Το ηλεκτρονικό επιχειρείν σε μία περίοδο κρίσης
Η ασφάλεια σε κίνδυνο

Μπελίδης Αθανάσιος, Καργίδης Θεόδωρος
Τμήμα Εμπορίας και Διαφήμισης, Σχολή ΣΔΟ,
ΑΤΕΙ Θεσσαλονίκης,
abelidis@mkt.teithe.gr, kargidis@mkt.teithe.gr

Χατζηπουλίδης Αριστείδης
Τμήμα Εφαρμοσμένης Πληροφορικής,
Πανεπιστήμιο Μακεδονίας,
chataris@uom.gr

Περίληψη
Το ηλεκτρονικό επιχειρείν (ebusiness) έχει αναπτυχθεί σε παγκόσμιο επίπεδο και έχει δημιουργήσει ένα διαδικτυακό κόσμο που κατοικείται ήδη από ένα δισεκατομμύριο πελάτες. Εντούτοις, η τρέχουσα χρονική περίοδος χαρακτηρίζεται από αβεβαιότητα και οικονομική κρίση. Αυτό έχει άμεση επιρροή στην προοπτική των διαδυκτιακών εμπορικών συναλλαγών. Θέματα μείζονος σημασίας αποτελούν η ασφάλεια, η μυστικότητα και η εμπιστοσύνη των προσωπικών στοιχείων. Ο τελικός προορισμός είναι η ικανοποίηση των πελατειακών αναγκών. Οι προτεινόμενες συστάσεις γίνονται με βάση την μεγιστοποίηση της ασφάλειας, την μείωση των δαπανών και την κοινωνική αφύπνιση του κοινού. Το μάρκετινγκ πρέπει να ενσωματώσει όλες τις δυνάμεις που επηρεάζουν την λειτουργία του ηλεκτρονικό επιχειρείν πείθοντας το κοινό για τις δυνατότητες του και την ασφάλεια. Ένα είναι σίγουρο, οι εταιρίες που επιθυμούν να κερδίσουν ένα ανταγωνιστικό πλεονέκτημα βάση ηλεκτρονικών συναλλαγών διατρέχουν πολλές προκλήσεις, ιδιαίτερα σε μια περίοδο αστάθειας.

Λέξεις - Κλειδιά: ηλεκτρονικό επιχειρείν, μάρκετινγκ, ασφάλεια διαδικτύου, τεχνολογία πληροφοριών, καταναλωτική συμπεριφορά.

Τυποποίηση JEL: D81, G20, M15, M31

Εισαγωγή

Όλες οι επιχειρήσεις έχουν συνειδητοποιήσει ότι επιτακτική χρίζεται η ανάγκη για συνεχή και διαρκή καινοτομία όπως και προσαρμογή στις εξελίξεις των καιρών. Αυτό επιβάλουν οι νέες συνθήκες στην ασφάλεια των υπολογιστών και στις ανάγκες των πελατών που γίνονται ολοένα και πιο απαιτητικές. Οι προκλήσεις οδηγούν πλέον στην δημιουργία νέων προϊόντων και υπηρεσιών, προσανατολισμένα στις εξατομικευμένες ανάγκες του εκάστοτε πελάτη. Η τάση αυτή έχει οδηγήσει πολλές εταιρίες στην υιοθέτηση του διαδικτύου ως μέσο προβολής της εταιρικής εμπορικής παρουσίας (Barnes & Hinton, 2007). Ο σκοπός του εν λόγω άρθρου είναι η έρευνα σε θέματα ανθρώπινης συμπεριφοράς και διαχείρισης της ασφάλειας στο διαδίκτυο, αναλύοντας τα εργαλεία που μπορούν να βοηθήσουν στην βελτίωση τους.

Ο Porter (2001) είχε προβλέψει ότι το διαδίκτυο θα άλλαζε την παραδοσιακή σχέση μεταξύ προμηθευτών και πελατών. Με την πάροδο των ετών οι περισσότερες εταιρίες αντιλήφθηκάν τη δυναμικότητα και την

απήχηση του διαδικτύου στο ευρύ κοινό και αρκετές το ενέταξαν επιτυχώς στις κύριες εμπορικές τους δραστηριότητες. Σήμερα, το διαδίκτυο προβάλλεται ως στρατηγικό μέσο ενημέρωσης και προβολής θέτοντας νέα δεδομένα στην επιχειρησιακή δυναμική των εταιριών που γνωρίζουν να το χειρίζονται ανάλογα. Ο ορισμός που χαρακτηρίζει τις εν λόγω διαδικτυακές εμπορικές δραστηριότητες, είναι γνωστός ως ηλεκτρονικό επιχειρείν (electronic business).

Γεγονός είναι ότι το ηλεκτρονικό επιχειρείν, έχει ανάγει την έννοια του ανταγωνισμού σε άλλο επίπεδο. Ενσωματώνει πολλαπλά πλεονεκτήματα όπως η 24ωρη διαθεσιμότητα των προϊόντων και υπηρεσιών, η άμεση δυνατότητα σύγκρισης τιμών και χαρακτηριστικών όπως επίσης και η δυνατότητα επαφής με μεγαλύτερο μερίδιο της αγοράς. Επιπλέον, το ηλεκτρονικό επιχειρείν έχει επαναπροσδιορίσει την επικοινωνία μεταξύ πελάτη και εμπόρου χτίζοντας ακόμα πιο άμεση σχέση χωρίς την ανάγκη μεσαζόντων (Johnson et al., 2006; Shunk et al., 2007). Η διαδικασία αυτή είναι γνωστή και ως αποδιαμεσολάβηση (disintermediation).

Παρόλο όμως την δυναμικότητα που χαρακτηρίζει το ηλεκτρονικό επιχειρείν, η σημερινή χρονική περίοδος επηρεάζει την αποτελεσματικότητα του και θέτει εκ νέου ερωτηματικά πίσω από χρόνια ζητήματα όπως η ασφάλεια των διαδικτυακών συναλλαγών. Πλέον, οι επιχειρήσεις καλούνται να ενσωματώσουν στρατηγικές μεθόδους στην διαδικτυακή τους παρουσία. Γεγονός είναι ότι η ασφάλεια και το απόρρητο των προσωπικών στοιχείων έχουν προταχθεί (Smith & Chaffey, 2005) ως τα μεγαλύτερα εμπόδια στην εξάπλωση και ανάπτυξη των ηλεκτρονικών συναλλαγών. Επίσης, η εμπιστοσύνη των πελατών από και προς το διαδίκτυο είναι ιδιαίτερης σημασίας. Η ηλεκτρονική εμπιστοσύνη (e-trust) έχει προταθεί ως πρωτεύον θέμα που επιδρά σημαντικά στον τρόπο της ηλεκτρονικής ανθρώπινης συμπεριφοράς (Jin et al., 2008).

Σημαντικές προκλήσεις σε θέματα ασφάλειας στον χώρο της επιχειρηματικής λειτουργίας παρουσίαζε ανέκαθεν η χρήση των τεχνολογιών πληροφορικής και επικοινωνιών. Η εν λόγω χρήση προκαλεί σοβαρές ηθικές ερωτήσεις στην ευρύτερη κοινωνία. Πέρα όμως από τις απειλές που εμφανίζονται από τη χρήση των τεχνολογιών πληροφορικής, αυτό που δεν μπορεί να αμφισβητηθεί είναι η αποτελεσματικότητα τους. Για παράδειγμα αποτελεί η πληρέστερη οργάνωση και συστηματοποίηση των πληροφοριών που σε αντίθετη περίπτωση θα επικρατούσε χαοτική κατάσταση (Matten & Moon, 2004). Κατά συνέπεια, είναι επιχειρησιακή ευθύνη να ελαχιστοποιήσει τα καταστρεπτικά αποτελέσματα και να μεγιστοποιήσει τα ευεργετικά, αποσκοπώντας στην ασφάλεια και την αρτιότερη διαχείριση των πιθανών κινδύνων.

Το μάρκετινγκ μπορεί να υποστηρίξει την συγκεκριμένη επιχειρησιακή προσπάθεια, για την πληρέστερη αντιμετώπιση των κινδύνων, με προωθητικές εκστρατείες επιβάλλοντας στην κοινωνική συνείδηση ότι το ηλεκτρονικό επιχειρείν αποτελεί αναπόσπαστο κομμάτι των επιχειρησιακών δραστηριοτήτων και όχι συμπληρωματικό. Για την επίτευξη του στόχου απαιτείτε ένας συνεπής προγραμματισμός και σχεδιασμός των επιχειρησιακών προτύπων ώστε να μετατραπεί ακόμα και η χειρότερη κρίση σε ευκαιρία για επιτυχή διαφοροποίηση και ανάκαμψη. Το συστατικό επιτυχίας έγκειται στη διατήρηση της ψυχραιμίας και του ελέγχου των μεταβλητών που επηρεάζουν την εκάστοτε χρονική και επιχειρηματική περίοδο.

Η διοίκηση των αλλαγών

Ζούμε σε μια ευρύτερη κοινωνία της πληροφορίας επομένως η διαχείριση των στοιχείων και πληροφοριών οφείλει να εναρμονιστεί με τον επιχειρησιακό σκοπό, την ηθική και την ευθύνη. Οποιοδήποτε εργαλείο της τεχνολογίας των πληροφοριών που μπορεί να παράγει αποτελέσματα, πέρα από ένα συγκεκριμένο επιχειρησιακό φάσμα λειτουργίας, οφείλει να αναθεωρείτε σε τακτά χρονικά διαστήματα, κυρίως κατά τη φάση του σχεδιασμού. Απώτερος στόχος είναι η δημιουργία ικανότητας προσφοράς ανανεώσιμων πελατοκεντρικών προϊόντων και υπηρεσιών με τη μέγιστη δυνατή χρησιμότητα (Chaffey et al., 2003).

Η «αλλαγή» και ο «επαναπροσδιορισμός» πρέπει να γίνουν συνώνυμες έννοιες με τις αρχές της εταιρικής διοίκησης. Οι εποχές αλλάζουν, ο χρόνος φθείρει και ανανεώνει ενώ η σταθερότητα επιφέρει στασιμότητα. Χαρακτηριστικό γνώρισμα ενός οικονομικά δομημένου συστήματος είναι ότι οι συναλλαγές στηρίζονται σε οικονομικούς κύκλους ζωής (economic life cycles), που διαμορφώνουν την προσφορά και την ζήτηση και επηρεάζουν την συμπεριφορά της κοινωνίας (Facchini & Verdier, 2008). Συγκεκριμένα, η μεταβολή της παρούσας χρονικής περιόδου επιφέρει εξελίξεις στο ηλεκτρονικό επιχειρείν, επισημαίνοντας την ευπάθειά του μέσα από το περιβάλλον της ασφάλειας των πληροφοριών. Συνοδευόμενο από την τρέχουσα οικονομική κρίση, αποτελεί ένα κίνητρο για την διερεύνηση της εμπορικής συμπεριφοράς στις διαδικτυακές συναλλαγές. Οι έμποροι και τα κυβερνητικά όργανα έχουν επενδύσει μεγάλα χρηματικά ποσά σε έναν αντίστοιχο μεγάλο αριθμό τεχνολογιών ασφάλειας και μηχανισμών μυστικότητας με την ελπίδα ότι οι καταναλωτές θα αποκτήσουν μεγαλύτερη άνεση στις απευθείας σύνδεσης ηλεκτρονικές συναλλαγές τους. Αυτές οι επενδύσεις είναι πρωτίστως υπό την μορφή τεχνολογιών, που στόχο είχαν την προστασία των πληροφοριών και την εξασφάλιση της διακριτικότητας στις ηλεκτρονικές συναλλαγές (Nowhan, 2006).

Εντούτοις το αποτέλεσμα μάλλον αρνητικό μπορεί να χαρακτηριστεί, διότι μια πρώτης τάξεως απειλή είναι το ανεξέλεγκτο κυβερνοέγκλημα (cybercrime) (Hinduja, 2008). Η υποκλοπή και η παραποίηση προσωπικών στοιχείων όπως και οικονομικών κεφαλαίων βρίσκεται σε αυξανόμενη κλίμακα. Πρόσφατη δημοσίευση ερευνών σε παγκόσμιο επίπεδο, αποκαλύπτει πως περισσότερες εταιρίες αποφεύγουν την συμμόρφωση με διεθνή κριτήρια ασφάλειας (π.χ. ISO, NIST) μέχρι να υποστούν οι ίδιες παραβίαση ασφάλειας (Delloite, 2007; ESG, 2008). Λόγω έλλειψης της απευθείας επαφής με την τεχνολογία, οι καταναλωτές αντιλαμβάνονται συχνά ότι έχουν λιγότερο έλεγχο στις ηλεκτρονικές τους συναλλαγές. Επίσης, η μη φιλική προς το χρήστη τεχνολογία, η έλλειψη αυθεντικότητας, η εγγενής πολυπλοκότητα του διαδικτύου και η ανεπάρκεια πιστοποίησης αυθεντικότητας της ασφάλειας έχουν ενεργήσει ως αποτρεπτικοί παράγοντες στην επέκταση του ηλεκτρονικού επιχειρείν (Complinet, 2009). Η ασφάλεια των υπολογιστών υπάρχει για την υπεράσπιση των εταιρικών κεφαλαίων ενάντια στην κατάχρηση και την αναρμόδια χρήση τους, καθώς επίσης και στην προστασία των εταιρικών στοιχείων από τυχαία ή σκόπιμη κοινοποίηση, τροποποίηση ή παραποίηση κατά τη διάρκεια της μετάδοσής πληροφοριών στα δίκτυα υπολογιστών και τα διανεμημένα συστήματα (NIST, 2002).

Παρόλο αυτά, δεν υπάρχει «τέλεια» ή «απόλυτη» ασφάλεια. Συχνά αυτό σημαίνει ότι απαιτείται μια ισορροπία μεταξύ της εφαρμογής των μέτρων ασφάλειας και της αποδοχής ορισμένων κινδύνων. Η διοίκηση κινδύνων (risk management) είναι αποφάσεις που παίρνονται από την διοίκηση της εταιρίας για την διαχείριση κινδύνων και απειλών είτε ασφαλίζοντας

τους σε κάποιο βαθμό ή εφαρμόζοντας οικονομικά αποδεκτούς ελέγχους (Ronald et al., 2006).

Σύμφωνα με την RSA Security (2007), οι φόβοι ασφάλειας και εμπιστοσύνης δημιουργούνται από την άνοδο στις διαδικτυακές απάτες. Τα αποτελέσματα της έρευνας αποδεικνύουν ότι οι καταναλωτές είναι υπέρ κάποιας μορφής ισχυρής επικύρωσης που να υπερβαίνει το τυποποιημένο όνομα και τον κωδικό πρόσβασης χρηστών. Αυτό συμβαίνει διότι ευρέως γνωστά στο διαδικτυακό κόσμο είναι η εμφάνιση νέων ιών (virus), κακόβουλων προγραμμάτων (spyware) και Δούρειων ίππων (Trojan horses). Αυτά συνήθως εγκαθίσταται στον ηλεκτρονικό υπολογιστή λαθραία με σκοπό την υποκλοπή και μερικό έλεγχο της επικοινωνίας του χρήστη με τον υπολογιστή, χωρίς να υπάρχει προηγουμένως η απαραίτητη συγκατάθεση του χρήστη. Αυτό έχει άμεση επίδραση στο ηλεκτρονικό επιχειρείν και ιδιαίτερα στην ανθρώπινη εμπιστοσύνη προς το μέσο αυτό.

Χαρακτηριστικές προσεγγίσεις που στοχεύουν στην βελτίωση της ασφάλειας των υπολογιστών περιλαμβάνουν την εφαρμογή (1) μηχανισμών επιβολής συγκεκριμένων κανόνων στα προγράμματα υπολογιστών, (2) μηχανισμών λειτουργικών συστημάτων που επιβάλλουν κανόνες στα προγράμματα για την αποφυγή (δια)μεσολάβησης διαφορετικών προγραμμάτων υπολογιστών και (3) προηγμένου προγραμματισμού ικανού να καταστήσει τους υπολογιστές αξιόπιστους και να αντισταθεί σε οποιαδήποτε αναρμόδια τροποποίηση (Chellappa et al., 2002; Hinton & Barnes, 2007). Από την πλευρά των χρηστών, η μεγιστοποίηση της ασφάλειας μπορεί να επιτευχθεί (1) με τη χρησιμοποίηση βέλτιστων εφαρμογών ασφάλειας ηλεκτρονικών υπολογιστών και μηχανών αναζήτησης, (2) με την χρήση ασφαλών λογισμικών και ζωνών προστασίας ιών, (3) με τη συνεχή αλλαγή των προσωπικών αριθμών αναγνώρισης (Pin numbers) και των αριθμών συναλλαγής (Tan numbers) (4) με την διατήρηση της μυστικότητας των κωδικών από τρίτους και (5) τη συνεχής παρατήρηση της οικονομικής τους δραστηριότητας και αναφορά οποιασδήποτε μη προσδεχόμενης αλλαγής (NIST, 2002).

Από την πλευρά των επιχειρήσεων, η ασφάλεια βασίζεται στην ικανότητα διοίκησης και διαχείρισης της ποικιλομορφίας των κινδύνων. Προτεινόμενες τεχνικές αντιμετώπισης των διαδικτυακών απειλών περιλαμβάνουν (1) την καθιέρωση μιας ενδελεχούς διαδικασίας ελέγχου ασφάλειας, (2) την χρήση ενός ισχυρού πρωτόκολλου επικύρωσης για τους χρήστες που επιθυμούν τις σε απευθείας σύνδεση διαδικτυακές συναλλαγές, (3) την επιβεβαίωση αποστολέα και τη μη δυνατότητα άρνησης αποστολής (non-repudiation), (4) την εφαρμογή κατάλληλων ελέγχων έγκρισης μέσα από τα επιχειρησιακά συστήματα και τις βάσεις δεδομένων, (5) την διασφάλιση της ακεραιότητας των στοιχείων, αρχείων και πληροφοριών, (6) την διατήρηση της μυστικότητας των προσωπικών ευαίσθητων στοιχείων και (7) την ανάγκη ενός προγραμματισμού επιχειρησιακής συνοχής ικανού να εξασφαλίσει την διαθεσιμότητα των συστημάτων και των διαδικτυακών υπηρεσιών (Treck, 2003; Zuccato, 2005).

Γεγονός είναι ότι η ασφάλεια έχει πολλά πρόσωπα και παρουσιάζει ποικιλομορφία από κινδύνους και απειλές. Επίσης, η ασφάλεια αποτελεί επιχειρησιακό προβληματισμό και συνεπώς επιδέχεται διοικητική μέριμνα. Η διοίκηση της ασφάλειας είναι μια διαδικασία ανάλυσης και αξιολόγησης των προβλεπόμενων κινδύνων και κατά συνέπεια, το επίπεδο ελέγχου της ασφάλειας εξαρτάται κυρίως από τον ανθρώπινο τρόπο συνεργασίας, επικοινωνίας και καινοτομίας.

Η τέχνη του μάρκετινγκ

Για την πλειοψηφία των επιχειρήσεων οι οποίες έχουν έρθει αντιμέτωπες με την οικονομική κρίση, το δυσκολότερο σημείο, εκτός από το ίδιο το γεγονός, είναι ο χειρισμός της σχέσης τους με τον Τύπο και τα μέσα ενημέρωσης. Η αποτελεσματική επικοινωνία ή ακόμα καλύτερα, η έναρξη τακτικών προώθησης, είναι βασικός παράγοντας που θα επιτρέψει στις επιχειρήσεις να ανακάμψουν από προηγούμενα λάθη. Ο στόχος είναι να αποκτηθεί ο έλεγχος του μηνύματος (Bajgoric & Moon, 2009). Η σημασία του μάρκετινγκ συνίσταται στην οργανωμένη προσπάθεια μίας επιχείρησης να ικανοποιήσει τις ανάγκες αλλά και τις επιθυμίες των καταναλωτών. Με άλλα λόγια αποτελεί μια συνεχή διαδικασία κατανόησης και αντίληψης των κοινωνικών τάσεων και παραγωγής αντίστοιχων προϊόντων / υπηρεσιών γνωστοποιώντας τα μέσω διαφήμισης και προώθησης (Kotler, 1991). Στη παρούσα φάση οι μεταβλητές της ασφάλειας δυσκολεύουν τον ρόλο του μάρκετινγκ διότι η διαχείριση τους είναι δύσκολη, ιδίως σε μια περίοδο κρίσης που παράγει αβεβαιότητα, φόβο παραποίησης και εκμετάλλευσης προσωπικών πληροφοριών. Λόγω αυτών των κινδύνων η ασφάλεια πρέπει να θεωρηθεί ως ύψιστη προτεραιότητα ενός σχεδίου συστημάτων ηλεκτρονικού επιχειρείν.

Σύμφωνα με ειδικούς (Singh & Sirdeshmukh, 2000) η βελτίωση της διαδικτυακής ασφάλειας δεν είναι αρκετή. Οι επιχειρήσεις οφείλουν να δημοσιοποιούν τις βελτιώσεις τους στα θέματα ασφάλειας μέσω των μέσων μαζικής ενημέρωσης προκειμένου να ενισχύσουν την εμπιστοσύνη και την οξυδέρκεια του καταναλωτή. Προφανώς η καλύτερη στρατηγική για τις επιχειρήσεις δεν είναι να αντιμετωπίζεται ο Τύπος ως εχθρός, αλλά ως πιθανός σύμμαχος. Οι καταναλωτές θα χρησιμοποιήσουν μία διαδικτυακή εφαρμογή μόνο όταν αισθάνονται ότι αποκομίζουν όλα τα πλεονεκτήματα της, σε σχέση με μία συναλλαγή που γίνεται σε φυσικό περιβάλλον (Richardson, 2007). Για όσους έχουν προηγούμενη εμπειρία στους υπολογιστές, η πλοήγηση στο διαδίκτυο μπορεί να φαίνεται απλή υπόθεση. Ωστόσο, για την πλειοψηφία των ανθρώπων, η έκθεση των προσωπικών τους δεδομένων σε έναν άγνωστο κόσμο μπορεί να αποδειχθεί λίαν εκφοβιστική. Κατά συνέπεια, οι επιχειρήσεις που ψάχνουν τρόπους να ξεφύγουν από οικονομικά αδιέξοδα, πρέπει να εκπαιδεύουν τους πελάτες τους στο να χρησιμοποιούν διαδικτυακές υπηρεσίες. Η εκπαίδευση μπορεί να κατευθυνθεί μέσα από περιφερειακά κέντρα κατάρτισης μιας επιχείρησης, ενώ δεν πρέπει να περιοριστεί μόνο στους τρέχοντες πελάτες. Πάντα σε αναζήτηση ενός αυξανόμενου μεριδίου αγοράς, οι επιχειρήσεις πρέπει να εκπαιδεύουν και τους εν δυνάμει χρήστες. Στη εν λόγω εκπαίδευση πρέπει να συμπεριληφθεί το εργατικό και διαχειριστικό δυναμικό της επιχείρησης, προκειμένου να διευκολυνθεί η επικοινωνία και να καλλιεργηθεί ένα περιβάλλον ηλεκτρονικού επιχειρείν (Mirchandani & Motwani, 2000).

Σύμφωνα με τον Kotler (1991), «το μάρκετινγκ είναι ο προσδιορισμός των αναγκών του πελάτη, παρέχοντας ικανοποίησή υπό μορφή προϊόντων και υπηρεσιών αποφέροντας κέρδος στην επιχείρηση». Εκείνοι που προσπαθούν να κερδίσουν το ανταγωνιστικό πλεονέκτημα στο σημερινό αβέβαιο περιβάλλον, πρέπει να εισαγάγουν την τεχνολογία ηλεκτρονικού εμπορίου στο επικοινωνιακό τους οικοδόμημα, αλλά και στις δραστηριότητες μάρκετινγκ, μια και η επιχειρησιακή βιομηχανία οδηγείται από την τεχνολογική πρόοδο (Zuccato, 2005). Οι επιχειρήσεις, για να συνάψουν σχέσεις ουσίας, πρέπει να επικοινωνούν με το πελατολόγιο τους χρησιμοποιώντας διαδικτυακές και μη διαδικτυακές υπηρεσίες, όπως διαφημίσεις στον Τύπο, σε φυλλάδια και περιοδικά, διανομή ενημερωτικών δελτίων καθώς και επικοινωνία μέσω διαδικτύου με την μορφή

συνεργασιών. Σημαντική θεωρείτε επίσης η δημοσίευση των καινοτομιών ασφάλειας, δεδομένου ότι αυτό παίζει έναν πρωταρχικό ρόλο στη βελτίωση της εμπιστοσύνης του καταναλωτή στις διαδικτυακές συναλλαγές. Εάν οι πελάτες γνωρίζουν αυτό που προσφέρεται, σύντομα θα θελήσουν να το δοκιμάσουν (Mirchandani & Motwani, 2000).

Οι μεταβλητές ασφάλειας δεν είναι σταθερά μέρη και αυτή η μεταβλητότητα τους μεταφράζεται σε διάφορους κινδύνους προκαλώντας τριγμούς στην ασφάλεια του ηλεκτρονικού επιχειρείν. Για την καλύτερη δυνατή πρόβλεψη των παραβιάσεων της ασφαλείας, συστήνεται μια συνολική προσέγγιση για την πιο ολοκληρωμένη αντιμετώπιση των κινδύνων. Τα περιβάλλοντα που διαμορφώνουν την ύπαρξη και τη λειτουργία των συστημάτων του ηλεκτρονικού επιχειρείν είναι διαφορετικά και είναι το κοινωνικό, το τεχνολογικό και το επιχειρησιακό περιβάλλον (Zuccato, 2005). Το πρώτο περιλαμβάνει την κοινωνική συμπεριφορά ως μέτρηση των θετικών ή αρνητικών συναισθημάτων ενός ατόμου ως προς την εκτέλεση ενός στόχου. Οι διαφορετικές συμπεριφορές απέναντι σε μια καινοτομία, όπως είναι το ηλεκτρονικό επιχειρείν, μπορούν να μετρηθούν χρησιμοποιώντας τις πέντε αντιληπτές ιδιότητες: σχετικό πλεονέκτημα, συμβατότητα, πολυπλοκότητα, δυνατότητα δοκιμής και κίνδυνος (Fishbein & Ajzen, 1975). Το τεχνολογικό περιβάλλον περιλαμβάνει όλους εκείνους τους μηχανισμούς και τις πηγές της τεχνολογίας πληροφοριών που είναι σε ισχύ και επηρεάζουν τις διαδικτυακές συναλλαγές. Λόγω της προόδου της τεχνολογίας, ακόμη και σε περίοδο κρίσης, η μη έγκυρη αντίληψη κινδύνων (security awareness), μπορεί να αποβεί καθοριστικός παράγοντας στις προοπτικές του ηλεκτρονικού επιχειρείν.
Το επιχειρησιακό περιβάλλον αποτελείται από την ανάλυση, διαχείριση και διοίκηση των κινδύνων ενώ περιλαμβάνει διαδικασίες αναγνώρισης των πηγών και των κινδύνων που απορρέουν από αυτές (Farkhanda, 2007). Όλα τα διαφορετικά περιβάλλοντα, αλληλεπιδρούν μεταξύ τους προκαλώντας μεταβλητότητα στις συνθήκες ασφάλειας και ανθρώπινης συμπεριφοράς.

Συμπεράσματα

Η ανάπτυξη του διαδικτύου και η πρόοδος του ηλεκτρονικού επιχειρείν είναι αναμφισβήτητα θέματα ασφάλειας και διασφάλισης προσωπικών στοιχείων και αποτελούν ακόμη την αχίλλειο πτέρνα της διάχυσης του ηλεκτρονικού επιχειρείν. Ειδικά σε μια περίοδο οικονομικής αστάθειας, συγχωνεύσεων και πτωχεύσεων, ο έλεγχος και η διοίκηση των κινδύνων γίνονται αρκετά περίπλοκα. Ωστόσο, πιστεύουμε ότι τα μόνα όρια που τίθενται για τον έλεγχο της ασφάλειας είναι η διοικητική ικανότητα διαχείρισης της ασφάλειας και ο απαιτούμενος προϋπολογισμός για την εκτέλεση διαδικασιών αξιολόγησης κινδύνων και εκπαίδευσης ανθρωπίνου δυναμικού.

Η διοίκηση και ο έλεγχος των αλλεπάλληλων αλλαγών πρέπει να γίνει επιχειρησιακή νοοτροπία και όχι να προωθείτε ως μήνυμα για την αύξηση των πωλήσεων. Γεγονός είναι ότι οι περισσότερες εταιρίες με μειωμένη κερδοφορία, δεν έχουν τα περιθώρια να επενδύσουν σε τεχνολογίες ασφάλειας και τεχνικές διαχείρισης κινδύνων για την προστασία της διαδικτυακής τους παρουσίας. Το μάρκετινγκ έρχεται σε δεύτερη μοίρα διότι η μειωμένη κερδοφορία απλά δεν το επιτρέπει να αναδείξει την δυναμικότητα του ως εταιρικό εργαλείο. Όμως το ηλεκτρονικό επιχειρείν έχει την δυνατότητα να προβληθεί ως ανταγωνιστικό πλεονέκτημα μόνο από εκείνους που γνωρίζουν σε βάθος τις πτυχές του και τις μεταβλητές που το επηρεάζουν.

Η ποικιλομορφία των κινδύνων στο ηλεκτρονικό επιχειρείν προϋποθέτει την υιοθέτηση μιας ολιστικής και ομαδοποιημένης προσέγγισης αντιμετώπισης των κινδύνων της ασφάλειας (holistic and unified security approach). Τα διαφορετικά περιβάλλοντα που υπάρχουν και επηρεάζουν την επιχείρηση πρέπει να μελετηθούν σε βάθος και βάση θεωρητικών και εμπειρικών αποτελεσμάτων να παρθούν οι ανάλογες αποφάσεις και ενέργειες. Σαν επίλογο μπορούμε να πούμε ότι ο ρόλος του μάρκετινγκ στοχεύει στη δημιουργία μιας αληθινής ιστορίας ασφάλειας, πίσω από κάθε ενδεχόμενο κινδύνου ή απειλής. Η ρήση του Ιπποκράτη, "το προλαμβάνειν μείζον εστί του θεραπεύειν" προσομοιώνει την κατάσταση στο ηλεκτρονικό επιχειρείν για θέματα προληπτικής ασφάλειας των περουσιακών στοιχείων σε έναν κόσμο που εμφανίζεται εύθραυστος και πλασματικός.

Βιβλιογραφία

Bajgoric, N., Moon, Y.B. (2009), "Enhancing systems integration by incorporating business continuity drivers", Industrial Management & Data Systems, Vol. 109, No.1, pp.74-97.

Barnes, D., Hinton, M., (2007), "Searching for e-business performance measurement systems", Electronic Journal of Information Systems Evaluation, Vol. 10, No.1, pp.87-99.

Chaffey, D., Mayer, R., Johnston, K. and Ellis-Chadwick, F. (2003), "Internet Marketing: Strategy, implementation and practice". Financial Times/Prentice Hall, Harlow, 2nd edition.

Chellappa, R.K. and Pavlou, P. (2002), "Perceived Information Security, Financial Liability, and Consumer Trust in Electronic Commerce Transactions", Journal of Logistics Information Management, Vol. 15, No. 5, pp. 358-368.

Complinet, (2009) "Annual Cost of Compliance Survey 2009: More regulation with less resource means greater risk" (press release), [Online], Retrieved 20th March 2009 from http://www.complinet.com/connected/news-and-events/press-releases/complinets-annual-cost-of-compliance-survey-2009.html

Delloite Global Security Survey, (2007) [Online], Retrieved 21st March 2009 from http://www.deloitte.com/dtt/research/0,1002,sid=1013&cid=170582,00.html

Enterprise Strategy Group (2008) "ISO, ITIL and COBIT triple play fosters optimal security management execution" [Online], Retrieved 4th April 2009 from http://www.scmagazineus.com/ISO-ITIL-and-COBIT-triple-play-fosters-optimal-security-management-execution/article/108620/

Facchini, G., Verdier T., (2008), "Symposium on organization, heterogeneity and trade Export", Economic Theory, June, Vol. 38, No. 3., pp. 433-436.

Farkhanda S., (2007), "The ICT environment, financial sector and economic growth: a cross-country analysis", Journal of Economic Studies, Vol. 34, No. 4, pp. 352-370.

Fishbein, M., Ajzen, I. (1975). "Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research.", Reading, MA.: Addison-Wesley.

Hinduja, S. (2008), "Investigating computer crime", in Schmalleger, F., Pittaro, M. (Eds), Crimes of the Internet, Prentice-Hall, Upper Saddle River, NJ, .

Jin B, Park J. Y and Kim Jiyoung, (2008), "Cross-cultural examination of the relationships among firm reputation, e-satisfaction, e-trust,

and e-loyalty", International Marketing Review, Vol. 25, No. 3, pp. 324 – 337.
Johnson G., Scholes K., and Whittington R., (2006), "Exploring Corporate Strategy", Financial Times-Prentice Hall, 7th Ed., pp. 286-290.
Kotler, P., (1991), "Marketing management: Analysis, planning, implementation, and control", Englewood Cliffs, NJ: Prentice Hall.
Matten, D., Moon, J. (2004), "'Implicit' and 'explicit' CSR: a conceptual framework for understanding CSR in Europe", [Online], Retrieved 4th April 2009 from: www.rhul.ac.uk/Management/News-andEvents/seminars/Dirk%20Matten%20RHUL%20SOM%20Seminar.pdf.
Mirchandani, A.A., Motwani, J. (2000), "Understanding small business electronic commerce adoption: an empirical analysis", Journal of Computer Information Systems, Vol. 41 No. 3, pp.70-73.
National Institute of Standards and Technology, (2002), "Risk Management Guide for Information Technology Systems", Special Publication 800-30.
Nowlan M., (2006), "How to Save Face in a Business Crisis", February 17, [Online], Retrieved 4th April 2009 from http://www.entrepreneur.com/marketing/publicrelations/prcolumnist/article83710.html
Porter, M.E. (2001), "Strategy and the Internet", Harvard Business Review, March, pp. 63-78.
Richardson, R., (2007), "The 12th annual computer crime and security survey", [Online], Retrieved 4th April 2009 from http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf.
RSA Security (2007), "Rapid Development of Secure e-Banking Solution", [Online], Retrieved 8th April 2009 from http://whitepapers.zdnet.co.uk/0,1000000651,260053700p-39000584q,00.html
Ronald L., Sang-Hyop L., Andrew M. (2006) "Charting the Economic Life Cycle", Information Security Governance, [Online], Retrieved 10th April 2009 from http://www.nber.org/papers/w12379
Shunk, D., Carter, J., Hovis, J., Talwar, A. (2007), "Electronics industry drivers of intermediation and disintermediation", International Journal of Physical Distribution & Logistics Management, Vol. 37, No. 3, pp. 248-61.
Smith PR., Chaffey D., (2005), "eMarketing eXcellence – The Heart of eBusiness" 2nd Edition, Published by Elsevier Ltd.
Trcek D. (2003), "An integral framework for information systems security management", Computers & Security (2003), Vol. 22, No.4, pp. 337–360.
Zuccato, A., (2005), "Holistic security management framework applied in electronic commerce", computers & security, Vol. 26, No. 3, May 2007, pp. 256-265.