτρονικού ταχυδρομείου (electronic mail ή e-mail).

Τα ηλεκτρονικά μηνύματα που ανταλλάσσονται καθημερινά υπολογίζονται πλέον σε εκατομμύρια και αποτελούν έναν άνετο, γρήγορο και φθηνό τρόπο επικοινωνίας.

- *Ηλεκτρονικές αγορές προϊόντων και υπηρεσιών*. Η αγορά προϊόντων και υπηρεσιών από το σπίτι, είναι μία ακόμα δυνατότητα της σύγχρονης τεχνολογίας. Οι ηλεκτρονικές αγορές αποτελούν τη συνέχεια των αγορών μέσω τηλεόρασης, τηλεφώνου ή καταλόγων. Συνδυάζουν ταχύτητα, ευκολία, μειωμένο κόστος, αποφυγή μετακινήσεων και τεράστια ποικιλία προϊόντων και υπηρεσιών. Παρέχεται η δυνατότητα στο χρήστη να αγοράσει και να πληρώσει οποιοδήποτε προϊόν μέσω του ηλεκτρονικού του υπολογιστή. Επίσης παρέχεται τεράστια ποικιλία υπηρεσιών, όπως για παράδειγμα χρηματοπιστωτικές υπηρεσίες, νομικές και συμβουλευτικές υπηρεσίες, ιατρικές υπηρεσίες και ηλεκτρονικές κρατήσεις (για θεατρικές παραστάσεις, κινηματογραφικές προβολές, συνέδρια, ταξίδια κ.λ.π.)

- *Εργασία εξ αποστάσεως*. Σήμερα εκατοντάδες άνθρωποι χρησιμοποιούν τους ηλεκτρονικούς υπολογιστές ως κύριο μέσο για την εκτέλεση της καθημερινής εργασίας τους, χωρίς να βρίσκονται απαραίτητα στο φυσικό εργασιακό τους χώρο. Μπορούν λοιπόν το ίδιο καλά να εργαστούν κατά τη διάρκεια ενός ταξιδιού ή από το σπίτι τους.

- *Εκπαίδευση εξ αποστάσεως*. Η παροχή εκπαιδευτικών προγραμμάτων εξ αποστάσεως μέσω Η/Υ, παρέχει δυνατότητα εκπαίδευσης σε ανθρώπους οι οποίοι είτε βρίσκονται γεωγραφικά απομονωμένοι, είτε για οικονομικούς λόγους ή λόγους υγείας δεν έχουν τη δυνατότητα να βρίσκονται σε κάποιον φυσικό εκπαιδευτικό χώρο.

- *Ηλεκτρονική ψυχαγωγία*. Οι δυνατότητες ψυχαγωγίας μέσω ηλεκτρονικού υπολογιστή είναι πλέον ανεξάντλητες. Ξεκινούν από τα εκατοντάδες δικτυακά παιχνίδια, τις ψυχαγωγικές ιστοσελίδες και το Play Station, μέχρι τις

υπηρεσίες Διαλογικής Τηλεόρασης (Interactive T.V.), όπου ο χρήστης αλληλεπιδρά με τη συσκευή επιλέγοντας τα προγράμματα τα οποία επιθυμεί να δει, έχει τη δυνατότητα να συνδεθεί στο Διαδίκτυο κ.ά.

1.1 Επιχειρηματικές πρακτικές: Ηλεκτρονικό Εμπόριο & Ηλεκτρονικό Επιχειρείν

Το Ηλεκτρονικό Εμπόριο (e-commerce) και το Ηλεκτρονικό Επιχειρείν (e-business) είναι ίσως οι πλέον χαρακτηριστικές επιχειρηματικές πρακτικές της νέας αυτής εποχής. Η εποχή αυτή που έχει χαρακτηριστεί ως εποχή της Νέας Οικονομίας αναφέρεται στη σταδιακή ανατροπή των όρων της παραγωγής που στηρίζουν την οικονομία, και στη διαμόρφωση μιας οικονομίας που στηρίζεται στην παραγωγή επί παραγγελία.

Οποιαδήποτε μορφή εμπορικής συναλλαγής η οποία πραγματοποιείται μέσω ηλεκτρονικών δικτύων, με την υποστήριξη των τεχνολογιών των επικοινωνιών και των πληροφοριών, μπορεί να θεωρηθεί ότι εμπίπτει στις αρχές και τα χαρακτηριστικά του ηλεκτρονικού εμπορίου. Η νέα μορφή διενέργειας συναλλαγών βασίζεται στην ηλεκτρονική ανταλλαγή δεδομένων μεταξύ των ενδιαφερομένων με τη μορφή κειμένου, ήχου και εικόνας σε πραγματικό χρόνο (Αναστασιάδης, 2001). Δίδεται έτσι η δυνατότητα να εκτελούνται ηλεκτρονικές συναλλαγές από επιχείρηση προς επιχείρηση (B2B), από επιχειρήσεις προς καταναλωτές (B2C) ή από επιχειρήσεις και καταναλωτές προς το κράτος. Μία επιχείρηση, με το ηλεκτρονικό εμπόριο, μπορεί να αναζητήσει προμηθευτές πρώτων υλών, αλλά και πελάτες των προϊόντων της σε ολόκληρο τον κόσμο, εξασφαλίζοντας μια μεγάλη αγορά και συνεπώς καλύτερες τιμές. Αποτελεί λοιπόν ένα σύγχρονο και οικονομικό τρόπο πώλησης προϊόντων, με παγκόσμια απήχηση, που περικλείει όλες τις τεχνικές ενός καλού πωλητή, ο οποίος

στοχεύει στην οδήγηση των πελατών στο κατάλληλο προϊόν. Μπορεί επίσης να ανταλλάσσει ηλεκτρονικά τιμολόγια και άλλα παραστατικά με τους συνεργάτες της, μέσω του ηλεκτρονικού εμπορίου, καθώς και να υποβάλλει ηλεκτρονικά διάφορα έντυπα σε διάφορες υπηρεσίες (Slater, 1999).

Το Ηλεκτρονικό Εμπόριο (e-commerce) λοιπόν ορίζεται ως το σύνολο των επιχειρηματικών στρατηγικών που μπορούν να υποστηρίξουν συγκεκριμένους τομείς επιχειρηματικής δραστηριότητας και συγκεκριμένες επιχειρηματικές πρακτικές οι οποίες επιτρέπουν, μέσω της χρήσης νέων τεχνολογιών, τη διεκπεραίωση εμπορικών διαδικασιών με ηλεκτρονικά μέσα (Roger, 2000).

Στο σημείο αυτό είναι απαραίτητο να τονιστεί ότι ο όρος Ηλεκτρονικό Εμπόριο (e-commerce) αποτελεί εννοιολογικά μέρος του όρου Ηλεκτρονικό Επιχειρείν (e-business). Το Ηλεκτρονικό Επιχειρείν περιγράφει επιχειρήσεις η ύπαρξη και στρατηγική των οποίων στηρίζεται στο διαδίκτυο ή/και επιχειρήσεις που έχουν αναθεωρήσει-προσαρμόσει την αποστολή τους, τη στρατηγική τους και τις λειτουργίες τους με βάση τα δεδομένα του διαδικτύου. Ο πολλαπλασιασμός των διαφόρων ειδών ψηφιακών δικτύων, η σύγκλιση ψηφιακών τεχνολογιών, η δημιουργία ψηφιακού περιεχομένου και υπηρεσιών καθώς και τα νέα αναπτυσσόμενα επιχειρηματικά μοντέλα, αποτελούν πλέον το περιβάλλον του Ηλεκτρονικού Επιχειρείν.

Οι έννοιες του Ηλεκτρονικού Εμπορίου και του Ηλεκτρονικού Επιχειρείν πολλές φορές συγχέονται και είναι δύσκολο να διακριθούν μεταξύ τους με ακρίβεια. Το Ηλεκτρονικό Εμπόριο εστιάζεται περισσότερο σε μια στιγμιαία, δομημένη και περιορισμένη ενέργεια, όπως η ηλεκτρονική συναλλαγή. Ο όρος Ηλεκτρονικό Εμπόριο συνάδει με την τεχνολογία και την εφαρμογή αυτής για τη διεξαγωγή επιτυχημένων ηλεκτρονικών συναλλαγών. Προσφέρει τη δυνατότητα εκτέλεσης

πράξεων για την ανταλλαγή προϊόντων ή υπηρεσιών μεταξύ δύο ή περισσοτέρων μερών με χρήση ηλεκτρονικών υπολογιστών και δικτύων υπολογιστών. Χωρίζεται σε πολλούς επιμέρους τομείς όπως οι ηλεκτρονικοί κατάλογοι (electronic catalogues), η ηλεκτρονική τραπεζική (electronic banking ή web banking) ανάλογα με το περιεχόμενο της συναλλαγής και τον τρόπο με τον οποίο αυτή διεξάγεται και αφορά τόσο προϊόντα όσο και υπηρεσίες (Καλεμικεράκη, 2003).

Από την άλλη πλευρά, το Ηλεκτρονικό Επιχειρείν σχετίζεται περισσότερο με τη μεταμόρφωση του τρόπου λειτουργίας και των διαδικασιών μιας επιχείρησης εξαιτίας της υιοθέτησης του Ηλεκτρονικού Εμπορίου, του διαδικτύου και των δικτυακών τεχνολογιών. Αναφέρεται στην τεχνολογία ως στρατηγικό επιχειρηματικό εργαλείο το οποίο θα χρησιμοποιηθεί προκειμένου να καταστεί ανταγωνιστική και βιώσιμη μία επιχείρηση. Στα πλαίσια αυτά, το Ηλεκτρονικό Επιχειρείν προσπαθεί να οριοθετήσει το ρόλο της επιχείρησης μέσα στο εξωτερικό της περιβάλλον (πελάτες, προμηθευτές, κλάδος κ.λ.π.) μετά την υιοθέτηση της τεχνολογίας.

Συμπερασματικά, η έννοια του Ηλεκτρονικού Εμπορίου περιλαμβάνει πολλές διαφορετικές δραστηριότητες όπως:

- Ηλεκτρονική εμπορία αγαθών και υπηρεσιών.
- Παράδοση ψηφιακού περιεχομένου (άυλων αγαθών).
- Ηλεκτρονική αγοραπωλησία μετοχών.
- Εμπορικές δημοπρασίες.
- Συλλογικές εργασίες σχεδίασης και τεχνικές μελέτες.
- Ενημέρωση από πηγές σε απευθείας σύνδεση.
- Κρατικές προμήθειες.
- Πωλήσεις απευθείας στον καταναλωτή και μετα-αγοραστική εξυπηρέτηση.

Ενώ είναι ξεκάθαρο ότι ανοίγονται νέοι τρόποι επικοινωνίας με πλήθος πλεονεκτημάτων, όπως γρηγορότερη ανταπόκριση, μείωση του κόστους, παροχή εναλλακτικών καναλιών για προσφορά υπηρεσιών, υπάρχει παράλληλα ένας αριθμός επιχειρηματικών κινδύνων που πρέπει να προβλεφθεί, ώστε οι επιχειρήσεις να μη φοβηθούν να υποστηρίξουν την καινοτομία και έτσι να μη χάσουν την ευκαιρία που προσφέρει το Ηλεκτρονικό Εμπόριο και γενικότερα το Ηλεκτρονικό Επιχειρείν (Πασχόπουλος, 2000).

Μία επιχείρηση η οποία δραστηριοποιείται ηλεκτρονικά θα πρέπει να έχει υπόψη ότι οφείλει να είναι εξοικειωμένη με τη διαχείριση ηλεκτρονικών κρίσεων (e-risk management) και τον η-επιχειρηματικό κίνδυνο, δηλαδή τον κίνδυνο από την υλοποίηση της στρατηγικής του ηλεκτρονικού εμπορίου. Λέγοντας διαχείριση ηλεκτρονικών κρίσεων εννοεί κανείς ένα σύνολο ενεργειών από μια εξειδικευμένη ομάδα που στόχο έχουν την ελαχιστοποίηση της επίδρασης ενός απροσδόκητου γεγονότος στη λειτουργία της επιχείρησης (Spillan, 2003). Το γεγονός αυτό είναι κρίση (κίνδυνος) που αφορά είτε στην ασφάλεια της τεχνολογίας των πληροφοριών (information technology), είτε σε οποιαδήποτε άλλη συνιστώσα όπως για παράδειγμα στις επιχειρηματικές διαδικασίες που συντελούν στην παραγωγική λειτουργία της επιχείρησης.

Συνάγεται λοιπόν από τα προηγούμενα ότι η ασφάλεια των πληροφοριών αποτελεί έννοια η οποία συμπεριλαμβάνεται στην ευρύτερη έννοια της διαχείρισης του επιχειρηματικού κινδύνου στο πλαίσιο του η-επιχειρείν[1].

Η παρούσα διπλωματική εργασία πραγματεύεται την αποτελεσματική διαχείριση του η-επιχειρηματικού κινδύνου (e-risk) και ειδικότερα επιχειρείται η παρουσίαση

[1] http://www.go-online.gr/ebusiness/specials

μιας ανάλυσης ρίσκου σε όλες εκείνες τις συνιστώσες που απαρτίζουν το επιχειρηματικό περιβάλλον.

Στο δεύτερο κεφάλαιο δίνεται έμφαση στους κινδύνους που απειλούν την ασφάλεια των πληροφοριών, μιας και αποτελούν σύγχρονο αγαθό που εύκολα μετατρέπεται σε αξία, καθώς είναι και μια από τις σημαντικότερες υποκατηγορίες της Διαχείρισης Κρίσεων. Επίσης, τονίζεται η ανάγκη για ασφάλεια στο ηλεκτρονικό εμπόριο και εξετάζονται διεξοδικά οι κίνδυνοι από την υιοθέτηση της στρατηγικής του ηλεκτρονικού εμπορίου με τους τρόπους αντιμετώπισής τους.

Στο τρίτο κεφάλαιο γίνεται αναφορά γενικά σε διαχείριση κρίσεων από τις επιχειρήσεις, σε ομάδες που είναι υπεύθυνες για την αντιμετώπιση αυτών των κρίσεων καθώς επίσης τονίζονται οι παραλείψεις που οδηγούν στην εμφάνιση της κρίσης. Στη συνέχεια παρουσιάζονται αναλυτικά τα στάδια της διαχείρισης κρίσεων που είναι η αναγνώριση του κινδύνου, η ανάλυση του κινδύνου (ποσοτική και ποιοτική) η απόκριση σε κινδύνους, η παρακολούθηση και ο έλεγχος. Στην ποσοτική ανάλυση του κινδύνου προσδιορίζονται σημαντικά μεγέθη όπως η στιγμιαία αναμενόμενη απώλεια, η ετήσια αναμενόμενη απώλεια, η απόδοση της επένδυσης σε σχέση με την ασφάλεια, το κόστος του ελέγχου και το ετήσιο ποσοστό εμφάνισης του κινδύνου. Αντίθετα η ποιοτική ανάλυση του κινδύνου δεν επιμένει σε αυστηρά χρηματοοικονομικούς υπολογισμούς. Σε ό,τι αφορά στην απόκριση σε κινδύνους αναλύονται στρατηγικές οι οποίες είναι συναφείς με τη φύση των κινδύνων. Οι στρατηγικές αυτές είναι για αρνητικούς κινδύνους ή απειλές, για θετικούς κινδύνους ή ευκαιρίες, για απειλές και ευκαιρίες και για έκτακτη απόκριση. Τέλος, δίνεται έμφαση στο ρόλο της ασφάλισης και των ασφαλιστικών εταιριών απέναντι στους κινδύνους του ηλεκτρονικού εμπορίου σε χώρες του εξωτερικού και στην Ελλάδα.

Στο τέταρτο κεφάλαιο, που ξεκινά και το δεύτερο μέρος της παρούσας εργασίας, γίνεται αρχικά σύντομη επισκόπηση της παρουσίας του ηλεκτρονικού εμπορίου στην Ελλάδα. Σχολιάζονται έρευνες που έχουν πραγματοποιηθεί στο παρελθόν σχετικά με την ύπαρξη και ασφάλεια του ηλεκτρονικού εμπορίου στην Ελλάδα. Δίνεται ιδιαίτερη βαρύτητα στα εμπόδια του ηλεκτρονικού εμπορίου στην Ευρώπη και ειδικότερα στην Ελλάδα καθώς επίσης αναλύονται και οι λόγοι που συντρέχουν για τη δημιουργία ηλεκτρονικού καταστήματος. Ακόμα, σημειώνονται και τα συστατικά επιτυχίας μιας ιστοσελίδας σε συνδυασμό με τις επιχειρηματικές στρατηγικές του Porter και τις δυνατότητες που προσφέρει το Διαδίκτυο

Τέλος, στο πέμπτο κεφάλαιο μελετάται η περίπτωση του ηλεκτρονικού καταστήματος papasotiriou.gr. Αναλύεται ο κίνδυνος μέσω της αναγνώρισης των κρίσιμων περιουσιακών του στοιχείων, της αναγνώρισης των απειλών και της ανάλυσης των αδυναμιών. Χρησιμοποιείται ο τύπος της ποσοτικής ανάλυσης του κινδύνου και προσδιορίζονται τα σχετικά μεγέθη. Έπειτα δίνεται έμφαση στον κατεξοχήν κίνδυνο που ενυπάρχει για το papasotiriou.gr και στον έλεγχό του από τη διοίκηση της εταιρίας καθώς επίσης σχολιάζεται και το σχέδιο ασφάλειας που εφαρμόζεται. Μέσα στα πλαίσια του σχεδίου ασφάλειας, αναφέρονται τα αντίμετρα (countermeasures) που χρησιμοποιούνται, τα οποία είναι μέτρα προστασίας απέναντι σε τεχνικές κυρίως απειλές και η συγκεκριμένη πολιτική ασφάλειας. Επιπλέον, προτείνεται ένα σχέδιο επιχειρησιακής συνέχειας που στόχο έχει την αποτροπή των παρεμβολών στις δραστηριότητες της ηλεκτρονικής επιχείρησης και την προστασία κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών.

.

ΚΕΦΑΛΑΙΟ 2ο : ΚΙΝΔΥΝΟΙ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ & ΤΗΣ ΥΛΟΠΟΙΗΣΗΣ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Μία επιχείρηση η οποία δραστηριοποιείται ηλεκτρονικά θα πρέπει να μπορεί να αντιμετωπίζει κρίσεις που αφορούν τόσο στην ασφάλεια των πληροφοριών της όσο και κινδύνους που σχετίζονται με την υλοποίηση της στρατηγικής του ηλεκτρονικού εμπορίου. Οι κρίσεις στην ασφάλεια των πληροφοριών δεν είναι τίποτα άλλο από απειλές και επιθέσεις στα πληροφοριακά συστήματα της επιχείρησης οι οποίες έχουν αντίκτυπο στην παραγωγική της λειτουργία. Οι κίνδυνοι που σχετίζονται με την υλοποίηση της στρατηγικής του ηλεκτρονικού εμπορίου αφορούν τέσσερις κατηγορίες και είναι i) κίνδυνοι από τον ανταγωνισμό (competitive risks), δηλαδή κίνδυνοι που σχετίζονται τόσο με τους ίδιους τους ανταγωνιστές, όσο και με πελάτες και προμηθευτές εξαιτίας της αύξησης της δύναμής τους η οποία απορρέει από την εφαρμογή του ηλεκτρονικού εμπορίου σε βάρος βέβαια της επιχείρησης που πραγματοποιεί την καινοτομία, ii) κίνδυνοι αλλαγής (transition risks) οι οποίοι προκύπτουν από τον αργό ρυθμό της οργανωσιακής αλλαγής της επιχείρησης, από το μετασχηματισμό της υπάρχουσας γραμμής προϊόντων, iii) κίνδυνοι που επηρεάζουν τους πελάτες (customer-induced risks) και αφορούν σε συνιστώσες που έχουν σχέση με τη διατήρηση της εμπιστοσύνης τους και iv) κίνδυνοι σε σχέση με τους επιχειρηματικούς εταίρους (business partner risks) αφού αναπτύσσονται σχέσεις εξάρτησης τόσο με την αυξανόμενη χρήση υπηρεσιών που ανατίθενται σε εξωτερικούς συνεργάτες (outsourcing), όσο και με την εφαρμογή διαδικασιών διανομής χωρίς καθυστερήσεις (just-in-time).

2.1 Ασφάλεια πληροφοριών (Information Security)

Η ραγδαία ανάπτυξη των πληροφοριακών συστημάτων συνέβαλλε στην απελευθέρωση της πληροφορίας από τα χρονικά και γεωγραφικά της δεσμά, καθιστώντας την το πολυτιμότερο ίσως περιουσιακό στοιχείο της επιχείρησης. Η ανάπτυξη ενιαίων πληροφοριακών περιβαλλόντων με δυνατότητα συνεργατικής διαχείρισης, ανέδειξε το πληροφοριακό σύστημα ως το κέντρο αυτοματοποίησης της επιχειρηματικής διαδικασίας και της υποστήριξης σύνθετων αποφάσεων σε όλα τα επίπεδα διοικητικής διάρθρωσης (Αναστασιάδης, 2001).

Η επέκταση της επιχειρηματικής δραστηριότητας στον κόσμο της εικονικής πραγματικότητας, αποτελεί απτή καθημερινότητα για χιλιάδες μικρές και μεγάλες επιχειρήσεις σε ολόκληρο τον κόσμο. Στις λεωφόρους των πληροφοριών, εκατομμύρια καταναλωτές συνωστίζονται στις ηλεκτρονικές βιτρίνες των καταστημάτων αναζητώντας προϊόντα και υπηρεσίες προκειμένου να ικανοποιήσουν τις καταναλωτικές τους ανάγκες. Μια ιδιότυπη, χωρίς ιστορικό προηγούμενο αγορά, η οποία λειτουργεί 24ώρες το 24ωρο, 365 ημέρες το χρόνο, απαλλαγμένη από γεωγραφικούς και χρονικούς περιορισμούς τείνει να αντικαταστήσει την παραδοσιακή αγορά, έτσι όπως ήταν γνωστή αιώνες.

Οι επιθέσεις στα πληροφοριακά συστήματα της επιχείρησης δεν απειλούν τίποτα άλλο από την ασφάλεια των πληροφοριών. Η πληροφορία (information) είναι ένας πόρος, ένα περιουσιακό στοιχείο, που όπως και όλα τα άλλα περιουσιακά στοιχεία έχει αξία για μια επιχείρηση και κατά συνέπεια χρειάζεται επαρκή προστασία (Finne, 2000). Σύμφωνα με τον Ronald Reagan (πρώην πρόεδρο των Η.Π.Α.) η πληροφορία είναι το οξυγόνο της νέας εποχής. Χαρακτηριστική για την αξία των πληροφοριών

είναι η έρευνα του Brookings Institute[2] σε 500 επιχειρήσεις που δείχνει πως από το τέλος της δεκαετίας του 1990, το 85% κατά μέσο όρο, της αγοραίας αξίας των επιχειρήσεων βασιζόταν σε άυλα στοιχεία όπως φήμη, επωνυμία, στοιχεία που περιέχουν πληροφορίες. Το υπόλοιπο 15% της αξίας αφορούσε κεφαλαιουχικά στοιχεία όπως κτίρια, οχήματα (Lev, 2001). Γενικά, η ασφάλεια των πληροφοριών στόχο έχει την προστασία των συμφερόντων εκείνων των ατόμων που βασίζονται στις πληροφορίες (Horton et al., 2000). Η άποψη αυτή ενισχύεται από την Top Technologies Survey του AICPA[3] (2005) που έδειξε ότι κύρια ανησυχία της Αμερικής σε θέματα τεχνολογίας για τρία συνεχόμενα έτη ήταν η ασφάλεια των πληροφοριών. Ειδικότερα, η ασφάλεια των πληροφοριών (information security) τις προστατεύει από ένα σύνολο απειλών, ώστε να διασφαλίσει την επιχειρησιακή συνέχεια (business continuity), να ελαχιστοποιήσει τη ζημιά και να μεγιστοποιήσει τις επιχειρηματικές ευκαιρίες και την απόδοση (return on investment-ROI).

Η ασφάλεια των πληροφοριών χαρακτηρίζεται ως η διαφύλαξη των ακόλουθων ιδιοτήτων-απαιτήσεων:

- Εμπιστευτικότητα (confidentiality): Διασφάλιση της προσπελασιμότητας της πληροφορίας μόνον από όσους έχουν τα απαραίτητα δικαιώματα.
- Ακεραιότητα (integrity): Διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας αυτής (Boritz, 2004).
- Διαθεσιμότητα (availability): Διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται.

[2] http://www.icgrowth.com/resources/documents/Brookings.Lev.Intangibles.01.02.20.pdf
[3] http://www.aicpa.org/download/news/2005_0103.pdf

Η ασφάλεια των πληροφοριών επιτυγχάνεται με την υλοποίηση των κατάλληλων μηχανισμών ελέγχου, οι οποίοι μπορεί να είναι πολιτικές, πρακτικές, διαδικασίες, οργανωτικές δομές και λειτουργίες λογισμικού (Lindberg, 2005). Αυτοί οι μηχανισμοί ελέγχου είναι απαραίτητοι προκειμένου να διασφαλιστεί ότι ικανοποιούνται οι απαιτήσεις ασφάλειας της επιχείρησης, οι οποίες είναι ιδιαίτερα σημαντικές για τη διατήρηση κάποιου ανταγωνιστικού πλεονεκτήματος, τη συμμόρφωση με τους νόμους, την εταιρική εικόνα, τα κέρδη και τα έσοδα μιας επιχείρησης.

Οι επιχειρήσεις και τα πληροφοριακά τους συστήματα συνεχώς αντιμετωπίζουν απειλές της ασφάλειάς τους από ένα μεγάλο εύρος διαφορετικών πηγών όπως ηλεκτρονική απάτη, βιομηχανική κατασκοπεία, βανδαλισμός, φυσικά φαινόμενα κ.ά. Επιπλέον, επιθέσεις με ιούς (viruses), hacking, cracking και επιθέσεις τύπου άρνησης παροχής υπηρεσιών (denial of service) έχουν πλέον γίνει συνήθεις και όλο πιο πολύπλοκες στην αντιμετώπισή τους. Καθώς οι επιχειρήσεις βασίζονται όλο και περισσότερο στα πληροφοριακά τους συστήματα, οι απειλές προς αυτά επηρεάζουν σημαντικά τις λειτουργίες των ίδιων των επιχειρήσεων.

Σε εκατοντάδες εκατομμύρια δολάρια ανήλθαν τα προηγούμενα χρόνια, οι ζημιές επιχειρήσεων, τραπεζών και δημοσίου εξαιτίας του ηλεκτρονικού εγκλήματος. Τα στοιχεία αυτά βέβαια δε συγκεκριμενοποιούνται ποτέ γιατί καμία εταιρία δε θα ήθελε να διατυμπανίσει ότι το σύστημα εμπορικών συναλλαγών που έχει εγκαταστήσει στο διαδίκτυο δεν είναι αξιόπιστο και ασφαλές. Σύμφωνα με τον Allan Paller, πρόεδρο του SANS Institute for Internet Security, κάθε μέρα εγκαθίστανται στο διαδίκτυο περίπου 7.000 έως 10.000 υπολογιστές με γνωστές και σοβαρές ευαισθησίες όσον αφορά στην ασφάλεια. Επίσης, 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα, τρέχουν

περίπου 2.000 έως 3.000 προγράμματα, τα οποία ανιχνεύουν τρωτούς υπολογιστές ώστε να σχεδιαστούν μελλοντικές ηλεκτρονικές εισβολές και επιθέσεις.

Στην αρχική σχεδίαση πολλών πληροφοριακών συστημάτων δεν έχουν συμπεριληφθεί χαρακτηριστικά ασφαλείας. Η ασφάλεια που προσφέρουν είναι ελάχιστη και πρέπει να συμπληρωθεί από κατάλληλη διαχείριση και υλοποίηση επιμέρους διαδικασιών (Coles & Moulton, 2003). Η επιλογή των κατάλληλων μηχανισμών ελέγχου, προϋποθέτει προσεκτικό και λεπτομερή σχεδιασμό. Η ασφάλεια των πληροφοριών απαιτεί τη συμμετοχή όλων των εργαζομένων της επιχείρησης (Conner and Coviello, 2004). Επιπλέον, μπορεί να χρειάζεται και η συμμετοχή των προμηθευτών, των πελατών ή ακόμα και η συνδρομή εξωτερικών εμπειρογνωμόνων συνεργατών εξειδικευμένων σε θέματα ασφάλειας. Οι μηχανισμοί ελέγχου ενσωματώνονται με το μικρότερο κόστος και αποδίδουν τα μέγιστα όταν περιλαμβάνονται στα αρχικά στάδια καταγραφής των απαιτήσεων και του σχεδιασμού.

2.2 Η ανάγκη για ασφάλεια στο ηλεκτρονικό εμπόριο

Μια απλή περιήγηση στον κυβερνοχώρο από έναν προσωπικό υπολογιστή δεν είναι και τόσο απλή, ούτε τόσο μοναχική υπόθεση όσο αρχικά φαίνεται. Η αλήθεια είναι ότι κατά τη διάρκεια μιας περιπλάνησης στις σελίδες του παγκόσμιου ιστού, ο χρήστης αφήνει, συνήθως εν αγνοία του, κάποια στοιχεία που αφορούν στην ταυτότητά του, στις προτιμήσεις του και στην προσωπικότητά του. Τέτοια στοιχεία μπορεί να είναι ο αριθμός μιας πιστωτικής κάρτας, οι μουσικές προτιμήσεις ή τα ενδιαφέροντα του χρήστη. Αυτό είναι εφικτό μέσω κάποιων πολύ μικρών τμημάτων κώδικα, τα επονομαζόμενα cookies, που εγκαθιστούν οι απομακρυσμένοι δικτυακοί

τόποι στο σκληρό δίσκο και τα οποία λειτουργούν σαν κατάσκοποι, συλλέγοντας και στέλνοντας στη συγκεκριμένη ιστοσελίδα πληροφορίες για το χρήστη.

Μια επίσκεψη στην ιστοσελίδα ενός βιβλιοπωλείου για παράδειγμα, στην οποία σε μια προηγούμενη επίσκεψή του ο χρήστης είχε εισάγει τα στοιχεία του, μπορεί να του επιφυλάσσει μία έκπληξη, όταν η αρχική σελίδα τον καλωσορίσει με το όνομά του και του προτείνει νέα βιβλία που εμπίπτουν στις προτιμήσεις του. Όλα αυτά φαίνονται ενδεχομένως ακίνδυνα και βολικά αλλά δεν είναι πάντοτε έτσι. Κανείς δεν μπορεί να γνωρίζει πώς διαχειρίζονται οι υπεύθυνοι της κάθε ιστοσελίδας τα στοιχεία που αφορούν τον κάθε χρήστη. Συνήθως, τα στοιχεία αυτά είναι ακίνδυνα μέχρι να συνδυαστούν με άλλα. Από τα στοιχεία της προσωπικότητάς του που αφήνει ο κάθε χρήστης στις διάφορες ιστοσελίδες, μπορεί σχετικά εύκολα να χτιστεί μια πελώρια βάση δεδομένων, ένας φάκελος για κάθε χρήστη. Ο φάκελος αυτός, θα μπορεί πλέον να διακινείται ελεύθερα και αδιαφανώς, και θα έχουν πρόσβαση σε αυτόν κυβερνήσεις, υπηρεσίες ασφαλείας, οργανισμοί, διαφημιστές κ.ο.κ. Αν παρατηρήσει κανείς ότι οι τυχαίες διαφημίσεις που βλέπει κατά την περιπλάνηση του στο web σχετίζονται σχεδόν πάντα με τους προηγούμενους σταθμούς του, αντιλαμβάνεται ότι όλα αυτά δεν είναι επιστημονική φαντασία.

Τα προβλήματα όμως δε σταματούν εκεί. Η ηλεκτρονική αλληλογραφία, το γνωστό e-mail, μπορεί να είναι ένας εντυπωσιακά γρήγορος και σχετικά αξιόπιστος τρόπος επικοινωνίας, δεν παρέχει όμως μεγαλύτερη προστασία του απορρήτου της αλληλογραφίας από μια καρτ-ποστάλ. Και μάλλον δε θα ήταν πολλοί αυτοί που θα έστελναν τον αριθμό της πιστωτικής τους κάρτας ή απόρρητες επαγγελματικές πληροφορίες σε καρτ-ποστάλ! Το e-mail μπορεί να διαβαστεί από παροχείς υπηρεσιών Internet, προϊσταμένους και γενικότερα οποιονδήποτε διαθέτει κάποιες τεχνικές γνώσεις, εξουσία ή επαφές με αναξιόπιστους διαχειριστές συστημάτων.

Η εικόνα που παρουσιάζεται παραπέμπει δυστυχώς στο «Μεγάλο Αδερφό» του Όργουελ και δεν αποτελεί πλέον επιστημονική φαντασία. Είναι προφανές λοιπόν ότι πρέπει να ληφθούν αξιόπιστα μέτρα για την προστασία της ιδιωτικής ζωής των χρηστών και των εμπορικών συναλλαγών στην ψηφιακή κοινωνία. Δεν είναι τυχαίο που ο Bill Gates, σε μία επιστολή του προς τους υπαλλήλους του, τόνισε ότι όταν βρίσκονται μπροστά στο δίλημμα της προσθήκης καινοτομικών χαρακτηριστικών στα προϊόντα της Microsoft, ή στην επίλυση του προβλήματος της ασφάλειας, πρέπει πάντα να επιλέγουν το τελευταίο.

2.3 Συνήθεις κίνδυνοι πληροφοριακών συστημάτων

Τα προβλήματα στο ηλεκτρονικό εμπόριο αφορούν κυρίως κινδύνους που απειλούν τα μηχανογραφημένα συστήματα πληροφοριών όπως: (Laudon, 2002)

- Η βλάβη του υλικού
- Η βλάβη του λογισμικού
- Ενέργειες του προσωπικού
- Μη εξουσιοδοτημένη διείσδυση
- Κλοπή δεδομένων, υπηρεσιών εξοπλισμού
- Φωτιά
- Προβλήματα ηλεκτρικής παροχής
- Σφάλματα των χρηστών
- Αλλαγές του προγράμματος
- Προβλήματα τηλεπικοινωνιών

Τα παραπάνω προβλήματα περιορίζουν την ικανότητα της επιχείρησης να διεξαγάγει με ασφάλεια τις κύριες εμπορικές διαδικασίες, συμπεριλαμβανομένης της επικοινωνίας με τους προμηθευτές, τους διανομείς και τους πελάτες. Επιπλέον η

δημοσιοποίηση απόρρητων εταιρικών πληροφοριών, σχεδίων ή άλλων εμπιστευτικών εμπορικών στοιχείων, με τη μη εξουσιοδοτημένη εσωτερική ή εξωτερική πρόσβαση σε εφαρμογές ή δεδομένα της επιχείρησης καθώς και η αποτυχία διεξαγωγής online συναλλαγών εντείνουν την κατάσταση. Επίσης τα παραπάνω προβλήματα δηλώνουν την αποτυχία των εσωτερικών διαδικασιών της επιχείρησης να ελέγξουν την ασφάλεια δικτύωσης, με αποτέλεσμα τη μη διαθεσιμότητα εταιρικών δικτύων ή εφαρμογών, και την πιθανή εισβολή και ζημιά των ευαίσθητων πληροφοριών από επίδοξους εισβολείς.

Συνεπώς η φήμη και το γόητρο της επιχείρησης πλήττονται ανεπανόρθωτα αν δεν αξιολογηθεί σωστά ο κίνδυνος από τους εισβολείς και δε ληφθούν τα κατάλληλα μέτρα προστασίας. Η χρήση της ταυτότητας της εταιρίας από κάποιον τρίτο στο διαδίκτυο μπορεί να βλάψει σοβαρά την επιχείρηση και να δυσφημιστεί εξαιτίας των πράξεών του. Ταυτόχρονα το γεγονός ότι κλάπηκαν ή παραποιήθηκαν δεδομένα, χτυπήθηκε η ιστοσελίδα της εταιρίας είναι λόγοι για να μειωθεί σημαντικά το κύρος και η αξιοπιστία της εταιρίας τόσο ως προς τους πελάτες της όσο και απέναντι στις συνεργαζόμενες με αυτή επιχειρήσεις.

Σύμφωνα με έρευνα που διεξήχθη από το Computer Emergency Response Team (CERT)[4] οι επιθέσεις στον κυβερνοχώρο βρίσκονται σε έξαρση. Το 2003, ο αριθμός των επιθέσεων οι οποίες αναφέρθηκαν ανήλθαν στις 138.000, σε σχέση με τις 82.000 που σημειώθηκαν το 2002. Επίσης, σύμφωνα με άλλη έρευνα που πραγματοποιήθηκε τον Απρίλιο του 2004 (CSO Magazine 2004)[5] αναφέρθηκε ότι το 70% των επιχειρήσεων που συμμετείχαν βίωσαν τουλάχιστον μία επίθεση, ενώ το 43% σημείωσε ότι ο αριθμός των επιθέσεων είχε αυξηθεί σε σχέση με το προηγούμενο

[4] http://www.cert.org/stats/cert_stats.html
[5] http://www.cve.mitre.org

έτος. Το συνολικό κόστος αυτών των επιθέσεων ήταν περίπου $666 εκατομμύρια. Αυτοί που συμμετείχαν στην παραπάνω έρευνα του CSO Magazine σημείωσαν επίσης ότι χρησιμοποίησαν πολλές από τις δυνατότητες που τους παρέχει η τεχνολογία για να αντεπεξέλθουν στις παραπάνω επιθέσεις όπως firewalls[6], φυσικά συστήματα ασφάλειας κ.ά.

2.4 Τύποι απειλών και επιθέσεων

Οι ειδικοί σε θέματα ασφάλειας διακρίνουν δύο τύπους επιθέσεων, τους τεχνικούς (technical) και τους μη τεχνικούς (nontechnical). Τεχνικές είναι οι επιθέσεις εκείνες που για να πραγματοποιηθούν απαιτούν καλή γνώση λογισμικού και των συστημάτων. Μη τεχνικές είναι οι επιθέσεις εκείνες που βασίζονται στην ψυχολογία του χρήστη και καταφέρνουν να του αποσπάσουν σημαντικές πληροφορίες.

2.4.1 Επίδοξοι εισβολείς – τεχνικές επιθέσεις

Οι εν δυνάμει εχθροί ενός πληροφοριακού συστήματος κατηγοριοποιούνται στις ακόλουθες ομάδες:

- Hackers-Crackers[7]

Είναι οι αναρχικοί του κυβερνοχώρου που εισβάλουν στα πληροφοριακά συστήματα είτε για διασκέδαση, είτε για να καταστρέψουν, είτε για επίδειξη. Τους ελκύουν όλοι οι απαγορευμένοι χώροι. Εκμεταλλεύονται τα κενά ασφαλείας του λειτουργικού συστήματος και του περιηγητή (browser) και αποκτούν εύκολα πρόσβαση σε όλα τα αρχεία του υπολογιστή, συγκεντρώνοντας μεγάλο αριθμό πληροφοριών σχετικά με τις δικτυακές συνήθειες αλλά και όποια ευαίσθητα

[6] Σύστημα που χρησιμοποιείται για να ενισχύσει τον έλεγχο πρόσβασης & την ασφάλεια ενός δικτύου.
[7] http://www.hackerwatch.org/

προσωπικά δεδομένα συνηθίζει να διατηρεί κάποιος στον υπολογιστή του καθώς επίσης προκαλούν άρνηση εξυπηρέτησης του συστήματος σε έγκυρους χρήστες. Το 1999 ο Mitre Corporation και 15 άλλοι οργανισμοί που σχετίζονται με θέματα ασφάλειας ξεκίνησαν να απαριθμούν όλες τις γνωστές αδυναμίες (vulnerabilities) ασφάλειας των λειτουργικών συστημάτων. Ο αριθμός τους από 320 που ήταν το 1999 είχε αυξηθεί σε πάνω από 3.000 το 2004. Πολλές εταιρίες συνηθίζουν να προσλαμβάνουν άτομα που εισέβαλαν στα συστήματά τους με τη λογική καλύτερα να δουλεύουν για αυτούς παρά εναντίον τους. Άλλωστε αυτοί που παραβίασαν ένα σύστημα ασφαλείας ξέρουν καλύτερα από τον καθένα που μειονεκτεί και μπορούν να το βελτιώσουν.

Σύμφωνα με το νόμο περί τρομοκρατίας[8] που έχει ψηφιστεί από τη βρετανική κυβέρνηση, οι crackers στη Μ. Βρετανία θεωρούνται τρομοκράτες. Ο συγκεκριμένος νόμος βάλλει κατά αυτών που πραγματοποιούν ηλεκτρονικές επιθέσεις σε κυβερνητικά και άλλα δίκτυα έχοντας ιδεολογικά κίνητρα. Ο νόμος αυτός διευρύνει την έννοια της τρομοκρατίας, έτσι ώστε αυτή να συμπεριλαμβάνει τους crackers που πραγματοποιούν επιθέσεις σε κυβερνητικά συστήματα υπολογιστών ή δικτυακούς τόπους επιχειρήσεων. Στο εξής, όποιος προσπαθεί να παρακωλύσει τη λειτουργία ενός ηλεκτρονικού συστήματος με πρόθεση να απειλήσει και να επηρεάσει την κυβέρνηση ή το κοινό, για να προωθήσει έναν πολιτικό, θρησκευτικό ή ιδεολογικό στόχο, θεωρείται τρομοκράτης. Οι υπέρμαχοι της νομοθεσίας, πάντως, υποστηρίζουν ότι αυτή αποτελεί ένα σημαντικό βήμα για την προάσπιση των δικαιωμάτων των πολιτών απέναντι σε επιθέσεις κακόβουλων crackers.

Κατά τη διάρκεια του 2005 επιθέσεις δέχτηκαν οι Barclays Bank, Bank of America, The Marriot, CardSystems Solutions (Hunter, 2006).

[8] http://www.cybercrime.gov/

- Κλέφτες

Είναι όλοι αυτοί που εισβάλουν σε ένα σύστημα έχοντας ως στόχο την κλοπή δεδομένων που θα τους αποφέρει οικονομικά οφέλη είτε χρησιμοποιώντας τα, είτε πουλώντας τα.

- Ανταγωνιστές

Ένας ανταγωνιστής συνήθως, δεν εισβάλει για να κλέψει χρήματα, ούτε για να καταστρέψει αλλά για να αποκτήσει πληροφορίες που είναι σημαντικές προκειμένου να κυριαρχήσει στον επιχειρηματικό στίβο.

- Εσωτερικοί εχθροί

Δυσαρεστημένοι, αποξενωμένοι και άπληστοι υπάλληλοι μπορούν να αποτελέσουν ένα ιδιαίτερα σοβαρό εκ των έσω κίνδυνο για τις βάσεις δεδομένων μιας εταιρίας.

- Ατυχήματα

Πολλές καταστροφές δεν είναι αποτέλεσμα πρόθεσης ούτε οργανωμένης επίθεσης, αλλά πρόκειται για ατυχήματα ή λάθη από αφέλεια. Δεν είναι καθόλου ασυνήθιστο γεγονός εταιρίες να καταστρέφουν από μόνες τους τις βάσεις δεδομένων τους, ή να τις απελευθερώνουν στο Διαδίκτυο κατά λάθος.

2.4.2 Το τρίπτυχο του τρόμου: ιοί, δούρειοι ίπποι, σκουλήκια (viruses, trojans, worms)

- Ιοί[9]

Αναμφίβολα το Διαδίκτυο έδωσε μεγάλη ώθηση στην εξάπλωση των πάσης φύσεως ιών και....μικροβίων. Στις μέρες της Amiga και των PC XT ο μόνος τρόπος για να κολλήσει κάποιος ένα ειδεχθές πρόγραμμα ήταν να χρησιμοποιήσει

[9] http://www.vil.nai.com

μολυσμένες δισκέτες, κυρίως με παιχνίδια. Τότε η μόλυνση με έναν ιό ήταν κάτι το συνηθισμένο μέχρι και γοητευτικό (το γνωστό μπαλάκι που έκανε βόλτες στην οθόνη). Βέβαια, το αστείο τελείωνε με την οδυνηρή ανακάλυψη ότι οι δισκέτες ή ο σκληρός δίσκος ήταν άχρηστα. Η κατάσταση άλλαξε δραματικά με την είσοδο του Διαδικτύου, και συγκεκριμένα με το ηλεκτρονικό ταχυδρομείο (e-mail). Το ηλεκτρονικό ταχυδρομείο εκμηδένισε τις αποστάσεις και έκανε την επικοινωνία ανάμεσα στους εταιρικούς και τους οικιακούς χρήστες πολύ εύκολη και ευχάριστη υπόθεση. Το ηλεκτρονικό ταχυδρομείο (e-mail) όμως είναι προς το παρόν το κυριότερο μέσο για τη μετάδοση κάθε είδους ιών και σκουληκιών, μετατρέποντάς τα σε πραγματική επιδημία λόγω της μεγάλης ταχύτητας με την οποία εξαπλώνονται. Χαρακτηριστικοί είναι ο ιοί MyDoom.A που εμφανίστηκαν στις αρχές του 2004 μέσω του ηλεκτρονικού ταχυδρομείου και μόλυναν χιλιάδες υπολογιστές σε ολόκληρο τον κόσμο (Fisher, 2004). Στη συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν κάποιος δεν τρέξει τα εκτελέσιμα αρχεία / script που τα μεταφέρουν. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου word, παραπλανώντας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Σύμφωνα με έρευνα του Computer Security Association (ICSA 2004)[10] 90% των επιχειρήσεων που ερωτήθηκαν είχαν βιώσει επίθεση κακόβουλου λογισμικού. Το κόστος της αποκατάστασης ανήλθε στα $100.000 για κάθε επιχείρηση.

Παίρνοντας λοιπόν τα πράγματα από την αρχή όταν αναφέρεται κάποιος σε ιούς, εννοεί ένα κακόβουλο λογισμικό (malicious software=malware) με μερικές γραμμές κώδικα που εισέρχονται στον υπολογιστή με τη μορφή συνημμένου αρχείου ηλεκτρονικού ταχυδρομείου (e-mail attachment) ή ενός κατεβασμένου αρχείου από

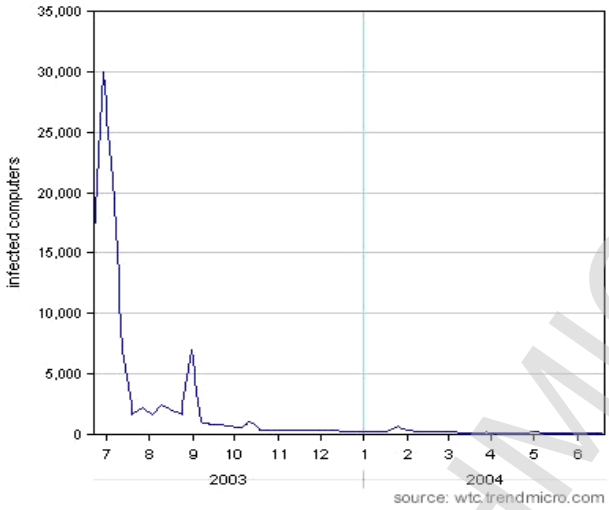
[10] http://www.trusecure.com/company/press/pr_20040322.shtml

το Διαδίκτυο. Οι ιοί είναι προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκριση του χρήστη και να μολύνουν άλλα αρχεία. Είναι μικρά κομμάτια ηλεκτρονικού κώδικα, που έχουν τη δυνατότητα να αντιγράφουν και να εισάγουν τον εαυτό τους σε ένα εκτελέσιμο πρόγραμμα, αρχείο, δισκέτα ή μέρος σκληρού δίσκου με την παρεμβολή βέβαια του ανθρώπινου παράγοντα. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο διαδίκτυο. Υπάρχουν αρκετά είδη ιών: i) αυτοί που προσβάλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου (boot sector viruses) και είναι σχετικά σπάνιοι σήμερα, ii) αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program / File viruses), iii) αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών, όπως π.χ., του Word και του Excel (Macro viruses), και iv) οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή όλες τις προαναφερθείσες κατηγορίες. Υπάρχει και μια ειδική κατηγορία ιών, η οποία εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως, για παράδειγμα, το Outlook Express, με αποτέλεσμα ένα απλό e-mail κειμένου να μπορεί να κάνει τη ζημιά. Βέβαια, οι ιοί αυτοί είναι σπάνιοι και παροπλίζονται με την εγκατάσταση νεότερων εκδόσεων των προβληματικών εφαρμογών. Σε αυτό το σημείο οι ειδικοί προτρέπουν να αναβαθμίζουν οι χρήστες στη νεότερη έκδοση όλες τις εφαρμογές τους, ειδικά αυτές που σχετίζονται με το Διαδίκτυο. Με αυτόν τον τρόπο μειώνονται αρκετά οι πιθανότητες μόλυνσης. Επιπλέον επιχειρήσεις όπως η Network Associates (ιδιοκτήτης των McAfee προϊόντων) και η Symantec[11] (ιδιοκτήτης των Norton προϊόντων) παρέχουν αντι-ικά λογισμικά σε ιδιώτες και επιχειρήσεις.

[11] http://www.enterprisesecurity.symantec.com/content.cfm?articleid=1539

Χαρακτηριστικό είναι το ακόλουθο γράφημα και οι πίνακες που δείχνουν τους υπολογιστές που προσβλήθηκαν από ιό από τον Ιούνιο του 2003 έως τον Ιούνιο του 2004 σε διάφορες γεωγραφικές περιοχές του εξωτερικού. Από το γράφημα φαίνεται ότι ο ιός βρίσκεται σε έξαρση κατά το μήνα Ιούλιο και στη συνέχεια παρουσιάζει μικρές αυξομειώσεις μέχρι το τέλος της ετήσιας περιόδου.

Γράφημα 1: Υπολογιστές που προσβλήθηκαν από ιό από τον Ιούνιο του 2003 μέχρι σήμερα



Πίνακας 1:
Υπολογιστές που προσβλήθηκαν από ιό ανά γεωγραφική περιοχή από το 2003

Βόρεια Αμερική	61.633
Ευρώπη	24.172
Ασία	8.912
Αυστραλία και Ν. Ζηλανδία	2.698
Ν. Αμερική	340
Αφρική	186
(άγνωστης προέλευσης)	5.954
Σύνολο	**103.895**

Πηγή: wtc.trendmicro.com

Παρατηρεί κανείς επίσης από τον πίνακα 1 ότι στη Β. Αμερική υπάρχει η μεγαλύτερη επίθεση των ιών και στην Αφρική η μικρότερη, γεγονός που εξηγείται αν λάβει κανείς υπόψη το διαφορετικό μέγεθος χρήσης των υπολογιστών στις δύο αυτές

ηπείρους. Μετά τη Β. Αμερική ακολουθούν η Ευρώπη, η Ασία, ήπειροι, που έχουν αναπτύξει σε σημαντικό βαθμό τα πληροφοριακά τους συστήματα.

Πίνακας 2:
Χώρες με το μεγαλύτερο αριθμό προσβολών πληροφορικών συστημάτων

ΗΠΑ	59.972
Ιταλία	7.185
Γερμανία	5.298
Αγγλία	3.785
Δανία	2.392
Αυστραλία	2.214
Γαλλία	2.004
Ιαπωνία	1.897

Πηγή: wtc.trendmicro.com

Από τον πίνακα 2 επίσης φαίνεται ότι οι χώρες που έχουν παρουσιάσει το μεγαλύτερο αριθμό προσβολών είναι οι Η.Π.Α. με μεγάλη διαφορά, η Ιταλία, η Γερμανία, η Αγγλία και τελευταία η Ιαπωνία.

- Δούρειοι ίπποι

Δε θα ήταν υπερβολή, εάν έλεγε κάποιος ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών διαδικτύου, προέρχεται από τους δούρειους ίππους (Trojan horses). Τα Trojan horses έχουν πάρει το όνομά τους από το Δούρειο ίππο, κυρίως λόγω των ομοιοτήτων που παρουσιάζουν στον τρόπο λειτουργίας τους, αφού συνήθως μεταμφιέζονται σε κάτι χρήσιμο για το χρήστη και περιμένουν την κατάλληλη στιγμή για να ανοίξουν τις πύλες, που εν προκειμένω δεν είναι άλλες από τα ports του υπολογιστή. Ειδικότερα, τα Trojan horses ενώ εμφανίζονται απόλυτα ακίνδυνα για το χρήστη, έχουν έμμεσες ή άμεσες καταστρεπτικές συνέπειες για τον υπολογιστή, επιτρέποντας σε έναν ή περισσότερους crackers να έχουν πρόσβαση σε αυτόν. Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής φωλιάζει με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το διαδίκτυο, το Trojan-διακομιστής, που

τρέχει σιωπηρά στο υπόβαθρο (background), στέλνει ένα σήμα το οποίο λαμβάνει το Trojan-πελάτης (στο μηχάνημα του θύτη). Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο cracker αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτιθέμενου στο άλλο μηχάνημα ποικίλλει, αναλόγως του Trojan. Ο πρώτος μπορεί απλώς να ενοχλεί τον ανυποψίαστο χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του οδηγού CD-ROM ή εμφανίζοντας γαργαλιστικά μηνύματα στην οθόνη του. Μπορεί όμως και να του διαγράψει αρχεία ή ακόμα και να του προκαλέσει ζημιές στο υλικό του υπολογιστή, όπως, π.χ., να του διαγράψει το BIOS ή να χτυπήσει τις κεφαλές του σκληρού δίσκου. Με το πρόσχημα των δωρεάν γραφικών, αστείων εικόνων, αστείων video κ.λ.π. το Trojan horse ξεγελά το χρήστη, ώστε να το τρέξει, και κατόπιν δημιουργεί ένα backdoor (σημείο πρόσβασης) με ανοιχτά δικαιώματα χρήσης. Αξίζει να σημειωθεί ότι τα καθαρόαιμα προγράμματα Trojan (δηλαδή τα πρώτα Trojans που δεν ενσωματώνουν λειτουργίες ιού) δεν πολλαπλασιάζουν τον εαυτό τους στο μολυσμένο σύστημα.

Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το Trojan-διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη.

Ο συνηθέστερος τρόπος να μπει ένα Trojan σε έναν υπολογιστή είναι να έρχεται ως επισυναπτόμενο σε κάποιο e-mail ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι freeware ή shareware, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λ.π. Γνωστά προγράμματα Trojan είναι ο Sub7, το Netbus (με όλα τα παράγωγά του), ενώ το είδος, ο σκοπός χρήσης και η τεχνολογία αυτής της κατηγορίας προγραμμάτων παρουσιάζει εντυπωσιακή ποικιλία. Λίστες με τα ports

που χρησιμοποιούν τα πιο δημοφιλή Trojan βρίσκονται σε διάφορες διευθύνσεις[12]. Υπάρχουν δύο τρόποι για να αποφεύγει κανείς τα Trojan. Ο πρώτος είναι να χρησιμοποιεί ένα πρόγραμμα αντι-ιικό[13] (antivirus) ή (antitrojan). Πολλά προγράμματα του είδους μπορούν να τα ανιχνεύουν όταν κατεβαίνουν ακόμα και στην περίπτωση που είναι ήδη εγκαταστημένα στον ηλεκτρονικό υπολογιστή και να τα διαγράφουν. Ο άλλος τρόπος είναι η χρησιμοποίηση ενός προσωπικού firewall. Κάθε φορά που ένα Trojan-διακομιστής θα προσπαθεί να βγει στο διαδίκτυο, το firewall θα ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία. Τέλος, καλό είναι να κατεβαίνουν στον υπολογιστή μόνο έμπιστα προγράμματα, από γνωστούς, επίσημους δικτυακούς τόπους.

- Σκουλήκια

Είναι ικανά να μεταδοθούν από ένα μηχάνημα στο άλλο επί του δικτύου εκμεταλλευόμενα λογικά κενά σε πρωτόκολλα του Διαδικτύου.

Τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται, ωστόσο σε αντίθεση με τους παραδοσιακούς ιούς, δεν απαιτούν την παρεμβολή του ανθρώπινου παράγοντα για να μεταδοθούν από το ένα σύστημα στο άλλο. Η επικινδυνότητα των σκουληκιών (worms) έγκειται στο ότι επιτρέπουν μια ποικιλία επιθέσεων μέσω του Διαδικτύου χρησιμοποιώντας για τη μετάδοσή τους μέρη του λειτουργικού συστήματος που δρουν αυτόματα και είναι αφανή στο χρήστη-έτσι ώστε να μη γίνονται αντιληπτά. Για παράδειγμα, ένα καλογραμμένο worm μπορεί να αναζητήσει μόνο του συστήματα που παρουσιάζουν μια

[12] http://www.sys.security.com/html/papers/trojan_list.html
[13] http://www.avien.org/

συγκεκριμένη αδυναμία στην ασφάλειά τους, να τα μολύνει και να περιμένει την κατάλληλη στιγμή για να εκκινήσει μια συγχρονισμένη επίθεση DoS (Denial of Service) σε έναν καθορισμένο στόχο. Συνήθως δε μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των Melissa και Love Letter, εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό. Μάλιστα, το Melissa worm έχει αρχίσει ένα νέο γύρο καλυμμένο αυτήν τη φορά ως έγγραφο του Office για Mac. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα e-mail σε όλη τη λίστα επαφών του Outlook. Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα e-mail από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο και μαζί τον ασκό του Αιόλου. Στις περισσότερες περιπτώσεις διαπιστώνει κανείς την ύπαρξη του worm στον υπολογιστή του μόνο όταν αρχίσει η καταστροφική δράση του. Η μαζική αποστολή e-mail, εκτός από την κατασπατάληση του ήδη μικρού εύρους ζώνης του modem σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Internet, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας.

Σήμερα-σε αντίθεση με το πρόσφατο παρελθόν-ο μέσος χρήστης είναι ενήμερος για τους κινδύνους που παρουσιάζουν τα συνημμένα αρχεία e-mail, ωστόσο η εξέλιξη στο χώρο των ιών είναι τέτοια που ακόμα και ένα κλικ σε ένα φαινομενικά αθώο link μιας ιστοσελίδας μέσα από τη χρήση ActiveX περιεχομένου μπορεί να επιτρέψει την εκτέλεση προγραμμάτων στον υπολογιστή.

Ακόμα και τα πιο ακραία μέτρα προστασίας δε μπορούν να εγγυηθούν την απόλυτη ασφάλεια, αφού πάντα τα προγράμματα που χρησιμοποιούνται θα είναι ατελή, υπό την έννοια ότι θα παρουσιάζουν αδυναμίες τις οποίες ενίοτε θα εκμεταλλεύονται οι αποφασισμένοι cracker. Πρόκειται για τα λεγόμενα exploits,

προγραμματιστικές αδυναμίες σε γνωστές και ευρέως χρησιμοποιούμενες εφαρμογές, τα οποία μπορούν να αξιοποιούν καταλλήλως οι crackers για να αποκτούν μη εξουσιοδοτημένη πρόσβαση ή έλεγχο σε συστήματα, να προκαλούν ζημιές σε υπολογιστές-στόχους κ.ο.κ. Συχνά, πάντως, οι εταιρίες κυκλοφορούν αναβαθμίσεις ή διορθώσεις (bug fixes, patches) προγραμμάτων με γνωστά προβλήματα.

Τέλος, η συνδυαστική χρήση μιας πληθώρας εργαλείων μπορεί να εξασφαλίσει τη διατήρηση της ασφάλειας και της ανωνυμίας κατά τη διάρκεια της σύνδεσης στο Internet. Πέρα από την αυτονόητη χρήση προγραμμάτων antivirus, η χρήση ενός firewall είναι επιβεβλημένη.

Χώροι που έχουν βανδαλιστεί στο παρελθόν είναι: (Hunter, 2006)

- Το υπουργείο δικαιοσύνης των Η.Π.Α.
- Η C.I.A.
- Η αεροπορική δύναμη των Η.Π.Α. (Air Force)
- Το έθνος του Ισλάμ
- N.A.S.A
- Το εργατικό κόμμα της Αγγλίας
- Telia (Σουηδική εταιρία τηλεπικοινωνιών)
- Nesthosting ISP (βανδαλίστηκαν 1500 σελίδες συνδρομητών)

2.4.3 Social engineering – μη τεχνικές επιθέσεις

Ακούγεται ειρωνικό αλλά αποτελεί μία πραγματικότητα, το γεγονός ότι μία από τις ύπουλες μεθόδους επίθεσης σε ένα σύστημα ασφαλείας δεν βασίζεται στην τεχνολογία αλλά στην ψυχολογία! Ως social engineering ορίζεται η τέχνη του να

αποκτά κανείς πρόσβαση σε ένα σύστημα, εξαπατώντας τους χρήστες και τους διαχειριστές του και αποσπώντας τους όλες εκείνες τις πληροφορίες που χρειάζεται.

Υπάρχουν δύο κατηγορίες social engineering. Αυτές που βασίζονται στον άνθρωπο (human-based) και αυτές που βασίζονται στον υπολογιστή (computer-based). Η human-based κατηγορία αφορά παραδοσιακές μεθόδους επικοινωνίας όπως πρόσωπο με πρόσωπο ή μέσω τηλεφώνου. Χαρακτηριστικό αυτής της κατηγορίας είναι το ακόλουθο πείραμα.

Σε ένα πείραμα που έγινε, μια ομάδα από hackers ξεκίνησαν την προσπάθειά τους να διεισδύσουν σε ένα πληροφοριακό σύστημα μεγάλης εταιρίας. Μοναδικό τους όπλο είχαν τον τηλεφωνικό κατάλογο της εταιρίας. Τηλεφώνησαν στην εταιρία, ζήτησαν να μιλήσουν με τη γραμματεία του δικτύου και κατόρθωσαν μέσα σε 24ώρες η ίδια η εταιρία να τους δημιουργήσει λογαριασμό, να τους δώσει ID και κωδικό μέσω τηλεφώνου και μάλιστα να τους στείλει με ταχυμεταφορά (courier) μέσα στη νύχτα το απαιτούμενο, για την είσοδό τους στο δίκτυο, λογισμικό (software).

Η computer-based κατηγορία σχετίζεται με τη χρησιμοποίηση ποικίλων τεχνικών που στόχο έχουν να παροτρύνουν τους χρήστες να αποκαλύψουν ευαίσθητες πληροφορίες. Για παράδειγμα, ένας hacker μπορεί να στείλει απλά ένα e-mail ζητώντας πληροφορίες ή να κατασκευάσει μια ιστοσελίδα που να γίνεται χρήση προσωπικών ID και passwords.

Ο Kevin Mitnick, που καταδικάστηκε σε 5 χρόνια φυλάκιση για παράνομη εισβολή σε πληροφοριακά συστήματα, ανέφερε πως περισσότερες από τις μισές επιτυχημένες του επιθέσεις βασίζονταν στο social engineering. Ο Mitnick πιστεύει (Mitnick and Simon, 2002) πως η εμπιστοσύνη είναι αυτή που κάνει το social engineering επιτυχημένο. Αναφέρει: «πως προσπαθείς να δημιουργήσεις ένα κλίμα εμπιστοσύνης και πάνω σε αυτό να στηριχτείς» (Lemos, 2000).

Υπάρχουν συγκεκριμένες θέσεις μέσα στις επιχειρήσεις που γίνονται στόχοι επιθέσεων του social engineering. Στις θέσεις αυτές οι εργαζόμενοι έχουν πρόσβαση σε ιδιωτικές και εμπιστευτικές πληροφορίες και αλληλεπιδρούν με το εξωτερικό περιβάλλον σε καθημερινή βάση. Τέτοιες θέσεις έχουν να κάνουν με γραμματειακή υποστήριξη, με διαχειριστές δικτύων, με τηλεφωνικά κέντρα.

Μια σειρά από συγκεκριμένες ενέργειες χρειάζονται για να αντιμετωπιστεί το φαινόμενο του social engineering (Damle, 2002).

- *Εκπαίδευση*. Όλοι οι εργαζόμενοι και ιδιαίτερα εκείνοι που βρίσκονται σε ευαίσθητες θέσεις πρέπει να είναι ενήμεροι σχετικά με τους κινδύνους που συνδέονται με το social engineering, τις τεχνικές που χρησιμοποιούνται από τους hackers, καθώς και τους τρόπους και τα μέσα να αντιμετωπίσουν αυτές τις επιθέσεις.
- *Πολιτικές και διαδικασίες*. Ειδικές πολιτικές και διαδικασίες πρέπει να αναπτυχθούν για την ασφάλεια εμπιστευτικών πληροφοριών. Σε αυτό θα συμβάλει και η ανάλογη συμπεριφορά των εργαζομένων που θα σέβεται αυτές τις εμπιστευτικές πληροφορίες λαμβάνοντας συνάμα μέτρα ανταπόκρισης σε επιθέσεις social engineering.
- *Τεστ διείσδυσης*. Οι πολιτικές, οι διαδικασίες και η δραστηριότητα των εργαζομένων χρειάζονται να εξετάζονται κατά τακτά διαστήματα από ειδικούς του εξωτερικού περιβάλλοντος της επιχείρησης παίζοντας το ρόλο του hacker. Μετά το πέρας του τεστ οποιαδήποτε πιθανή αδυναμία θα πρέπει να διορθώνεται.

2.5 Spamming[14]

Το spamming αναφέρεται στην πρακτική της αδιάκριτης διανομής μηνυμάτων χωρίς την άδεια του παραλήπτη και χωρίς σκέψη για την καταλληλότητα του

[14] http://www.spam.abuse.net/

μηνύματος. Στο νόμο περί Προστασίας Ηλεκτρονικής Θυρίδας Αλληλογραφίας παρουσιάζεται πως το spamming προκαλεί σημαντική βλάβη, έξοδα, ενόχληση και πρέπει να ελέγχεται.

Η αλληλογραφία spam αποτελεί το 30% όλης της αλληλογραφίας που στέλνεται στο America Online. (του μεγαλύτερου πάροχου υπηρεσιών Internet στην Αμερική) Αυτός ο όγκος μειώνει σημαντικά ένα ήδη περιορισμένο εύρος ζώνης επιβραδύνοντας το Internet γενικά και, σε μερικές περιπτώσεις, κλείνοντας τελείως τον ISP. Ο νόμος αυτός απαιτεί αυτοί που στέλνουν spam να το δηλώσουν σαν διαφήμιση, να δηλώσουν το όνομα του αποστολέα και να περιλαμβάνουν έγκυρες πληροφορίες δρομολόγησης. Οι παραλήπτες μπορούν να παραιτηθούν του δικαιώματος να δεχθούν τέτοιες πληροφορίες. Επίσης, οι ISP απαιτείται να προσφέρουν λογισμικό μπλοκαρίσματος spam, και οι παραλήπτες του spam έχουν το δικαίωμα να ζητήσουν τερματισμό μελλοντικού spam από τον ίδιο αποστολέα και να χρησιμοποιήσουν ένδικα μέσα, αν χρειάζεται. (Τώρα το spam είναι λιγότερο από 10%)

Το spamming κοστίζει χρόνο και χρήματα καταναλωτών, αλλά παρά ταύτα μέχρι σήμερα δεν υπάρχει νομική επανόρθωση διαθέσιμη για τέτοια ηλεκτρονική παρενόχληση και βομβαρδισμό απρόσκλητης διαφήμισης. Το λογισμικό εξέτασης και το πλήκτρο διαγραφή (delete) ίσως είναι τα καλύτερα εργαλεία του ατόμου για αυτοάμυνα από τον ηλεκτρονικό αυτό πόλεμο. Δικτυακοί τόποι[15] παρέχουν δωρεάν λογισμικό που μπλοκάρει ανεπιθύμητες διαφημίσεις και προστατεύει τους χρήστες από cookies και άλλες απειλές (Turban, 2000).

[15] http://www.getlost.com , http://www.junkbusters.com

2.6 Κίνδυνοι της στρατηγικής του ηλεκτρονικού εμπορίου και τρόποι διαχείρισής τους

Πέρα από τις κρίσεις που σχετίζονται με την ασφάλεια των πληροφοριών, η επιχείρηση έχει να αντιμετωπίσει και επιχειρηματικούς κινδύνους οι οποίοι αφορούν στην υλοποίηση της στρατηγικής του ηλεκτρονικού εμπορίου και στις ενδεχόμενες αρνητικές συνέπειες που έχει αυτή στην παραγωγική λειτουργία της επιχείρησης. Λέγοντας στρατηγική ηλεκτρονικού εμπορίου εννοεί κανείς είτε το λανσάρισμα μιας ιστοσελίδας, είτε τη δημιουργία εφοδιαστικής αλυσίδας στα πλαίσια του η-επιχειρείν. Πολλές φορές η στρατηγική του ηλεκτρονικού εμπορίου λειτουργεί ως απειλή για τους ανταγωνιστές και ως μέσο βελτιώσεων σε όλο τον κλάδο. Οι κίνδυνοι από την εφαρμογή της στρατηγικής του ηλεκτρονικού εμπορίου είναι οι εξής: (Viehland, 2001)

Κίνδυνοι από ανταγωνιστές (competitive risks). Όλες οι επιχειρήσεις επιδιώκουν να αποκτήσουν ανταγωνιστικό πλεονέκτημα στην αγορά στην οποία δραστηριοποιούνται. Είναι πιθανό μια στρατηγική κίνηση προς το ηλεκτρονικό εμπόριο να έχει αρνητικές συνέπειες για την επιχείρηση που την πραγματοποιεί. Ο κίνδυνος εμφανίζεται από τη στιγμή που η στρατηγική αλλάζει το επίπεδο του ανταγωνισμού εις βάρος της επιχείρησης (Vitale, 1986). Όταν μια επιχείρηση αρχίζει να ασκεί δραστηριότητα και μέσω του ηλεκτρονικού εμπορίου, οι ανταγωνιστές της όχι μόνο θα ακολουθήσουν, αλλά θα προσπαθήσουν να ανεβάσουν το επίπεδο του ανταγωνισμού με πιο σύγχρονες τακτικές. Χαρακτηριστική είναι η περίπτωση της Tower Insurance[16] που ήταν η πρώτη επιχείρηση παροχής χρηματοοικονομικών υπηρεσιών στη Νέα Ζηλανδία με ιστοσελίδα. Η ιστοσελίδα της ωστόσο περιείχε μερικές μόνο πληροφορίες για πολιτικές ασφάλισης και χρηματοοικονομικές

[16] http://www.tower.co.nz

υπηρεσίες καθώς και ορισμένους συνδέσμους επικοινωνίας με πράκτορες. Στη συνέχεια η AMP[17] κατασκεύασε τη δική της ιστοσελίδα, η οποία περιείχε όλη τη λειτουργικότητα της ιστοσελίδας της Tower, καθώς επίσης και μια σειρά από χρηματοοικονομικούς υπολογισμούς οι οποίοι ενθάρρυναν περισσότερη αλληλεπίδραση με τους επισκέπτες. Η AMP είναι η μοναδική ασφαλιστική εταιρία, τώρα, στη Νέα Ζηλανδία που πουλά ασφάλιση αυτοκινήτων online και η Tower, που έκανε πρώτη την εμφάνισή της στο Διαδίκτυο, ακολουθεί. Η περίπτωση αυτή δείχνει ότι επιχειρήσεις οι οποίες δεν είναι διατεθειμένες να κάνουν συνεχείς επενδύσεις στη στρατηγική τους στο ηλεκτρονικό εμπόριο θα πρέπει να μην εισέρχονται πρώτες σε αυτή τη διαδικασία.

Μέσα στα πλαίσια των κινδύνων από τους ανταγωνιστές εντάσσεται επίσης και η αύξηση της δύναμης των πελατών ή των προμηθευτών σε βάρος βέβαια της επιχείρησης που πραγματοποιεί την καινοτομία. Η στρατηγική του ηλεκτρονικού εμπορίου ενδυναμώνει τις σχέσεις της επιχείρησης με τους πελάτες της και τους προμηθευτές της και σε πολλές περιπτώσεις παρέχει εκπαίδευση και τεχνογνωσία που δίνει τη δυνατότητα σε αυτούς να λειτουργήσουν από μόνοι τους. Έτσι, εάν ο ανταγωνιστής παρέχει καλύτερη ευκαιρία οι πελάτες θα στραφούν προς αυτόν και οι επενδύσεις που έχουν γίνει από την αρχική επιχείρηση δε θα προσφέρουν κανένα μακροπρόθεσμο πλεονέκτημα.

Μια άλλη περιοχή που σχετίζεται με κινδύνους από ανταγωνιστές είναι η χρονική στιγμή της υλοποίησης της στρατηγικής του ηλεκτρονικού εμπορίου. Η κατάλληλη χρονική στιγμή διαδραματίζει πολύ σημαντικό ρόλο και απαιτεί πολύ καλή γνώση της αγοράς. Για παράδειγμα πολλές αμερικανικές τράπεζες ξόδεψαν εκατομμύρια δολάρια σε τραπεζικά συστήματα τα οποία έδιναν τη δυνατότητα εξυπηρέτησης των

[17] http://www.amp.co.nz

πελατών τους από το σπίτι, σε μια εποχή που οι πελάτες δεν ήταν εξοικειωμένη με τέτοιου είδους συστήματα, δεν είχαν εμπιστοσύνη στις ηλεκτρονικές συναλλαγές και πολλοί από αυτούς δεν είχαν καν υπολογιστές.

Πολλοί υποστηρίζουν ότι αυτοί που θέλουν να αναπτύξουν στρατηγική ηλεκτρονικού εμπορίου πρέπει να την πραγματοποιήσουν πρώτοι. Ωστόσο, αυτοί που πολλές φορές ακολουθούν είναι πιο επιτυχημένοι διότι κατανοούν καλύτερα τις ανάγκες της αγοράς και την πραγματοποιούν τη στιγμή που είναι απαραίτητη. Πάνω σε αυτό συνηγορεί και το παράδειγμα της Tower με την AMP που αναφέρθηκε παραπάνω.

Τέλος μια εξίσου σημαντική περιοχή κινδύνου που σχετίζεται με τους ανταγωνιστές είναι οι απειλές από την είσοδο νέων επιχειρήσεων. Από τη σκοπιά του ανταγωνιστικού πλεονεκτήματος, οι νέες επιχειρήσεις σε μια αγορά έχουν πλεονεκτήματα σε σχέση με τις ήδη υπάρχουσες. Οι επιχειρήσεις που ήδη υπάρχουν ακολουθούν πολύ συγκεκριμένες επιχειρηματικές κουλτούρες, αρνούνται να μετασχηματίσουν υπάρχουσες γραμμές προϊόντων και δεν αναλαμβάνουν κινδύνους που θα μπορούσαν να αναβαθμίσουν την αγορά. Αντίθετα, οι νεοεισερχόμενες επιχειρήσεις αναγνωρίζουν ευκαιρίες πολύ πιο εύκολα και μπορούν να εκτελέσουν σχέδια ηλεκτρονικού εμπορίου πιο γρήγορα.

Με δεδομένη την ύπαρξη λοιπόν των παραπάνω κινδύνων που σχετίζονται με τον ανταγωνισμό στην εφαρμογή της στρατηγικής του ηλεκτρονικού εμπορίου, θα αναρωτιέται κανείς τι χρειάζεται να συμβεί για να ελαχιστοποιηθούν, αν όχι να εξαλειφθούν οι παραπάνω κίνδυνοι. Η κατανόηση των κινδύνων του ανταγωνισμού είναι το πρώτο πράγμα που πρέπει να συμβεί. Σε συνδυασμό με το ποιοι είναι οι ανταγωνιστές, ποιες είναι οι δυνάμεις και οι αδυναμίες τους, οι διαχειριστές κρίσεων θα πρέπει να λάβουν υπόψη και τα ακόλουθα:

- Το είδος των κινήτρων στην υλοποίηση της στρατηγικής του ηλεκτρονικού εμπορίου.
- Τις αλλαγές που θα επιφέρει μια τέτοια στρατηγική σε ολόκληρη τη λειτουργία της επιχείρησης.
- Ο πρώτος που θα υλοποιήσει μια τέτοια στρατηγική, αν θα μπορέσει να αποκτήσει τα οφέλη που αυτή υπόσχεται.
- Το χρόνο αντίδρασης των ανταγωνιστών (αργά ή γρήγορα).
- Αν ο ανταγωνιστής αντιδράσει με παρόμοια αλλά πιο βελτιωμένη στρατηγική, πόσο έτοιμη είναι η επιχείρηση να ανταπαντήσει και πως.
- Είναι η συγκεκριμένη στρατηγική αναπόφευκτη; Ποιες είναι οι επιδράσεις στην επιχείρηση αν την πραγματοποιήσει πρώτη; Αν την πραγματοποιήσουν πρώτοι οι ανταγωνιστές;
- Οι αρνητικές επιδράσεις αντισταθμίζουν τα οφέλη που αναμένονται από την υλοποίηση της στρατηγικής;

Η καλύτερη στρατηγική να αντιμετωπίσει κανείς μια νέα είσοδο είναι να σκέφτεται και να ενεργεί σαν να αποτελεί νέα είσοδο. Η ανώτερη διοίκηση θα πρέπει να ανιχνεύει νέες τάσεις νωρίτερα από τους ανταγωνιστές, να λαμβάνει αποφάσεις με ταχείς ρυθμούς και να είναι αρκετά ευέλικτη στη δημιουργία ή υιοθέτηση επιχειρηματικών μοντέλων. Μια χρήσιμη στρατηγική διαχείρισης κρίσης αποτελεί η ίδρυση ξεχωριστής θυγατρικής με την επωνυμία της μητρικής επιχείρησης. Αυτή πρόκειται για μια νέα είσοδο που ενώ έχει κάποια από τα μειονεκτήματα της μητρικής, μπορεί να αποτελέσει επιχειρηματική επιτυχία. Αν αποδειχθεί αποτυχημένη ενέργεια η φήμη της μητρικής επιχείρησης παραμένει άθικτη. Στη Νέα Ζηλανδία, η τράπεζα ASB, μια από τις πιο τεχνολογικά προηγμένες τράπεζες στη χώρα, ίδρυσε τη BankDirect ως την πρώτη online τράπεζα της Νέας Ζηλανδίας. Η BankDirect

λειτουργεί αποκλειστικά στο Διαδίκτυο χωρίς φυσικά καταστήματα. Η τράπεζα ASB εξακολουθεί να καινοτομεί στην τραπεζική αγορά της Νέας Ζηλανδίας, αλλά η BankDirect λειτουργεί περισσότερο σαν νέα είσοδο και προσφέρει ποικίλες τραπεζικές υπηρεσίες στην αγορά της Νέας Ζηλανδίας όπως μεγαλύτερη ποικιλία πιστωτικών καρτών από αυτές που είναι διαθέσιμες σε άλλες τράπεζες.

Κίνδυνοι αλλαγής (transition risks). Η υιοθέτηση της στρατηγικής του ηλεκτρονικού εμπορίου είναι πιθανό να απαιτεί ανασχεδιασμό των εσωτερικών διαδικασιών της επιχείρησης, νέες πρακτικές σε σχέση με το προσωπικό και μακροπρόθεσμη δέσμευση της ομάδας των στελεχών. Ενώ η αγορά απαιτεί ραγδαίες αλλαγές, ο ρυθμός της οργανωσιακής αλλαγής της επιχείρησης μπορεί να είναι αργός με κινδύνους και κόστος.

Οι κίνδυνοι αλλαγής είναι ιδιαίτερα υψηλοί στην πραγματοποίηση εφαρμογών η-επιχειρείν όπως σε συστήματα ενδο-επιχειρησιακού σχεδιασμού το γνωστό σε όλους ERP, σε συστήματα διαχείρισης πελατών (CRM) ή σε συστήματα ηλεκτρονικών προμηθειών (e-procurement). Εάν οι εργαζόμενοι, οι προμηθευτές καθώς και οι άλλοι συνεργάτες της επιχείρησης δεν κατανοήσουν το λόγο ύπαρξης αυτών των αλλαγών, η επίδρασή τους θα είναι ανεπιτυχής.

Μέρος των κινδύνων αλλαγής ενυπάρχει στο μετασχηματισμό της υπάρχουσας γραμμής προϊόντων. Χαρακτηριστικό παράδειγμα είναι τα φυσικά καταστήματα που δραστηριοποιούνται και ηλεκτρονικά. Εάν ένας σημαντικός αριθμός νέων πελατών πραγματοποιούν τις αγορές τους online, τότε είναι επιτυχία. Εάν όμως αυτοί που πραγματοποιούν αγορές online αντιπροσωπεύουν ήδη υπάρχοντες πελάτες οι οποίοι δεν επισκέπτονται το φυσικό κατάστημα τότε τα συνολικά έσοδα δεν αυξάνονται ενώ τα κόστη αυξάνονται (για παράδειγμα το κόστος συντήρησης της ιστοσελίδας). Οι τράπεζες επίσης αντιμετωπίζουν τα ίδια προβλήματα με τη Διαδικτυακή τραπεζική,

συνήθως στην αρχή αυτής της δραστηριότητας, διότι τείνουν να προσελκύουν ήδη υπάρχοντες πελάτες και όχι απαραίτητα μεγάλο αριθμό νέων πελατών.

Για να μπορέσει να αντιμετωπίσει κανείς τους κινδύνους αλλαγής θα πρέπει να θυμηθεί τις βασικές αρχές της διοίκησης αλλαγών. Η διοίκηση αλλαγών αναλύει τις αλλαγές που αντιμετωπίζει μια επιχείρηση και αναπτύσσει σχέδια ελαχιστοποίησης των κινδύνων και μεγιστοποίησης των ωφελειών που προκύπτουν από την αλλαγή. Για παράδειγμα, κατά την εφαρμογή ενός συστήματος ERP απαιτείται ένα σχέδιο δράσης αλλαγής που να περιλαμβάνει στελέχη καθώς και ομάδες εργαζομένων οι οποίοι θα ενθαρρύνουν την επικοινωνία και την ανατροφοδότηση σχετικά με τις οργανωσιακές αλλαγές.

Οι αρχές της διοίκησης αλλαγών θα πρέπει να αναγνωρίζονται και να ακολουθούνται. Για παράδειγμα (Stokes, 1989):

- Καθένας ο οποίος επηρεάζεται από μια αλλαγή, την αντιλαμβάνεται διαφορετικά και συμπεριφέρεται σύμφωνα με την αντίληψή του.
- Οι επιχειρήσεις αποτελούνται από πολλά συστήματα (technical, social, administration systems) και η αλλαγή σε ένα από αυτά επηρεάζει τα άλλα.
- Η διοίκηση της αλλαγής σημαίνει διοίκηση του διαφορετικού.
- Η αρνητική συμπεριφορά απέναντι στην αλλαγή συχνά καταλήγει σε αρνητική αυτοεκπληρούμενη προφητεία. Το αντίθετο είναι επίσης σωστό.
- Η επιχειρησιακή κουλτούρα είναι σπουδαίος παράγοντας στη διαχείριση της αλλαγής.
- Η αμφιβολία είναι μια συνιστώσα που συνοδεύει σχεδόν πάντα την αλλαγή και πρέπει να γίνεται σωστά η χρήση της.

Οι στρατηγικές για διαχείριση της αλλαγής μπορεί να απαιτούν είτε μεγάλη συμμετοχή από αυτούς στους οποίους επιδρά η αλλαγή, είτε μικρή συμμετοχή. Έχει παρατηρηθεί ότι οι στρατηγικές με μεγάλη συμμετοχή είναι πιο αποτελεσματικές.

Κίνδυνοι σε σχέση με τους πελάτες (customer-induced risks). Το ηλεκτρονικό εμπόριο στην προσπάθειά του να ικανοποιήσει τις ανάγκες των πελατών έχει να διαχειριστεί πολλαπλά και διαφορετικά δίκτυα διανομής πληροφοριών. Οι κίνδυνοι που ενυπάρχουν σε αυτή την κατηγορία συνοψίζονται στα ακόλουθα (Kanagalingam, 2000):

- Έλλειψη συνοχής των πληροφοριών οι οποίες στέλνονται μέσω διαφορετικών καναλιών.
- Λανθασμένος συγχρονισμός των πληροφοριών που αποστέλλονται έτσι ώστε να είναι ενημερωμένοι όλοι οι παραλήπτες για τις νέες αλλαγές.
- Διαχείριση αποθήκης (Repository Management). Αυτό σημαίνει ότι εάν υπάρχουν πολλαπλά κανάλια διανομής, όλες οι ψηφιακές συναλλαγές θα πρέπει να συλλέγονται σε μια κεντρική τοποθεσία για να καταχωρούνται και να κατηγοριοποιούνται.
- Αναβάθμιση τοπικών αποθηκών αν η επιχείρηση έχει πολλαπλά αποθηκευμένα δεδομένα.

Ένας άλλος πιο συνήθης κίνδυνος σχετίζεται με τη διατήρηση της εμπιστοσύνης των πελατών. Η εμπιστοσύνη είναι σχετικά εύκολο να αποκτηθεί στις διαπροσωπικές σχέσεις. Ένας πελάτης αγοράζει ένα προϊόν σε ένα κατάστημα λιανικής. Έχει την ευκαιρία να αγγίξει το προϊόν (feel and touch), να ρωτήσει τον πωλητή για το προϊόν και να φύγει με τη διαβεβαίωση ότι εάν κάτι δεν πάει καλά ο πωλητής θα είναι την επόμενη ημέρα εκεί και θα τον περιμένει.

Η ηλεκτρονική αγορά είναι διαφορετική. Το κατάστημα είναι εικονικό και η σχέση που αναπτύσσεται είναι συχνά ανώνυμη βασισμένη στην κίνηση των bits και όχι σε έναν εγκάρδιο χαιρετισμό ή σε μια πρόσωπο με πρόσωπο επικοινωνία. Η ανάγκη να κατανοήσει κάποιος τη σημασία της εμπιστοσύνης (trust) είτε σε προσωπικές συναλλαγές, είτε σε επιχειρηματικές μέσω του ηλεκτρονικού εμπορίου αποτελεί και το κομβικό σημείο της εξέλιξής του. Η εμπιστοσύνη και όχι η τεχνολογία για κάποιους είναι αυτή που καθορίζει την εξέλιξη του ηλεκτρονικού εμπορίου (Keen et al.,2000).

Ο πιο αποτελεσματικός λοιπόν τρόπος να μειωθούν οι κίνδυνοι σε σχέση με τους πελάτες είναι να αυξηθεί η εμπιστοσύνη. Πολλοί μελετητές πιστεύουν ότι υπάρχει άμεση, αντίστροφη σχέση ανάμεσα στην εμπιστοσύνη και στους κινδύνους που επηρεάζουν τους πελάτες. Αποτελεσματικοί τρόποι για τη δημιουργία εμπιστοσύνης περιλαμβάνουν (Huff et al., 2000):

- Τη χρήση τηλεφωνικών αριθμών με ελάχιστο χρόνο αναμονής έτσι ώστε να διευκολύνεται για τους πελάτες η απόκτηση προσωπικής επαφής.
- Τη χρήση ηλεκτρονικού ταχυδρομείου έτσι ώστε οι πελάτες να είναι ενήμεροι για την κατάσταση των παραγγελιών τους.
- Τη χρήση ασφαλών συστημάτων τεχνολογίας έτσι ώστε να βελτιωθεί η αίσθηση ασφάλειας των πελατών και να δοθεί ώθηση στην πεποίθησή τους για ηλεκτρονικές αγορές.
- Την παροχή σελίδας χρήσιμων ερωτήσεων (FAQ page).
- Την παρουσίαση φυσικών χαρακτηριστικών της επιχείρησης όπως του προσωπικού της.
- Την έκδοση πολιτικής σχετικά με την ασφάλεια των πληροφοριών.

- Τη χρήση απλής και σαφούς διαδικασίας αγοράς με την παροχή κατάλληλων πληροφοριών σχετικά με τις πολιτικές επιστροφής προϊόντων.

Κίνδυνοι σε σχέση με τους επιχειρηματικούς εταίρους (business partner risks). Μέσα στα πλαίσια του η-επιχειρείν οι επιχειρήσεις αυτοματοποιούν τις επιχειρησιακές τους διαδικασίες, βελτιώνουν τις ταμειακές ροές τους, μειώνουν τα κόστη και τις καθυστερήσεις. Αυτοί είναι μερικοί από τους λόγους που οι επιχειρήσεις υιοθετούν την ηλεκτρονική ανταλλαγή δεδομένων, εφαρμόζουν διανομές χωρίς καθυστερήσεις (just-in-time), αναθέτουν τον έλεγχο της τεχνολογικής ολοκλήρωσης των διαδικασιών τους σε εξωτερικούς συνεργάτες (outsourcing).

Σχηματίζοντας λοιπόν αυτές τις επικοινωνίες οι επιχειρήσεις αναπτύσσουν σχέσεις εξάρτησης μέσα στον αυξανόμενα πολύπλοκο επιχειρηματικό κόσμο. Για παράδειγμα οι επιχειρήσεις εκείνες που εφαρμόζουν διαδικασίες just-in-time κατά μήκος της εφοδιαστικής τους αλυσίδας, αυξάνουν το κόστος της αποθήκευσης σε μικρότερες επιχειρήσεις. Ταυτόχρονα, ενώ μπορεί να έχει μειωθεί το κόστος μέσω του just-in-time, ουσιαστικά έχει γίνει μεταφορά του κόστους, η εξάρτηση από τους προμηθευτές έχει αυξηθεί και ο κίνδυνος από τους επιχειρηματικούς εταίρους έχει τελικά αυξηθεί.

Παρόμοιοι κίνδυνοι αναπτύσσονται και με την αυξανόμενη χρήση υπηρεσιών outsourcing. Αυτού του είδους η εξάρτηση δεν είναι καινούρια και αφορά υπηρεσίες παροχής υποδομών, υπηρεσίες τεχνικής υποστήριξης, υπηρεσίες παροχής λογισμικών εφαρμογών, υπηρεσίες τήρησης αντιγράφων ασφαλείας καθώς και ανάκτησης δεδομένων ύστερα από ένα απρόσμενο γεγονός. Η συγκεκριμένη μέθοδος πρωτοεμφανίστηκε το 1988 όταν ο E.Kodak παραχώρησε σε άλλες εταιρίες (IBM, DEC, Businessland) το σχεδιασμό και την υλοποίηση πληροφοριακών συστημάτων για την επιχείρησή του (Αναστασιάδης, 2001).

Όπως σημειώθηκε παραπάνω ένας βασικός κίνδυνος των δραστηριοτήτων just-in-time είναι ότι τα κόστη μεταφέρονται στους προμηθευτές οι οποίοι σπάνια μπορούν να αντεπεξέλθουν. Ωστόσο, οι επιχειρήσεις πρέπει να συνεργαστούν. Η νέα μέθοδος της διαχείρισης των επιχειρηματικών συμμαχιών βασίζεται στο γεγονός ότι οι αγοραστές επιθυμούν την ύπαρξη των προμηθευτών στον επιχειρηματικό στίβο. Για παράδειγμα η εταιρία Chrysler κατάφερε μετά από 10 χρόνια να συνεργάζεται με μικρό αριθμό προμηθευτών, ελαχιστοποιώντας τον κίνδυνο από τους εξωτερικούς της συνεργάτες και απολαμβάνοντας τα οφέλη και εκείνη και οι προμηθευτές της από το σχεδιασμό και την ανάπτυξη των προϊόντων της.

Τα στελέχη για να διαχειριστούν τους κινδύνους που επιφέρει το outsourcing θα πρέπει να λάβουν υπόψη τα ακόλουθα:

- Τον αριθμό των στοιχείων της επιχείρησης που θα αναθέσουν σε εξωτερικούς συνεργάτες.
- Αναγνώριση και κατηγοριοποίηση των στοιχείων που ανατίθενται ανάλογα με τη σπουδαιότητά τους για την επιχείρηση.
- Εξέταση του μεγέθους της τεχνογνωσίας των ατόμων που αναλαμβάνουν να κάνουν το outsourcing. Αν έχουν κοινώς αποδεκτή πιστοποίηση ή όχι.
- Αν υπάρχει κάποιο στοιχείο που η ανώτερη διοίκηση έχει παραβλέψει και είναι σημαντικό για την επιχείρηση.
- Αν υπάρχει ομάδα εξειδικευμένων ατόμων μέσα στην επιχείρηση που θα μπορούσε να δουλέψει σε περίπτωση που οι εξωτερικοί συνεργάτες δεν παρέχουν ικανοποιητικά αποτελέσματα.

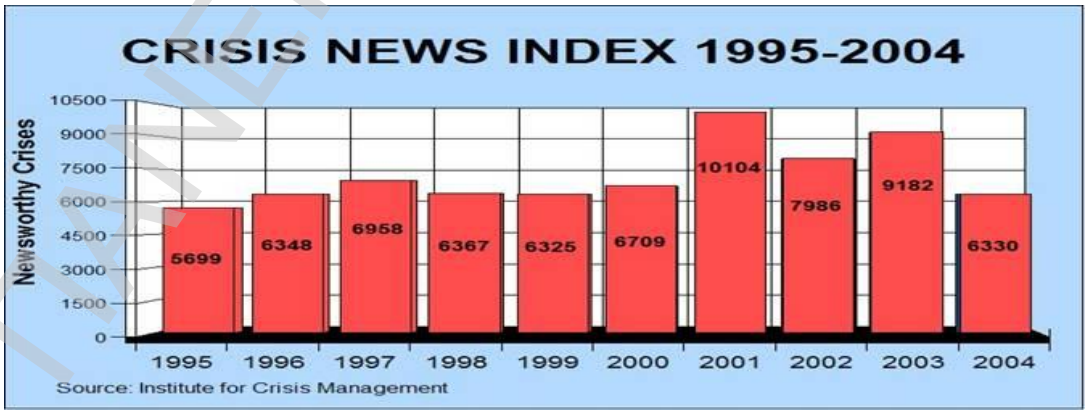
- Τους όρους της συνεργασίας ιδιαίτερα αν ο outsourcer είναι από διαφορετική χώρα προέλευσης σε σχέση με την επιχείρηση που κάνει την ανάθεση των εργασιών της.

ΚΕΦΑΛΑΙΟ 3ο : ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΕΩΝ

3.1 Γενικά περί διαχείρισης κρίσεων

Όλες οι επιχειρήσεις, από εμπορικούς οργανισμούς και χρηματοπιστωτικά ιδρύματα έως δημόσιες υπηρεσίες, αντιμετωπίζουν ποικιλία από κινδύνους κατά τη διάρκεια των καθημερινών δραστηριοτήτων τους. Αυτοί οι κίνδυνοι ίσως να μην είναι δυνατό να αποφευχθούν, ωστόσο θα πρέπει να ελέγχονται σε κάποιο βαθμό και να αντιμετωπίζονται με τον πλέον αποτελεσματικό τρόπο από πλευράς κόστους σε σχέση με την αξία των περιουσιακών στοιχείων της επιχείρησης.

Λέγοντας διαχείριση κρίσεων εννοεί κανείς ένα σύνολο ενεργειών από μια εξειδικευμένη ομάδα που στόχο έχουν την ελαχιστοποίηση (το μετριασμό) της επίδρασης ενός απροσδόκητου γεγονότος στη λειτουργία της επιχείρησης (Spillan, 2003). Το γεγονός αυτό είναι κρίση (κίνδυνος) που θέτει σε ενέργεια μια πραγματική ή ακόμα και πιθανή απειλή η οποία μπορεί να αναφέρεται στην υγεία, την ασφάλεια, το περιβάλλον και επιπλέον τη φήμη και την αξιοπιστία της επιχείρησης. Σύμφωνα με το Institute for Crisis Management, υπάρχουν πάνω από 100.000 καταγεγραμμένες επιχειρηματικές κρίσεις από το 1990 και μετά ενώ οι κρίσεις κορυφώνονται το 2001 (Σχήμα 1)[18].



[18] http://www.crisisexperts.com/02creport.htm

Σχήμα 1: Crisis News Index 1995-2004

(πηγή: Institute for Crisis Management)

Για πάνω από τρεις δεκαετίες η διαχείριση κρίσεων και ο σχεδιασμός ενδεχομένων έχουν αναγνωριστεί ως σημαντική περιοχή για ακαδημαϊκούς και ερευνητές (Πανηγυράκης, Βεντούρα, 2001).

Καθώς το περιβάλλον αναπτύσσεται περισσότερο πολύπλοκο, οι κρίσεις που αντιμετωπίζουν οι επιχειρήσεις θα αναπτύσσονται επίσης περισσότερο και συχνότερα (Hwang, 2000). Η ικανότητα της διοίκησης είναι ουσιαστικής σημασίας διότι η πίεση από τις κρίσεις μπορεί να έχει καταστροφική επίδραση για την επιχείρηση (Kuklan, 1988).

Ιστορικά, οι επιχειρηματικές κρίσεις θεωρούνταν σημαντικές αλλά ήταν απομονωμένα γεγονότα επηρεάζοντας κυρίως μεγάλες επιχειρήσεις. Παρόλα αυτά, η εμπειρία έχει δείξει ότι τελικά, οι περισσότερες επιχειρήσεις επηρεάζονται από μια κατάσταση κρίσης. Η κρίση μπορεί να εμφανιστεί με ή χωρίς προειδοποίηση, οπουδήποτε, οποιαδήποτε στιγμή. Ο Steven Fink (2000) αναφέρει, ότι η κρίση διαφαίνεται στον ορίζοντα κάθε επιχείρησης. Μια λάθος απόφαση, ακόμα και η μικρότερη, από τη διοίκηση μπορεί να είναι η αιτία σοβαρού επιχειρηματικού κινδύνου[19]. Ο Darling (1994) πιστεύει ότι εάν η διοίκηση αποδεχτεί το αναπόφευκτο μιας κρίσης ως πραγματικότητα, τότε όχι μόνο θα μπορέσει να σχεδιάσει απάντηση στην κρίση αλλά θα βρει ευκαιρίες οι οποίες περιέχονται μέσα σε αυτή.

Πολλές μεγάλες επιχειρήσεις έχουν αναπτύξει σχέδια διαχείρισης κρίσεων και ομάδες οι οποίες είναι έτοιμες στην εμφάνιση γεγονότος κρίσης. Ωστόσο, κάποιοι πιστεύουν ότι το θέμα της διαχείρισης κρίσεων δεν είναι σημαντικό. Υιοθετούν την άποψη ότι η κρίση δε θα εμφανιστεί σε αυτούς ή ότι έχουν μια καλά οργανωμένη

[19] http://www.crisisnavigator.org

επιχείρηση που θα μπορούσε να διαχειριστεί μια κρίση χωρίς σχέδιο (Caponigro, 2000). Υποστηρίζουν ότι οι κρίσεις συμβαίνουν μόνο σε άλλες επιχειρήσεις ή ότι αυτές είναι προστατευμένες με κάποιο τρόπο (Mitroff, 1989). Θεωρούν ότι οι πιθανότητες εμφάνισης κρίσης είναι τόσο μικρές ώστε η επιπλέον προσπάθεια σχεδιασμού αντιμετώπισής τους δεν είναι απαραίτητη (Hickman and Crandall, 1997). Ένα άλλο επιχείρημα που οι επιχειρήσεις παραθέτουν σχετικά με το γεγονός ότι δεν προετοιμάζονται επαρκώς για τη διαχείριση μιας κρίσης είναι ότι δεν έχουν τις πηγές που απαιτούνται για να βρίσκονται σε κατάσταση ετοιμότητας (Barton, 1993). Μερικές επιχειρήσεις ισχυρίζονται ότι δεν υπάρχει αρκετός χρόνος για να ασχοληθούν με τη διαχείριση κρίσεων. Αυτές οι θέσεις δηλώνουν ότι τα σημερινά προβλήματα είναι τόσο δύσκολα και χρονοβόρα που δεν υπάρχει χρόνος να σχεδιάσουν μελλοντικές αβεβαιότητες (Caponigro, 2000). Ενώ οι προηγούμενες απόψεις είναι κατανοητές, είναι χωρίς διορατικότητα και αν συνεχιστούν, μπορεί να είναι επιβλαβείς στην επιτυχία της λειτουργίας της επιχείρησης.

3.2 Ομάδες διαχείρισης κρίσεων

Οι ομάδες διαχείρισης κρίσεων αναλαμβάνουν το σχεδιασμό της κρίσης πριν εμφανιστεί και διαχειρίζονται τα προβλήματα που αναδύονται κατά τη διάρκειά της (Pearson and Clair, 1998). Οι ενέργειές τους δεν είναι τίποτα άλλο από αναλύσεις ρίσκου οι οποίες εφαρμόζονται στη διοίκηση της ασφάλειας των πληροφοριών και στη διοίκηση της επιχειρησιακής συνέχειας του οργανισμού. Η ανάλυση ρίσκου είναι περισσότερο χρήσιμη όταν διεξάγεται κατά τη διάρκεια του πλάνου κρίσης διότι πιθανές απώλειες αναγνωρίζονται νωρίς και τίθενται ευθύς εξαρχής οι απαιτήσεις της επιχειρησιακής συνέχειας. Είναι απαραίτητο να συσταθεί ομάδα διαχείρισης της κρίσης πριν το πλάνο της αναπτυχθεί, καθώς η διοίκηση είναι πιο ανήσυχη εάν

εμφανιστεί η κρίση και δεν υπάρχει η κατάλληλη ομάδα να την αντιμετωπίσει. Πολλοί ακόμα υποστηρίζουν (Fink, 2000) ότι στις επιχειρήσεις που δεν είχαν αναπτύξει σχέδιο αντιμετώπισης της κρίσης, η κρίση διήρκησε 3,5 φορές περισσότερο από τις επιχειρήσεις που είχαν αναπτύξει σχέδιο.

Η σπουδαιότητα των ομάδων διαχείρισης κρίσεων πηγάζει από δύο βασικούς παράγοντες. Πρώτον, ο καλύτερος τρόπος να βοηθηθεί μια επιχείρηση να απομονωθεί από τις καταστροφικές συνέπειες μιας κρίσης είναι να καλλιεργηθεί κουλτούρα διαχείρισης κρίσεων. Η καλλιέργεια μιας τέτοιας κουλτούρας είναι ευθύνη της ανώτερης διοίκησης (Caponigro, 2000) και οδηγεί στο σχεδιασμό του γεγονότος του κινδύνου και στο σχηματισμό της ομάδας. Δεύτερον, πολλές φορές η κρίση προκαλείται όταν η διοίκηση δε λαμβάνει υπόψη τις προειδοποιήσεις του κινδύνου που μπορούν να υπάρξουν (Smith, 1990). Το ίδιο το προσωπικό μπορεί να συμβάλλει προς τη σωστή κατεύθυνση σε αυτή την περίπτωση και να βοηθήσει τη διοίκηση στην προετοιμασία της αντιμετώπισης του κινδύνου.

3.3 Συχνές παραλείψεις στην εμφάνιση της κρίσης

Αν και η ενημέρωση σχετικά με τα θέματα ασφάλειας έχει αυξηθεί τα τελευταία χρόνια, πολλές επιχειρήσεις συνεχίζουν να πραγματοποιούν μια σειρά από λάθη στην προσπάθειά τους να αντιμετωπίζουν έναν κίνδυνο (McConnell, 2002). Τα λάθη αυτά ταξινομούνται ως εξής:

- *Υποτίμηση πληροφοριών.* Λίγες είναι εκείνες οι επιχειρήσεις που έχουν κατανοήσει την αξία των πληροφοριών τους.
- *Στενά ορισμένα όρια ασφάλειας.* Οι περισσότερες επιχειρήσεις δίνουν έμφαση στην ασφάλεια των εσωτερικών δικτύων τους και αδυνατούν να

κατανοήσουν πρακτικές ασφάλειας σε σχέση με τους συνεργάτες τους στα πλαίσια της εφοδιαστικής αλυσίδας.

¥ *Διαχείριση του κινδύνου αφού έχει πραγματοποιηθεί.* Πολλές επιχειρήσεις ενεργούν μετά την εμφάνιση του γεγονότος κρίσης αντί να δίνουν έμφαση πριν την εμφάνισή του.

¥ *Απαρχαιωμένες διαδικασίες ασφάλειας.* Οι επιχειρήσεις σπάνια αναβαθμίζουν ή αλλάζουν τις πρακτικές ασφάλειας για να αντεπεξέλθουν σε νέες ανάγκες. Παράλληλα, σπάνια δίνουν έμφαση στην αναβάθμιση των γνώσεων και των ικανοτήτων του προσωπικού τους που σχετίζονται με θέματα της ασφάλειας των πληροφοριών.

¥ *Έλλειψη επικοινωνίας για θέματα ευθυνών απέναντι στην ασφάλεια.* Η ασφάλεια συχνά αντιμετωπίζεται ως ένα θέμα σχετικό μόνο με την τεχνολογία των πληροφοριών και όχι ως ένα γενικότερο οργανωσιακό πρόβλημα.

Με δεδομένες τις παραπάνω παραλείψεις, είναι σαφές ότι απαιτείται μια γενικότερη προσέγγιση για την ασφάλεια μιας ιστοσελίδας ηλεκτρονικού εμπορίου. Οι επιχειρήσεις θα πρέπει να εκτιμήσουν αναδυόμενες αδυναμίες και απειλές και οι χρήστες θα πρέπει να κατανοήσουν ότι η ασφάλεια της τεχνολογίας των πληροφοριών είναι το ίδιο σημαντική με οποιαδήποτε άλλη μορφή ασφάλειας και να υιοθετήσουν υπεύθυνη συμπεριφορά. Η ανώτερη διοίκηση πρέπει να υποστηρίξει ένθερμα την ανάγκη της ασφάλειας των πληροφοριακών συστημάτων, μιας και αποτελεί απαρχή της καλής οργάνωσης της επιχείρησης. Οι επιχειρήσεις που έχουν πολύ καλές πρακτικές ασφάλειας βασίζονται σε ένα πλάνο διαχείρισης κρίσεων το οποίο καθορίζει τις συγκεκριμένες ανάγκες τους (Kay, 2003).

3.4 Στάδια διαχείρισης κρίσεων

Η διαχείριση κρίσεων περιλαμβάνει τις διαδικασίες εκείνες που ασχολούνται με τον προσδιορισμό, την ανάλυση και την απόκριση σε κινδύνους (PMBOK, 2004).

Ειδικότερα οι διαδικασίες αυτές είναι οι εξής:

3.4.1 Αναγνώριση του κινδύνου

Η αναγνώριση του κινδύνου δεν είναι τίποτα άλλο από τον προσδιορισμό του κινδύνου ο οποίος ενδέχεται να έχει αρνητική επίδραση για την επιχείρηση. Πολλοί υποστηρίζουν (Simbo, 1993) ότι ένας από τους βασικούς λόγους που οι επιχειρήσεις δεν έχουν αποτελεσματικά σχέδια διαχείρισης κρίσεων είναι το γεγονός ότι δεν έχουν αναγνωρίσει τους κινδύνους που τις απειλούν. Έτσι δεν έχουν αναπτύξει τα εργαλεία εκείνα που οδηγούν στη δημιουργία σχεδίων αποτελεσματικών για τη διαχείριση κρίσιμων καταστάσεων. Κατά το Fink (2000) η αναγνώριση του κινδύνου είναι σημαντική για δύο λόγους. Πρώτον, όταν ένας κίνδυνος είναι κατάλληλα ορισμένος, είναι εύκολο για κάποιον να μπορέσει να τον διαχειριστεί. Δεύτερον, ο προσδιορισμός του κινδύνου επιτρέπει στα στελέχη να ορίσουν το βαθμό της επιρροής τους στο επιθυμητό αποτέλεσμα. Επειδή οι κίνδυνοι γενικά ακολουθούνται από ποικιλία προβλημάτων είναι σημαντικό για τα στελέχη να μπορούν να εστιάζουν στον πυρήνα του αληθινού προβλήματος και να μην παρασύρονται από τα υπόλοιπα.

Αξίζει να σημειωθεί ότι για να αναγνωριστεί ένα γεγονός ως κίνδυνος θα πρέπει πρώτα η επιχείρηση να ορίσει την αξία των περιουσιακών της στοιχείων είτε αυτά είναι πληροφορίες, είτε δίκτυα. Λέγοντας αξία των περιουσιακών στοιχείων εννοεί κανείς το κόστος απόκτησης, το κόστος συντήρησης, το κόστος αντικατάστασης καθώς επίσης και το κόστος που περικλείεται στην περίπτωση που το περιουσιακό στοιχείο ανατεθεί σε κάποια άλλη οντότητα. Από τη στιγμή λοιπόν που τα

περιουσιακά στοιχεία έχουν αναγνωριστεί και κατηγοριοποιηθεί η επιχείρηση είναι σε θέση να εντοπίσει τις απειλές, τις αδυναμίες και τους κινδύνους που περικλείονται σε αυτά (Turban, 2006).

3.4.2 Ανάλυση του κινδύνου

Αφού η επιχείρηση έχει εντοπίσει τα κρίσιμα περιουσιακά της στοιχεία, είναι έτοιμη να αναλύσει τους κινδύνους που τα απειλούν. Η ανάλυση περιλαμβάνει τον ορισμό των απειλών, των αδυναμιών και των κινδύνων. Η αλληλεπίδραση των απειλών με τις αδυναμίες παράγουν τον κίνδυνο. Στις απειλές εντάσσονται οι φυσικές καταστροφές, η δυσλειτουργία του εξοπλισμού, οι ίδιοι οι εργαζόμενοι της επιχείρησης, οι εισβολείς όπως hackers, crackers, οι τρομοκρατικές επιθέσεις κ.ά. Οι αδυναμίες είναι εκείνα τα σημεία των περιουσιακών στοιχείων τα οποία είναι επιρρεπή σε πιθανές απειλές. Οι αδυναμίες προκύπτουν καθώς το διαδίκτυο αναπτύσσεται με γεωμετρική πρόοδο σε καθημερινή βάση. Σύμφωνα με το SANS Institute[20] οι λόγοι για τους οποίους οι αδυναμίες συνεχίζουν να υπάρχουν είναι οι εξής:

- 1,2 εκατομμύρια νέοι υπολογιστές προστίθενται στο Διαδίκτυο κάθε μήνα.
- Υπάρχει έλλειψη ειδικών σε θέματα ασφάλειας για να αντιμετωπίσουν το πρόβλημα.

Οι κίνδυνοι περιλαμβάνουν τις πιθανότητες των αδυναμιών να εκτεθούν σε πολλαπλές απειλές καθώς επίσης και τις πιθανές χρηματοοικονομικές απώλειες που προέρχονται από την έκθεση. Ο κίνδυνος αφορά κυρίως στην εμπιστευτικότητα, στην ακεραιότητα και στη διαθεσιμότητα των πληροφοριών. Ο κίνδυνος της

[20] http://www.sans.org/

εμπιστευτικότητας συμβαίνει όταν κάτι το οποίο είναι ευαίσθητη και ιδιωτική πληροφορία μετατρέπεται σε θέμα ευρέως γνωστό. Η ακεραιότητα χάνεται όταν η διοίκηση χάνει και αυτή την εμπιστοσύνη της. Σε ό,τι αφορά στη διαθεσιμότητα, ο κίνδυνος εμφανίζεται όταν υπάρχει άρνηση πρόσβασης ή εξυπηρέτησης από το ίδιο το σύστημα. Ένας τρόπος να εκτιμήσει η επιχείρηση τις απειλές και τις αδυναμίες της είναι να βασιστεί στη γνώση των στελεχών της στον τομέα της τεχνολογίας των πληροφοριών ή να χρησιμοποιήσει έναν εξωτερικό συνεργάτη όπως για παράδειγμα τη Granite Systems[21] για να διεξάγει μια μελέτη εκτίμησης της ασφάλειας. Ένας άλλος τρόπος είναι η χρήση κατάλληλου λογισμικού το οποίο ανιχνεύει αδυναμίες ή καθιστά την επιχείρηση να αντιμετωπίζει και να μελετά με ασφάλεια τις επιθέσεις καθώς αυτές συμβαίνουν (Turban, 2006).

3.4.2.1 Ποσοτική ανάλυση του κινδύνου[22]

Η ανάλυση του κινδύνου είναι είτε *ποσοτική*, είτε *ποιοτική* και πραγματοποιείται πριν από την εμφάνισή του. Στην *ποσοτική* ανάλυση ο στόχος είναι ο υπολογισμός της αξίας των κρίσιμων περιουσιακών στοιχείων της επιχείρησης. Για παράδειγμα, προσπαθεί κανείς να υπολογίσει την αξία ενός περιουσιακού στοιχείου σε όρους κόστους αντικατάστασης, σε όρους χαμένης παραγωγικότητας ή σε όρους κακής φήμης της επιχείρησης. Ωστόσο υπάρχουν κάποιες αδυναμίες στο συγκεκριμένο τύπο ανάλυσης. Για παράδειγμα, δεν μπορεί κάποιος να υπολογίσει με ακρίβεια την επίδραση που θα είχε ένα απρόσμενο γεγονός στη φήμη και το κύρος της επιχείρησης. Κάποιοι βασίζονται σε ιστορικά στοιχεία τα οποία δεν είναι πάντα διαθέσιμα. Επιπλέον επιχειρήσεις που έχουν χρησιμοποιήσει αυτόν τον τύπο ανάλυσης, τον βρίσκουν εξαιρετικά δαπανηρό και χρονοβόρο. Τέτοια σχέδια

[21] http://www.granitesystems.net
[22] http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx

εργασίας χρειάζονται μεγάλο χρονικό διάστημα για να ολοκληρωθούν και εμπεριέχουν συχνά διαφωνίες ανάμεσα στους συμμετέχοντες για τον υπολογισμό της αξίας των περιουσιακών στοιχείων. Ακόμα σε επιχειρήσεις που η αξία των περιουσιακών τους στοιχείων είναι μεγάλη, το κόστος έκθεσης σε οποιαδήποτε απειλή μπορεί να είναι τόσο υψηλό που να χρειάζεται να δαπανήσουν σημαντικά ποσά για την ελαχιστοποίηση του κινδύνου στον οποίο εκτίθενται. Βέβαια κάτι τέτοιο δεν είναι ρεαλιστικό με την έννοια ότι καμία επιχείρηση δε θα δαπανούσε τον προϋπολογισμό της για να προστατεύσει ένα ή πέντε από τα πιο κρίσιμα περιουσιακά της στοιχεία.

Είναι σημαντικό να μπορέσει κάποιος να κατανοήσει την ποσοτική ανάλυση των κινδύνων. Τα μεγέθη τα οποία υπολογίζονται κατά τη διεξαγωγή της ποσοτικής ανάλυσης αφορούν στην αξία των περιουσιακών στοιχείων της επιχείρησης, στο κόστος των ελέγχων, στον ορισμό της απόδοσης της επένδυσης σε σχέση με την ασφάλεια (Return on Security Investment-ROSI), στον υπολογισμό των τιμών της στιγμιαίας αναμενόμενης απώλειας (Single Loss Expectancy-SLE), του ετήσιου ποσοστού εμφάνισης του κινδύνου (Annual Rate of Occurrence-ARO) και της ετήσιας αναμενόμενης απώλειας (Annual Loss Expectancy-ALE).

Στη συνέχεια ακολουθεί διεξοδική ανάλυση των παραπάνω μεγεθών που μετρώνται στην ποσοτική ανάλυση των κινδύνων ενός ηλεκτρονικού καταστήματος και βάσει αυτών, η διοίκηση της επιχείρησης, οδηγείται στη λήψη των κατάλληλων αποφάσεων και στην υλοποίησή τους.

Αξία περιουσιακών στοιχείων της επιχείρησης. Ο ορισμός της αξίας ενός περιουσιακού στοιχείου είναι σημαντικό κομμάτι της διαχείρισης κρίσεων. Τα στελέχη συχνά βασίζονται στην αξία ενός περιουσιακού στοιχείου για να ορίσουν τα χρήματα και το χρόνο που απαιτούνται για την ασφάλειά του. Πολλές επιχειρήσεις

διατηρούν μια λίστα με τις αξίες των περιουσιακών στοιχείων τους ως μέρος του σχεδίου της επιχειρησιακής τους συνέχειας (business continuity plan). Παρόλα αυτά οι αριθμητικές τιμές των αξιών αποτελούν εκτιμήσεις μιας και δεν υπάρχει αντικειμενική μέθοδος προσδιορισμού των. Για να προσεγγίσει κανείς την αξία ενός περιουσιακού στοιχείου χρειάζεται να υπολογίσει τους ακόλουθους τρεις παράγοντες:

☺ *Τη συνολική αξία του περιουσιακού στοιχείου στην επιχείρηση*. Η διαδικασία αυτή περιλαμβάνει τον υπολογισμό της αξίας του περιουσιακού στοιχείου σε απευθείας χρηματοοικονομικούς όρους. Για παράδειγμα, ας αναλογιστεί κάποιος την επίδραση μιας προσωρινής διακοπής σε μια ιστοσελίδα ηλεκτρονικού καταστήματος που σε κανονικές συνθήκες λειτουργεί 7 ημέρες την εβδομάδα, 24 ώρες την ημέρα δημιουργώντας κατά μέσο όρο 2.000 € την ώρα έσοδα από τις παραγγελίες των πελατών. Μπορεί λοιπόν κανείς να συμπεράνει ότι η αξία της ιστοσελίδας σε ετήσια βάση σε όρους εσόδων από τις πωλήσεις είναι 17.520.000 €.

☺ *Την άμεση χρηματοοικονομική επίδραση όταν χάνεται ένα περιουσιακό στοιχείο*. Εάν απλοποιηθεί περαιτέρω το παραπάνω παράδειγμα και υποτεθεί ότι η ιστοσελίδα δημιουργεί σταθερό έσοδο την ώρα, τότε παραμένοντας εκτός λειτουργίας για 6 ώρες η υπολογίσιμη έκθεση σε κίνδυνο είναι 0,000685 ή 0,0685% το έτος. Πολλαπλασιάζοντας το ποσοστό αυτό της έκθεσης με την ετήσια αξία του περιουσιακού στοιχείου, μπορεί να προβλεφθεί ότι οι άμεσες απώλειες σε αυτή την περίπτωση θα είναι περίπου 12.000 €. Στην πραγματικότητα, τα περισσότερα ηλεκτρονικά καταστήματα δημιουργούν έσοδα από μια μεγάλη ποικιλία παραγόντων η οποία εξαρτάται από τη συγκεκριμένη ώρα της ημέρας, τη συγκεκριμένη ημέρα της εβδομάδας, τη συγκεκριμένη εποχή, τη διαφημιστική καμπάνια που έχει εφαρμόσει η επιχείρηση. Ταυτόχρονα κάποιοι πελάτες μπορεί να προτιμήσουν κάποιον ανταγωνιστή και συνεπώς το ηλεκτρονικό κατάστημα θα χάσει μέρος της

επισκεψιμότητάς του. Λαμβάνοντας υπόψη τους παραπάνω παράγοντες ο υπολογισμός της απώλειας των εσόδων είναι αρκετά περίπλοκος για κάποιον που θέλει να είναι εξαιρετικά ακριβής.

☺ *Την έμμεση επίδραση στην επιχείρηση όταν χάνεται ένα περιουσιακό στοιχείο*. Αν στο προηγούμενο παράδειγμα υποτεθεί ότι η επιχείρηση δαπανά 10.000 € για τη διαφημιστική της καμπάνια προκειμένου να αντιμετωπίσει την αρνητική δημοσιότητα και η απώλεια στα ετήσια έσοδά της είναι 0,01 ή 1% ή 175.200 €, τότε συνδυάζοντας τα επιπλέον έξοδα για τη διαφημιστική καμπάνια μαζί με την απώλεια στα ετήσια έσοδα από τις πωλήσεις, μπορεί να προβλέψει κάποιος ότι οι συνολικές έμμεσες απώλειες σε αυτή την περίπτωση θα είναι 185.200 €.

Προσδιορισμός της στιγμιαίας αναμενόμενης απώλειας (SLE). Η στιγμιαία αναμενόμενη απώλεια είναι το συνολικό ποσό των εσόδων το οποίο χάνεται από μια μεμονωμένη εμφάνιση του κινδύνου. Πρόκειται για το ποσό το οποίο αποδίδεται σε ένα μεμονωμένο γεγονός που αντιπροσωπεύει την πιθανή απώλεια της επιχείρησης εάν μια συγκεκριμένη απειλή εκμεταλλευτεί μια αδυναμία. Η στιγμιαία αναμενόμενη απώλεια υπολογίζεται εάν πολλαπλασιαστεί η αξία του περιουσιακού στοιχείου με τον παράγοντα έκθεσης (exposure factor-EF) στον κίνδυνο. Ο παράγοντας έκθεσης στον κίνδυνο αντιπροσωπεύει το ποσοστό της απώλειας που η απειλή προκαλεί στο συγκεκριμένο περιουσιακό στοιχείο. Εάν για παράδειγμα, στην ιστοσελίδα ενός ηλεκτρονικού καταστήματος ένα περιουσιακό στοιχείο έχει αξία 1.000 € και η εμφάνιση φωτιάς προκαλεί την απώλεια του 25% αυτής της αξίας, τότε η στιγμιαία αναμενόμενη απώλεια σε αυτή την περίπτωση είναι 250 €. Πρόκειται βέβαια για ένα απλοποιημένο παράδειγμα καθώς και άλλες δαπάνες θα πρέπει να ληφθούν υπόψη.

Προσδιορισμός του ετήσιου ποσοστού εμφάνισης του κινδύνου (ARO). Το ετήσιο ποσοστό εμφάνισης του κινδύνου προσδιορίζει τη συχνότητα εμφάνισης του

κινδύνου κατά τη διάρκεια ενός έτους. Ο υπολογισμός του συγκεκριμένου μεγέθους είναι δύσκολος διότι υπάρχουν λίγα διαθέσιμα δεδομένα τα οποία αποτελούν εμπιστευτικές πληροφορίες ασφαλιστικών εταιριών. Τον υπολογισμό αυτού του μεγέθους αναλαμβάνουν εταιρίες συμβούλων στα πλαίσια της ανάλυσης ρίσκου που πραγματοποιούν για τις επιχειρήσεις που τους τις αναθέτουν. Χαρακτηριστικό παράδειγμα είναι η εταιρία Space[23] που πραγματοποίησε πρόσφατα (τον Απρίλιο του 2006) ανάλυση ρίσκου για λογαριασμό της εταιρίας Vivodi Telecom. Η τιμή του ARO κυμαίνεται από 0% έως 100%.

Προσδιορισμός της ετήσιας αναμενόμενης απώλειας (ALE). Η ετήσια αναμενόμενη απώλεια είναι το συνολικό χρηματικό ποσό που η επιχείρηση θα χάσει σε ένα έτος εάν δεν γίνει τίποτα για την ελαχιστοποίηση του κινδύνου. Η ετήσια αναμενόμενη απώλεια υπολογίζεται από τον πολλαπλασιασμό της στιγμιαίας αναμενόμενης απώλειας με το ετήσιο ποσοστό εμφάνισης του κινδύνου. Δηλαδή ALE = SLE * ARO. Για παράδειγμα, αν η φωτιά στην ιστοσελίδα ενός ηλεκτρονικού καταστήματος προκαλέσει απώλεια της τάξης των 250 € και η πιθανότητα εμφάνισης της φωτιάς είναι 0,1 δηλαδή ARO = 0,1 που σημαίνει η φωτιά εμφανίζεται κάθε 10 έτη, τότε η τιμή της ετήσιας αναμενόμενης απώλειας θα είναι ALE = 25 € (250 € * 0,1 = 25 €). Ο προσδιορισμός της τιμής του συγκεκριμένου μεγέθους έχει μεγάλη σημασία για μια επιχείρηση διότι της δίνει τη δυνατότητα να εκτιμήσει το κόστος των μέτρων ασφαλείας που χρειάζεται να λάβει για να έχει επαρκές επίπεδο προστασίας. Στη συγκεκριμένη περίπτωση η επιχείρηση χάνει 25 € ή και λιγότερα το έτος. Γνωρίζοντας λοιπόν αυτό η επιχείρηση είναι σε θέση να υπολογίσει το κόστος εφαρμογής ενδεχόμενης προστασίας απέναντι στις επιπτώσεις της απειλής.

[23] http://www.space.gr

Προσδιορισμός του κόστους των ελέγχων. Για τον προσδιορισμό του κόστους των ελέγχων απαιτείται η ακριβής εκτίμηση του ποσού απόκτησης, διατήρησης, λειτουργίας, ανάπτυξης, εφαρμογής κάθε επιπέδου ελέγχου. Τέτοια ποσά είναι κόστη που αφορούν στην απόκτηση (αγορά) του επιπέδου ελέγχου, στη διατήρησή του, στη μέτρησή του (απόδοσή του), στην εκπαίδευση των στελεχών πάνω στο συγκεκριμένο επίπεδο ελέγχου και στην απώλεια της παραγωγικότητας που ενδέχεται αυτό να προκαλέσει στην επιχείρηση. Στο παραπάνω παράδειγμα, για να μειωθεί ο κίνδυνος της φωτιάς η επιχείρηση μπορεί να εγκαταστήσει ένα αυτόματο σύστημα καταστολής της. Θα χρειαστεί να προσλάβει κάποιον ειδικό για να σχεδιάσει και να εγκαταστήσει το σύστημα και στη συνέχεια να μετρήσει την απόδοσή του. Ο έλεγχος του συστήματος θα πρέπει να γίνεται σε περιοδική βάση και περιστασιακά, τροφοδοτώντας το με κάθε λογής χημικά επιβραδυντικά που το σύστημα χρησιμοποιεί.

Προσδιορισμός της απόδοσης της επένδυσης σε σχέση με την ασφάλεια (ROSI). Η απόδοση της επένδυσης σε σχέση με την ασφάλεια υπολογίζεται αν από την ετήσια αναμενόμενη απώλεια πριν την εφαρμογή συστήματος ελέγχου αφαιρεθεί η ετήσια αναμενόμενη απώλεια μετά την εφαρμογή του συστήματος ελέγχου και το ετήσιο κόστος του συστήματος ελέγχου. Τα προηγούμενα φαίνονται στην ακόλουθη σχέση: ROSI = (ALE before control) – (ALE after control) – (annual cost of control). Για παράδειγμα, αν η ετήσια αναμενόμενη απώλεια που προκαλεί ένας εισβολέας όταν θέτει εκτός λειτουργίας έναν δικτυακό εξυπηρετητή είναι 12.000 € και μετά την εφαρμογή συστήματος ασφαλείας είναι 3.000 € καθώς και το ετήσιο κόστος συντήρησης και λειτουργίας του συστήματος ασφαλείας είναι 650 €, τότε η απόδοση της επένδυσης είναι 8.350 € το έτος (ROSI = 12.000 – 3.000 – 650 = 8.350 €)

Από τα παραπάνω συνάγεται ότι από την ποσοτική ανάλυση του κινδύνου πηγάζουν τα ακόλουθα:

- Η αξία σε χρηματικές μονάδες των περιουσιακών στοιχείων.
- Μια λίστα με συγκεκριμένες απειλές.
- Η πιθανότητα εμφάνισης κάθε απειλής.
- Η πιθανή απώλεια για την επιχείρηση από την εμφάνιση απειλής σε ετήσια βάση.
- Προτεινόμενα μέτρα ασφάλειας, ελέγχου και δράσης.

Ωστόσο ο υπολογισμός των παραπάνω μεγεθών είναι υποκειμενικός και βασίζεται στις εκτιμήσεις των ατόμων που πραγματοποιούν την ανάλυση ύστερα από πολλές συζητήσεις και συμβιβασμούς.

3.4.2.2 Ποιοτική ανάλυση του κινδύνου

Αυτό που διαχωρίζει την ποιοτική ανάλυση του κινδύνου από την ποσοτική είναι ότι ο αναλυτής στην ποιοτική ανάλυση δεν προσπαθεί να εκφράσει σε αυστηρά χρηματοοικονομικούς όρους την αξία των περιουσιακών στοιχείων, τις αναμενόμενες απώλειες και τα κόστη των ελέγχων. Αυτό που χρησιμοποιεί είναι σχετικές αξίες. Η ανάλυση ρίσκου συνήθως διεξάγεται μέσω ερωτηματολογίων και σχεδίων εργασίας στα οποία συμμετέχουν πλήθος ομάδων από τα διαφορετικά τμήματα μιας επιχείρησης. Τα ερωτηματολόγια διανέμονται μερικές ημέρες ή εβδομάδες πριν την έναρξη ενός σχεδίου εργασίας και είναι σχεδιασμένα με σκοπό να ανακαλύψουν το είδος των περιουσιακών στοιχείων και των συστημάτων ελέγχου τα οποία ήδη έχουν αναπτυχθεί στην επιχείρηση, καθώς αποτελούν χρήσιμες πληροφορίες για τις ομάδες εργασίας που ακολουθούν. Οι συμμετέχοντες στα σχέδια εργασίας αναγνωρίζουν τα περιουσιακά στοιχεία και τους αποδίδουν σχετικές αξίες. Στη συνέχεια προσπαθούν

να ανακαλύψουν το είδος των απειλών που ένα περιουσιακό στοιχείο ενδέχεται να αντιμετωπίζει, και τότε προσπαθούν να φανταστούν τις αδυναμίες που η απειλή θα ενεργοποιήσει στο μέλλον. Οι ειδικοί στην ασφάλεια των πληροφοριών καθώς και οι διαχειριστές συστημάτων συνήθως επινοούν συστήματα ελέγχων για την ελαχιστοποίηση των κινδύνων λαμβάνοντας υπόψη και το κόστος αυτών των συστημάτων. Τα αποτελέσματα αυτά δίδονται στη διοίκηση για μελέτη στα πλαίσια της ανάλυσης κόστους-οφέλους.

3.4.2.3 Σύγκριση ποσοτικής & ποιοτικής ανάλυσης

Από τα παραπάνω φαίνεται πως η ποιοτική ανάλυση στα βασικά της σημεία έχει κοινά στοιχεία με την ποσοτική ανάλυση. Η διαφορά έγκειται σε λεπτομέρειες. Οι συγκρίσεις ανάμεσα στην αξία ενός περιουσιακού στοιχείου και ενός άλλου είναι σχετικές όπως αναφέρθηκε στην ποιοτική ανάλυση και οι συμμετέχοντες δεν αφιερώνουν πολύ χρόνο στον υπολογισμό της αξίας των περιουσιακών στοιχείων σε αυστηρά χρηματοοικονομικούς όρους. Η ίδια διαδικασία ακολουθείται και στην περίπτωση του υπολογισμού της πιθανής επίδρασης ενός κινδύνου και του κόστους εφαρμογής συστήματος ελέγχου.

Η ποιοτική ανάλυση πρόκειται για λιγότερο απαιτητική διαδικασία για το προσωπικό μιας επιχείρησης, αφού δεν υπολογίζει με ακρίβεια χρηματοοικονομικά μεγέθη. Τα σχέδια εργασίας της ποιοτικής ανάλυσης ξεκινούν να δείχνουν τα αποτελέσματα μέσα σε διάρκεια μερικών εβδομάδων, ενώ πολλές επιχειρήσεις που επιλέγουν την ποσοτική ανάλυση βλέπουν τα αποτελέσματά της ύστερα από μήνες και μερικές έτη, προσπαθειών. Ωστόσο το μειονέκτημα της ποιοτικής ανάλυσης, όπως έχει ήδη αναφερθεί, είναι ότι τα αποτελέσματά της είναι αχανή και μερικοί υπεύθυνοι στη λήψη αποφάσεων, κυρίως εκείνοι με χρηματοοικονομικό υπόβαθρο,

δεν αισθάνονται άνετα με τις σχετικές αξίες που προσδιορίζονται κατά τη διάρκειά της.

Και οι δύο αναλύσεις λοιπόν, η ποσοτική και η ποιοτική, έχουν τα πλεονεκτήματα και τα μειονεκτήματά τους. Συγκεκριμένες καταστάσεις, πολλές φορές, αναγκάζουν τις επιχειρήσεις να χρησιμοποιήσουν την ποσοτική ανάλυση. Παράλληλα, επιχειρήσεις μικρού μεγέθους και με περιορισμένους πόρους βρίσκουν την ποιοτική ανάλυση να τους ταιριάζει περισσότερο. Ο ακόλουθος πίνακας παρουσιάζει τα πλεονεκτήματα και τα μειονεκτήματα της κάθε μεθόδου ανάλυσης.

Πίνακας 3 : Πλεονεκτήματα και Μειονεκτήματα ποσοτικής & ποιοτικής ανάλυσης

	Ποσοτική ανάλυση	**Ποιοτική ανάλυση**
Πλεονεκτήματα	- Οι κίνδυνοι κατηγοριοποιούνται σύμφωνα με τη χρηματοοικονομική τους επίδραση και τα περιουσιακά στοιχεία σύμφωνα με τη χρηματοοικονομική τους αξία. - Τα αποτελέσματα της διοίκησης του κινδύνου φαίνονται στην απόδοση της επένδυσης. - Τα αποτελέσματα εκφράζονται με συγκεκριμένη ορολογία και οι πιθανότητες εκφράζονται με συγκεκριμένο ποσοστό.	- Παρέχει κατανόηση της κατηγοριοποίησης των κινδύνων. -Επιτυγχάνεται ευκολότερα η ομοφωνία. - Δεν είναι απαραίτητη η ποσοτικοποίηση της συχνότητας της απειλής. - Δεν είναι απαραίτητος ο ορισμός της χρηματοοικονομικής αξίας των περιουσιακών

	- Η ακρίβεια αυξάνεται διαχρονικά καθώς οι επιχειρήσεις εξασφαλίζουν ιστορικά στοιχεία μέσα από την εμπειρία τους.	στοιχείων. - Περιλαμβάνει άτομα τα οποία δεν είναι ειδικά σε θέματα ασφάλειας και υπολογιστών.
Μειονεκτήματα	- Οι αξίες που αποδίδονται στους κινδύνους βασίζονται σε υποκειμενική γνώμη των συμμετεχόντων. - Η διαδικασία για την κατάκτηση αξιόπιστων αποτελεσμάτων και ομοφωνίας είναι χρονοβόρα. - Οι υπολογισμοί είναι πολύπλοκοι και χρονοβόροι. - Τα αποτελέσματα εκφράζονται σε χρηματοοικονομικούς όρους μόνο και οι μη ειδικοί είναι δύσκολο να τους ερμηνεύσουν. - Η διαδικασία απαιτεί τεχνογνωσία.	- Μη επαρκής διαφοροποίηση ανάμεσα σε σημαντικούς κινδύνους. - Δυσκολία αιτιολογίας επένδυσης σε συγκεκριμένο σύστημα ελέγχου αφού δεν υπάρχει ανάλυση κόστους-οφέλους να βασιστεί. - Τα αποτελέσματα εξαρτώνται από την ομάδα διαχείρισης κρίσης που έχει σχηματιστεί.

Τα προηγούμενα έτη η ποσοτική ανάλυση κυριαρχούσε στην ανάλυση ρίσκου, ωστόσο αυτό έχει αλλάξει πρόσφατα, αφού έχει παρατηρηθεί από μελετητές ότι η ποσοτική ανάλυση καταλήγει σε δύσκολα, μακροχρόνια σχέδια εργασίας χωρίς χειροπιαστά οφέλη. Αυτό που πραγματοποιούν πλέον πολλές επιχειρήσεις είναι ο

συνδυασμός των δύο τύπων ανάλυσης, εκμεταλλευόμενες βέβαια τα πλεονεκτήματα του καθενός.

Σε ό,τι αφορά στους δικτυακούς τόπους γίνεται είτε συνδυασμός των δύο τύπων ανάλυσης αποκομίζοντας τα οφέλη του καθενός, είτε ακολουθείται η ποσοτική ανάλυση αφού πολλές φορές ανατίθεται η πραγματοποίησή της σε εξειδικευμένους εξωτερικούς συνεργάτες (outsourcing) που διαθέτουν την απαιτούμενη τεχνογνωσία.

3.4.3 Απόκριση σε κινδύνους

Ο σχεδιασμός απόκρισης σε κινδύνους είναι η διαδικασία ανάπτυξης επιλογών και προσδιορισμού ενεργειών ώστε να βελτιωθούν οι ευκαιρίες και να μειωθούν οι κίνδυνοι. Έπεται της ποσοτικής και ποιοτικής ανάλυσης και εξετάζει τους κινδύνους κατά προτεραιότητα. Οι σχεδιασμένες αποκρίσεις σε κινδύνους πρέπει να είναι κατάλληλες προς τη σοβαρότητα του κινδύνου, να είναι αποτελεσματικές ως προς το κόστος τους και συμφωνημένες από όλα τα εμπλεκόμενα μέρη. Οι κίνδυνοι περιλαμβάνουν απειλές και ευκαιρίες που επηρεάζουν τη λειτουργία της επιχείρησης. Αρκετές στρατηγικές απόκρισης σε κινδύνους είναι διαθέσιμες. Για κάθε κίνδυνο θα πρέπει να επιλέγεται η στρατηγική ή το μίγμα στρατηγικών που δείχνει πιο αποτελεσματικό για αυτόν. Οι στρατηγικές ανάλογα με τη φύση του κινδύνου είναι οι ακόλουθες:

3.4.3.1 Στρατηγικές για αρνητικούς κινδύνους ή απειλές

Τρεις στρατηγικές συνήθως ασχολούνται με απειλές ή με κινδύνους που μπορούν να έχουν αρνητικές επιπτώσεις στη λειτουργία της επιχείρησης. Οι στρατηγικές αυτές είναι η αποφυγή, η μεταβίβαση και ο μετριασμός.

Αποφυγή. Ένας τρόπος αντιμετώπισης ενός κινδύνου είναι η αποφυγή του κινδύνου, δηλαδή η αποφυγή του παράγοντα που είναι εκτεθειμένος στον κίνδυνο. Ο παράγοντας αυτός μπορεί να είναι ένα περιουσιακό στοιχείο, μια δραστηριότητα ή ένα πρόσωπο. Η αποφυγή του κινδύνου γίνεται με άρνηση ή με εγκατάλειψη. Κατά την άρνηση η επιχείρηση αρνείται να αναλάβει έναν παράγοντα ο οποίος είναι εκτεθειμένος στον κίνδυνο και κατά την εγκατάλειψη η επιχείρηση εγκαταλείπει έναν τέτοιο παράγοντα τον οποίο έχει ήδη αναλάβει.

Η αποφυγή του κινδύνου θεωρείται ως η πλέον δραστική και αποτελεσματική τεχνική αντιμετώπισης του κινδύνου. Όταν η αποφυγή του κινδύνου γίνεται με άρνηση του παράγοντα ο οποίος είναι εκτεθειμένος στον κίνδυνο τότε η τεχνική αυτή περιλαμβάνει το κόστος ευκαιρίας, δηλαδή το κέρδος που δεν πραγματοποιήθηκε από την απώλεια μιας ευκαιρίας για κέρδος. Όταν όμως η αποφυγή του κινδύνου γίνεται με εγκατάλειψη ενός τέτοιου παράγοντα ο οποίος έχει ήδη αναληφθεί, τότε η αποφυγή του κινδύνου περιλαμβάνει το κόστος ανάληψης του παράγοντα αυτού.

Η αποφυγή του κινδύνου με άρνηση ή εγκατάλειψη του σχετικού παράγοντα πρέπει να διαχωρίζεται από τις τεχνικές αντιμετώπισης της ζημιάς. Σύμφωνα με τις τεχνικές αυτές, η επιχείρηση διατηρεί το περιουσιακό στοιχείο, το πρόσωπο ή τη δραστηριότητα που δημιουργούν τον κίνδυνο και συνεχίζει να λειτουργεί με τον ασφαλέστερο δυνατό τρόπο.

Η αποφυγή του κινδύνου αποτελεί συνήθης τεχνική αντιμετώπισης του κινδύνου. Όταν η επιχείρηση εφαρμόζει την τεχνική αυτή για την αντιμετώπιση ενός κινδύνου είναι βέβαιο ότι η επιχείρηση δεν θα υποστεί τις συνέπειες του κινδύνου αυτού. Επειδή όμως κάθε κίνδυνος συνδέεται και με κάποια ωφέλεια αυτό σημαίνει ότι η εφαρμογή της αποφυγής του κινδύνου συνεπάγεται και την απώλεια της ωφέλειας

αυτής. Μερικοί παράγοντες οι οποίοι υπεισέρχονται στην εφαρμογή της τεχνικής αυτής είναι οι ακόλουθοι:

1) Η δυνατότητα εφαρμογής της αποφυγής του κινδύνου. Η εφαρμογή της αποφυγής του κινδύνου μπορεί να είναι αδύνατη. Όσο ευρύτερα ορίζεται ένας κίνδυνος τόσο δυσχερέστερα γίνεται η αποφυγή του κινδύνου αυτού. Ο μόνος τρόπος αποφυγής όλων των κινδύνων που συνδέονται με τη λειτουργία μιας επιχείρησης είναι η διακοπή της λειτουργίας της επιχείρησης αυτής.

2) Η απώλεια ωφελειών από την εφαρμογή της αποφυγής του κινδύνου. Η απασχόληση ενός προσώπου, η χρήση ενός περιουσιακού στοιχείου, η πραγματοποίηση μιας δραστηριότητας, που δημιουργούν κάποιον κίνδυνο, μπορεί να συνεπάγονται μεγαλύτερες ωφέλειες από τις ωφέλειες που προκύπτουν από την άρνηση ή εγκατάλειψη του προσώπου, του περιουσιακού στοιχείου ή της δραστηριότητας. Στην περίπτωση αυτή ο διαχειριστής κινδύνου δεν δίνει μεγάλη σημασία στην εφαρμογή της αποφυγής του κινδύνου. Η λειτουργία μιας επιχείρησης χωρίς τη χρήση ηλεκτρονικών υπολογιστών είναι δύσκολη ή σχεδόν αδύνατη. Επομένως η άρνηση ή εγκατάλειψη της χρήσης ηλεκτρονικών υπολογιστών είναι δύσκολη ή σχεδόν αδύνατη. Επομένως η άρνηση ή εγκατάλειψη της χρήσης ηλεκτρονικών υπολογιστών για την αποφυγή των σχετικών κινδύνων δεν έχει καμία πρακτική σημασία.

3) Η δημιουργία νέων κινδύνων από την εφαρμογή της αποφυγής του κινδύνου. Η αποφυγή ενός κινδύνου με άρνηση ή εγκατάλειψη του προσώπου, του περιουσιακού στοιχείου ή της δραστηριότητας που δημιουργούν τον κίνδυνο, μπορεί να συνεπάγεται ένα νέο κίνδυνο. Αν μια επιχείρηση δεν κάνει χρήση των ηλεκτρονικών υπολογιστών για να αποφύγει τους σχετικούς κινδύνους και κάνει χρήση άλλων

μεθόδων, τότε η επιχείρηση αναλαμβάνει τους νέους κινδύνους αυτών των μεθόδων (Αρτίκης, 2002).

Μεταβίβαση. Η μεταβίβαση κινδύνων απαιτεί τη μετάθεση των αρνητικών επιπτώσεων μιας απειλής σε ένα τρίτο μέρος. Η μεταβίβαση του κινδύνου απλά δίνει την ευθύνη για τη διαχείρισή του σε ένα τρίτο μέρος, όμως δεν απαλείφει τον κίνδυνο. Η μεταβίβαση των ευθυνών ενός κινδύνου είναι πιο αποτελεσματική κατά την αντιμετώπιση της έκθεσης σε οικονομικό κίνδυνο. Η μεταβίβαση του κινδύνου σχεδόν πάντα περιλαμβάνει πληρωμή ενός επιμισθίου (premium) για τον κίνδυνο προς το μέρος που τον αναλαμβάνει. Τα εργαλεία μεταβίβασης μπορεί να διαφέρουν και περιλαμβάνουν, χωρίς να περιορίζονται σε αυτά, το κόστος της ασφάλισης, ρήτρες απόδοσης, εγγυήσεις κ.ά. Ενδέχεται να χρησιμοποιηθούν συμβόλαια για τη μεταβίβαση των ευθυνών συγκεκριμένων κινδύνων σε ένα τρίτο μέρος.

Μετριασμός. Ο μετριασμός κινδύνου επιδιώκει τη μείωση της πιθανότητας ή των επιπτώσεων ενός γεγονότος κινδύνου. Η λήψη μέτρων για τη μείωση της πιθανότητας ή των επιπτώσεων εμφάνισης ενός κινδύνου, είναι συχνά πιο αποτελεσματική από την προσπάθεια αποκατάστασης των ζημιών αφού ο κίνδυνος έχει πραγματοποιηθεί. Η υιοθέτηση μη πολύπλοκων διαδικασιών ή η εκπόνηση περισσότερων δοκιμών αποτελούν παραδείγματα ενεργειών μετριασμού.

3.4.3.2 Στρατηγικές για θετικούς κινδύνους ή ευκαιρίες

Τρεις στρατηγικές προτείνονται για την αντιμετώπιση κινδύνων με δυνητικά θετικές επιπτώσεις στη λειτουργία μιας επιχείρησης. Οι στρατηγικές αυτές είναι η εκμετάλλευση, η κοινοχρησία και η βελτίωση.

Εκμετάλλευση. Η στρατηγική αυτή μπορεί να επιλεγεί για κινδύνους με θετικές επιπτώσεις όπου η επιχείρηση επιθυμεί να διασφαλίσει ότι θα υλοποιηθεί η ευκαιρία.

Η στρατηγική αυτή επιδιώκει να απαλείψει την αβεβαιότητα που σχετίζεται με έναν συγκεκριμένο ευνοϊκό κίνδυνο κάνοντας την ευκαιρία να συμβεί οπωσδήποτε.

Κοινοχρησία (share). Η κοινοχρησία ενός θετικού κινδύνου περιλαμβάνει τη διάθεση της κυριότητας σε ένα τρίτο μέρος το οποίο είναι περισσότερο ικανό να εκμεταλλευτεί την ευκαιρία προς όφελος της επιχείρησης. Παραδείγματα κοινοχρησίας ενεργειών περιλαμβάνουν το σχηματισμό ομάδων, εταιριών ειδικού σκοπού μοιρασιάς του κινδύνου, οι οποίες θεσπίζονται με αποκλειστικό σκοπό τη διαχείριση των ευκαιριών.

Βελτίωση. Η στρατηγική αυτή τροποποιεί το μέγεθος μιας ευκαιρίας αυξάνοντας την πιθανότητα ή τις θετικές επιπτώσεις και αναγνωρίζοντας και μεγιστοποιώντας τα κίνητρα για αυτούς τους κινδύνους με θετική επίδραση. Η επιδίωξη της διευκόλυνσης ή της ενδυνάμωσης της αιτίας της ευκαιρίας και η προληπτική στοχοποίηση και ενθάρρυνση των συνθηκών ενεργοποίησής της, μπορούν να αυξήσουν τις πιθανότητες. Πολλές φορές επιδιώκονται και κίνητρα επιπτώσεων τα οποία αυξάνουν την έκθεση της επιχείρησης στην ευκαιρία.

3.4.3.3 Στρατηγική για απειλές και ευκαιρίες

Αποδοχή. Μια στρατηγική που υιοθετείται διότι σπανίως είναι δυνατό να εξαλειφθούν όλοι οι κίνδυνοι που απειλούν μια επιχείρηση. Η τεχνική αυτή υποδεικνύει ότι η διοίκηση της επιχείρησης έχει αποφασίσει να μη μεταβάλει το σχέδιό της σχετικά με την αντιμετώπιση του κινδύνου ή ότι δεν έχει την ικανότητα να προσδιορίσει κάποια άλλη κατάλληλη στρατηγική αντιμετώπισης. Υιοθετείται τόσο για απειλές όσο και για ευκαιρίες και μπορεί να είναι είτε παθητική, είτε ενεργητική. Η παθητική αποδοχή δεν απαιτεί καμία ενέργεια, αφήνοντας το διαχειριστή του κινδύνου να αντιμετωπίσει τις απειλές ή τις ευκαιρίες καθώς συμβαίνουν. Η πιο

συνηθισμένη ενεργητική αποδοχή είναι η θέσπιση έκτακτου αποθέματος, περιλαμβανομένων ποσοτήτων για χρόνο, χρήμα ή πόρους προκειμένου να γίνει διαχείριση γνωστών ή ακόμη άγνωστων απειλών ή ευκαιριών.

3.4.3.4 Στρατηγική έκτακτης απόκρισης

Ορισμένες τεχνικές αντιμετώπισης του κινδύνου είναι σχεδιασμένες για χρήση μόνο αν συμβούν ορισμένα γεγονότα. Για ορισμένους κινδύνους, είναι απαραίτητο να κατασκευαστεί ένα σχέδιο απόκρισης το οποίο θα εκτελεστεί μόνο υπό ορισμένες προϋποθέσεις. Τέλος, γεγονότα που ενεργοποιούν την έκτακτη απόκριση θα πρέπει να ορίζονται και να παρακολουθούνται.

3.4.4 Παρακολούθηση και έλεγχος κινδύνων

Η παρακολούθηση και ο έλεγχος των κινδύνων είναι η διαδικασία του προσδιορισμού, της ανάλυσης και του σχεδιασμού νέων αναδυόμενων κινδύνων, της παρακολούθησης των ήδη αναγνωρισμένων κινδύνων και της εκ νέου ανάλυσης υπαρχόντων κινδύνων.

Μετά την ανάλυση των κινδύνων και την κατηγοριοποίησή τους σύμφωνα με την πιθανότητα εμφάνισης και τη πιθανή ζημία που προκαλούν, μια λίστα από μέτρα αντιμετώπισης προτείνονται και αξιολογούνται για τους κινδύνους υψηλής συχνότητας. Τα συγκεκριμένα μέτρα αντιμετώπισης εκτιμώνται σε όρους ανάλυσης κόστους-οφέλους - μιας και οποιαδήποτε επιχείρηση δε θα δαπανούσε π.χ. 50.000 € για ένα σύστημα ασφάλειας όταν η αξία του περιουσιακού στοιχείου για το οποίο θα εφαρμοζόταν ήταν 25.000 €- και σε σχέση με το ήδη υπάρχον σύστημα ασφάλειας. Ύστερα λοιπόν από την επιλογή του συστήματος ασφάλειας και την εφαρμογή του, η επιχείρηση χρειάζεται να ελέγξει, όχι μόνο την απόδοση και την αποτελεσματικότητά

του, αλλά συνεχώς την κατάσταση στην οποία βρίσκεται το περιουσιακό στοιχείο και τις απειλές, τις αδυναμίες και τους κινδύνους που ενδέχεται να εμφανιστούν (Turban, 2006).

3.5 Ο ρόλος της ασφάλισης και των ασφαλιστικών εταιριών

Η ασφάλιση δεν είναι τίποτα άλλο παρά η μεταβίβαση του κινδύνου σε μια άλλη οντότητα εκτός της επιχείρησης που φέρει τον κίνδυνο. Μερικές επιχειρήσεις υποστηρίζουν ότι δεν χρειάζεται να ανησυχούν σε έναν επικείμενο κίνδυνο διότι έχουν ασφαλιστική κάλυψη η οποία τις προστατεύει από πιθανή ζημία ή διακοπή εργασίας. Αν και το συγκεκριμένο επιχείρημα έχει κάποια αξία, η σημασία της ασφάλισης σε κατάσταση κρίσης είναι ανολοκλήρωτη. Η ανάλυση του Simbo (1993) για το ρόλο της ασφάλισης δείχνει ότι η ασφάλιση παρέχει προστασία για εκτεταμένες δαπανηρές εφαρμογές, αλλά, από μόνη της είναι ανεπαρκής σχετικά με την επιβίωση και την ανάκαμψη της επιχείρησης. Η ασφάλιση παρουσιάζει μια βασική αδυναμία. Δεν προστατεύει ενάντια της απώλειας της καλής φήμης, της μειωμένης παραγωγικότητας, του χαμηλού συναισθήματος ηθικής των εργαζομένων, του άγχους (Fink, 2000). Επίσης δεν παρέχει λύσεις σε προβλήματα δημοσίων σχέσεων και κοινωνικής ευθύνης που συνδέονται με την κρίση. Χαρακτηριστικό είναι πως στην Ελλάδα δεν υπάρχει ασφάλιση επιχειρηματικού λάθους. Στο εξωτερικό είναι πάρα πολύ αναπτυγμένη και καλείται Indemmnity Bond, καλύπτοντας ζημία πολλών δισεκατομμυρίων που έχει προκύψει από επιχειρηματικό λάθος (Αρτίκης, 2002).

Σε ό,τι αφορά στην ασφάλιση των δικτύων, των υπολογιστών και γενικότερα της επιχειρηματικής δραστηριότητας στα πλαίσια του ηλεκτρονικού εμπορίου, έχουν αναπτυχθεί διάφορα είδη συμβολαίων από ασφαλιστικές εταιρίες σε ολόκληρο τον

κόσμο. Ανάμεσά τους η ασφαλιστική εταιρία AIG (American International Group, Inc)[24] έχει διευρύνει το χαρτοφυλάκιο των προϊόντων της και έχει εισάγει λύσεις ασφάλισης η-επιχειρείν από το 2000 (AIG eBusiness Risk Solutions) που καλύπτουν κινδύνους που προέρχονται από επιθέσεις στον κυβερνοχώρο. Άλλες ασφαλιστικές εταιρίες που παρέχουν συμβόλαια σχετικά με την ασφάλεια των ηλεκτρονικών υπολογιστών είναι η Lloyds με το ασφαλιστήριο συμβόλαιο Computer Information and Data Security Insurance (CIDSI), η Zurich Financial Services Group που παρέχει το E-Risk Protection Program, η J&H March με το NetSecure (Reid and Floyd, 2001).

Στην Ελλάδα όμως τα πράγματα είναι λίγο διαφορετικά. Οι ασφαλιστικές εταιρίες που δραστηριοποιούνται στις παραδοσιακές ασφαλιστικές υπηρεσίες δεν επεκτείνουν τα συμβόλαιά τους σε μια ολοκληρωτική κάλυψη της λειτουργίας ενός ηλεκτρονικού καταστήματος με αποτέλεσμα αρκετοί τομείς επιχειρηματικής ευθύνης να μένουν εκτός ασφαλιστικής κάλυψης.

Τα ασφαλιστήρια συμβόλαιά τους στον τομέα των τεχνικών ασφαλειών καλύπτουν τον ηλεκτρονικό εξοπλισμό και ενδεχόμενες μηχανικές βλάβες. Στην ελληνική αγορά, κλάδο τεχνικών ασφαλειών παρέχει η Interamerican, η Commercial Value και η Ασπίς Πρόνοια. Σύμφωνα με την Κα Τουλίδα Μ., Προϊσταμένη Τεχνικών Ασφαλειών στην ασφαλιστική εταιρία Interamerican, η κάλυψη του συγκεκριμένου κλάδου αφορά στον τεχνολογικό, ηλεκτρονικό, μηχανολογικό εξοπλισμό και μόνο και δεν επεκτείνεται στην ανάληψη του η-επιχειρηματικού κινδύνου. Ευελπιστεί στο μέλλον να αναπτυχθεί ξεχωριστός ασφαλιστικός κλάδος η-επιχειρείν και στην Ελλάδα, παρόλο που εκφράζει μερικές ανησυχίες σχετικά με τη δυνατότητα των ελληνικών ηλεκτρονικών επιχειρήσεων να δαπανήσουν σημαντικά

[24] http://www.aig.com

χρηματικά ποσά για την αποτίμηση του κινδύνου τους και την αγορά της κατάλληλης ασφαλιστικής κάλυψης. Επιπλέον θεωρεί πως αυτή τη στιγμή οι ελληνικές ηλεκτρονικές επιχειρήσεις δεν έχουν το κατάλληλο υπόβαθρο οργάνωσης έτσι ώστε να κατανοήσουν πλήρως και να αποτυπώσουν την ευπάθειά τους στο η-επιχειρείν.

Μέρος Β

ΚΕΦΑΛΑΙΟ 4ο : ΤΑ ΕΜΠΟΔΙΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ - ΟΙ ΛΟΓΟΙ ΥΠΑΡΞΗΣ & ΤΑ ΣΥΣΤΑΤΙΚΑ ΕΠΙΤΥΧΙΑΣ ΜΙΑΣ ΙΣΤΟΣΕΛΙΔΑΣ

4.1 Εισαγωγή

Σε ένα συνεχώς διευρυνόμενο μέσο, όπως είναι το Διαδίκτυο, με τα κεφάλαια για επενδύσεις στην ιδέα του ηλεκτρονικού εμπορίου να ρέουν άφθονα και συνεχώς, υπάρχει μεγάλο περιθώριο για κέρδος αλλά και για ζημία. Μέσα σε αυτό το κλίμα, αυξάνονται και οι ευκαιρίες για ηλεκτρονική απάτη, άλλωστε οι επιτήδειοι δε λείπουν ποτέ. Μία από τις απαραίτητες προϋποθέσεις για την άνθιση του ηλεκτρονικού εμπορίου είναι η ασφάλεια των συναλλαγών. Ο χρήστης που κάνει μια αγορά online πρέπει να είναι σίγουρος ότι ο αριθμός της πιστωτικής κάρτας του δεν θα υποκλαπεί. Όταν αποστέλλει μέσω του Διαδικτύου ευαίσθητα δεδομένα, θέλει να γνωρίζει ότι θα παραληφθούν από τον άμεσα ενδιαφερόμενο. Τα προηγούμενα δεν είναι υπερβολικά διότι ο κίνδυνος ενυπάρχει.

Χαρακτηριστική είναι η έρευνα που πραγματοποιήθηκε για τις νέες τεχνολογίες και την Κοινωνία της Πληροφορίας από το Ε.Δ.Ε.Τ. το 2005. Σύμφωνα με την έρευνα αυτή, από τα 535 άτομα που χρησιμοποιούν το Internet σε ένα δείγμα 2.741 ατόμων στην Ελλάδα, μόνο το 20% πραγματοποιεί ηλεκτρονικές αγορές. (Σχήμα 2)

Σχήμα 2: Ηλεκτρονικές αγορές (e-shopping) στην Ελλάδα, 2005

(πηγή: Ε.Δ.Ε.Τ. Α.Ε.)

Οι αγορές λοιπόν αυτές που πραγματοποιεί ένα 20%, προέρχονται κυρίως από ξένα sites κατά 43,5%, από ελληνικά sites κατά 34% και από ξένα και ελληνικά κατά 19,3%. (Σχήμα 3)

Σχήμα 3: Προέλευση αγορών από ξένα και ελληνικά sites στην Ελλάδα, 2005

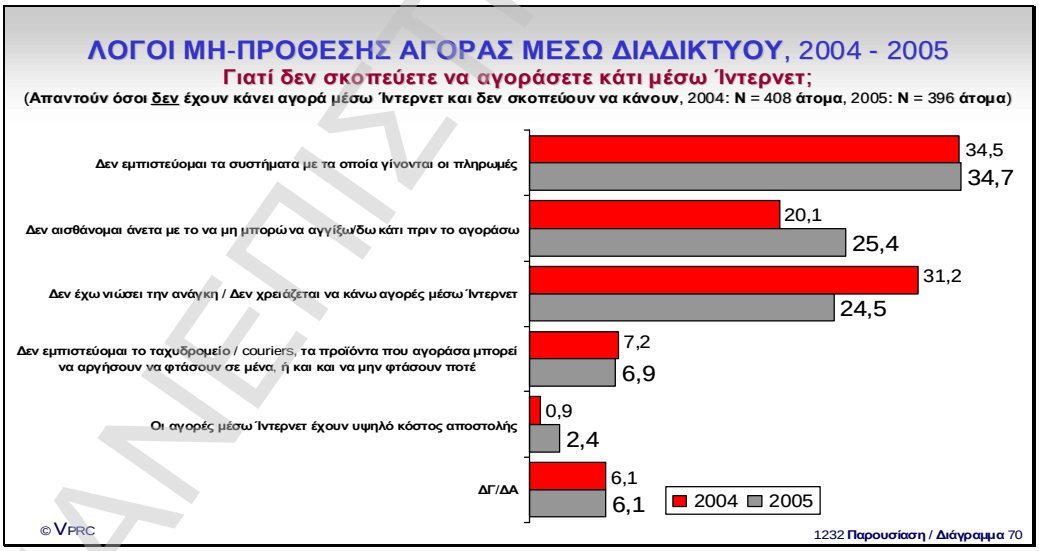
(πηγή: Ε.Δ.Ε.Τ. Α.Ε.)

Η πρόθεση αγοράς των Ελλήνων μέσω του Διαδικτύου κατά την περίοδο 2004-2005 είναι αφοπλιστική. Το 88,6% δεν σκοπεύει να κάνει καμία αγορά μέσα στο δεύτερο εξάμηνο του 2005, ποσοστό που αυξήθηκε αφού το 2004 ήταν 87,1%. (Σχήμα 4)

Σχήμα 4: Πρόθεση αγοράς μέσω Διαδικτύου, 2004-2005

(πηγή: Ε.Δ.Ε.Τ. Α.Ε.)

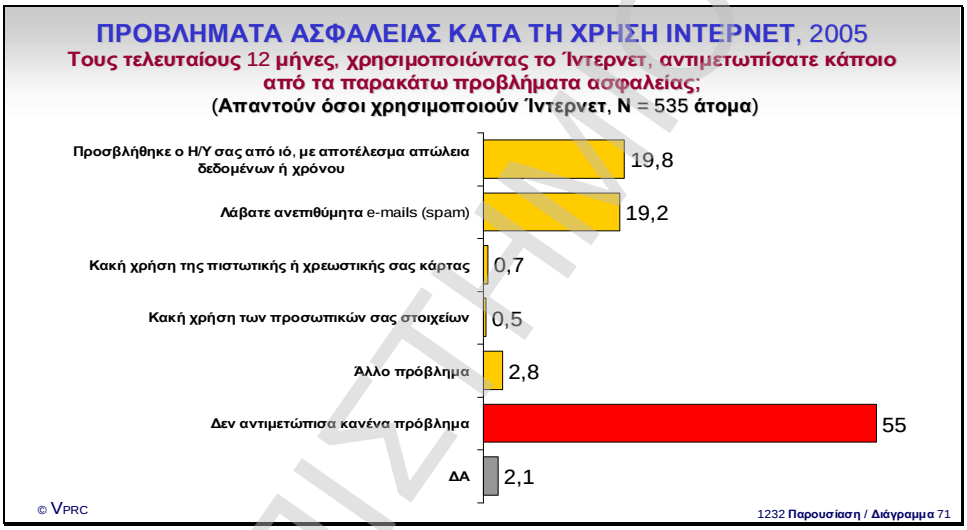
Η στάση αυτή εξηγείται από το γεγονός ότι οι Έλληνες καταναλωτές δεν εμπιστεύονται τα συστήματα των συναλλαγών σε ποσοστό 34,7% το 2005, δεν αισθάνονται άνετα εάν δε μπορούν να αγγίξουν το προϊόν σε ποσοστό 25,4% καθώς υπάρχουν και άλλοι λόγοι όπως φαίνονται στο Σχήμα 5.



Σχήμα 5: Λόγοι μη πρόθεσης αγοράς μέσω Διαδικτύου, 2004-2005

(πηγή: Ε.Δ.Ε.Τ. Α.Ε.)

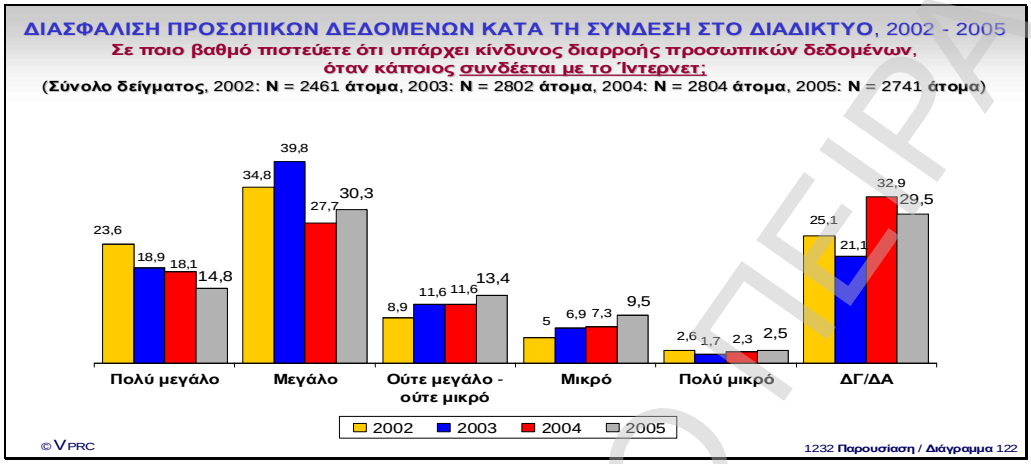
Ωστόσο, στην ίδια έρευνα, τα 535 άτομα που κάνουν χρήση του Διαδικτύου, απάντησαν σε ποσοστό 55% πως δεν αντιμετώπισαν κανένα πρόβλημα ασφάλειας, γεγονός που δείχνει πως οι τεχνολογικές λύσεις για την αντιμετώπιση απειλών, συνεχώς κερδίζουν έδαφος. Ανάμεσα σε αυτούς, το 19,8% αναφέρει πως έχει προσβληθεί ο ηλεκτρονικός υπολογιστής τους από ιό με αποτέλεσμα την απώλεια χρόνου και δεδομένων, καθώς επίσης το 19,2 αναφέρει πως έχει λάβει ανεπιθύμητα μηνύματα. Τα ανεπιθύμητα μηνύματα είναι πλέον λιγότερα από 10% σε παγκόσμια κλίμακα και οι παραλήπτες τέτοιων μηνυμάτων με τη χρησιμοποίηση του πλήκτρου διαγραφής μπορούν να αμυνθούν απέναντι στον ηλεκτρονικό αυτό πόλεμο. (Σχήμα 6)



Σχήμα 6: Προβλήματα ασφάλειας κατά τη χρήση του Διαδικτύου, 2005 (πηγή: Ε.Δ.Ε.Τ. Α.Ε.)

Τέλος, όσον αφορά στην ασφάλεια των προσωπικών δεδομένων στην ίδια έρευνα τα αποτελέσματα είναι επίσης εντυπωσιακά. Κατά 14,8%, ποσοστό που εμφανίζεται κατά πολύ μειωμένο το 2005 σε σχέση με τα προηγούμενα έτη, τα άτομα που πήραν μέρος στην έρευνα απάντησαν ότι ο κίνδυνος διαρροής προσωπικών δεδομένων όταν κάποιος συνδέεται στο Διαδίκτυο είναι πολύ μεγάλος. Και στις υπόλοιπες κατηγορίες οι απαντήσεις που δόθηκαν το 2005 είναι ευνοϊκές απέναντι στην ασφάλεια των

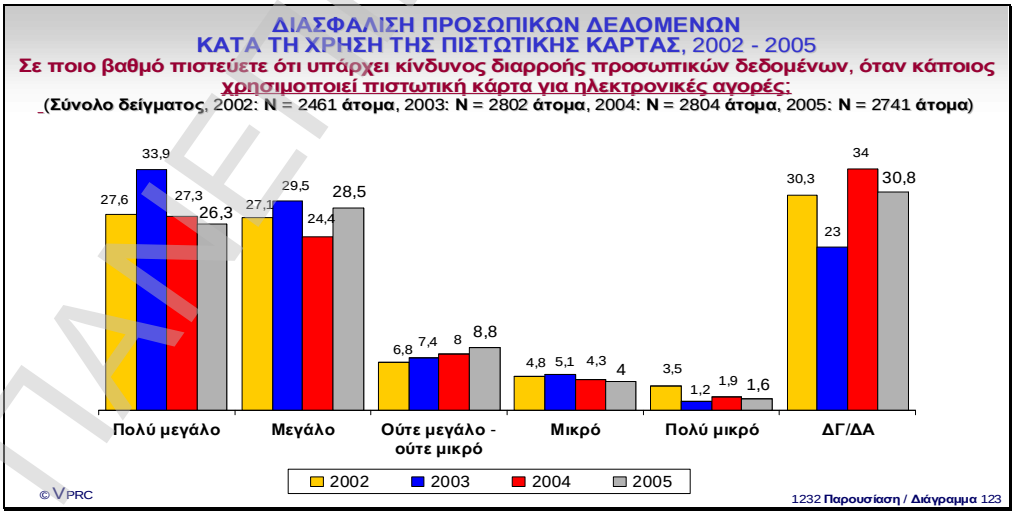
προσωπικών δεδομένων. Λέγοντας προσωπικά δεδομένα εννοεί κανείς την κάθε είδους προσωπική και ευαίσθητη πληροφορία που αναφέρεται στις δραστηριότητες των ατόμων, επαγγελματικές και μη. (Σχήμα 7)



Σχήμα 7: Διασφάλιση προσωπικών δεδομένων κατά τη σύνδεση στο Διαδίκτυο, 2002-2005

(πηγή: Ε.Δ.Ε.Τ. Α.Ε.)

Επιπλέον, ο κίνδυνος διαρροής των προσωπικών δεδομένων κατά τη χρήση της πιστωτικής κάρτας ήταν ένα θέμα που απασχόλησε την έρευνα. Σχετικά με το θέμα αυτό παρουσιάζονται διάφορες αυξομειώσεις από το 2002 έως το 2005. (Σχήμα 8)



Σχήμα 8: Διασφάλιση προσωπικών δεδομένων κατά τη χρήση πιστωτικής κάρτας, 2002-2005

(πηγή: Ε.Δ.Ε.Τ. Α.Ε.)

Ακόμα σε μια έρευνα που διεξήχθη το 2003 (Κατραμάδος, 2003) για την ασφάλεια των συναλλαγών ανάμεσα σε διάφορες επιχειρήσεις (φαρμακευτικές εταιρίες, εταιρίες κινητής τηλεφωνίας, εταιρίες που διαθέτουν μόνο ηλεκτρονικά καταστήματα), διαπιστώθηκε ότι το 80% των επιχειρήσεων που χρησιμοποιούν το ηλεκτρονικό εμπόριο είχαν εντοπίσει επιθέσεις στα συστήματά τους. Τα συστήματα ασφάλειας ανταποκρίθηκαν άριστα σε αυτές τις επιθέσεις σε ποσοστό 70% ενώ ικανοποιητικά σε ποσοστό 20% και μόνο το 10% δήλωσε πως υπέστησαν μικρής έκτασης ζημιές από τις επιθέσεις. Το συμπέρασμα που προκύπτει είναι ιδιαίτερα ενθαρρυντικό για την εξέλιξη του ηλεκτρονικού εμπορίου. Από τη μια μεριά διαπιστώνεται πως, απέναντι στους κινδύνους που περιγράφηκαν στα προηγούμενα κεφάλαια, η τεχνολογία έχει τις λύσεις και από την άλλη οι χρήστες, έχοντας κατανοήσει τις πραγματικές τους ανάγκες, έχουν επιλέξει τα κατάλληλα συστήματα προστασίας. Απόδειξη του γεγονότος ότι οι χρήστες αντιλαμβάνονται πλήρως πως οι κίνδυνοι όχι μόνο είναι υπαρκτοί αλλά και προοδεύουν αποτελεί το ότι η πλειοψηφία τους πραγματοποιεί δοκιμές ελέγχου στα συστήματα ασφάλειας. Παράλληλα, όλες σχεδόν οι εταιρίες διαθέτουν πολιτική ασφάλειας αν και ο βαθμός αφομοίωσής της από τους υπαλλήλους γενικά κυμαίνεται από μέτριο έως ικανοποιητικό επίπεδο.

4.2 Τα προβλήματα του ηλεκτρονικού εμπορίου στην Ευρώπη

Το αυστηρό νομοθετικό πλαίσιο, τα θέματα ασφάλειας, οι περίπλοκοι τρόποι πληρωμών και οι μικρού μεγέθους επιχειρήσεις αποτελούν τους βασικούς

ανασταλτικούς παράγοντες για την άνθιση του ηλεκτρονικού εμπορίου στην Ευρώπη, σύμφωνα με έρευνα της Forrester Research.

Σε ό,τι αφορά στους τρόπους πληρωμής, η κατάσταση στην Ευρώπη παρουσιάζει μια ιδιομορφία. Άλλες είναι, για παράδειγμα, οι μορφές πληρωμής που χαρακτηρίζουν τους Γάλλους καταναλωτές και άλλες τους Γερμανούς. Έτσι, για να γνωρίσει επιτυχία στην ευρωπαϊκή αγορά κάποια ιστοσελίδα ηλεκτρονικού εμπορίου, θα πρέπει να διαθέτει πολλαπλούς τρόπους πληρωμής για τα προϊόντα και τις υπηρεσίες που προσφέρει.

Από την άλλη πλευρά, αναγκαία κρίνεται και η χαλάρωση του πραγματικά ασφυκτικού νομικού πλαισίου, όπως στην περίπτωση των χωρών της νότιας Ευρώπης. Οι λιγότερο αυστηροί κανόνες στον τομέα του λιανεμπορίου, επιτρέπουν την ανάπτυξη του ηλεκτρονικού εμπορίου, όπως συμβαίνει για παράδειγμα στη Βρετανία.

Ένα επιπρόσθετο εμπόδιο για την άνθιση του ηλεκτρονικού εμπορίου στη Γηραιά Ήπειρο, είναι το πνεύμα τοπικισμού που κυριαρχεί στις διάφορες ευρωπαϊκές αγορές. Ακόμα και οι μεγάλοι δικτυακοί τόποι ηλεκτρονικού εμπορίου αναγκάζονται να περιορίζουν τις επιχειρηματικές τους δραστηριότητες στα πλαίσια των τοπικών αγορών.

Σύμφωνα με μια έρευνα που διεξήχθη το 2000 από την CommerceNet 2000 (“Barriers to Electronic Commerce”), τα δέκα μεγαλύτερα εμπόδια για την ευημερία και την πλήρη άνθιση του ηλεκτρονικού εμπορίου παγκοσμίως είναι κατά σειρά τα εξής:

1. Το θέμα της ασφάλειας και της κρυπτογράφησης.
2. Το θέμα της εμπιστοσύνης και του κινδύνου.

3. Η έλλειψη εξειδικευμένου προσωπικού.
4. Η έλλειψη επιτυχώς εφαρμοσμένων επιχειρηματικών μοντέλων.
5. Η κουλτούρα των οργανισμών.
6. Ο έλεγχος αυθεντικότητας των χρηστών.
7. Η οργάνωση.
8. Η απάτη και ο κίνδυνος της απώλειας.
9. Το internet / web είναι πολύ αργό και αναξιόπιστο.
10. Νομικά θέματα.

Το σημαντικότερο εμπόδιο εξακολουθεί και είναι το πρόβλημα της ασφάλειας. Οι συμμετέχοντες στην έρευνα ανακήρυξαν ομόφωνα το θέμα της ασφάλειας ως κυρίαρχο εμπόδιο, αναφέροντας τα θέματα της κρυπτογράφησης, της εμπιστοσύνης και του κινδύνου, τον έλεγχο αυθεντικότητας των χρηστών, την απάτη και το φόβο της απώλειας και τα νομικά θέματα, όπως τα συμβόλαια και οι συμμετοχές. Μία ακόμα ανησυχία αποτελεί η έλλειψη εξειδικευμένου προσωπικού για τη σωστή διεξαγωγή του ηλεκτρονικού εμπορίου στις επιχειρήσεις. Επίσης, η έλλειψη δοκιμασμένων και αποδεδειγμένης αποτελεσματικότητας επιχειρηματικών μοντέλων και οι περιορισμοί ανάπτυξης της ηλεκτρονικής επιχειρηματικότητας, εξαιτίας της κουλτούρας των επιχειρήσεων και της ατελούς οργάνωσης, αποτελούν τροχοπέδη για την εξέλιξη του ηλεκτρονικού εμπορίου.

4.3 Τα εμπόδια του ηλεκτρονικού εμπορίου στην Ελλάδα

Τα κυριότερα εμπόδια για την ανάπτυξη του ελληνικού ηλεκτρονικού εμπορίου είναι τα εξής:

1) Οι αγορές εξ' αποστάσεως δεν αναπτύχθηκαν ποτέ στην Ελλάδα σε τέτοιο βαθμό, όπως για παράδειγμα στις Η.Π.Α. όπου οι καταναλωτές έχουν έναν τυπωμένο κατάλογο και μία ταχυδρομική παραγγελία και αγοράζουν τηλεφωνικώς. Στην Ελλάδα επικρατεί κυρίως δυσπιστία όσον αφορά στις εξ' αποστάσεως, και κατ' επέκταση και στις ηλεκτρονικές αγορές, εξαιτίας κυρίως του τρόπου πληρωμής με πιστωτική κάρτα που θεωρείται πιο επισφαλής. Οι Έλληνες χρησιμοποιούν πιστωτικές κάρτες συνήθως μόνο για αγορές μεγάλης αξίας.

2) Η τηλεπικοινωνιακή υποδομή της Ελλάδας δεν είναι ακόμα τόσο αναπτυγμένη όπως σε άλλες χώρες, όπου εκτεταμένα δίκτυα προσφέρουν ταχύτερη και πιο αξιόπιστη πρόσβαση στο χρήστη του Διαδικτύου.

3) Παρουσιάζεται έλλειψη κινήτρων για τον Έλληνα καταναλωτή ώστε να πραγματοποιήσει τις αγορές του μέσω Διαδικτύου, καθότι πολλά προϊόντα έχουν την ίδια τιμή και ποιότητα όπως και στα παραδοσιακά καταστήματα.

4) Ανασταλτικό παράγοντα για την ταχύτερη αύξηση των ηλεκτρονικών πωλήσεων, τόσο στην Ελλάδα όσο και σε ολόκληρη την Ευρώπη, αποτελεί ο ανεπαρκής έλεγχος των αποθεμάτων.

5) Το ηλεκτρονικό εμπόριο επιχείρησης-προς-καταναλωτή (B2C) δεν θα μπορέσει να φτάσει σε υψηλά επίπεδα, παρά μόνο αν προσφέρει στον καταναλωτή το πλεονέκτημα να αγοράζει περισσότερα προϊόντα on-line από αυτά που ήδη προσφέρονται στα καταστήματα.

6) Η ένταξη της Ελλάδας στην τρίτη κατηγορία χωρών με τους βραδύτερους ρυθμούς ανάπτυξης του on-line shopping, μαζί με την Ιταλία, την Ισπανία και την Πορτογαλία, ήταν φυσικό επακόλουθο. Αυτό, διότι υπάρχει πολύ μικρότερη εμπειρία, εφόσον οι Έλληνες χρήστες του Διαδικτύου είναι από τους πιο

νέους συγκριτικά με άλλες ευρωπαϊκές χώρες. Η μικρή εμπειρία στο Διαδίκτυο αποτελεί ανασταλτικό παράγοντα αγορών, καθώς, όπως υποστηρίζουν πολλοί διεθνείς αναλυτές, όσο περισσότερο χρόνο δαπανά ένας χρήστης στο Διαδίκτυο τόσο αυξάνονται οι πιθανότητες να προχωρήσει σε αγορές προϊόντων ή υπηρεσιών. Η ελληνική αγορά λοιπόν έχει τη δυνατότητα να παρουσιάσει υψηλότερες on-line πωλήσεις την επόμενη τετραετία, καθώς όλο και περισσότεροι Έλληνες παρουσιάζουν υψηλό βαθμό εξοικείωσης με το Διαδίκτυο, ενώ η διείσδυση του νέου αυτού μέσου στην Ελλάδα αυξάνεται συνεχώς (Καλαμποκά, 2001).

4.4 Προκλήσεις σχετικά με το ηλεκτρονικό εμπόριο

Όπως προαναφέρθηκε, μία δυσκολία για τη διεξαγωγή του ηλεκτρονικού εμπορίου πανευρωπαϊκά, αποτελεί η ανεπαρκής διαχείριση και έλεγχος των αποθεμάτων. Οι υποψήφιοι πελάτες οι οποίοι επισκέπτονται μία ηλεκτρονική επιχείρηση πολλές φορές δεν καταφέρνουν να πραγματοποιήσουν μία αγορά τους, λόγω προβλημάτων διαθεσιμότητας. Σε αυτήν την περίπτωση, ο χρήστης μπορεί να μην επιστρέψει στο ίδιο κατάστημα για μεγάλο χρονικό διάστημα. Πρέπει λοιπόν να εστιαστούν οι προσπάθειες βελτίωσης τόσο στον τομέα των αποθεμάτων όσο και της διανομής, καθότι αμφότεροι αυτοί οι τομείς είναι νευραλγικής σημασίας για τη σωστή εξυπηρέτηση των πελατών.

Επίσης, η έλλειψη οικονομικών κινήτρων στο ελληνικό Διαδίκτυο, με τη μορφή προσφορών για παράδειγμα, δεν παροτρύνουν τους Έλληνες χρήστες να πραγματοποιούν τις αγορές τους on-line. Τα οικονομικά κίνητρα που μπορεί να παρέχει ένα ηλεκτρονικό κατάστημα στους πελάτες του, όπως για παράδειγμα η

αγορά τριών προϊόντων στην τιμή των δύο, έχουν αποδειχθεί ιδιαίτερα αποτελεσματικά για την αύξηση του τζίρου (Ναυτεμπορική, 2002).

Επιπροσθέτως, πρέπει να δίνεται έμφαση και στο σωστό σχεδιασμό των ιστοσελίδων καθώς αυτές αποτελούν την εικόνα μιας ηλεκτρονικής επιχείρησης προς τα έξω, με άλλα λόγια την ηλεκτρονική βιτρίνα της επιχείρησης. Σύμφωνα με έρευνες, έχει αποδειχθεί ότι τα ηλεκτρονικά καταστήματα με τον καλύτερο σχεδιασμό είναι αυτά που παρουσιάζουν και τις υψηλότερες πωλήσεις.

Τέλος, μία τακτική που έχουν ακολουθήσει τα ηλεκτρονικά καταστήματα σε άλλες χώρες με χαμηλή διείσδυση στο Διαδίκτυο, όπως η Ισπανία, είναι ότι σταματούν την προσπάθεια προσέλκυσης όλων των καταναλωτών και επικεντρώνονται μόνο σε αυτούς που χρησιμοποιούν το Internet. Αντί δηλαδή να υλοποιούν υψηλές δαπάνες για να δημιουργήσουν ένα ισχυρό brand name για ολόκληρη την αγορά στην οποία απευθύνονται, εστιάζονται στην ισχυροποίηση της θέσης τους μόνο στους on-line καταναλωτές (Καλαμποκά, 2002).

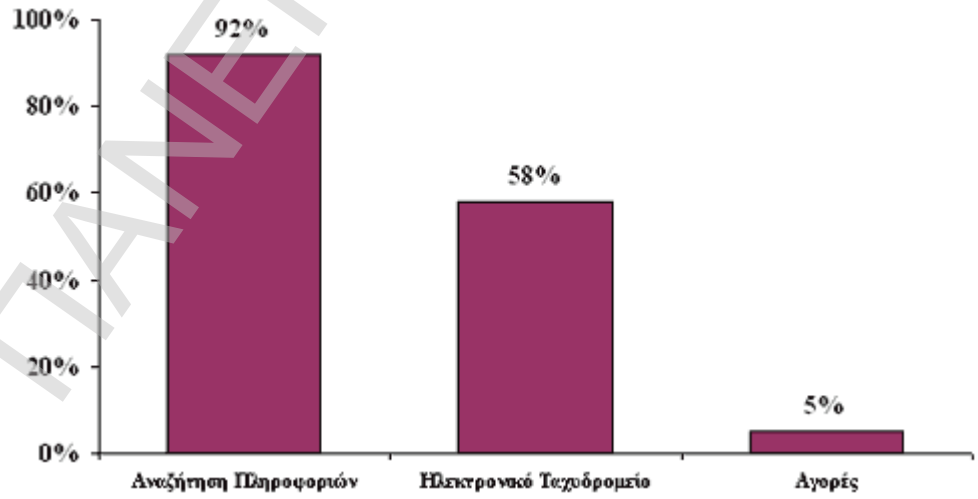
4.5 Ελληνικά websites

Από τον Ιούνιο του 2001 έως τον Οκτώβριο του ίδιου έτους η εταιρία συμβουλευτικών υπηρεσιών Deloitte & Touche διεξήγαγε μία έρευνα με τίτλο “Web Assessment: Pan-European analysis of the quality of the user experience offered by major websites”. Μελετήθηκαν περισσότερα από 200 websites ευρωπαϊκών χωρών (Αυστρία, Βέλγιο, Δανία, Γαλλία, Ελλάδα, Γερμανία, Ιταλία, Ολλανδία, Πορτογαλία, Ισπανία, Σουηδία, Ελβετία και Αγγλία). Στόχος της έρευνας ήταν να μελετήσει την ποιότητα και το επίπεδο εξυπηρέτησης και λειτουργικότητας που παρέχουν οι

ιστοσελίδες στους χρήστες τους και τη συνολική εμπειρία που αυτοί αποκομίζουν από τη χρήση των μεγαλύτερων εταιριών ηλεκτρονικού εμπορίου σε 13 χώρες.

Σύμφωνα με την έρευνα οι γαλλικές και οι γερμανικές ιστοσελίδες ξεχωρίζουν για την ποιότητά τους, αντίθετα οι σουηδικές και οι ελληνικές βρέθηκαν σε σχετικά χαμηλές θέσεις. Τα ελληνικά websites έχουν σημαντικά περιθώρια βελτίωσης. Τα επίπεδα ικανοποίησης που παρέχουν στους πελάτες είναι χαμηλότερα από το μέσο όρο της Ευρώπης. Αυτό μπορεί εν μέρει να αποδοθεί στο γεγονός ότι ο ελληνικός πληθυσμός που κάνει χρήση του Διαδικτύου είναι χαμηλότερος από το μέσο όρο της Ευρώπης, όπως ήδη έχει αναφερθεί. Έτσι, οι ελληνικές επιχειρήσεις παρουσιάζουν δισταγμούς στο να προχωρήσουν σε εκτεταμένες επενδύσεις στο ηλεκτρονικό εμπόριο.

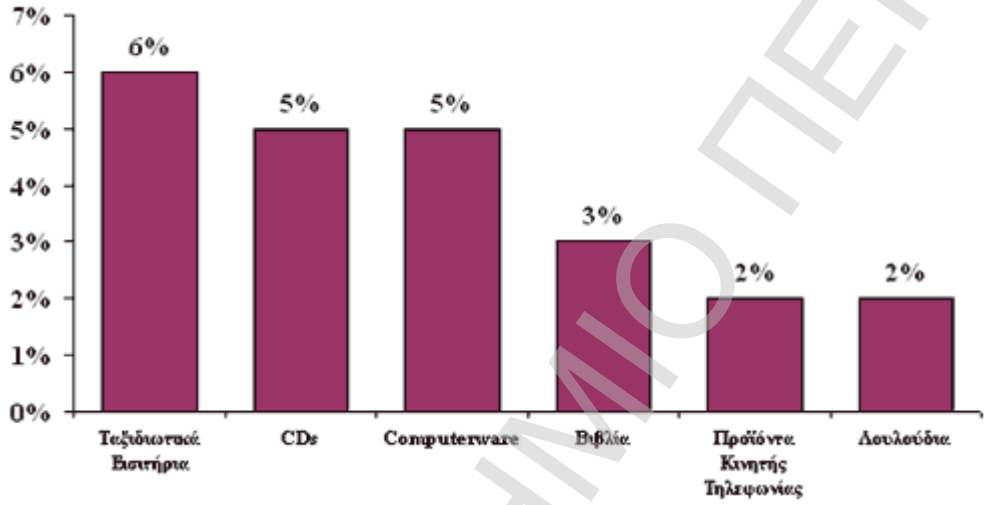
Στο γράφημα 2 απεικονίζονται οι κυριότεροι λόγοι χρησιμοποίησης του ελληνικού Internet για το 2000, ενώ στο 3 τα προϊόντα που αγοράστηκαν on-line το 2000. Η αναζήτηση πληροφοριών και η ηλεκτρονική επικοινωνία-και τα δύο χωρίς κόστος για το χρήστη- είναι οι βασικές αιτίες για τη χρήση του Internet στην Ελλάδα. Οι on-line αγορές πραγματοποιούνται μόνο από το 5% των χρηστών του Διαδικτύου.



Πηγή: Focus-Bari

Γράφημα 2: Λόγοι χρησιμοποίησης του Internet στην Ελλάδα-2000

(πηγή: Focus-Bari)

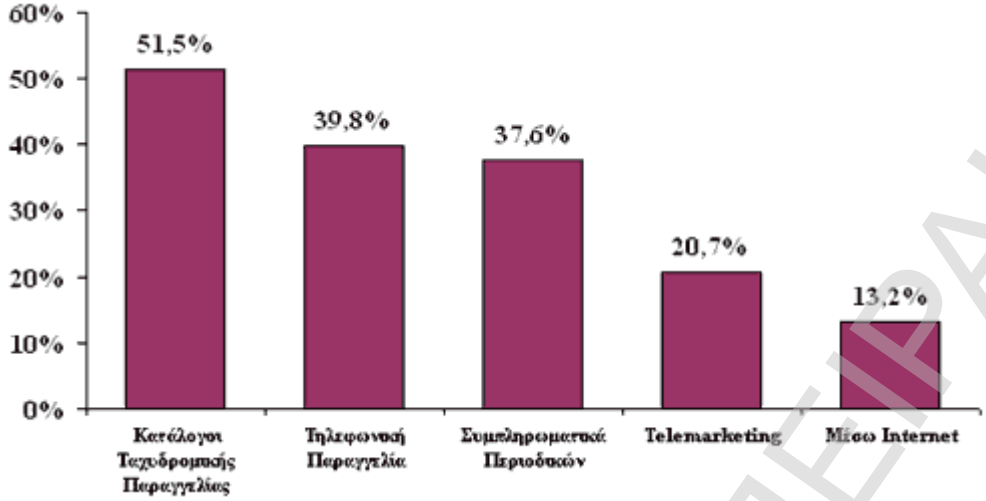


Πηγή: Focus-Bari

Γράφημα 3: Προϊόντα που αγοράστηκαν on-line στην Ελλάδα-2000

(πηγή: Focus-Bari)

Βλέποντας από την πλευρά του τρόπου της αγοράς, φαίνεται πως το B2C μπορεί να αντικαταστήσει πιο εύκολα άλλα εξ' αποστάσεως μέσα αγοράς όπως το telemarketing και τις τηλεφωνικές παραγγελίες παρά να απομακρύνει τους πελάτες από τα πραγματικά καταστήματα. Σήμερα, προτιμούνται άλλοι τρόποι αγοράς εξ' αποστάσεως από ότι το Διαδίκτυο, το οποίο χρησιμοποιείται μόνο από το 13,2% όσων χρησιμοποιούν εναλλακτικούς τρόπους αγοράς. (γράφημα 4)



Πηγή: Focus-Bari

Γράφημα 4: Χρήστες εναλλακτικών τρόπων αγοράς, Ελλάδα-2000

(πηγή: Focus-Bari)

4.5.1 Λόγοι δημιουργίας ηλεκτρονικού καταστήματος για μια επιχείρηση

Η δημιουργία ενός ηλεκτρονικού καταστήματος για μια επιχείρηση είναι ένα σημαντικό επενδυτικό βήμα. Οι προβλέψεις για την πορεία και την εξέλιξη του ηλεκτρονικού εμπορίου στην Ελλάδα είναι αισιόδοξες και δίνουν ένα κίνητρο στους Έλληνες επιχειρηματίες ώστε να προχωρήσουν σε επενδύσεις και να προσφύγουν στη δημιουργία ηλεκτρονικών καταστημάτων προκειμένου να αποκτήσουν ένα σημαντικό ανταγωνιστικό πλεονέκτημα. Υπάρχουν πολλά και σημαντικά επιχειρήματα για τη δημιουργία μιας επιχείρησης on-line:

1. Διότι οι συνεργάτες και οι ανταγωνιστές είναι ήδη εκεί.
2. Υπάρχει δυνατότητα προσέγγισης ευρύτερου κοινού-στόχου.
3. Υπάρχει περισσότερη, ευκολότερη, γρηγορότερη, οικονομικότερη και αποτελεσματικότερη επικοινωνία με τους προμηθευτές.

4. Ευκολότερη εξεύρεση νέων πελατών και διερεύνηση άγνωστων αγορών.

5. Ευκολότερη διείσδυση στις υπάρχουσες αγορές, ευκολότερη προσέγγιση νέων αγορών.

6. Σημαντική αναβάθμιση εξυπηρέτησης πελατών.

7. Προώθηση ενός σύγχρονου επαγγελματικού προφίλ μιας επιχείρησης που παρακολουθεί τις εμπορικές και τεχνολογικές εξελίξεις και δεν θέλει να μείνει πίσω.

8. Μείωση του κόστους, μέσω ηλεκτρονικών συναλλαγών, χτίζοντας στενότερες και πιο εύκαμπτες εμπορικές σχέσεις με τους πελάτες και τους προμηθευτές.

9. Καλύτερη και γρηγορότερη διανομή προϊόντων και υπηρεσιών.

10. Ευκαιρίες για εφαρμογή νέων επιχειρηματικών ιδεών.

11. Βελτιωμένο και φθηνότερο one-to-one marketing.

12. Άμεση και γρηγορότερη πληροφόρηση για νόμους, υπηρεσίες του δημοσίου τομέα και της κυβέρνησης, φορολογικά θέματα κ.ά.

13. Τέλος, το Διαδίκτυο επιτρέπει ακόμα και στις μικρές επιχειρήσεις να ευδοκιμήσουν, καθώς το μέγεθος της επιχείρησης δεν παίζει πια κανένα ρόλο, γιατί αυτό που είναι σημαντικότερο είναι απλά να δικτυωθεί η επιχείρηση. Επίσης, υπάρχει η δυνατότητα συμμετοχής σε κοινότητες επιχειρήσεων προκειμένου να είναι δυνατός ο προγραμματισμός της ανάπτυξης και της μείωσης του κόστους των προμηθειών, καθώς και η άντληση χρήσιμων πληροφοριών από την εμπειρία των άλλων επιχειρήσεων όσον αφορά στην τεχνολογία και στις μεθόδους παραγωγής και προσέγγισης της αγοράς.

4.5.2 Σημαντικά ερωτήματα πριν το σχεδιασμό ενός website

Πριν ξεκινήσει ο σχεδιασμός και η λειτουργία ενός website πρέπει προηγουμένως να καθοριστούν τα εξής:

- Ποιος είναι ο επιχειρηματικός στόχος των ιστοσελίδων (π.χ. πωλήσεις, παροχή πληροφόρησης, διαφήμιση).
- Ποιο είναι το κοινό-στόχος στο οποίο απευθύνεται, ποιες οι ανάγκες και οι συνήθειές του.
- Η στρατηγική προσέλκυσης αυτού του κοινού.
- Το είδος της πληροφορίας που θα είναι διαθέσιμη.
- Η φόρμα εμφάνισης αυτής της πληροφορίας, π.χ. κείμενο, γραφικά, video.
- Ένας δημιουργικός τρόπος παρουσίασης της πληροφορίας μέσω σύγχρονων τεχνολογιών όπως, Java, RealAudio κ.λ.π.
- Ο τρόπος χρηματοδότησης για την ανάπτυξη αλλά και τη συντήρηση των ιστοσελίδων (π.χ. από έσοδα που προέρχονται από τον ίδιο ή από άλλους προϋπολογισμούς).

4.5.3 Συστατικά επιτυχίας ενός website

- **Διεύθυνση (URL ή domain name):** Η διεύθυνση ενός website έχει τη μορφή www.onoma.gr ή www.onoma.com. Μία σωστή διεύθυνση μπορεί να συμβάλλει σημαντικά σε αυξημένο αριθμό επισκέψεων. Επίσης, η διεύθυνση μπορεί να λειτουργήσει ως μέσο για την ευκολότερη απομνημόνευση της εμπορικής ταυτότητας της επιχείρησης.

- **Αισθητικά όμορφο ηλεκτρονικό κατάστημα:** Το ηλεκτρονικό κατάστημα πρέπει να αντιμετωπίζεται σαν ένα κανονικό κατάστημα. Αν είναι όμορφο αισθητικά και άρτια τεχνικά κατασκευασμένο, τότε θα δημιουργήσει καλή διάθεση στον επισκέπτη και θα του εμπνεύσει εμπιστοσύνη για την σοβαρότητα και τον επαγγελματισμό της επιχείρησης.

- **Διάθεση ποιοτικών προϊόντων και υπηρεσιών:** Μπορεί να φαίνεται προφανές, αλλά πολλές φορές παραβλέπεται. Δεν υπάρχει λόγος επένδυσης σε ένα ηλεκτρονικό κατάστημα εάν η επιχείρηση δεν έχει κάτι πραγματικά καλό να προσφέρει.

- **Μέτρα ασφάλειας στις συναλλαγές:** Ο μεγαλύτερος φόβος των χρηστών του Διαδικτύου που τους εμποδίζει να πραγματοποιούν on-line συναλλαγές, είναι τα θέματα ασφάλειας των διαφόρων ηλεκτρονικών καταστημάτων. Αν και είναι αδύνατον να εγγυηθεί απόλυτη ασφάλεια, η σύγχρονη τεχνολογία παρέχει τα καλύτερα δυνατά εργαλεία ασφάλειας τα οποία είναι σημαντικό να υιοθετούνται στις ηλεκτρονικές συναλλαγές. Από τις προτεραιότητες ενός ηλεκτρονικού καταστήματος θα πρέπει να είναι η χρήση των πιο σύγχρονων τεχνικών προδιαγραφών ασφαλείας (κρυπτογράφηση, έλεγχος αυθεντικότητας, σαφείς όροι χρήσης της ιστοσελίδας, πολιτικές προστασίας δεδομένων κ.λ.π.), ώστε ο επισκέπτης να αισθάνεται ασφάλεια κατά την περιήγησή του και την παραγγελία προϊόντων.

- **Ευκολία στους τρόπους πληρωμής:** Έχει αποδειχθεί με έρευνες και στατιστικές που αφορούν στην αλληλεπίδραση ανάμεσα σε δημοφιλή ηλεκτρονικά καταστήματα και χρήστες τους, ότι όσο πιο απλή και εύκολη είναι η παραγγελία ενός προϊόντος on-line, τόσο πιο πολλές είναι και οι πωλήσεις του καταστήματος και οι

ικανοποιημένοι πελάτες του. Το ηλεκτρονικό κατάστημα πρέπει να παρέχει στους επισκέπτες εναλλακτικούς τρόπους πληρωμής.

- **Σωστή διαφήμιση του ηλεκτρονικού καταστήματος στο χώρο του Internet:** Ένα άρτια κατασκευασμένο ηλεκτρονικό κατάστημα, με καλαίσθητες ιστοσελίδες και σύγχρονες τεχνικές ασφάλειας, είναι καταδικασμένο σε αποτυχία εάν οι χρήστες του Διαδικτύου αγνοούν την ύπαρξή του. Η αποτελεσματική διαφημιστική προώθηση σε sites, μηχανές αναζήτησης και banners, θα φέρει νέους επισκέπτες και πιθανούς πελάτες.

- **Άριστη εξυπηρέτηση πελατών:** Η υψηλού επιπέδου και αξιόπιστη εξυπηρέτηση πελατών μπορεί να αποδώσει σε ένα ηλεκτρονικό κατάστημα μεγάλο μερίδιο αγοράς, φέρνοντάς το σε ηγετική θέση. Ο συνδυασμός του καλού προϊόντος και υπηρεσίας με την άρτια εξυπηρέτηση, δημιουργούν ικανοποιημένους πελάτες, δηλαδή πιστούς πελάτες.

- **Προσθήκη επιπλέον στοιχείων:** Η προσθήκη εργαλείων, όπως για παράδειγμα οι διαγωνισμοί και η διάθεση διαφόρων τρεχόντων ειδήσεων σε ένα ηλεκτρονικό κατάστημα, δεν αποτελεί τον καθοριστικό παράγοντα αύξησης του αριθμού των επισκέψεων, αλλά δημιουργεί κάποιες προϋποθέσεις προσέλκυσης μιας μερίδας επισκεπτών οι οποίοι φυσικά αποτελούν και υποψήφιους πελάτες.

- **Η χρησιμοποίηση μιας αξιόπιστης υπηρεσίας φιλοξενίας του website:** Τίποτα δεν απωθεί περισσότερο τους επισκέπτες ενός δικτυακού τόπου, από την αναξιόπιστη ανταπόκριση της σύνδεσής του με τον επισκέπτη εξαιτίας της κακής λειτουργίας του hosting server του. Η φιλοξενία ενός website δεν είναι ακριβή υπόθεση και για αυτό αξίζει να πληρώσει μία επιχείρηση επιπλέον, προκειμένου να έχει αξιόπιστη συνδεσιμότητα με τους υποψήφιους πελάτες.

Για να υπάρχει μεγαλύτερη επιτυχία και συμβατότητα μεταξύ επιχείρησης και του νέου μέσου, δηλαδή του Internet, οι Bloch, Pigneur και Segev (On the Road of Electronic Commerce-March 1996) προτείνουν ένα συνδυασμό τριών επιχειρηματικών στρατηγικών του Porter (Διαφοροποίηση, Ηγεσία Τιμής, Εστίαση) με τις δυνατότητες που προσφέρει το Διαδίκτυο. Η ανταγωνιστική στρατηγική της επιχείρησης συνίσταται σε τρεις επιλογές:

- Στην ηγεσία κόστους, καθώς το Διαδίκτυο δίνει τη δυνατότητα ακόμα και σε πολύ μικρές επιχειρήσεις να ανταγωνιστούν τις υπόλοιπες, σχεδόν επί ίσης όροις, εφόσον οποιαδήποτε επιχείρηση μπορεί να προχωρήσει σε μια επένδυση για τη δημιουργία ηλεκτρονικού καταστήματος.
- Στη διαφοροποίηση, προσφέροντας κάτι πραγματικά ελκυστικό για τον πελάτη και αποκτώντας ανταγωνιστικό πλεονέκτημα.
- Στην εστίαση, επωφελούμενη από τις τεχνικές και πληροφοριακές δυνατότητες που παρέχονται χάρη στο Διαδίκτυο, η επιχείρηση μπορεί να επικεντρωθεί σε πολύ συγκεκριμένο κοινό-στόχο.

Όσον αφορά στα υποκατάστατα προϊόντα και τις νέες εισόδους, έχει ήδη αναφερθεί ότι με τη βοήθεια του ηλεκτρονικού εμπορίου καθίσταται ευκολότερη η είσοδος σε νέες αγορές και η διείσδυση σε ήδη υπάρχουσες. Βέβαια, παράλληλα δημιουργούνται συχνά εμπόδια εισόδου σε αγορές όπου οι ήδη εγκαταστημένες επιχειρήσεις γνωρίζουν πολύ καλά πως να αποκτήσουν ανταγωνιστικό πλεονέκτημα, κυρίως μέσω διαφοροποίησης, εφόσον γνωρίζουν άριστα τους καταναλωτές αυτών των αγορών.

Τέλος, με την είσοδο στο ηλεκτρονικό εμπόριο μπορεί μία επιχείρηση να μειώσει ή και να εξαλείψει τις πιέσεις που δέχεται από προμηθευτές και πελάτες, εφόσον είναι

πολύ εύκολο πλέον να αποκλείσει εντελώς τους ενδιάμεσους ή να τους αντικαταστήσει με νέες μορφές διαμεσολαβητών.

Συνάγεται λοιπόν από τα παραπάνω πως το ηλεκτρονικό εμπόριο αποτελεί σημαντική επιχειρηματική πρακτική, που ενώ κρύβει κινδύνους, οι αποφασισμένες διοικήσεις των επιχειρήσεων σε συνδυασμό με την τεχνολογία μπορούν να αντιμετωπίσουν και να εισέλθουν ενεργά στη νέα αυτή επιχειρηματική πραγματικότητα σε ό,τι αφορά στην Ελλάδα.

ΚΕΦΑΛΑΙΟ 5ο : ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΕΩΝ & ΠΡΟΤΑΣΗ ΣΧΕΔΙΟΥ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΓΙΑ ΤΟ ΔΙΚΤΥΑΚΟ ΤΟΠΟ PAPASOTIRIOU.GR

5.1 Εισαγωγή

Όπως όλες οι επιχειρήσεις αντιμετωπίζουν κινδύνους κατά τη διάρκεια της καθημερινής λειτουργίας τους, έτσι και οι επιχειρήσεις που δραστηριοποιούνται και στο Διαδίκτυο έχουν ένα λόγο παραπάνω να ανησυχούν για επικείμενες κρίσεις.

Αν και οι κίνδυνοι δεν είναι δυνατό να αποφευχθούν, ωστόσο θα πρέπει να αντιμετωπίζονται με τον πλέον αποτελεσματικό τρόπο από πλευράς κόστους σε σχέση με την αξία των περιουσιακών στοιχείων της επιχείρησης.

Στη συνέχεια επιχειρείται παρουσίαση διαχείρισης κρίσης (ανάλυση κινδύνου και έλεγχος κινδύνου) και προτείνεται σχέδιο διαχείρισης επιχειρησιακής συνέχειας για το ηλεκτρονικό κατάστημα papasotiriou.gr αφού πρώτα αναφερθούν κάποια στοιχεία γνωριμίας με το συγκεκριμένο ηλεκτρονικό κατάστημα. Στην παρουσίαση αυτή διαχείρισης κρίσης καταγράφονται τα περιουσιακά στοιχεία, μελετώνται οι απειλές (threats) και τα σημεία ευπάθειας (vulnerabilities) της εν λόγω ηλεκτρονικής επιχείρησης. Επιπλέον αναπτύσσεται το σχέδιο ασφάλειας (security plan) το οποίο περιλαμβάνει τόσο τη λήψη κατάλληλων αντιμέτρων (countermeasures), όσο και την πολιτική ασφάλειας (security policy). Τέλος, συνιστάται σχέδιο επιχειρησιακής συνέχειας για το papasotiriou.gr δίνοντας έμφαση στους βασικούς άξονες από τους οποίους αποτελείται ένα σχέδιο διαχείρισης επιχειρησιακής συνέχειας και λαμβάνοντας υπόψη συνιστώσες από την ανάλυση ρίσκου που έχει προηγηθεί.

5.2 Λίγα λόγια για το δικτυακό τόπο papasotiriou.gr[25]

Το papasotiriou.gr είναι ένα ηλεκτρονικό κατάστημα πώλησης προϊόντων μέσω του Διαδικτύου, της ανώνυμης εταιρίας με την επωνυμία ΠΑΠΑΣΩΤΗΡΙΟΥ Α.Ε. Εμπνευστής και δημιουργός της ΠΑΠΑΣΩΤΗΡΙΟΥ Α.Ε είναι ο Γεώργιος Παπασωτηρίου. Ξεκίνησε την πορεία του στο χώρο του βιβλίου το 1974 εκδίδοντας τεχνικά βιβλία.

Το 1981 δημιουργήθηκε το πρώτο βιβλιοπωλείο στην περιοχή του Εθνικού Μετσόβιου Πολυτεχνείου στην οδό Στουρνάρη 23, δρόμος που τώρα πια έχει ταυτιστεί με το τεχνικό-επιστημονικό βιβλίο και την πληροφορική.

Το 1998, η εταιρία ενισχύοντας το πρωτοποριακό της πνεύμα, εγκαινίασε το πρώτο ηλεκτρονικό βιβλιοπωλείο. Η αποδοχή από το κοινό ήταν θετική και το 2001 το ύψος των πωλήσεων έφτασε τα 50 - 60 εκ.δρχ. παρά το γεγονός ότι βρισκόταν σε στάδιο ανανέωσης και εκσυγχρονισμού.

Μετά από 22 χρόνια εμπειρίας στο χώρο των εξειδικευμένων και μη βιβλίων, περιοδικών, CD-ROM, κ.λ.π, συνεισφέρει στην εκπαίδευση, στην πληροφόρηση και στην ενημέρωση, κάνοντας το βιβλίο πιο προσιτό και την πληροφόρηση για τις τεχνολογικές εξελίξεις και την πληροφορική πιο άμεση.

Πέραν αυτών, τα βιβλιοπωλεία Παπασωτηρίου έχουν πλέον επεκτείνει τη θεματολογία που προσφέρουν και σε άλλες κατηγορίες γενικότερου ενδιαφέροντος, όπως λογοτεχνία, παιδικό βιβλίο, λεξικά, φιλοσοφία, ταξιδιωτικούς οδηγούς κ.ά, παρουσιάζοντας έτσι στο κοινό μια πληρέστερη ποικιλία βιβλίων, που καλύπτουν όλες τις ανάγκες για διάβασμα και ενημέρωση.

Σήμερα, τα βιβλιοπωλεία Παπασωτηρίου έχουν ήδη αναπτύξει ένα δυναμικό δίκτυο καταστημάτων, δίνοντας έτσι τη δυνατότητα εξυπηρέτησης σε ένα ευρύτερο

[25] http://www.papasotiriou.gr

κοινό τόσο στην Αθήνα όσο και σε άλλες μεγάλες επαρχιακές πόλεις καθώς και στην Λευκωσία της Κύπρου.

Για την ανάπτυξη καταστημάτων στην περιφέρεια έχει επιλεγεί η μέθοδος του franchising.

Έτσι σήμερα, αποτελούν ήδη την μεγαλύτερη αλυσίδα βιβλιοπωλείων στην Ελλάδα τόσο από άποψη γεωγραφικής εξάπλωσης και από αριθμό καταστημάτων όσο και από κύκλο εργασιών.

5.3 Ανάλυση ρίσκου (κινδύνου)

Η ανάλυση ρίσκου βοηθά τους υπευθύνους του papasotiriou.gr να προσδιορίσουν τις δραστηριότητες εκείνες στις οποίες η ηλεκτρονική επιχείρηση θα ξοδέψει χρόνο και χρήμα. Χρησιμοποιείται ο τύπος της ποσοτικής ανάλυσης του κινδύνου, αφού απουσιάζει η ύπαρξη ερωτηματολογίων, ο οποίος εκτιμά το επίπεδο της επίδρασης της εμφάνισης απώλειας στην επιχείρηση ορίζοντας συνάμα το επίπεδο της ασφάλειας που απαιτείται. Καλύπτει λειτουργίες και ελέγχους σχετικές με το προσωπικό, τη διοίκηση, την τεχνολογική υποδομή, τις πληροφορίες. Ωστόσο πριν γίνει αναφορά στα μεγέθη της ποσοτικής ανάλυσης σχετικά με τον δικτυακό τόπο papasotiriou.gr, χρειάζεται να ληφθούν υπόψη τα ακόλουθα:

- Η αναγνώριση των κρίσιμων περιουσιακών στοιχείων της ηλεκτρονικής επιχείρησης.
- Η αναγνώριση των απειλών.
- Η ανάλυση των αδυναμιών.

Αναγνώριση κρίσιμων περιουσιακών στοιχείων. Το πιο κρίσιμο περιουσιακό στοιχείο για το ηλεκτρονικό κατάστημα papasotiriou.gr είναι η ύπαρξη και διαθεσιμότητα του ίδιου του δικτυακού τόπου. Επιπλέον το προσωπικό της

ηλεκτρονικής επιχείρησης, η τεχνολογική υποδομή, οι πληροφορίες που διαθέτει, η φήμη και η επωνυμία της που έχουν αναπτυχθεί κατά τη διάρκεια της δραστηριότητάς της, κατατάσσονται στα σημαντικά περιουσιακά της στοιχεία. Ακόμα στα περιουσιακά στοιχεία εντάσσεται η χρηματοοικονομική αξία των συναλλαγών, η εμπιστοσύνη των πελατών σχετικά με την ακρίβεια με την οποία πραγματοποιούνται οι συναλλαγές και με την αντίσταση σε θέματα απάτης.

Αναγνώριση απειλών. Οι απειλές αποτελούν διαδικασίες που αν πραγματοποιηθούν μπορούν να προκαλέσουν ανεπανόρθωτη ζημιά ή ακόμα και να καταστρέψουν περιουσιακά στοιχεία αξίας για την ηλεκτρονική επιχείρηση. Οι απειλές που προκαλούν κινδύνους σε σχέση με τη λειτουργία του papasotiriou.gr είναι η ανεπαρκής και ανακριβής παροχή πληροφοριών η οποία οδηγεί στη λήψη λανθασμένων αποφάσεων από τη διοίκηση, η αποτυχία στην πρόσληψη και ανάπτυξη του ήδη υπάρχοντος προσωπικού με γνώσεις και δεξιότητες που οδηγεί στην κακή διοίκησή του και στη μείωση της αποδοτικότητας και αποτελεσματικότητάς του, η αποτυχία των εσωτερικών ελέγχων, του συστήματος των πληροφοριών, τα λάθη και οι παραλείψεις που προκαλούν προβλήματα σχετικά με την εξυπηρέτηση και τη διανομή των προϊόντων. Ακόμα η αποτυχία στη διοίκηση των δημοσίων σχέσεων που τα στελέχη του papasotiriou.gr προσπαθούν να αποφύγουν με κάθε τρόπο, δημιουργεί αρνητική εντύπωση στους καταναλωτές και το κοινό προκαλώντας πλήγμα στη φήμη και την επωνυμία της ηλεκτρονικής επιχείρησης. Από την άλλη πλευρά, το papasotiriou.gr έχει να αντιμετωπίσει και απειλές τεχνικής φύσης, όπως λέγονται, που αφορούν στα πληροφοριακά του συστήματα. Οι υπεύθυνοι της ηλεκτρονικής επιχείρησης θεωρούν ότι οι επιθέσεις από hackers που εκμεταλλεύονται τις αδυναμίες του λειτουργικού συστήματος, αποτελούν τη σημαντικότερη τεχνική απειλή σήμερα. Επίσης η παρουσία κακόβουλου λογισμικού όπως ιοί, σκουλήκια, δούρειοι ίπποι

συνιστούν σημαντική απειλή. Όλα αυτά, μαζί με πτώση παροχής ηλεκτρικού ρεύματος ή οτιδήποτε άλλο όπως μια φυσική απειλή, οδηγούν στην άρνηση της εξυπηρέτησης του συστήματος και στη μη διαθεσιμότητα της ιστοσελίδας.

Ανάλυση αδυναμιών. Οι αδυναμίες ενεργοποιούν την απειλή να συμβεί. Για τις επιδράσεις της απειλής οι οποίες είναι σοβαρές, όπως για παράδειγμα τα λάθη και οι παραλείψεις που προκαλούν προβλήματα στην εξυπηρέτηση και διανομή των προϊόντων, επιχειρείται ανάλυση αδυναμιών έτσι ώστε να προσδιοριστεί το επίπεδο ελέγχου που απαιτείται. Οι αδυναμίες κατηγοριοποιούνται σε μια κλίμακα ως:

- Υψηλό επίπεδο αδυναμίας. Στην περίπτωση αυτή το σύστημα παρουσιάζει σημαντικές αδυναμίες και σύμφωνα με τους υπευθύνους των δικτύων του papasotiriou.gr η απουσία ή η ύπαρξη ασθενών passwords οδηγεί στην παραβίασή τους με αποτέλεσμα η επίδραση της απειλής να είναι σοβαρή, αφού είναι δυνατό να αποσπαστούν σημαντικές πληροφορίες από τους λογαριασμούς των χρηστών και το επίπεδο ελέγχου να χρειάζεται οπωσδήποτε βελτίωση. Επίσης, η άρνηση εξυπηρέτησης υποδηλώνει υψηλό επίπεδο αδυναμίας του συστήματος που πολλές φορές καθιστά την ιστοσελίδα μη διαθέσιμη.
- Μέτριο επίπεδο αδυναμίας. Στην περίπτωση αυτή παρουσιάζονται μερικές αδυναμίες, όπως τα λάθη και οι παραλείψεις που αναφέρθηκαν στην εξυπηρέτηση και διανομή των προϊόντων εξαιτίας ενδεχομένως κακής επικοινωνίας μεταξύ των εργαζομένων. Στο σημείο αυτό η επίδραση είναι σημαντική, το επίπεδο ελέγχου μπορεί να βελτιωθεί.
- Χαμηλό επίπεδο αδυναμίας. Στην περίπτωση αυτή το σύστημα είναι καλά οργανωμένο και λειτουργεί σωστά. Δεν χρειάζεται επιπρόσθετο επίπεδο ελέγχου. Το ήδη υπάρχον είναι επαρκές. Το papasotiriou.gr συνήθως παρουσιάζει

χαμηλά επίπεδα αδυναμίας που μόνο σε κάποιες έκτακτες περιπτώσεις, όπως αδυναμίας παράδοσης προϊόντων έγκαιρα, υποστηρίζει μέτριο επίπεδο αδυναμίας.

Αφού λοιπόν έχουν εντοπιστεί τα κρίσιμα περιουσιακά στοιχεία της ηλεκτρονικής επιχείρησης, έχουν αναγνωριστεί οι απειλές και αναλυθεί οι αδυναμίες απαιτείται η αποτίμηση του επιπέδου της επίδρασης των απειλών στη λειτουργία της επιχείρησης.

Όπως αναφέρθηκε παραπάνω οι απειλές προκαλούν ζημία στην επωνυμία και τη φήμη της ηλεκτρονικής επιχείρησης, απώλεια στη χρηματοοικονομική αξία των συναλλαγών, απώλεια της εμπιστοσύνης των πελατών στις συναλλαγές. Οι επιδράσεις κατηγοριοποιούνται σε μια κλίμακα ως εξής:

- Σοβαρή επίδραση. (υψηλή) Είναι πιθανό να προκληθεί σοβαρή ζημία στην πορεία της επιχείρησης και στην ανάπτυξή της, ακόμα και να τεθεί εκτός αγοράς. Η περίπτωση αυτή αφορά είτε στην άρνηση εξυπηρέτησης του συστήματος για μεγάλο χρονικό διάστημα η οποία έχει προέλθει από την υλοποίηση τεχνικής απειλής, όπως για παράδειγμα από απανωτές εισβολές, είτε σε φυσικές απειλές οι οποίες οδηγούν σε καταστροφή με μικρά περιθώρια ανάκαμψης.
- Σημαντική επίδραση. (μέση) Είναι πιθανό να προκληθεί σημαντική ζημία, αλλά η επιχείρηση θα επιβιώσει. Στην κατηγορία αυτή εμπεριέχονται οι καθυστερήσεις στην παράδοση των προϊόντων λόγω πολλές φορές κακής συνεννόησης.
- Μικρή επίδραση. (χαμηλή) Ο τύπος αυτός της επίδρασης είναι δυνατό να αντιμετωπιστεί στα πλαίσια της λειτουργίας της επιχείρησης. Πλήγμα στη φήμη και το κύρος του papasotiriou.gr αποτελεί η εμφάνιση προσβλητικού μηνύματος τη στιγμή που ο καταναλωτής εισέρχεται στο δικτυακό τόπο. Η επίδραση της συγκεκριμένης απειλής αντιμετωπίζεται με άμεση αφαίρεση του συγκεκριμένου

μηνύματος και σχετική ανακοίνωση από το γραφείο δημοσίων σχέσεων και επικοινωνίας της ηλεκτρονικής επιχείρησης.

Ο προσδιορισμός των μεγεθών της ποσοτικής ανάλυσης σχετικά με το papasotiriou.gr αφορά:

α) στην αναγνώριση της αξίας των κρίσιμων περιουσιακών στοιχείων της ηλεκτρονικής επιχείρησης σε όρους κόστους αντικατάστασης, κόστους συντήρησης, χαμένης παραγωγικότητας, κακής φήμης της επιχείρησης. Όπως έχει ήδη αναφερθεί, το πιο κρίσιμο περιουσιακό στοιχείο για το ηλεκτρονικό κατάστημα είναι η ύπαρξη και διαθεσιμότητα του δικτυακού τόπου. Συνεπώς η επίδραση έστω και μιας προσωρινής διακοπής της ιστοσελίδας είναι κόστος σε όρους αντικατάστασης, συντήρησης, κακής φήμης.

Υποθέτοντας ότι το ηλεκτρονικό κατάστημα λειτουργεί 7 ημέρες την εβδομάδα, 24 ώρες την ημέρα με μέσο αριθμό εσόδων ανά ώρα X € από τις παραγγελίες των πελατών, τότε ο μέσος αριθμός εσόδων ανά έτος από τις πωλήσεις είναι 365*24*X = 8.760*X €. Ο μέσος αριθμός εσόδων ανά ώρα προκύπτει είτε από εκτίμηση, είτε από στατιστική επεξεργασία των εσόδων του δικτυακού τόπου. Εάν επίσης υποτεθεί ότι η ιστοσελίδα δημιουργεί σταθερό έσοδο την ώρα, X €, τότε παραμένοντας εκτός λειτουργίας για 6 ώρες η υπολογίσιμη έκθεση σε κίνδυνο είναι 6*X / 8.760*X = 0,000685 = 0,0685% το έτος. Πολλαπλασιάζοντας το ποσοστό αυτό της έκθεσης με το μέσο αριθμό εσόδων ανά έτος από τις πωλήσεις, προβλέπεται ότι η χρηματοοικονομική επίδραση του κινδύνου αυτού στην αξία του περιουσιακού στοιχείου θα είναι 0,0685%*8.760*X = 6*X €.

β) στον υπολογισμό της ετήσιας αναμενόμενης απώλειας (ALE) η οποία πραγματοποιείται εάν το ηλεκτρονικό κατάστημα δε λάβει μέτρα για την ελαχιστοποίηση των κινδύνων. Για παράδειγμα, η εμφάνιση φωτιάς είναι δυνατό να

προκαλέσει απώλεια της τάξης των 2.000 € με πιθανότητα εμφάνισης 0,1, δηλαδή ARO = 0,1 που σημαίνει ότι η φωτιά εμφανίζεται κάθε 10 έτη. Η τιμή της ετήσιας αναμενόμενης απώλειας θα είναι ALE = 2.000*0,1 = 200 €, δηλαδή η πραγματοποίηση της συγκεκριμένης φυσικής απειλής προκαλεί απώλεια για το ηλεκτρονικό κατάστημα 200 € ή και λιγότερα το έτος. Ο προσδιορισμός αυτού του μεγέθους βοηθά τους υπευθύνους του papasotiriou.gr να εκτιμήσουν το κόστος των μέτρων ασφαλείας που θα προσδώσουν επαρκές επίπεδο προστασίας.

γ) στον υπολογισμό του κόστους των ελέγχων για τον οποίο απαιτείται η ακριβής εκτίμηση του ποσού απόκτησης, διατήρησης, λειτουργίας, ανάπτυξης, εφαρμογής κάθε επιπέδου ελέγχου. Η χρήση κατάλληλου λογισμικού, για παράδειγμα, που ανιχνεύει αδυναμίες ή καθιστά την ηλεκτρονική επιχείρηση ικανή να αντιμετωπίζει και να μελετά με ασφάλεια τις επιθέσεις, καθώς αυτές συμβαίνουν, περικλείει κόστος, τόσο στην απόκτησή του όσο και στη διατήρηση και εφαρμογή του.

δ) στον υπολογισμό της απόδοσης της επένδυσης σε σχέση με την ασφάλεια (ROSI). Εάν η ετήσια αναμενόμενη απώλεια που προκαλεί ένας εισβολέας όταν θέτει εκτός λειτουργίας το δικτυακό εξυπηρετητή είναι 12.000 € και ύστερα από την εφαρμογή συστήματος ασφάλειας είναι 3.000 €, καθώς επίσης εάν το ετήσιο κόστος συντήρησης και λειτουργίας του συστήματος ασφάλειας είναι 650 €, τότε η απόδοση της επένδυσης είναι 8.350 € το έτος. (ROSI = 12.000 - 3.000 - 650 = 8.350 €)

5.4 Έλεγχος κινδύνου

Ο μεγαλύτερος κίνδυνος που απασχολεί τη λειτουργία του papasotiriou.gr σχετίζεται με την ασφάλεια των συναλλαγών. Οι υπεύθυνοι τον κίνδυνο αυτό προσπαθούν να ελέγξουν και να αντιμετωπίσουν και για το λόγο αυτό χρησιμοποιούν το πρωτόκολλο SSL, με κρυπτογράφηση 128 bit (την πιο ισχυρή σήμερα), για

ασφαλείς on-line εμπορικές συναλλαγές. Με αυτόν τον τρόπο κρυπτογραφούνται όλες οι προσωπικές πληροφορίες των πελατών, συμπεριλαμβανομένων του αριθμού της πιστωτικής κάρτας, του ονόματος και της διεύθυνσης έτσι ώστε να μην μπορούν να διαβαστούν ή να αλλαχτούν κατά τη μεταφορά τους στο Διαδίκτυο. Το πρωτόκολλο SSL (Secure Sockets Layer) είναι σήμερα το παγκόσμιο standard στο Διαδίκτυο για την πιστοποίηση δικτυακών τόπων (web sites) στους δικτυακούς χρήστες και για την κρυπτογράφηση στοιχείων μεταξύ των δικτυακών χρηστών και των δικτυακών εξυπηρετητών. (web servers)

Μία κρυπτογραφημένη SSL επικοινωνία απαιτεί όλες τις πληροφορίες που αποστέλλονται μεταξύ ενός πελάτη και ενός εξυπηρετητή (server) να κρυπτογραφούνται από το λογισμικό αποστολής και να αποκρυπτογραφούνται από το λογισμικό αποδοχής, προστατεύοντας έτσι προσωπικές πληροφορίες κατά τη μεταφορά τους. Επιπλέον, όλες οι πληροφορίες που αποστέλλονται με το πρωτόκολλο SSL, προστατεύονται από ένα μηχανισμό που αυτόματα εξακριβώνει εάν τα δεδομένα έχουν αλλαχτεί κατά τη μεταφορά. Το σύστημα ασφαλούς επικοινωνίας του papasotiriou.gr είναι πιστοποιημένο από την εταιρεία Verisign.

5.5 Στρατηγικές για αρνητικούς κινδύνους ή απειλές

Αναφορικά με τις στρατηγικές απόκρισης σε κινδύνους οι οποίες είναι διαθέσιμες, το papasotiriou.gr, ακολουθεί στρατηγικές για απειλές ή κινδύνους που έχουν αρνητικές επιπτώσεις στη λειτουργία του. Οι στρατηγικές αυτές είναι η μεταβίβαση και ο μετριασμός.

Στη στρατηγική της μεταβίβασης οι υπεύθυνοι του papasotiriou.gr χρησιμοποιούν συμβόλαια μεταβίβασης ευθυνών συγκεκριμένων κινδύνων σε τρίτο μέρος, κυρίως σε

ασφαλιστική εταιρία. Τα συμβόλαια αυτά περιλαμβάνουν το κόστος της ασφάλισης, εγγυήσεις, ρήτρες απόδοσης κ.ά.

Στη στρατηγική του μετριασμού, το ηλεκτρονικό κατάστημα, λαμβάνει μέτρα για τη μείωση της πιθανότητας ή των επιπτώσεων εμφάνισης του κινδύνου. Μέσα στα πλαίσια αυτής της στρατηγικής οι υπεύθυνοι του papasotiriou.gr εντάσσουν το σχέδιο ασφάλειας που εφαρμόζουν.

5.6 Σχέδιο ασφάλειας

Το σχέδιο ασφάλειας που εφαρμόζεται στο papasotiriou.gr εμπεριέχει το σχέδιο προστασίας της τεχνολογικής υποδομής. Ο σχεδιασμός συστήματος προστασίας της τεχνολογικής υποδομής περιλαμβάνει την ανάπτυξη, τη συντήρηση και την προστασία των βάσεων δεδομένων μιας και αυτές εξασκούν σημαντική επίδραση στη διεκπεραίωση των εμπορικών συναλλαγών. Επίσης στο σχέδιο ασφάλειας εμπεριέχονται οι δοκιμές υπερφόρτωσης δικτύων και η ανάπτυξη συστήματος έγκαιρης ειδοποίησης σε περίπτωση κινδύνου. Αξίζει να σημειωθεί ότι η αναβάθμιση εφαρμογών καθώς και η λειτουργία της ανάκαμψης είναι συνιστώσες του σχεδίου ασφάλειας.

Επιπλέον οι εκτιμήσεις ετοιμότητας σε εξωτερικές εισβολές όπως hackers, ιοί, η διαχείριση δικαιωμάτων πρόσβασης του προσωπικού βάσει ρόλων στην επιχείρηση εντάσσονται στο σχέδιο ασφάλειας.

Γενικά στόχος του σχεδίου ασφάλειας σύμφωνα με τους υπευθύνους του papasotiriou.gr είναι τόσο η πρόληψη (π.χ. η εκτίμηση, η διόρθωση και η ενίσχυση των λειτουργικών συστημάτων και του γενικότερου πλαισίου υποδομής της επιχείρησης), όσο και η αποτελεσματική αντίδραση (π.χ. ο εντοπισμός, η αναφορά και η καταστολή παραβιάσεων στο σύστημα ασφάλειας).

Αναφορικά με τα προσωπικά δεδομένα, η προστασία τους σημαίνει παρεμπόδιση της μη εξουσιοδοτημένης πρόσβασης στα προσωπικά στοιχεία των πελατών βάσει των οποίων πραγματοποιούνται οι συναλλαγές, διαχείριση των επιλογών opt-in ή opt-out των πελατών σε σχέση με την κοινοποίηση ή μη των προσωπικών τους στοιχείων σε συνεργαζόμενες εταιρίες για λόγους προώθησης / marketing. Στο σημείο αυτό αξίζει να σημειωθεί ότι το papasotiriou.gr δεν κοινοποιεί με κανένα τρόπο τα προσωπικά δεδομένα των πελατών του σε συνεργαζόμενες με αυτό εταιρίες. Η προστασία των προσωπικών δεδομένων αφορά επίσης και στην προστασία όλων των εσωτερικών και εξωτερικών επικοινωνιών που διεξάγονται μέσω Διαδικτύου, στην εκούσια ή ακούσια κοινοποίηση εμπιστευτικών πληροφοριών εμπορικών συνεργατών και τέλος στη συμμόρφωση προς τη διεθνή νομοθεσία σχετικά με τις online συναλλαγές από χώρες του εξωτερικού.

Το σχέδιο ασφάλειας δίνει έμφαση και στις επιχειρηματικές διαδικασίες που κύριο μέλημά τους είναι η διατήρηση της ακεραιότητας των online συναλλαγών και πληρωμών συμπεριλαμβανομένων των ανολοκλήρωτων συναλλαγών και των συναλλαγών που πραγματοποιούνται περισσότερες από μια φορά από λάθος του πελάτη, στην ικανότητα ολοκλήρωσης των συναλλαγών σε περιπτώσεις πτώσης του δικτύου ή άλλης βλάβης, στη χρήση και διασύνδεση τρίτων μερών για την ασφαλή διαχείριση και ολοκλήρωσή τους. Ακόμα η παρακολούθηση και διαχείριση του ηλεκτρονικού ταχυδρομείου και των επισυναπτόμενων αρχείων (e-mail attachments) καθώς και ο εντοπισμός και η διαχείριση καίριων ηλεκτρονικών αρχείων συμβάλλουν στις επιτυχείς επιχειρηματικές διαδικασίες.

Μέσα στα πλαίσια του σχεδίου ασφάλειας εντάσσεται και η στάση της διοίκησης της επιχείρησης απέναντι στο προσωπικό. Η διοίκηση παρακολουθεί την επαγγελματική συμπεριφορά του προσωπικού, ώστε να εναρμονίζεται με τους

κανονισμούς και τις διαδικασίες που διέπουν το ηλεκτρονικό εμπόριο και επιπλέον μεριμνά για την εκπαίδευσή του η οποία είναι απαραίτητη στην υποστήριξη των αναγκών που σχετίζονται με τις νέες τεχνολογίες.

Τέλος, η ασφαλιστική κάλυψη τόσο των τεχνολογικών υποδομών όσο και των γενικότερων δραστηριοτήτων του ηλεκτρονικού εμπορίου συμπεριλαμβανομένων των επαγγελματικών σφαλμάτων ή παραλείψεων και της αντιμετώπισης του ηλεκτρονικού εγκλήματος αποτελούν συνισταμένες ενός ολοκληρωμένου συστήματος ασφάλειας που διαθέτει το papasotiriou.gr.

5.6.1 Αντίμετρα

Τα αντίμετρα αφορούν σε μηχανισμούς προστασίας απέναντι σε τεχνικές κυρίως απειλές. Για την αποτροπή και τον εντοπισμό του κακόβουλου λογισμικού για παράδειγμα, το papasotiriou.gr έχει προβεί στην εγκατάσταση και τακτική ενημέρωση προγραμμάτων antivirus ώστε να ελέγχονται οι προσωπικοί υπολογιστές και τα αποθηκευτικά μέσα.

Επειδή σκοπός είναι η διατήρηση της ακεραιότητας και της διαθεσιμότητας του πληροφοριακού συστήματος, υπάρχουν διαδικασίες ρουτίνας που αφορούν στην καθημερινή λήψη εφεδρικών αντιγράφων του συστήματος καθώς και στην καταγραφή γεγονότων και λαθών στο σύστημα.

Σε ό,τι αφορά στη χρήση συνθηματικών (passwords), δεν αποθηκεύονται ποτέ σε κάποιο υπολογιστικό σύστημα ή σε εκτεθειμένα σημεία. Ακόμα οι υπεύθυνοι του ηλεκτρονικού καταστήματος έχουν πολλές φορές σκεφτεί να χρησιμοποιήσουν στις περιπτώσεις φυσικά που κρίνεται απαραίτητο, ειδικούς βιομετρικούς μηχανισμούς αυθεντικοποίησης χρηστών (π.χ. δακτυλικά αποτυπώματα) με ταυτόχρονη χρήση ειδικών στοιχείων ασφάλειας, όπως έξυπνες κάρτες.

5.6.2 Πολιτική ασφάλειας

Επειδή η ομάδα διαχείρισης κινδύνων του papasotiriou.gr γνωρίζει πολύ καλά πως οι ηλεκτρονικές συναλλαγές και η μεταφορά δεδομένων μέσω του Διαδικτύου, είναι ευάλωτα σε ένα πλήθος δικτυακών κινδύνων που μπορούν να προκαλέσουν μη εξουσιοδοτημένη πρόσβαση και επέμβαση στα μεταφερόμενα δεδομένα, ή και τη διάπραξη απάτης, τα μέτρα ασφάλειας για την προστασία των ηλεκτρονικών συναλλαγών που εφαρμόζει, περιλαμβάνουν τα ακόλουθα:

- Αυθεντικοποίηση (authentication), η οποία αφορά στο επίπεδο εμπιστοσύνης που οι συναλλασσόμενοι απαιτούν σε σχέση με την ταυτότητα των εμπλεκόμενων μερών.
- Εξουσιοδότηση (authorization), η οποία αφορά στα δικαιώματα καθορισμού των παραμέτρων των συναλλαγών (τιμοκατάλογοι, ψηφιακά έγγραφα κ.τ.λ.). Επίσης οι συναλλασσόμενοι γνωρίζουν ποιος έχει τέτοια δικαιώματα.
- Διαδικασίες προστασίας και τήρησης ειδικών συμφωνιών ή συμβολαίων ανάμεσα στους συναλλασσόμενους.
- Ακεραιότητα (integrity) του τιμοκαταλόγου που γνωστοποιείται στους αγοραστές, καθώς και προστασία ευαίσθητων πληροφοριών για ειδικές επιπλέον εκπτώσεις.
- Επεξεργασία των παραγγελιών με τέτοιο τρόπο που να προστατεύει τα χαρακτηριστικά της κάθε παραγγελίας (στοιχεία αγοραστή, αγαθά, τρόπο πληρωμής κ.λ.π.)
- Διαδικασίες ελέγχου των πληροφοριών που παρέχει ο πελάτης για την πληρωμή των αγαθών.
- Καθορισμό του πλέον κατάλληλου τρόπου πληρωμής για την αποφυγή απάτης.

F Μηχανισμούς για την προστασία των στοιχείων της παραγγελίας αναφορικά με την ακεραιότητα και την εμπιστευτικότητα. Επιπλέον εξετάζονται τα κατάλληλα μέτρα προστασίας απέναντι στη διπλοεγγραφή ή την απώλεια των συναλλαγών.

F Καθορισμό των ευθυνών και ανάληψη κινδύνου για την περίπτωση απάτης.

Αρκετά από τα παραπάνω αντιμετωπίζονται με τη χρήση κρυπτογραφίας, στο papasotiriou.gr, σε συνδυασμό πάντα με τη σχετική νομοθεσία. Επιπλέον, το ηλεκτρονικό εμπόριο καλύπτεται από ειδική συμφωνία ανάμεσα στους συναλλασσόμενους. Σε αυτήν, ορίζονται οι όροι των συναλλαγών και αν κρίνεται απαραίτητο, το επίπεδο και η διαθεσιμότητα των παρεχόμενων υπηρεσιών. Τα δημόσια συστήματα ηλεκτρονικού εμπορίου έχουν στη διάθεση του κοινού, τους όρους συναλλαγών. Επίσης, ειδική προσοχή δίνεται στην προστασία των υπολογιστών που χρησιμοποιούνται για ηλεκτρονικό εμπόριο, όπως και των συνδέσεων που χρησιμοποιούν.

Επίσης για την ενίσχυση της πολιτικής ασφάλειας οι υπεύθυνοι του papasotiriou.gr ακολουθούν ορισμένες διαδικασίες σχετικά με τους κωδικούς πρόσβασης. Αυτές είναι:

- Εφαρμόζουν πολιτική συχνής αλλαγής των κωδικών πρόσβασης.
- Τηρούν αρχείο με τους κωδικούς πρόσβασης όλων των υπαλλήλων.
- Φροντίζουν οι υπάλληλοι να κατανοήσουν ότι οι κωδικοί πρόσβασης είναι ιδιοκτησία της επιχείρησης και όχι του προσωπικού.
- Αποθηκεύουν με ασφάλεια τους κωδικούς.
- Αποφεύγουν χρήση κωδικών που αποκαλύπτουν την ταυτότητα του χρήστη όπως ονοματεπώνυμο, ημερομηνίες γέννησης κ.τ.λ. Δημιουργούν κωδικούς

που συνδυάζουν αριθμούς, σημεία στίξης και πεζοκεφαλαία γράμματα του αλφαβήτου.

- Παρεμποδίζουν την πρόσβαση μη εξουσιοδοτημένων χρηστών, επισκεπτών στους υπολογιστές της εταιρίας
- Παρατηρούν ασυνήθιστες συμπεριφορές υπαλλήλων, όπως κατέβασμα μεγάλου αριθμού εταιρικών αρχείων, πρόσβαση στο δίκτυο της επιχείρησης τις νυχτερινές ώρες και εξετάζουν το ενδεχόμενο της εκ των έσω διαρροής εταιρικών πληροφοριών.

5.7 Διαχείριση επιχειρησιακής συνέχειας

Η διαχείριση της επιχειρησιακής συνέχειας στόχο έχει την αποτροπή των παρεμβολών στις δραστηριότητες της επιχείρησης και την προστασία των κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών. Μια διαδικασία διαχείρισης της επιχειρησιακής συνέχειας (business continuity management process) θα πρέπει να χρησιμοποιείται για τη μείωση σε κάποιο ανεκτό επίπεδο των επιπτώσεων από καταστροφές και συμβάντα σχετικά με την ασφάλεια της επιχείρησης. Έχουν αναπτυχθεί διάφορα σχέδια διαχείρισης επιχειρησιακής συνέχειας που πολλές φορές στη βιβλιογραφία αναφέρονται και ως σχέδια ανάκαμψης από καταστροφή (disaster recovery planning). Γενικά σε ένα σχέδιο ανάκαμψης από καταστροφή ακολουθούνται τα παρακάτω βήματα (Toigo, 2004):

- Προσδιορίζεται η πιθανή απειλή.
- Εφαρμόζεται διαδικασία επείγουσας ανάκαμψης.
- Ελέγχεται η ικανότητα ανάκαμψης του συστήματος.
- Εάν πραγματοποιηθεί ο κίνδυνος, τότε αποτιμάται και τίθεται άμεσα σε εφαρμογή το σχέδιο ανάκαμψης.

Το papasotiriou.gr απειλείται κυρίως από σκόπιμες ενέργειες και έτσι στο σχέδιο της επιχειρησιακής συνέχειας που προτείνεται θα πρέπει να περιλαμβάνονται μέτρα που στόχο έχουν την αποκατάσταση της φυσιολογικής λειτουργίας της ηλεκτρονικής επιχείρησης.

Ο σχεδιασμός και η υλοποίηση της επιχειρησιακής συνέχειας βασίζεται στην ακόλουθη διαδικασία:

- Στην κατανόηση των κινδύνων που ενδέχεται να απειλούν την επιχείρηση, στην πιθανότητα να υλοποιηθούν και στο κόστος που θα επιφέρουν. Χρειάζεται επίσης να καθοριστούν οι κρίσιμες λειτουργίες της επιχείρησης και να κατηγοριοποιηθούν με βάση την προτεραιότητά τους.
- Στην κατανόηση των επιπτώσεων κάθε παρεμβολής στη φυσιολογική λειτουργία της επιχείρησης. Θα πρέπει να υπάρχει σχέδιο αντιμετώπισης τόσο των μικρών, όσο και των σοβαρών συμβάντων.
- Στην πιθανή σύναψη κατάλληλου ασφαλιστηρίου συμβολαίου, το οποίο μπορεί να είναι μέρος του σχεδίου επιχειρησιακής συνέχειας.
- Στην κατάστρωση στρατηγικής επιχειρησιακής συνέχειας η οποία θα πρέπει να είναι σύμφωνη με τους στόχους και τις προτεραιότητες της επιχείρησης.
- Στην καταγραφή σχεδίου επιχειρησιακής συνέχειας που θα υλοποιεί την παραπάνω στρατηγική.
- Στον τακτικό έλεγχο και στην τακτική ενημέρωση του σχεδίου και των διαδικασιών που προβλέπονται σε αυτό.
- Στην ενσωμάτωση του σχεδίου σε όλες τις λειτουργίες της επιχείρησης και στην ευθύνη υλοποίησής του.

5.7.1 Καθορισμός επιπτώσεων

Η επιχειρησιακή συνέχεια βασίζεται στην αναγνώριση των γεγονότων που μπορούν να προκαλέσουν προβλήματα στη λειτουργία της ηλεκτρονικής επιχείρησης. Η αναγνώριση των γεγονότων αυτών και η ζημία που προξενείται στην επωνυμία και τη φήμη της επιχείρησης, στη χρηματοοικονομική αξία των συναλλαγών, σε θέματα σχετικά με την εμπιστοσύνη των πελατών στις συναλλαγές, σε ό,τι αφορά στο papasotiriou.gr, πραγματοποιείται μέσα στα πλαίσια της ανάλυσης ρίσκου η οποία καθορίζει πολλές φορές και την απαραίτητη χρονική περίοδο για την αποκατάσταση της ομαλής λειτουργίας της επιχείρησης. Στη διαδικασία αυτή συμμετέχει η διοίκηση της επιχείρησης που χαράσσει και τη στρατηγική που θα ακολουθηθεί στα πλαίσια της επιχειρησιακής συνέχειας.

5.7.2 Συγγραφή και υλοποίηση σχεδίου επιχειρησιακής συνέχειας

Στην ανάπτυξη του σχεδίου επιχειρησιακής συνέχειας πρέπει να εξετάζονται τα ακόλουθα:

- Η συμφωνία και ευθύνη των εμπλεκομένων.
- Ο καθορισμός ρεαλιστικών χρόνων αποκατάστασης της ομαλής λειτουργίας της επιχείρησης. Χρειάζεται ιδιαίτερη προσοχή στην αναγνώριση εξωτερικών παραγόντων που μπορούν να επηρεάσουν τις διαδικασίες αποκατάστασης.
- Η πλήρης καταγραφή των συμφωνηθέντων διαδικασιών.
- Η κατάλληλη εκπαίδευση του προσωπικού στην υλοποίηση του σχεδίου.
- Η δοκιμή και ενημέρωση του σχεδίου.

5.7.3 Πλαίσιο σχεδιασμού

Η επιχείρηση πρέπει να χρησιμοποιεί ένα ενιαίο πλαίσιο για την κατάστρωση του σχεδίου επιχειρησιακής συνέχειας, τον καθορισμό προτεραιοτήτων, τις δοκιμές και την τακτική ενημέρωση του σχεδίου. Πρέπει να αναφέρονται με σαφήνεια οι περιπτώσεις για τις οποίες ενεργοποιείται το σχέδιο (ή κάποιο μέρος του), καθώς και οι υπεύθυνοι για την εκτέλεσή του. Σε περίπτωση ύπαρξης νέων απαιτήσεων από την επιχείρηση το σχέδιο πρέπει να συμπληρώνεται κατάλληλα. Το πλαίσιο ανάπτυξης του σχεδίου επιχειρησιακής συνέχειας πρέπει να εξετάζει τα ακόλουθα:

- Τις συνθήκες ενεργοποίησης του σχεδίου.
- Τις διαδικασίες προσωρινής αποκατάστασης των λειτουργιών της επιχείρησης, έως ότου ολοκληρωθεί η πλήρης αποκατάσταση. (εφεδρικός εξοπλισμός, συνεργασία με τρίτους για παροχή υπηρεσιών)
- Τις διαδικασίες που απαιτούνται για την πλήρη αποκατάσταση των λειτουργιών της επιχείρησης.
- Το χρονοδιάγραμμα συντήρησης του σχεδίου, το οποίο πρέπει να περιλαμβάνει τις απαραίτητες δοκιμές και ενημερώσεις.
- Την εκπαίδευση του προσωπικού στην αναγκαιότητα και την εκτέλεση του σχεδίου επιχειρησιακής συνέχειας.
- Τον καταμερισμό των ευθυνών για την εκτέλεση του σχεδίου.

5.7.4 Δοκιμή του σχεδίου

Το σχέδιο επιχειρησιακής συνέχειας είναι πολύ πιθανό να αποτύχει κατά τη δοκιμή του. Αυτό συμβαίνει λόγω λανθασμένων υποθέσεων, αλλαγών στο προσωπικό και στον εξοπλισμό ή λόγω παραβλέψεων. Για το λόγο αυτό πρέπει να

δοκιμάζεται σε τακτά χρονικά διαστήματα, σε όλες του τις διαστάσεις προκειμένου να διασφαλιστεί η εγκυρότητα και η αποτελεσματικότητά του.

Κατά τη δοκιμή του σχεδίου, πρέπει να υπάρχει σαφές χρονοδιάγραμμα για κάθε τμήμα που θα εξεταστεί. Προτείνεται επίσης η συχνή δοκιμή των επιμέρους τμημάτων του σχεδίου. Υπάρχουν διάφορες τεχνικές με βάση τις οποίες μπορεί να γίνει η δοκιμή ενός σχεδίου. Πρέπει να περιλαμβάνουν τα ακόλουθα:

- Τον έλεγχο διαφόρων σεναρίων σε θεωρητικό επίπεδο.
- Την προσομοίωση διαφόρων γεγονότων, ειδικά κατά την εκπαίδευση του προσωπικού.
- Τον έλεγχο των δυνατοτήτων του εξοπλισμού να αντεπεξέλθει στις απαιτήσεις του σχεδίου.
- Τη δοκιμή του σχεδίου σε εναλλακτικές εγκαταστάσεις ώστε να μην δημιουργούνται παρεμβολές στη λειτουργία της επιχείρησης.
- Τις δοκιμές των δυνατοτήτων των εξωτερικών συνεργατών να αντεπεξέλθουν στις απαιτήσεις του σχεδίου.
- Τη διενέργεια πλήρους υλοποίησης του σχεδίου ώστε να δοκιμαστεί η δυνατότητα όλων να ενεργήσουν όπως προβλέπεται.

5.7.5 Ενημέρωση και επανέλεγχος του σχεδίου

Το σχέδιο επιχειρησιακής συνέχειας πρέπει να συντηρείται και να ενημερώνεται με χρήση τακτικών ελέγχων για τη διασφάλιση της αποτελεσματικότητάς του. Οι σχετικές διαδικασίες πρέπει να αποτελούν μέρος της γενικότερης διαχείρισης των αλλαγών μέσα στην επιχείρηση, ώστε να αποδίδεται η ανάλογη αξία στα ζητήματα επιχειρησιακής συνέχειας. Επιπλέον, με αυτό τον τρόπο οι όποιες αλλαγές στο σχέδιο θα επιβάλλονται και από τις αλλαγές που συντελούνται στις υπόλοιπες διαδικασίες

της επιχείρησης. Αλλαγές στο σχέδιο μπορούν να προκληθούν από αλλαγές στα ακόλουθα:

- Στο προσωπικό.
- Στους τρόπους επικοινωνίας με την επιχείρηση (τηλέφωνα, διευθύνσεις)
- Στη στρατηγική της επιχείρησης.
- Στη νομοθεσία.
- Στους εξωτερικούς συνεργάτες, στους προμηθευτές ή στους σημαντικούς πελάτες.
- Στους κινδύνους που απειλούν την επιχείρηση.

5.8 Συμπεράσματα

5.8.1 Ανακεφαλαίωση

Στην παρούσα διπλωματική εργασία που διακρίθηκε σε δύο μέρη, επιχειρήθηκε η προσέγγιση της διαχείρισης κινδύνων στην περιοχή του ηλεκτρονικού εμπορίου.

Στο πρώτο μέρος το οποίο αποτελεί το θεωρητικό μέρος της εν λόγω εργασίας, δόθηκε ιδιαίτερη έμφαση στους κινδύνους, τεχνικούς και μη, που απειλούν την εφαρμογή του ηλεκτρονικού εμπορίου ως επιχειρηματικής πρακτικής. Επίσης αναλύθηκαν διεξοδικά τα στάδια διαχείρισης κρίσεων και εντοπίστηκε ο ρόλος της ασφάλισης απέναντι στους κινδύνους του ηλεκτρονικού εμπορίου σε χώρες του εξωτερικού και στην Ελλάδα.

Στο δεύτερο μέρος στο οποίο περιέχεται το πρακτικό μέρος της παρούσας μελέτης, σχολιάστηκαν έρευνες που έχουν πραγματοποιηθεί στο παρελθόν για την ύπαρξη και την ασφάλεια του ηλεκτρονικού εμπορίου στην Ελλάδα και επιπλέον

δόθηκε ιδιαίτερη βαρύτητα στα εμπόδια και στους λόγους που συντρέχουν για τη δημιουργία ηλεκτρονικού καταστήματος. Τέλος, μελετήθηκε η περίπτωση του δικτυακού τόπου papasotiriou.gr. Στη μελέτη αυτή έγινε εφαρμογή της ποσοτικής ανάλυσης του κινδύνου και σχολιάστηκε το σχέδιο ασφάλειας που εφαρμόζεται. Επιπλέον προτάθηκε σχέδιο επιχειρησιακής συνέχειας για την αποτροπή των παρεμβολών στις δραστηριότητες της ηλεκτρονικής επιχείρησης και την προστασία κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών.

5.8.2 Κυριότερα συμπεράσματα

Αν και οι τεχνολογικές λύσεις για την αντιμετώπιση απειλών συνεχώς κερδίζουν έδαφος καθώς και οι χρήστες γνωρίζουν τις πραγματικές τους ανάγκες, λίγες είναι εκείνες οι επιχειρήσεις που έχουν ολοκληρωμένα συστήματα ασφάλειας προκειμένου να αντισταθούν σε επικείμενους κινδύνους οι οποίοι θέτουν σε αμφισβήτηση τη μελλοντική λειτουργία και βιωσιμότητά τους.

Οι απαρχαιωμένες διαδικασίες ασφάλειας και η διαχείριση του κινδύνου, αφού έχει πραγματοποιηθεί, υποδηλώνουν ανεύθυνη συμπεριφορά απέναντι στην ύπαρξη του κινδύνου και απουσία πλάνου διαχείρισης κρίσης που να καθορίζει συγκεκριμένες ανάγκες. Επίσης σε ό,τι αφορά στην ελληνική ηλεκτρονική αγορά στο σύνολό της, δεν υπάρχουν μελέτες που να αποδεικνύουν σοβαρές προσπάθειες αποτίμησης του κινδύνου.

Μπορεί η ύπαρξη ενός πλαισίου διαχείρισης κρίσεων να είναι μια δαπανηρή και χρονοβόρα διαδικασία για την πλειονότητα των ελληνικών ηλεκτρονικών καταστημάτων και έτσι να μην ακολουθείται, ωστόσο αποτελεί εμπορική δραστηριότητα που αποφέρει έσοδα.

Επιπλέον η δαπάνη μεγάλων χρηματικών ποσών για την αποτίμηση του κινδύνου και την αγορά της κατάλληλης ασφαλιστικής κάλυψης από την πλευρά των ελληνικών ηλεκτρονικών επιχειρήσεων, αποτελεί ανησυχία των στελεχών των ασφαλιστικών εταιριών, μιας και οι ηλεκτρονικές επιχειρήσεις στην Ελλάδα δεν έχουν ακόμα το κατάλληλο υπόβαθρο οργάνωσης έτσι ώστε να κατανοήσουν πλήρως και να αποτυπώσουν την ευπάθειά τους στο η-επιχειρείν.

Ηλεκτρονικές επιχειρήσεις όμως, σαν το δικτυακό τόπο papasotiriou.gr αποτελούν εξαίρεση του κανόνα και έχουν κατορθώσει να αναπτύξουν ένα εσωτερικό εργαλείο αποτίμησης και αποτελεσματικής διαχείρισης κρίσεων, κατέχοντας πλήρως τα ζητήματα που σχετίζονται με την τεχνολογία, το προσωπικό, τη διοίκηση. Δίνοντας έμφαση στην εκπαίδευση του προσωπικού, στη χρήση πολλές φορές ικανών εξωτερικών συνεργατών και συμβούλων και στην ανάθεση σε εξειδικευμένο ασφαλιστικό φορέα των δραστηριοτήτων του ηλεκτρονικού εμπορίου οδηγούνται στην καλύτερη προστασία της επιχείρησης από εσωτερικούς και εξωτερικούς κινδύνους. Επιπροσθέτως η κατάρτιση ειδικών πολιτικών διαχείρισης κρίσεων στόχο έχει τη στήριξη και τη βιωσιμότητα της επιχείρησης στον ηλεκτρονικό επιχειρηματικό στίβο.

5.8.3 Προτάσεις

Στην παρούσα διπλωματική εργασία προτείνεται ένα σχέδιο επιχειρησιακής συνέχειας (business continuity) που σε συνδυασμό με την ανάλυση και τον έλεγχο του κινδύνου εξασφαλίζεται η προστασία των κρίσιμων διαδικασιών του ηλεκτρονικού καταστήματος στην περίπτωση μερικών ή ολικών καταστροφών. Περιλαμβάνει μέτρα που στόχο έχουν την αποκατάσταση της φυσιολογικής

λειτουργίας της ηλεκτρονικής επιχείρησης καθώς επίσης αποτελούν αναγκαίες δραστηριότητες η δοκιμή, η ενημέρωση και ο επανέλεγχος του εν λόγω σχεδίου.

Αξίζει να σημειωθεί πως θα ήταν χρήσιμο να αναφερθούν προτάσεις οι οποίες να συστηματοποιούν τους κινδύνους που απειλούν μια ηλεκτρονική επιχείρηση οδηγώντας στην κατασκευή ενός συγκεκριμένου μοντέλου το οποίο να βρίσκει εφαρμογή σε όλους τους τύπους ηλεκτρονικών καταστημάτων μετρώντας τις επιπτώσεις των κινδύνων σε όρους εσόδων, κόστους συντήρησης, αντικατάστασης, απόκτησης και διαθεσιμότητας της ιστοσελίδας, παραγωγικότητας, φήμης. Στο μοντέλο αυτό πέρα από την ανάλυση και τον έλεγχο του κινδύνου θα μπορούσε να ενσωματώνεται και σχέδιο επιχειρησιακής συνέχειας, δίνοντας έτσι ένα ολοκληρωμένο πλαίσιο διαχείρισης κρίσης για μια ηλεκτρονική επιχείρηση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνικές αναφορές

1. Αναστασιάδης Π. Τα πληροφοριακά συστήματα διοίκησης στη νέα οικονομία. Η νέα ψηφιακή μεταμηχανογραφημένη επιχείρηση. *Information Society Library, Alfa books, Scientific Editions,* Αθήνα 2001.
2. Αρτίκης Θ. Σημειώσεις Διοίκησης Κινδύνου Πειραιάς 2002
3. Γεωργόπουλος Ν., Πανταζή Μ.-Α., Νικολαράκος Χ., Βαγγελάτος Ι. Ηλεκτρονικό Επιχειρείν εκδόσεις *Ε. Μπένου,* Αθήνα 2001
4. Δουκίδης Γ., Πολυμενάκου Α., Γεωργόπουλος Ν., Μότσιος Θ. Το Ηλεκτρονικό Επιχειρείν στις Μεγάλες Ελληνικές Επιχειρήσεις, Εταιρία Ανώτατων Στελεχών Επιχειρήσεων (Ε.Α.Σ.Ε.), 2001
5. Εθνικό Δίκτυο Έρευνας και Τεχνολογίας- Ε.Δ.Ε.Τ. Α.Ε. «Εθνική Έρευνα για τις Νέες Τεχνολογίες και την Κοινωνία της Πληροφορίας», Οκτώβριος – Νοέμβριος 2005
6. Καλαμποκά Μ. «Έκρηξη των on-line πωλήσεων στη χώρα μας», ΝΑΥΤΕΜΠΟΡΙΚΗ, Δευτέρα, 17 Δεκεμβρίου 2001
7. Καλαμποκά Μ. «Το on-line shopping σε εποχή άνθισης», ΝΑΥΤΕΜΠΟΡΙΚΗ, Πέμπτη, 9 Αυγούστου 2001
8. Καλαμποκά Μ. «Πενταετία ανάπτυξης για το ηλεκτρονικό εμπόριο», ΝΑΥΤΕΜΠΟΡΙΚΗ, Τετάρτη, 20 Φεβρουαρίου 2002
9. Καλεμικεράκη Χ. Διπλωματική εργασία με θέμα: Ηλεκτρονικό Εμπόριο και Ηλεκτρονική Τραπεζική του Π.Μ.Σ. στη «Διοίκηση Επιχειρήσεων», Πειραιάς 2003

10. Κατραμάδος Ι. Διπλωματική εργασία με θέμα: Ηλεκτρονικές βάσεις δεδομένων-Απειλές και μέθοδοι προστασίας του Π.Μ.Σ. «Εφοδιασμός και Διακίνηση Προϊόντων Logistics», Πειραιάς 2003
11. «Τώρα αρχίζει η επανάσταση στο ηλεκτρονικό εμπόριο», ΝΑΥΤΕΜΠΟΡΙΚΗ, Σάββατο, 9 Φεβρουαρίου 2002, http://www.naftemporiki.gr/news/static/02/02/09/196413.htm
12. Πανηγυράκης Γ. και Βεντούρα Ζ. Σύγχρονη Διοικητική Δημοσίων Σχέσεων εκδόσεις *Μπένου*, Αθήνα 2001
13. Πασχόπουλος Α. και Σκαλτσάς Π. Ηλεκτρονικό Εμπόριο (Νέο περιβάλλον, Νέα εργαλεία, Νέοι ηγέτες) εκδόσεις *Κλειδάριθμος*, www.klidarithmos.gr Αθήνα 2000

Ξένες αναφορές

1. A Guide to the Project Management Body of Knowledge (PMBOK Guide) *third edition* 2004 Project Management Institute U.S.A.
2. AICPA Top Technologies Survey *The American Institute of Certified Public Accountants* Available from: http://www.aicpa.org/download/news/2005_0103.pdf; 2005 (retrieved June 9, 2005)
3. Barton L. Crisis in Organisations: Managing and Communicating in the Heat of Chaos, *South-Western Publishing Co,* Cincinnati 1993
4. Bloch M., Pigneur Y., and Segev A.: "On the road of electronic commerce-a business value framawork, gaining competitive advantage and some research issues", March 1996 http://www.stern.nyu.edu/~mbloch/docs/roadtoec/ec.htm

5. Boritz JE Managing enterprise information integrity: security, control and audit issues, U.S.A.: *IT Governance Institute*, 2004
6. Caponigro J.R. The Crisis Counsellor: A Step-By-Step Guide to Managing a Business Crisis *Contemporary Books*, Chicago 2000
7. CERT/CC: CERT/CC Statistics 1998-2002 http://www.cert.org/stats/cert_stats.html (accessed April 2003)
8. Clarke, Roger Electronic Commerce Definitions, October 4, 2000 http://www.anu.edu.au/people/Roger.Clarke/EC/ECDefns.html
9. Coles S. Robert and Rolf Moulton Operationalizing IT Risk Management *Elsevier,* Computers and Security, 2003
10. CommerceNet 2000 Survey, "Barriers to Electronic Commerce", http://www.commerce.net/research/barriers-inhibitors/2000/Barriers2000.study.pdf
11. Conner FW, Coviello AW Information security governance: a call to action *The Corporate Governance Task Force* Available from: http://www.cyberpartnership.org/InfoSecGov4_04.pdf; 2004 (retrieved October 9, 2004)
12. CSO Magazine: "2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes" *CSO Magazine*, May, 25, 2004 http://www.cert.org/about/ecrime.html (accessed October 2004), http://www.cve.mitre.org (accessed 1999-2005)
13. Damle P. "Social Engineering: A Tip of the Iceberg" *Information Systems Control* Journal 2 (2002)

14. Darling J.R. Crisis Management in International Business: Keys to Effective Decision-Making *Leadership & Organisation Development Journal 15, issue 8* 1994
15. "e-Commerce in Greece: From Fiction to Reality", A Strategic International Research, June 2001, http://www.strategic.gr/marketreports/eCommerce-pdf.htm
16. Fink S. Crisis Management Planning for the Inevitable AMACOM, New York 2000
17. Finne T. Information Systems Risk Management: Key Concepts and Business Processes, *Elsevier,* Computers and Security, 2000
18. Fisher D. MyDoom E-Mail Worm Spreading Quickly eWeek, January 26, 2004, www.eweek.com/article2/0,1759,1460809,00.asp (accessed October 2004)
19. Hickman J. and Crandall W. Before Disaster Hits: A Multifaceted Approach to Crisis Management *Business Horizons 40, issue 2* 1997
20. Horton TR, Le Grand CH, Murray WH, Ozier WJ, Parker DB Information security management and assurance: a call to action for corporate governance *The Institute of Internal Auditors* Available from: http://www.thelia.org/download.cfm?file=22.398;2000 (retrieved October 6, 2003)
21. Huff S., Wade M., Parent M., Schneberger S. and Newson P. Critical Success Factors for Electronic Commerce Cases in E.C., *Irwin McGraw-Hill*, 2000
22. Hunter P. 2005 IT security highlights-the day of the amateur hacker has gone, but there are still plenty of amateur users…. *Elsevier,* Computer Fraud and Security, January 2006

23. Hwang P. and Lechtenthal D.J. Anatomy of Organisational Crises *Journal of Contingencies and Crisis Management* volume 8, issue 3 2000

24. ICSA "Malicious Code Problem Continues to Worsen, According to 9th Annual ICSA Labs Virus Prevalence Survey" *TruSecure Corporation*, 2004 http://www.trusecure.com/company/press/pr_20040322.shtml (accessed October 2004)

25. Kanagalingam A. Information Systems Supervision Unit at the Bank of Malaysia October 2000

26. Kay T. Security + Berkeley, CA: *McGraw-Hill* Osborne, 2003

27. Keen P., Balance C., Chan S. and Schrump S. Electronic Commerce Relationships, *Prentice Hall*, 2000

28. Laudon K.C., Laudon J.P. Management Information Systems *Prentice-Hall Editions, Seventh Edition,* 2002

29. Lemos R. Mitnick Teaches "Social Engineering" ZD Net News, July 17, 2000 www.zdnet.com.com/2100-11-522261.html?legacy=zdnn (accessed November 2004)

30. Lev B. Intangibles: management, measurement and reporting Washington D.C., U.S.A.: *Brookings Institute Press.* Available from: http://www.icgrowth.com/resources/documents/Brookings.Lev.Intangibles.01.02.20.pdf; 2001 (retrieved February 10, 2004)

31. Lindberg D. Corporate governance-the role of the audit committee Available from: http://www.cob.ilstu.edu/katie/WorkingPapers/CorporateGovernance.Paper1%5B1%5D.isu.doc; 2005 (retrieved July 9, 2005)

32. McConnell M. Information Assurance in the Twenty-First Century *IEEE Security and Privacy*, 2002 www.computer.org/security/supplement1/mcc/?smsession=no (accessed November 2004)
33. Mitnick K. and Simon W. The Art of Deception New York: *Wiley*, 2002
34. Mitroff L. Programming for Crisis Control *Security Management* October 1989
35. Pearson C. and Clair J.A. Reframing Crisis Management *The Academy of Management Review, volume 23, issue1* 1998
36. Reid R. and Floyd S. Extending the Risk Analysis Model to Include Market-Insurance *Elsevier*, Computers and Security, volume 20, issue 4, 2001
37. SANS "The SANS Top 20 Internet Security Vulnerabilities" *Sans Institute*, 2004, http://www.sans.org/top20/#threats (accessed October 2004)
38. Simbo A.K. Catastrophe Planning and Crisis Management *Risk Management* volume 40, issue 2 1993
39. Slater, Derek What is E-Commerce?, *CIO Enterprise Magazine* June 15, 1999, http://www.cio.com/archive/enterprise/061599_curve.html
40. Smith D. Beyond Contingency Planning Towards a Model of Crisis Management *Industrial Crisis Quarterly* volume 4, issue 4 1990
41. Spillan J. An Exploratory Model for Evaluating Crisis Events and Managers' Concerns in Non-Profit Organizations *Journal of Contingencies and Crisis Management* volume 11, number 4, December 2003.
42. Stokes S. Managing Change in the MIS Environment Handbook of MIS Management, *Auerbach Publishing*, 1989

43. Toigo J.W. Disaster Recovery Planning-Preparing for the unthinkable *3rd edition Prentice Hall* 2004

44. Turban E., Lee J., King D.,Chung H.M. Electronic Commerce: A Managerial Perspective *Prentice Hall Editions* 2000

45. Turban E., King D., Viehland D., Lee J. Electronic Commerce: A Managerial Perspective 2006 *Prentice Hall Editions* 2006

46. Viehland D. Managing Business Risk in Electronic Commerce Massey University, New Zealand, 2001

47. Vitale M. The Growing Risks of Information Systems Success Management Information Systems December 1986