Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ

ΤΜΗΜΑ Σ.Σ.Ο.Ε

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΣΠΟΥΔΑΣΤΕΣ : ΙΠΠΟΚΡΑΤΗΣ ΔΙΑΜΑΝΤΑΚΗΣ & ΧΡΗΣΤΟΣ ΤΣΑΤΣΟΣ

ΜΕΣΟΛΟΓΓΙ 2007

Εισηγητής
Κ.ΤΖΙΡΤΖΙΛΑΚΗΣ

Πίνακας Περιεχομένων

1 Εισαγωγή

Αποτελεί αδιαμφισβήτητο γεγονός ότι σήμερα στο κατώφλι της νέας χιλιετίας, η πληροφορική έχει διεισδύσει ολοκληρωτικά σε κάθε ατομική ή κοινωνική μας δραστηριότητα. Τα πλεονεκτήματα αλλά και τα μειονεκτήματα που προκύπτουν από την καθημερινή χρήση της τεχνολογίας της πληροφορικής είναι πολλαπλά, αλλά δεν αποτελούν κύριο στόχο του παρόντος κειμένου. Όμως, στα μειονεκτήματα συμπεριλαμβάνεται δυστυχώς και η χρήση των υπολογιστών από πρόσωπα που σχετίζονται με το σχεδιασμό και την πραγματοποίηση διάφορων «**ηλεκτρονικών εγκλημάτων**». Σήμερα, οι υπολογιστές διαδραματίζουν σημαντικό ρόλο σε σωρεία εγκλημάτων που διαπράττονται, είτε μέσω του *Διαδικτύου* είτε εκτός αυτού.

Τα τελευταία χρόνια γίνεται μεγάλη προσπάθεια παγκοσμίως, για την αντιμετώπιση των ηλεκτρονικών εγκλημάτων, καθώς επίσης και προσπάθειες διαμόρφωσης και επιβολής νέων νομοθετικών ρυθμίσεων που να συμβαδίζουν με τις τρέχουσες ανάγκες που επιβάλει η εξέλιξη της τεχνολογίας.

Ένα ιδιαίτερο στοιχείο που χαρακτηρίζει τα εγκλήματα μέσω διαδικτύου και που τα διαφοροποιεί από όλες τις άλλες κατηγορίες ηλεκτρονικών εγκλημάτων, είναι το γεγονός ότι τα τελευταία πραγματοποιούνται με ευρέως διαθέσιμο λογισμικό χωρίς ο μέσος χρήστης – θύμα να μπορεί να τα αποτρέψει ή ακόμα και να τα εντοπίσει. Επιπρόσθετα, πρέπει να σημειωθεί ότι με τη χρήση εξειδικευμένου λογισμικού αλλά και ειδικών τεχνικών κατά τη διαδικασία υλοποίησης εγκληματικών ενεργειών, μπορεί να επιτευχθεί πλήρης συγκάλυψη των μεθόδων που χρησιμοποιήθηκαν. Η διαθέσιμη τεχνολογία προς το παρόν δείχνει ότι δημιουργεί τις προϋποθέσεις υλοποίησης σχεδόν τέλειων ψηφιακών εγκλημάτων. Η ερώτηση που αυτόματα γεννιέται είναι, τι μπορεί να γίνει για την αντιμετώπισή τους;

Η απάντηση στην παραπάνω ερώτηση δεν είναι εύκολο να δοθεί, εφόσον οι εγκληματίες που χρησιμοποιούν την πληροφορική και κατ' επέκταση το διαδίκτυο είναι γενικά πολύ καλά καταρτισμένοι, σε πολλές περιπτώσεις ιδιαίτερα ευφυείς και άρτια προετοιμασμένοι για να χρησιμοποιήσουν τις νέες ***τεχνολογίες*** (που απλόχερα είναι στη διάθεσή τους). Ο σκοπός των «ηλεκτρονικών εγκληματιών» διαφέρει ανά περίπτωση αλλά συμπεριλαμβάνει την πραγματοποίηση εγκλημάτων όπως: επιθέσεις με την βοήθεια ιών (Trojan horses, worms, virus), απάτες, κλοπές, δολιοφθορές αλλά και το αδιανόητο έγκλημα της εκμετάλλευσης των παιδιών, μέσω της παιδικής πορνογραφίας.

Από την άλλη πλευρά οι κρατικοί μηχανισμοί δε μπορούν πάντα να εξασφαλίσουν όλα εκείνα τα απαραίτητα κονδύλια, για την παρακολούθηση των τεχνολογικών εξελίξεων. Επιπλέον, οι ραγδαίες εξελίξεις της τεχνολογίας μετατρέπουν πολύ γρήγορα τους σύγχρονους εξοπλισμούς, που πιθανά έχουν στη διάθεση τους οι διωκτικές αρχές, σε ξεπερασμένους. Όλα τα παραπάνω εμπόδια όπως είναι φυσικό δε βοηθούν στην επιβολή των νόμων, σε αντίθεση με το εγκληματικό στοιχείο που όχι μόνο παρακολουθεί την νέα τεχνολογία αλλά και δείχνει να διαθέτει τους σχετικούς πόρους για τη χρησιμοποίησή της.

Στα παραπάνω συνάδουν επίσης και τα εξής:

- Οι περισσότεροι cyber criminals παραμένουν ανώνυμοι, χρησιμοποιώντας τις ιδιαιτερότητες και τα τεχνολογικά χαρακτηριστικά του διαδικτύου, προς όφελός τους.
- Παρότι, σε πολλές ανεπτυγμένες χώρες έχουν πραγματοποιηθεί σημαντικές νομικές βελτιώσεις κατά τη διάρκεια των τελευταίων χρόνων, υπάρχουν πολλές χώρες ανά τον κόσμο όπου οι νόμοι για την αντιμετώπιση των θεμάτων σχετικά με τα cyber crimes είναι ελαστικοί έως και ανύπαρκτοι.
- Οι διωκτικές αρχές των περισσοτέρων χωρών στερούνται συχνά των πόρων αλλά και των κατάλληλων μηχανισμών, ώστε να είναι σε θέση να ερευνήσουν και να αντιμετωπίσουν τα ηλεκτρονικά εγκλήματα.
- Λόγω της φύσης του διαδικτύου, δημιουργούνται πολλές φορές ανυπέρβλητες δυσκολίες για τον εντοπισμό των ατόμων ή ομάδων που σχετίζονται με τα cyber crimes.
- Ελάχιστες περιπτώσεις cyber crimes στο διαδίκτυο καταγγέλλονται ή αποκαλύπτονται. Αυτό οφείλεται στο γεγονός ότι διακυβεύεται η αξιοπιστία των παθόντων, οι οποίοι κατά κανόνα είναι εταιρείες, δημόσιοι και ιδιωτικοί οργανισμοί (π.χ. τραπεζικοί όμιλοι). Κατά συνέπεια αποκρύπτονται πληροφορίες (έστω και καλοπροαίρετα), με αποτέλεσμα η εικόνα της εγκληματικότητας στο χώρο του διαδικτύου να είναι αρκετά ασαφής.

Οι τεχνολογίες των υπολογιστών αλλάζοντας τον τρόπο με τον οποίο επικοινωνούμε, εργαζόμαστε και συναλλασσόμαστε, τόσο σε προσωπικό επίπεδο όσο και σε επίπεδο οργανισμών (*στον ιδιωτικό αλλά και στο δημόσιο τομέα*), γεννούν ταυτόχρονα και την ανάγκη δημιουργίας νέων μεθόδων και τρόπων, για τη σωστή σχεδίαση και εφαρμογή της ασφάλειας των πληροφοριακών πόρων τους οποίους διαχειριζόμαστε. Οι μέθοδοι αυτές θα πρέπει να αποτελέσουν τα εργαλεία για τη συνεχή προστασία της διακίνησης πληροφοριών μέσω του διαδικτύου, που αφορούν ως επί το πλείστον οργανισμούς αλλά και ιδιώτες.

Ο βαθμός εξάπλωσης του διαδικτύου σήμερα καταρρίπτει το ένα ρεκόρ μετά το άλλο. Το ραδιόφωνο χρειάστηκε 38 χρόνια για να φθάσει σε 50 εκατομμύρια ανθρώπους. Η τηλεόραση έφθασε στον ίδιο αριθμό ανθρώπων σε 13 χρόνια. Το διαδίκτυο έκανε ακριβώς το ίδιο μόλις σε τέσσερα χρόνια. Μέσα σε αυτή τη πραγματικότητα που διαμορφώνεται παγκοσμίως με ολοένα και αυξανόμενους ρυθμούς, στο παρόν κείμενο γίνεται μια παρουσίαση των κυριότερων φαινομένων που συνοδεύουν το διαδίκτυο, όσο αφορά στο θέμα των οικονομικών και οικονομικών εγκλημάτων (που βέβαια μπορεί να διαπράττονται και χωρίς αυτό), μέσω των παρακάτω κεφαλαίων:

- **Ορισμοί και τύποι εγκλημάτων**
- **Νομοθεσία – Νομολογία - Συνθήκες**
- **Ηλεκτρονικό έγκλημα**
- **Οικονομικό έγκλημα**
- **Ηλεκτρονικό Εμπόριο**
- **Στατιστικά και έρευνες για το Ηλεκτρονικό Εμπόριο**

- **Έρευνες σχετικά με οικονομικά εγκλήματα**
- **Κατηγορίες οικονομικού εγκλήματος**
- **Μέτρα αντιμετώπισης του ηλεκτρονικού – οικονομικού εγκλήματος**

2 Ηλεκτρονικό Εμπόριο

2.1 Εισαγωγή

Στο πρόσφατο παρελθόν οι συναλλαγές και οι αγορές των καταναλωτών και αντίστοιχα ο πωλήσεις των εμπόρων γίνονταν με καθαρά συμβατικά μέσα. Οι καταναλωτές προκειμένου να αγοράσουν αυτό που επιθυμούσαν ή να δεχτούν μία υπηρεσία έπρεπε να μεταβούν στην έδρα του προμηθευτή των αγαθών ή των υπηρεσιών. Στις μέρες μας ο τρόπος διεξαγωγής των συναλλαγών έχει αλλάξει ριζικά.

Ένας από τους νέους και τάχιστους τρόπους εξυπηρέτησης των καταναλωτών είναι το Ηλεκτρονικό Εμπόριο το οποίο αναπτύσσεται ραγδαία στο εξωτερικό αλλά και στην Ελλάδα με πιο αργούς όμως ρυθμούς.

Ενδεικτικό της καθυστερημένης ανάπτυξης του ηλεκτρονικού εμπορίου στην Ελλάδα είναι οι δύο υπουργικές αποφάσεις 3035/Β2-48.2001 και 7681/Β2-255.2001 που προωθούν τη διενέργεια δοκιμαστικής έρευνας για το ηλεκτρονικό εμπόριο. Οι αποφάσεις αυτές είναι του 2001, χρονιά που σε άλλες ευρωπαϊκές χώρες ανθούσε το ηλεκτρονικό εμπόριο.

2.2 Ορισμός

Ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων. Το ηλεκτρονικό εμπόριο αποτελεί έκφανση των λεγόμενων υπηρεσιών εξ αποστάσεως (ΠΔ 39.2001) .

Ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση για αγορά η πώληση αγαθών ή υπηρεσιών.

Ηλεκτρονικό εμπόριο θεωρούνται επίσης και οι συναλλαγές μέσω τηλεφώνου και φαξ. Το ηλεκτρονικό εμπόριο διακρίνεται σε έμμεσο και άμεσο.

- Ο πρώτος όρος χρησιμοποιείται όταν πρόκειται για την ηλεκτρονική παραγγελία υλικών αγαθών που μπορούν να παραδοθούν μόνο με παραδοσιακούς τρόπους όπως είναι το ταχυδρομείο.
- Άμεσο είναι το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών. Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα με την αρωγή πάντα και τη σύμπραξη των τραπεζών.

Το Ηλεκτρονικό Εμπόριο θα μπορούσε να οριστεί επίσης ως «*ένα σύνολο 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» (Δουκίδης, Ηλεκτρονικό εμπόριο, Εκδ. Νέων Τεχνολογιών, 1998).

Οι τεχνολογίες που χρησιμοποιούνται για τις εφαρμογές του Ηλεκτρονικού Εμπορίου περιλαμβάνουν:

- όλες τις μορφές ηλεκτρονικών μηνυμάτων
- ηλεκτρονικής ανταλλαγής δεδομένων (**EDI**)
- ηλεκτρονικής μεταφοράς κεφαλαίων (**Electronic Funds Transfer**)
- ηλεκτρονικού ταχυδρομείου
- ηλεκτρονικών καταλόγων υπηρεσιών ηλεκτρονικού πίνακα ανακοινώσεων (**Bulletin Board Services**)
- κοινών βάσεων δεδομένων και οδηγών
- συστημάτων συνεχιζόμενης αγοράς και υποστήριξης για όλο τον κύκλο ζωής των προϊόντων
- ηλεκτρονικών ειδήσεων και υπηρεσιών πληροφόρησης
- ηλεκτρονικής μισθοδοσίας
- ηλεκτρονικών εντύπων
- πρόσβαση σε απευθείας σύνδεση σε υπηρεσίες μέσω **Internet**
- καθώς και κάθε άλλη μορφή ηλεκτρονικής μετάδοσης δεδομένων για εμπορικούς σκοπούς.

Οι τρεις κύριες κατηγορίες εφαρμογών Ηλεκτρονικού Εμπορίου, όπως έχουν διαμορφωθεί τα τελευταία χρόνια είναι οι ακόλουθες (*Dien D. Phan, 2002*):

- **Ηλεκτρονικές αγορές** (electronic marketplaces): αγορά και πώληση προϊόντων και υπηρεσιών μέσω διαδικτύου.
- **Ενδοεπιχειρησιακά συστήματα** (inter-organisational systems): διευκόλυνση της ροής αγαθών, υπηρεσιών, πληροφοριών, επικοινωνίας και συνεργασίας στο εσωτερικό του οργανισμού.
- **Εξυπηρέτηση πελατών** (customer service): παροχή εξυπηρέτησης και βοήθειας, χειρισμός παραπόνων, εντοπισμός παραγγελιών κ.α.

2.3 Στόχοι ασφάλειας στο ηλεκτρονικό εμπόριο.

Σε ένα συνεχώς διευρυνόμενο μέσο όπως το διαδίκτυο και με την ζωηρή άνθηση του ηλεκτρονικού επιχειρείν διαμορφώνεται όπως περιγράφθηκε και στις προηγούμενες παραγράφους μια κατάσταση, όπου αυξάνονται οι ευκαιρίες για (ηλεκτρονική) απάτη. Προκειμένου λοιπόν να αποφευχθούν καταστάσεις σαν αυτές που προαναφέρθηκαν, θα πρέπει να λαμβάνονται μέτρα ασφαλείας για την εξάλειψη αυτού του φαινομένου (ηλεκτρονικές απάτες ή κλοπές). Αυτά τα μέτρα θα πρέπει να έχουν τους παρακάτω στόχους:

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

- Έλεγχος αυθεντικότητας (**authentication**): Εξακρίβωση της ταυτότητας του χρήστη είτε με passwords είτε με προσωπικούς αριθμούς αναγνώρισης (*Personal Identification Numbers*), είτε με διάφορα άλλα τεχνολογικά μέσα.
- Μη αποποίηση της ευθύνης (**non – repudiation**): Με την ολοκλήρωση της οποιασδήποτε εμπορικής συναλλαγής, κανείς από τα συμβαλλόμενα μέρη δεν μπορεί να ισχυρισθεί ότι δεν συμμετείχε σ' αυτήν.
- Εξουσιοδότηση (**authorization**): Παραχώρηση δικαιωμάτων στο χρήστη από τον ιδιοκτήτη.

Για την διασφάλιση των συναλλαγών που πραγματοποιούνται στο διαδίκτυο και την αποφυγή των κινδύνων (απάτες, κλοπές) θα πρέπει να σχεδιάζονται και να υλοποιούνται μέτρα που έχουν τους παραπάνω στόχους. Σε αυτή τη κατεύθυνση βοηθά ένας σημαντικός αριθμός πρωτοκόλλων και εφαρμογών βασισμένων κυρίως σε τεχνικές κρυπτογράφησης, προκειμένου να εξουδετερωθούν στο σύνολό τους οι παραπάνω απειλές.

2.4 Μοντέλα Ηλεκτρονικού Εμπορίου

Το Ηλεκτρονικό Εμπόριο εφαρμόζεται σε όλα τα στάδια του εμπορικού κύκλου, από τη συλλογή πρώτων υλών μέχρι το σημείο κατανάλωσης. Τρίτοι φορείς που είναι απαραίτητοι για την λειτουργία του εμπορικού κύκλου (όπως τράπεζες, μεταφορείς, δημόσιος τομέας κλπ) συμμετέχουν επίσης στις διαδικασίες του Ηλεκτρονικού Εμπορίου. Η κάθε μία οντότητα που συμμετέχει στην εμπορική διαδικασία είναι ταυτόχρονα χρήστης και προμηθευτής πληροφορίας, σύμφωνα με την αντίστοιχη θέση στον εμπορικό κύκλο και προς όφελος όλης της αλυσίδας αξιών.

Ο τρόπος εφαρμογής του Ηλεκτρονικού Εμπορίου, εξαρτάται από το πεδίο εφαρμογής (προμήθειες, εμπόριο, τραπεζικές διαδικασίες, τουρισμός, μεταφορές κ.λ.π., ιδιωτικού και δημόσιου τομέα), όπως επίσης και από τις οντότητες που το εφαρμόζουν. Ιδιαίτερα σε σχέση με τις συμμετέχουσες οντότητες, το Ηλεκτρονικό Εμπόριο διαχωρίζεται σε τρία βασικά μοντέλα

- Το διεπιχειρησιακό (**Business-to-Business**)
- Το μοντέλο επιχείρησης προς Δημόσιο Τομέα (**Business-to-Public Administration**)
- και το μοντέλο επιχείρηση-καταναλωτής (**Business-to-Consumer**)

2.4.1 Το διεπιχειρησιακό μοντέλο

Το διεπιχειρησιακό μοντέλο αποσκοπεί στην υποστήριξη υπαρχόντων σχέσεων, οι οποίες διέπονται από συγκεκριμένα νομικά και τυπικά πλαίσια. Στο μοντέλο αυτό, το Ηλεκτρονικό Εμπόριο αποσκοπεί στην όσο το δυνατό μεγαλύτερη μείωση διαχειριστικών, μη-παραγωγικών εξόδων, μέσω της ανταλλαγής πλούσιας σε περιεχόμενο πληροφορίας απ' ευθείας μέσα από υπολογιστικά συστήματα. Στο διεπιχειρησιακό μοντέλο οι τεχνολογίες και μέθοδοι έχουν σαν κύριο στόχο την υποστήριξη και διευκόλυνση της εμπορικής συμφωνίας χρησιμοποιώντας κατάλληλα μηχανογραφικά

συστήματα, τα οποία επιτρέπουν τον έλεγχο, την αξιοποίηση και περαιτέρω προώθηση της πληροφορίας που ανταλλάσσεται.

Επιπλέον, η ίδια η πληροφορία απαιτεί την κατάλληλη αναπαράστασή της (κωδικοποίηση), καθώς πλέον οι διαδικασίες ελέγχου, αξιοποίησης και μεταφοράς της γίνονται από ηλεκτρονικά μέσα, απαλείφοντας προοδευτικά την ανάγκη συμμετοχής του ανθρώπινου παράγοντα, ιδιαίτερα στις διαχειριστικές (μη-παραγωγικές) διαδικασίες. Το διεπιχειρησιακό μοντέλο έχει τα χαρακτηριστικά της σταθερής σχέσης, η οποία υπόκειται σε συγκεκριμένες εμπορικές συμφωνίες, συνεπακόλουθους νόμους, θεσμούς και τυπικό. Επιπλέον, χαρακτηρίζεται από την αυξημένη ανάγκη ασφάλειας και αξιοπιστίας της επικοινωνίας, δεδομένου ότι η επιχειρηματική δραστηριότητα εξαρτάται από το μέσο αυτό.

2.4.2 Το μοντέλο επιχείρησης-καταναλωτή

Το μοντέλο επιχείρησης-καταναλωτή επιδιώκει κυρίως την εξυπηρέτηση του marketing των επιχειρήσεων, καθώς και τη διεύρυνση των ορίων της αγοράς αναπτύσσοντας νέα κανάλια πώλησης. Το μοντέλο επιχείρησης-καταναλωτή, χαρακτηρίζεται από τον αδόμητο χαρακτήρα του καταναλωτή σαν ανθρώπινη οντότητα και την έλλειψη σταθερών σχέσεων. Η ασφάλεια και η αξιοπιστία στο μοντέλο αυτό είναι σημαντικές επίσης, αλλά δεν έχουν τον κρίσιμο ρόλο του διεπιχειρησιακού μοντέλου. Στο μοντέλο επιχείρησης-καταναλωτή αντίθετα από το διεπιχειρησιακό μοντέλο, παρόλο που χρησιμοποιούνται ηλεκτρονικά μέσα για την επικοινωνία και ανταλλαγή της πληροφορίας, οι μέθοδοι παραμένουν ανθρωποκεντρικοί, λόγω του ότι με οποιοδήποτε άλλο τρόπο δεν θα ήταν εμπορικά αξιοποιήσιμες από τον καταναλωτή-άνθρωπο.

Και στα δύο μοντέλα, επιτρέπεται η πλήρης κάλυψη της εφοδιαστικής αλυσίδας, από τη παραγωγή της α΄ ύλης έως τη κατανάλωση: με το Ηλεκτρονικό Εμπόριο μπορεί να προσεγγιστεί η αγορά και η κατανάλωση, ώστε οι επιχειρήσεις να αντιληφθούν έγκαιρα και έγκυρα τις ανάγκες και τις τάσεις της και να δημιουργηθούν τα κατάλληλα προϊόντα, στις κατάλληλες ποσότητες και στη σωστή τιμή.

2.4.3 Το μοντέλο επιχείρησης προς Δημόσιο Τομέα

Τέλος, το μοντέλο επιχείρησης προς Δημόσιο Τομέα (business to public Administration) είναι συνδυασμός των δύο παραπάνω μοντέλων.

2.5 B2B (Business to Business) και B2C (Business to Consumer)

Λόγω της μεγάλης απήχησης που έχουν στο ευρύ κοινό οι επιχειρήσεις πώλησης καταναλωτικών προϊόντων (Amazon, CDnow κ.λπ.), οι περισσότεροι άνθρωποι έχουν την τάση να συνδέουν το ηλεκτρονικό εμπόριο με τις πωλήσεις καταναλωτικών προϊόντων (**Business to Consumer Commerce**). Ωστόσο, μέσα στο δίκτυο το 90% των συναλλαγών στις ΗΠΑ, και το 70% στην Ευρώπη, διεξάγεται μεταξύ επιχειρήσεων (**Business to Business Commerce**).

Η διαφορά μεταξύ B2B (Business to Business) και B2C (Business to Consumer) γίνεται ακόμη μεγαλύτερη αν συγκρίνουμε την κερδοφορία αυτών των δύο αγορών. Στο B2B πραγματοποιείται μικρός αριθμός παραγγελιών μεγάλης αξίας (ακριβά προϊόντα ή μεγάλες ποσότητες) από μικρό αριθμό πελατών (επιχειρήσεις), ενώ στο B2C πραγματοποιείται μεγάλος αριθμός παραγγελιών σχετικά μικρής αξίας (καταναλωτικά προϊόντα σε μικρές ποσότητες) από έναν πολύ μεγάλο αριθμό πελατών (ιδιώτες).

Όπως είναι φυσικό, οι δαπάνες εξυπηρέτησης χιλιάδων μικρών παραγγελιών από ένα B2C ηλεκτρονικό κατάστημα επιβαρύνουν σημαντικά το κόστος λειτουργίας του και περιορίζουν τα περιθώρια κέρδους όλων των καταστημάτων αυτής της μορφής. Γι' αυτό και, ενώ υπάρχουν ήδη χιλιάδες κερδοφόρα sites B2B, οι περισσότερες επιχειρήσεις B2C είναι ακόμη ζημιογόνες και συντηρούνται μόνο χάρη στην υψηλή χρηματιστηριακή τους αξία (οι μετοχές τους βρίσκονται σε εξαιρετικά υψηλά επίπεδα, καθώς όλοι προσδοκούν πως όταν γίνουν κερδοφόρα θα αποκτήσουν δεσπόζουσα θέση στο χώρο του ηλεκτρονικού εμπορίου).

- **Υπηρεσίες μεσολάβησης**

Σύμφωνα με μια άλλη θεώρηση, τα ηλεκτρονικά καταστήματα δεν πρέπει να αποκαλούνται καταστήματα, αλλά μεσίτες προϊόντων διότι σπανίως έχουν στην αποθήκη τους τα προϊόντα που πουλάνε. Το *Amazon.com* για παράδειγμα δεν είχε μέχρι πρόσφατα κανένα βιβλίο στις αποθήκες του. Διατηρεί όμως μια εξαιρετική βάση δεδομένων με όλα τα βιβλία που διαθέτουν τα καταστήματα βιβλίων (στην αγγλική ή σε και σε άλλες γλώσσες) και φροντίζει έγκαιρα να προμηθεύεται από αυτά ότι ζητούν οι πελάτες του.

2.6 Ηλεκτρονικό Εμπόριο και Προσωπικά Δεδομένα

Οι έμποροι προκειμένου να μετρήσουν τις καταναλωτικές προτιμήσεις του κοινού με σκοπό να προσαρμόσουν στη βάση ζήτησης τις γραμμές παραγωγής τους και να προωθήσουν τις πωλήσεις τους μέσω του διαδικτύου, δημιουργούν νέους τρόπους συλλογής, επεξεργασίας και διασύνδεσης των προσωπικών δεδομένων. Τα προσωπικά δεδομένα συνήθως συλλέγονται κατά την αρχική φάση σύνδεσης του πελάτη με το δικτυακό χώρο του πωλητή και στην συνέχεια χρησιμοποιούνται σύγχρονες τεχνικές εξόρυξης δεδομένων (**data mining**), για την περαιτέρω ανάλυσή τους. Αποτέλεσμα της παραπάνω διαδικασίας είναι η δημιουργία βάσεων καταναλωτικών προφίλ των πελατών. Προφίλ ενός ατόμου νοείται ως μια συλλογή δεδομένων που μπορεί μοναδικά να προσδιορίσει την ταυτότητα του ατόμου αυτού.
Οι οντότητες οι οποίες τυπικά εμπλέκονται στην εγκατάσταση μιας ηλεκτρονικής σύνδεσης, με έμφαση στων πραγματοποίηση ηλεκτρονικών συναλλαγών και οι οποίες είναι ταυτόχρονα η πηγή και ο αποδέκτης των προσωπικών δεδομένων των χρηστών είναι οι εξής:

- **Χρήστης (User)**: Ο ενδιαφερόμενος για την απόκτηση μιας υπηρεσίας του διαδικτύου, την απόκτηση ενός προϊόντος με χρήση τεχνολογιών που βοηθούν στην ανάπτυξη του ηλεκτρονικού εμπορίου κ.λ.π.

- **Παροχέας Υπηρεσιών Διαδικτύου, (Internet Service Provider, ISP)**: Η οντότητα που παρέχει, τυπικά σε χρήστες, το υλικό (hardware) και πιθανώς λογισμικό (software), για την απόκτηση πρόσβασης στις βασικές υπηρεσίες του διαδικτύου.
- **Παροχέας Φυσικού Μέσου επικοινωνίας, (Carrier Provider)**: Η οντότητα που παρέχει το φυσικό τεχνολογικό μέσο μετάδοσης και επικοινωνίας δεδομένων π.χ. αναλογικές ή ψηφιακές γραμμές, εξοπλισμός αναμετάδοσης σημάτων με χρήση ψηφιακών κέντρων, δορυφόρων κ.λ.π. Οι οντότητες αυτές τυπικά αντιπροσωπεύονται από μεγάλους τηλεπικοινωνιακούς οργανισμούς π.χ. ΟΤΕ στην Ελλάδα.
- **Παροχέας Τελικής Υπηρεσίας**. Η οντότητα που παρέχει με χρήση κάποιου πρωτοκόλλου επικοινωνίας, την ζητούμενη από τον χρήστη υπηρεσία π.χ. αναζήτηση πληροφοριών με χρήση μηχανών αναζήτησης (search engines), αγορά προϊόντων με χρήση τεχνολογιών ανάπτυξης ηλεκτρονικού εμπορίου κ.λ.π.

Δύο επιπλέον οντότητες που παίζουν σημαντικό ρόλο στην διεκπεραίωση των ηλεκτρονικών συναλλαγών αλλά δεν εμπλέκονται, συνήθως, άμεσα σε αυτές είναι:

- **Έμπιστες Τρίτες Οντότητες**: αυτές είναι έμπιστες οντότητες οι οποίες δεν εμπλέκονται άμεσα στην συναλλαγή αλλά μπορούν να καταφύγουν οι εμπλεκόμενοι μιας συναλλαγής σε περιπτώσεις διενέξεων, για την επαλήθευση των στοιχείων της συναλλαγής. Τυπικό έργο των οντοτήτων αυτών είναι η έκδοση και διαχείριση ψηφιακών πιστοποιητικών (**digital certificates**). Οι έμπιστες οντότητες συναντούνται στην βιβλιογραφία και με τον όρο «**Αρχές Πιστοποίησης**».
- **Λοιποί ενδιάμεσοι**: αυτές είναι τυπικά οι «**Τράπεζες**» που εμπλέκονται στην εκκαθάριση των πληρωμών είτε αυτές πραγματοποιούνται με τεχνολογίες ψηφιακού χρήματος είτε με χρήση πιστωτικών καρτών.

2.7 Οι κίνδυνοι

Ο χώρος του ηλεκτρονικού εμπορίου κρύβει πολλούς κινδύνους για τον ανυποψίαστο χρήστη. Οι περιπτώσεις όπου διακριτά καταγράφονται προσωπικά δεδομένα διακρίνονται στις παρακάτω κατηγορίες:

- Όταν με τη συγκατάθεσή του ο χρήστης δίνει τα προσωπικά του στοιχεία, όποτε για παράδειγμα επιθυμεί να αγοράσει κάποιο προϊόν /υπηρεσία ή να κατεβάσει (**download**) κάποιο πρόγραμμα στον προσωπικό του υπολογιστή ή και να εγγραφεί σε κάποια υπηρεσία του διαδικτύου. Προσωπικά δεδομένα, θεωρούνται: στοιχεία ταυτότητας, στοιχεία επαγγελματικά, στοιχεία εκπαίδευσης ή και ακόμα οικονομικά στοιχεία όπως είναι ο αριθμός της πιστωτικής κάρτας.
- Όταν χωρίς την συγκατάθεσή του χρήστη, συλλέγονται προσωπικά στοιχεία μέσω των λεγόμενων προγραμμάτων «**cookies**» τα οποία καταγράφουν και επεξεργάζονται την συμπεριφορά του χρήστη κατά την πλοήγησή του στο διαδίκτυο (πχ προτιμητέες ιστοσελίδες, συχνότητα επίσκεψης σε μια ηλεκτρονική διεύθυνση).

- Όταν στα πλαίσια του παροχέα υπηρεσιών πρόσβασης στο Internet τηρείται αρχείο με τα προσωπικά στοιχεία του χρήστη και κατ' επέκταση στοιχεία των ηλεκτρονικών διευθύνσεων (ιστοσελίδες) τις οποίες επισκέπτεται, τον ακριβή χρόνο και την ώρα ή τη διάρκεια της επίσκεψης.

Είναι γεγονός, ότι σε όλες τις παραπάνω περιπτώσεις, η συλλογή και επεξεργασία προσωπικών δεδομένων μπορεί να οδηγήσει σε παραβίαση της ιδιωτικής και προσωπικής ζωής του χρήστη όταν αυτή δεν εφαρμόζεται σύμφωνα με τις οικείες διατάξεις. Αποτελέσματα ερευνών έχουν δείξει ότι η έλλειψη προστασίας της ιδιωτικότητας στις επικοινωνίες (δηλαδή ή θεώρηση ότι το Internet δεν είναι 100% ασφαλές), είναι ο κύριος λόγος αποχής των δυνητικών χρηστών από την χρήση των υπηρεσιών του διαδικτύου.

Οι χρήστες θεωρούν ότι η έλλειψη ιδιωτικότητας στις επικοινωνίες είναι ο σημαντικότερος παράγοντας που εμποδίζει την ανάπτυξη του ηλεκτρονικού εμπορίου και τη θεωρούν σημαντικότερη από άλλους παράγοντες όπως το κόστος πραγματοποίησης ηλεκτρονικών συναλλαγών, οι δυσκολίες χρήσης του τεχνολογικού εξοπλισμού και η παραλαβή ανεπιθύμητων ηλεκτρονικών διαφημιστικών μηνυμάτων (σχετικά με παραπάνω θέματα παρατίθενται στις ενότητες που ακολουθούν, αποτελέσματα ερευνών με θέμα το Internet, το ηλεκτρονικό εμπόριο, τους κινδύνους του διαδικτύου κ.λ.π. τόσο για την Ελλάδα όσο και για το εξωτερικό).

2.8 Θέματα Ασφαλείας (Security) και συναλλαγών

Σύμφωνα με αποτελέσματα ερευνών που πραγματοποιήθηκαν από την εταιρεία «**Cyber Dialogue**», το 85% των αγοραστών που πραγματοποιούν συναλλαγές μέσω του διαδικτύου, δηλώνει πως η ασφάλεια δεδομένων αποτελεί έναν από τους σημαντικότερους παράγοντες επιλογής ηλεκτρονικού καταστήματος. Τα θέματα ασφαλείας δείχνουν να έχουν υψηλή προτεραιότητα στη συλλογιστική των χρηστών του διαδικτύου, αποδεικνύοντας παράλληλα πόσο σημαντικά είναι αυτά για την περαιτέρω εξέλιξη του ηλεκτρονικού εμπορίου. Τα ζητήματα ασφαλείας που σχετίζονται με το διαδίκτυο θα μπορούσαμε γενικά να τα χωρίσουμε σε δύο κατηγορίες:

- Θέματα ασφάλειας σχετικά με δίκτυα και πληροφοριακά συστήματα
- Θέματα ασφάλειας συναλλαγών μέσω διαδικτύου

Η πρώτη κατηγορία αποτελεί από μόνη της ένα ξεχωριστό και πολύπλοκο θέμα ασφάλειας και δεν θα μας απασχολήσει στο παρόν κείμενο, εφόσον αναφέρεται ειδικότερα στην τεχνική υποδομή των επιχειρήσεων, των οργανισμών και των παροχέων, που με τον ένα ή τον άλλο τρόπο εμπλέκονται με το διαδίκτυο ή μεταξύ τους. Μπορούμε να αναφέρουμε περιληπτικά ότι η ασφάλεια των δικτύων και των πληροφοριακών συστημάτων, αποτελεί ένα από τα δυσκολότερα προβλήματα για κάθε επιχείρηση η οποία είναι συνδεδεμένη σε κάποιο δίκτυο (εσωτερικό ή εξωτερικό) και απαιτούνται ειδικές γνώσεις, ικανότητες και επαγγελματισμός (από άλλες οντότητες διαχείρισης της ασφάλειας, όπως παραδείγματος χάριν ή **Encobde**), για την δημιουργία και διατήρηση συστημάτων σε υψηλά επίπεδα ασφάλειας.

Η δεύτερη κατηγορία με θέματα ασφάλειας επικεντρώνει το ενδιαφέρον της στις διαδικασίες και τους κινδύνους υλοποίησης από τις συναλλαγές μέσω του διαδικτύου (και όχι μόνο). Υπάρχουν βέβαια και άλλες μέθοδοι πληρωμών όπως: εμβάσματα, κάποιες μορφές ηλεκτρονικού χρήματος, αλλά αυτές αποτελούν ένα αμελητέο ποσοστό του συνόλου των συναλλαγών, οι οποίες όπως αποδεικνύει η πρακτική γίνονται σχεδόν πάντοτε με χρήση πιστωτικών καρτών χάρη στην ευελιξία και την ευκολία που παρέχει αυτό το «**πλαστικό**» μέσο στον καταναλωτή που χρησιμοποιεί το διαδίκτυο.

2.9 Συχνές ερωταποκρίσεις για το ηλεκτρονικό εμπόριο

- **Τι είναι το ηλεκτρονικό εμπόριο;**

Ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει Διαδικτυακή δέσμευση για αγορά η πώληση αγαθών ή υπηρεσιών . Ηλεκτρονικό εμπόριο θεωρούνται επίσης και οι συναλλαγές μέσω τηλεφώνου και Φαξ.

- **Ποιες οι έννοιες του προμηθευτή, του καταναλωτή και των μέσων επικοινωνίας εξ αποστάσεως;**

Προμηθευτής (πωλητής) είναι κάθε φυσικό ή νομικό πρόσωπο που ενεργεί μέσα στα πλαίσια της επαγγελματικής του δραστηριότητας. Καταναλωτής (αγοραστής) είναι κάθε φυσικό πρόσωπο που ενεργεί για λόγους , οι οποίοι δεν εμπίπτουν στα πλαίσια της επαγγελματικής δραστηριότητας. Μέσο επικοινωνίας εξ αποστάσεως είναι κάθε μέσο που μπορεί να χρησιμοποιηθεί για τη σύναψη σύμβασης μεταξύ προμηθευτή και καταναλωτή χωρίς την αυτοπρόσωπη και ταυτόχρονη παρουσία τους.

- **Τι είναι η σύμβαση εξ αποστάσεως;**

Η εξ αποστάσεως σύμβαση είναι αυτή που συνάπτεται μεταξύ ενός προμηθευτή και ενός καταναλωτή και για την κατάρτιση της οποίας ο προμηθευτής χρησιμοποιεί αποκλειστικά ένα ή περισσότερα μέσα επικοινωνίας εξ αποστάσεως, μέχρι και τη στιγμή σύναψης της σύμβασης .

- **Ποιες πληροφορίες πρέπει να έχει στη διάθεσή του ο καταναλωτής σε σχέση με τον προμηθευτή προτού δεσμευθεί από μια εξ αποστάσεως σύμβαση;**

Ο καταναλωτής πρέπει να έχει απαραίτητα στη διάθεσή του στοιχεία που αφορούν τον προμηθευτή ή τον αντιπρόσωπο του προμηθευτή, όπως την ταυτότητα, την κύρια δραστηριότητά του, τη γεωγραφική διεύθυνση στην οποία είναι εγκατεστημένος, το εμπορικό μητρώο στο οποίο είναι εγγεγραμμένος ο προμηθευτής, τον αριθμό καταχώρησής του αν είναι καταχωρημένος σε μητρώο καθώς και τα στοιχεία της αρμόδιας εποπτεύουσας αρχής αν η δραστηριότητα του προμηθευτή υπόκειται σε καθεστώς έγκρισης.

- **Ποιες πληροφορίες πρέπει να έχει στη διάθεσή του ο καταναλωτής σε σχέση με υπηρεσία / προϊόν προτού δεσμευθεί από μια εξ αποστάσεως σύμβαση;**

Ο καταναλωτής πρέπει να έχει απαραίτητα στη διάθεσή του την περιγραφή των κυριοτέρων χαρακτηριστικών στοιχείων της υπηρεσίας/προϊόντος, το συνολικό τίμημα που πρέπει να πληρώσει συμπεριλαμβανομένων όλων των συναφών τελών, επιβαρύνσεων και δαπανών και όλων των φόρων, τις ρυθμίσεις σχετικά με την πληρωμή και την εκτέλεση της σύμβασης, το τυχόν ειδικό επιπλέον κόστος που συνεπάγεται για τον καταναλωτή η χρήση των μέσων επικοινωνίας εξ αποστάσεως και εάν αυτό το επιπλέον κόστος χρεώνεται. Επίσης πρέπει να έχει στη διάθεσή του την προθεσμία και τους όρους υπαναχώρησής του.

- **Τι είναι το δικαίωμα υπαναχώρησης;**

Το δικαίωμα της υπαναχώρησης είναι το δικαίωμα που παρέχεται στον καταναλωτή να αποσυρθεί μέσα σε μικρό χρονικό διάστημα από την σύμβαση αφού έχει καταρτισθεί.

- **Πώς ασκείται το δικαίωμα υπαναχώρησης;**

Σύμφωνα με το Ευρωπαϊκό δίκαιο (Οδηγία 97/7/ΕΚ άρθρο 6) ο καταναλωτής-χρήστης του Διαδικτύου διαθέτει προθεσμία τουλάχιστον επτά ημερολογιακών ημερών για να υπαναχωρήσει, χωρίς καμία ποινή και χωρίς να αναφέρει αιτιολογία από την εξ αποστάσεως σύμβαση . Η αντίστοιχη προθεσμία αναιτιολόγητης υπαναχώρησης στο Ελληνικό δίκαιο (άρθρο 4 παρ. 10 Νόμος 2251/1994) είναι δέκα εργάσιμες. Η προθεσμία εντός της οποίας μπορεί να ασκηθεί το δικαίωμα υπαναχώρησης αρχίζει να μετράται είτε από την ημέρα σύναψης της σύμβασης εξ αποστάσεως είτε από την ημέρα που ο καταναλωτής παρέλαβε τους συμβατικούς όρους και τις πληροφορίες.

- **Υπάρχουν εξαιρέσεις ως προς το δικαίωμα της υπαναχώρησης;**

Το δικαίωμα υπαναχώρησης δεν εφαρμόζεται στις συμβάσεις των οποίων η εκτέλεση έχει ολοκληρωθεί πλήρως και από τα δύο μέρη με ρητή αίτηση του καταναλωτή προτού ασκήσει ο καταναλωτής το δικαίωμα υπαναχώρησης. Δεν ασκείται σε χρηματοοικονομικές υπηρεσίες η τιμή των οποίων εξαρτάται από διακυμάνσεις της κεφαλαιαγοράς επί των οποίων ο προμηθευτής δεν έχει καμία επίδραση και μπορεί να επέλθουν κατά τη διάρκεια της προθεσμίας υπαναχώρησης π.χ. υπηρεσίες που αφορούν πράξεις συναλλάγματος, τίτλους της χρηματαγοράς, διαπραγματεύσιμους τίτλους, μερίδια οργανισμών συλλογικών επενδύσεων και άλλα. Επίσης εξαιρούνται από την υπαναχώρηση ασφαλιστήρια συμβόλαια ταξιδιών και αποσκευών ή παρόμοια βραχυπρόθεσμα ασφαλιστήρια συμβόλαια με διάρκεια μικρότερη του ενός μηνός.

- **Τι είναι η ασφάλεια στις εξ αποστάσεως συμβάσεις του ηλεκτρονικού εμπορίου;**

Ασφάλεια στις εξ αποστάσεως συμβάσεις αποτελεί η μη γνωστοποίηση ή διαρροή σε τρίτους των προσωπικών δεδομένων του καταναλωτή, όπως είναι τα προσωπικά στοιχεία του, ο αριθμός της πιστωτικής του κάρτας κλπ. τα

οποία συλλέγονται από τον προμηθευτή κατά τη διάρκεια σύναψης της σύμβασης με ηλεκτρονικά μέσα.

- **Είναι υποχρεωτική η ασφάλεια στο ηλεκτρονικό εμπόριο;**

Ο προμηθευτής οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Τα μέτρα αυτά είναι οι όροι των on line συμβάσεων, η ασφαλής σύνδεση με την τράπεζα και οι προστατευμένες περιοχές να έχουν κάλυψη ισχύος ψηφιακού πιστοποιητικού. Τα παραπάνω μέτρα πρέπει να κατοχυρώνουν επίπεδο ασφαλείας ανάλογο προς τον κίνδυνο παραβίασης του δικτύου. Σε περίπτωση ύπαρξης ιδιαίτερου κινδύνου παραβίασης της ασφάλειας του δικτύου στο οποίο γίνεται η συναλλαγή ο προμηθευτής οφείλει να ενημερώνει τους καταναλωτές για τον κίνδυνο αυτό .

- **Τι είναι η ηλεκτρονική πληρωμή;**

Ηλεκτρονική πληρωμή αποτελούν οι εξής τρόποι εκκαθάρισης των διαδικτυακών συναλλαγών: 1. η ηλεκτρονική καταβολή μέσω της ηλεκτρονικής μεταφοράς κεφαλαίων (e- banking), 2. η χρήση πιστωτικών καρτών και 3. η ύπαρξη ηλεκτρονικού χρήματος. Η διαδικασία πληρωμής μέσω ηλεκτρονικού χρήματος στην Ελλάδα δεν έχει προχωρήσει ακόμα σε πρακτική εφαρμογή.

- **Πώς προστατεύεται ο καταναλωτής στις περιπτώσεις πληρωμής με κάρτα;**

Προληπτικά ο καταναλωτής για να προστατευθεί από την δόλια χρήση της πιστωτικής του κάρτας πρέπει να ερευνήσει τα στοιχεία της εταιρίας με την οποία πρόκειται να συναλλαγεί, δηλαδή αν υφίσταται αυτή η εταιρία, αν μπορεί να επικοινωνήσει με αυτή και γενικότερα την αξιοπιστία της. Επίσης αν πληρούνται κάποιοι τεχνικοί όροι ασφαλείας των δεδομένων μέσα στις ιστοσελίδες όπου δίνονται τα στοιχεία για την κατάρτιση της συναλλαγής.

Αν πάρα ταύτα χρησιμοποιηθεί παράνομα η κάρτα του ο καταναλωτής πρέπει να προβεί σε έγγραφη διαμαρτυρία στην τράπεζα με την οποία να αρνείται την παράνομη συναλλαγή και να ζητήσει την επαναπίστωση του ποσού στην κάρτα του.

2.10 Φορολόγηση ηλεκτρονικών υπηρεσιών

Στο πλαίσιο της Νέας Οικονομίας, έχουν δημιουργηθεί νέα δεδομένα όσον αφορά στη φορολόγηση υπηρεσιών που παρέχονται με ηλεκτρονικά μέσα. Στο κείμενο που ακολουθεί περιγράφεται -υπό μορφή Συχνών Ερωτήσεων και Απαντήσεων- το νομοθετικό πλαίσιο που αφορά στην υποβολή Φόρου Προστιθέμενης Αξίας και την online αποστολή τιμολογίων για ηλεκτρονικές υπηρεσίες που παρέχονται εντός και εκτός της Ευρωπαϊκής Ένωσης.

2.11 Φόρος Προστιθέμενης Αξίας

- **Για ποιες υπηρεσίες θεωρείται ότι ο τόπος παροχής των υπηρεσιών βρίσκεται στην Ελλάδα;**

Γενικά η παροχή υπηρεσιών θεωρείται ότι πραγματοποιείται στην Ελλάδα, εφόσον κατά το χρόνο γένεσης της φορολογικής υποχρέωσης αυτός που παρέχει τις υπηρεσίες έχει στο εσωτερικό της χώρας την έδρα ή τη μόνιμη εγκατάστασή του, από την οποία παρέχονται οι υπηρεσίες ή, αν δεν υπάρχει έδρα ή μόνιμη εγκατάσταση, την κατοικία ή τη συνήθη διαμονή του.

Κατ' εξαίρεση ο τόπος παροχής υπηρεσιών θεωρείται ότι βρίσκεται στο εσωτερικό της χώρας μεταξύ άλλων και στις περιπτώσεις των τηλεπικοινωνιών, των ραδιοφωνικών και τηλεοπτικών υπηρεσιών και των υπηρεσιών που παρέχονται ηλεκτρονικά.

Προϋπόθεση είναι οι υπηρεσίες αυτές να παρέχονται από πρόσωπα εγκαταστημένα σε άλλο κράτος-μέλος σε υποκειμένους στο φόρο, οι οποίοι έχουν στο εσωτερικό της χώρας την έδρα ή τη μόνιμη εγκατάστασή τους ή την κατοικία, ή τη συνήθη διαμονή τους ή, εφόσον παρέχονται από πρόσωπα εγκατεστημένα εκτός της Κοινότητας, σε οποιονδήποτε λήπτη εγκατεστημένο στο εσωτερικό της χώρας.

- **Ποιες θεωρούνται ηλεκτρονικά παρεχόμενες υπηρεσίες;**

Υπηρεσίες που παρέχονται ηλεκτρονικά είναι η δημιουργία και φιλοξενία ιστοσελίδων, η εξ αποστάσεως συντήρηση προγραμμάτων και εξοπλισμού, η παροχή λογισμικού και η ενημέρωσή του, η παροχή εικόνων, κειμένων, πληροφοριών και η διάθεση βάσεων δεδομένων, η παροχή μουσικής, ταινιών και παιγνιδιών συμπεριλαμβανομένων και κάθε είδους τυχερών παιγνιδιών, καθώς και πολιτικών, πολιτιστικών, καλλιτεχνικών, αθλητικών, επιστημονικών ή ψυχαγωγικών εκπομπών ή εκδηλώσεων και η παροχή διδασκαλίας εξ αποστάσεως (τηλεκπαίδευση).

Μόνη η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου μεταξύ παρέχοντος και λήπτη υπηρεσίας δεν αρκεί για να θεωρηθεί η υπηρεσία αυτή υπηρεσία που παρέχεται ηλεκτρονικά.

- **Ποιος συντελεστής ΦΠΑ δεν εφαρμόζεται στις παραπάνω ηλεκτρονικές υπηρεσίες;**

Στις ηλεκτρονικές υπηρεσίες δεν εφαρμόζεται ο συντελεστής ΦΠΑ 8% που εφαρμόζεται για τα αγαθά και τις υπηρεσίες που περιλαμβάνονται στο Παράρτημα ΙΙΙ του Κώδικα ΦΠΑ) .Ο συντελεστής του φόρου προστιθέμενης αξίας για τις υπηρεσίες αυτές ορίζεται σε δεκαοκτώ τοις εκατό (18%) στη φορολογητέα αξία.

- **Τι ισχύει στις περιπτώσεις που ο πάροχος ηλεκτρονικών υπηρεσιών δεν είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση;**

Ο μη εγκατεστημένος στην Κοινότητα υποκείμενος στο φόρο, ο οποίος παρέχει ηλεκτρονικές υπηρεσίες σε πρόσωπο εγκατεστημένο σε κράτος-μέλος της ΕΕ, μπορεί να χρησιμοποιεί το ειδικό καθεστώς του άρθρου 35α του

Κώδικα Φόρου Προστιθέμενης Αξίας (Ν. 2859/2000) που προστέθηκε με το άρθρο 5 του Ν. 3193/2003.

- **Τι υποχρεούται να κάνει ο μη εγκατεστημένος στην Κοινότητα υποκείμενος στο φόρο που υπάγεται στο παραπάνω ειδικό καθεστώς;**

Ο μη εγκατεστημένος στην Κοινότητα υποκείμενος στο φόρο ο οποίος επιλέγει ως κράτος-μέλος αναγνώρισης την Ελλάδα υποχρεούται να δηλώνει την ένταξη και την έξοδό του από το καθεστώς αυτό με την ηλεκτρονική υποβολή της κατά περίπτωση σχετικής δήλωσης.

Με τη δήλωση αυτή -δήλωση αναγνώρισης- δηλώνει το ονοματεπώνυμο ή την επωνυμία του, την ταχυδρομική του διεύθυνση, τις ηλεκτρονικές διευθύνσεις και ιστοσελίδες που διαθέτει, αριθμό φορολογικού μητρώου (αν του χορηγήθηκε στη χώρα του) καθώς και ότι δεν διαθέτει ΑΦΜ/ΦΠΑ εντός της Κοινότητας.

Μετά την υποβολή της δήλωσης αναγνώρισης χορηγείται ειδικός κωδικός αριθμός αναγνώρισης στον μη εγκατεστημένο υποκείμενο στο φόρο, ο οποίος εγγράφεται στο μητρώο αναγνώρισης. Ο αριθμός αυτός κοινοποιείται με ηλεκτρονικά μέσα στον μη εγκατεστημένο υποκείμενο στο φόρο.

Μετά την προαναφερθείσα διαδικασία υποχρεούται να υποβάλλει με ηλεκτρονικό τρόπο ειδική δήλωση φόρου προστιθέμενης αξίας κάθε ημερολογιακό τρίμηνο και μέχρι την 20ή ημέρα του μήνα που ακολουθεί το τρίμηνο, είτε έχει παρασχεθεί ηλεκτρονική υπηρεσία είτε όχι. Στην ειδική δήλωση ΦΠΑ περιλαμβάνονται ο ειδικός κωδικός αριθμός αναγνώρισης και η συνολική αξία της παροχής ηλεκτρονικών υπηρεσιών, χωρίς το ΦΠΑ, για τη φορολογική περίοδο, καθώς και το συνολικό ποσό του φόρου που αντιστοιχεί σε κάθε κράτος-μέλος κατανάλωσης στο οποίο οφείλεται φόρος. Αναφέρονται επίσης οι ισχύοντες φορολογικοί συντελεστές και το συνολικό ποσό του φόρου που οφείλεται.

Ο μη εγκατεστημένος υποκείμενος στο φόρο υποχρεούται να καταγράφει με επαρκείς λεπτομέρειες τα στοιχεία των συναλλαγών που καλύπτονται από το περιγραφόμενο ειδικό καθεστώς, ώστε να μπορούν οι φορολογικές αρχές του κράτους-μέλους κατανάλωσης να επαληθεύουν την ακρίβεια της ειδικής δήλωσης Φόρου Προστιθέμενης Αξίας.

- **Πώς και πότε μπορεί να διαγραφεί ο μη εγκατεστημένος στην Ευρωπαϊκή Ένωση υποκείμενος στο φόρο από το μητρώο αναγνώρισης;**
  - Ο υπαγόμενος στο παραπάνω ειδικό καθεστώς μη εγκατεστημένος μπορεί να διαγραφεί από το μητρώο αναγνώρισης όταν:
  - Γνωστοποιήσει ο ίδιος ότι δεν παρέχει πλέον ηλεκτρονικές υπηρεσίες
  - Διαπιστωθεί ότι η φορολογητέα του δραστηριότητα έχει τερματιστεί

- Δεν πληροί πλέον τις απαραίτητες προδιαγραφές που του επιτρέπουν να χρησιμοποιεί το ειδικό καθεστώς
- Έχει επανειλημμένως παραλείψει να συμμορφωθεί προς τους κανόνες που αφορούν στο ειδικό καθεστώς

2.12 Αποστολή τιμολογίων με ηλεκτρονικά μέσα

➢ **Με ποιους τρόπους μπορούν να αποστέλλονται τα τιμολόγια που ο επιτηδευματίας οφείλει να εκδίδει στους πελάτες του;**

Σύμφωνα με το άρθρο 18α του Κώδικα Βιβλίων και Στοιχείων (Π.Δ. 186/1992), που προστέθηκε με το άρθρο 1 του Ν. 3193/2003, τα τιμολόγια που εκδίδονται κατ' εφαρμογή των διατάξεων του Κώδικα Βιβλίων και Στοιχείων είναι δυνατόν να αποστέλλονται σε έντυπη μορφή ή, υπό τον όρο της αποδοχής του παραλήπτη, με ηλεκτρονικά μέσα.

➢ **Κάτω από ποιες προϋποθέσεις γίνονται δεκτά τα τιμολόγια που διαβιβάζονται με ηλεκτρονικά μέσα;**

Τα τιμολόγια που διαβιβάζονται με ηλεκτρονικά μέσα γίνονται δεκτά υπό την προϋπόθεση ότι η γνησιότητα της προέλευσής τους και η ακεραιότητα του περιεχομένου τους εξασφαλίζεται:

- Είτε μέσω προηγμένης ηλεκτρονικής υπογραφής
- Είτε μέσω ηλεκτρονικής ανταλλαγής δεδομένων (EDI), εφόσον η συμφωνία σχετικά με αυτή την ανταλλαγή προβλέπει τη χρησιμοποίηση διαδικασιών που να εξασφαλίζουν τη γνησιότητα της προέλευσης και την ακεραιότητα των δεδομένων.
- Ειδικά στην περίπτωση συναλλαγών με το εξωτερικό (μέσα στην Κοινότητα ή με χώρα εκτός ΕΕ) απαιτείται ως απαραίτητο ένα επιπλέον συνοπτικό έγγραφο σε έντυπη μορφή, το οποίο να περιέχει τουλάχιστον τα στοιχεία των αντισυμβαλλομένων και τη συνολική αξία της συναλλαγής. Το ανωτέρω έγγραφο δεν απαιτείται εφόσον φυλάσσονται αντίτυπα των τιμολογίων.

➢ **Ποια διαδικασία επιβάλλεται όταν τα τιμολόγια αποθηκεύονται ή διαβιβάζονται με ηλεκτρονικά μέσα;**

Με τον όρο "διαβίβαση και αποθήκευση τιμολογίου με ηλεκτρονικά μέσα" νοείται η διαβίβαση ή η θέση στη διάθεση του αποδέκτη και η αποθήκευση, που πραγματοποιούνται μέσω ηλεκτρονικού εξοπλισμού για την επεξεργασία (συμπεριλαμβανομένης της ψηφιακής συμπίεσης) και την αποθήκευση δεδομένων και μέσω τηλεφωνικής γραμμής, ραδιοφωνικής μετάδοσης, οπτικής ίνας ή άλλων ηλεκτρομαγνητικών μέσων.

Όταν τα τιμολόγια αποθηκεύονται ή διαβιβάζονται με ηλεκτρονικά μέσα, πρέπει να αποθηκεύονται και τα δεδομένα που εξασφαλίζουν τη γνησιότητα της προέλευσης και την ακεραιότητα του περιεχομένου του κάθε τιμολογίου, τα οποία δεν επιτρέπεται να τροποποιηθούν και πρέπει να είναι ευανάγνωστα για όσο χρόνο ορίζεται η διάρκεια φύλαξής τους από τον Κώδικα Βιβλίων και Στοιχείων.

Όταν ο επιτηδευματίας αποθηκεύει τα τιμολόγια τα οποία εκδίδει ή λαμβάνει με ηλεκτρονικά μέσα εξασφαλίζοντας επιγραμμική (online) πρόσβαση στα

δεδομένα και ο τόπος αποθήκευσης βρίσκεται σε άλλο κράτος-μέλος, η φορολογική αρχή έχει δικαίωμα πρόσβασης με ηλεκτρονικά μέσα, τηλεκφόρτωσης και χρήσης αυτών των τιμολογίων, όπου είναι αναγκαίο για το φορολογικό έλεγχο.

3 Στατιστικά και έρευνες για το Ηλεκτρονικό Εμπόριο

3.1 Το Ηλεκτρονικό Εμπόριο στον κόσμο (Στατιστικά)

Το Ηλεκτρονικό Εμπόριο αποτελεί αδιαμφισβήτητα μια πραγματικότητα στο διεθνές επιχειρηματικό πεδίο. Ολοένα και περισσότερες εταιρίες τα τελευταία χρόνια, τόσο στο εξωτερικό όσο και στην Ελλάδα, επενδύουν στον τομέα των νέων εμπορικών τεχνολογιών, σε μια προσπάθεια προσαρμογής τους στο νέο ηλεκτρονικό περιβάλλον και εδραίωσής τους σε σημαντικές θέσεις απέναντι στον ανταγωνισμό. Ωστόσο, η επιτυχία των εφαρμογών Ηλεκτρονικού Εμπορίου, εξαρτάται άμεσα από το βαθμό πρόσβασης των καταναλωτών στο διαδίκτυο (αγορά και χρήση υπολογιστών), τις κατάλληλες υποδομές και την πρόθεσή τους για αγορά με χρήση υπολογιστών.

Στους παρακάτω πίνακες παρουσιάζονται στοιχεία γενικά με τις παγκόσμιες τάσεις του ηλεκτρονικού εμπορίου όπως: ο βαθμός διείσδυσης του διαδικτύου και οι αγοραστικές συνήθειες των καταναλωτών όταν πρόκειται για ηλεκτρονικές συναλλαγές κ.α.

Online Αγοραστικές Συνήθειες σε σχέση με την διείσδυση του Διαδικτύου

Online Shopping Patterns In Terms of Internet Penetration			
Category	Country average	Lowest	Highest
Internet users	27%	6% (Indonesia)	58% (USA)
Online shoppers	10%	1% (Thailand/Turkey)	27% (USA)
Online dropouts	15%	1% (India)	32% (Korea)
Offline shoppers (but browse online)	13%	1% (Portugal)	36% (Hong Kong)
Future online shoppers	14%	3% (Poland)	31% (Italy)
Source: Taylor Nelson Sofres April 02			

Πηγή: http://www.epaynews.com/statistics/transactions.html

Πίνακας 3.1

Ποσοστιαία κατανομή των συνολικών εσόδων από εφαρμογές Ηλεκτρονικού Εμπορίου σε παγκόσμιο επίπεδο

Όπως δείχνει ο παρακάτω πίνακας 3.2, οι εκτιμήσεις που αφορούν την ποσοστιαία κατανομή των συνολικών εσόδων από εφαρμογές Ηλεκτρονικού Εμπορίου σε παγκόσμιο επίπεδο, δείχνουν ότι ενώ πριν από μερικά χρόνια περίπου το 50% των παγκόσμιων συναλλαγών Ηλεκτρονικού Εμπορίου λάμβαναν χώρα στις Ηνωμένες Πολιτείες της Αμερικής, οι οποίες θεωρούνται πρωτοπόρες στην υιοθέτηση νέων τεχνολογιών, τα επόμενα χρόνια παρατηρείται μια πιο ομαλή κατανομή των εσόδων, καθώς και άλλες χώρες, κυρίως της Δυτικής Ευρώπης, αρχίζουν και υιοθετούν εφαρμογές Ηλεκτρονικού Εμπορίου σε μεγαλύτερο βαθμό.

Regional Percentages of eCommerce Revenues, 2000 - 2004		
Region	Totals in 2000	Totals in 2004
United States	46%	38%
Western Europe	20%	33%
Japan	21%	12%
Asia-Pacific	5%	10%
Rest of World	7%	7%
Source: IDC, March 2001		

Πηγή: http://www.epaynews.com/statistics/transactions.html

Πίνακας 3.2

European Card Market Growth, 2000-2002			
Brand (in millions)	2000	2001	2002
MasterCard	239.5	298.6	313.1
Visa EU	177.2	194.6	211.7
Total	448.7	493.2	524.8
Increase %	13.7	9.8	6.5
* Includes MasterCard brands in CEE/CIS			
Source: European Card Review, June 2003			

Πίνακας 3.3

US Consumer Transactions In 2001, 2010 And 2020			
Payment Means (in USD billions)	2001	2010	2020
Electronic	2.5	10.5	30.25
Debit Card	11	28.5	49
Credit Card	21.5	31	38
Direct Checks	29	20	15
Consumer Checks	35	29	24
Cash	51	62	52
Source: The Nilson Report, April 2002			

Πίνακας 3.4

Παγκόσμια Πρόβλεψη για το Ηλεκτρονικό Εμπόριο για το 2004

Πηγή: http://www.epaynews.com/statistics/transactions.html

Μέσω των στοιχείων του παρακάτω πίνακα 3.4 η εταιρία Forrester Research εκτιμά, ότι το 2004 η αξία των αγαθών και υπηρεσιών που θα διακινούνται μέσω του διαδικτύου θα ανέρχεται σε 8.1 τρισεκατομμύρια δολάρια περίπου και θα είναι κατανεμημένη σε παγκόσμια κλίμακα ως εξής:

Forrester's Global eCommerce Predictions	
Region	**Total (USD)**
North America	3.5 trillion
Asia Pacific	1.6 trillion
Western Europe	1.5 trillion
Latin America	81.8 billion
Rest of World	68.6 billion
Source: Forrester	

Πηγή: http://www.epaynews.com/statistics/transactions.html

Πίνακας 3.5

Worldwide B2B eCommerce Market, 2000 - 2004	
Year	**Total (USD)**
2000	$433 billion
2001	$919 billion
2002	$1.9 trillion
2003	$3.6 trillion
2004	$6.0 trillion
2005	$8.5 trillion
Source: Gartner	

Πίνακας 3.6

Total Worldwide eCommerce Revenues, 2004 (B2B & B2C)	
Region	**Total**
North America	$3.5 trillion
Asia Pacific	$1.6 trillion
Western Europe	$1.5 trillion
Latin America	$81.8 billion
Rest of World	$68.6 billion
Source: Forrester Research	

Πίνακας 3.7

Διεπιχειρησιακές (B2B) συναλλαγές για Η.Π.Α, Ευρώπη και Ασία, για τις χρονιές 1998 – 2002 (σε δισεκατομμύρια δολάρια)

Πηγή: http://www.epaynews.com/statistics/transactions.html

Ενδιαφέρον επίσης παρουσιάζει το γεγονός ότι συναλλαγές μεταξύ επιχειρήσεων (Business to Business – B2B), που πραγματοποιούνται με τη

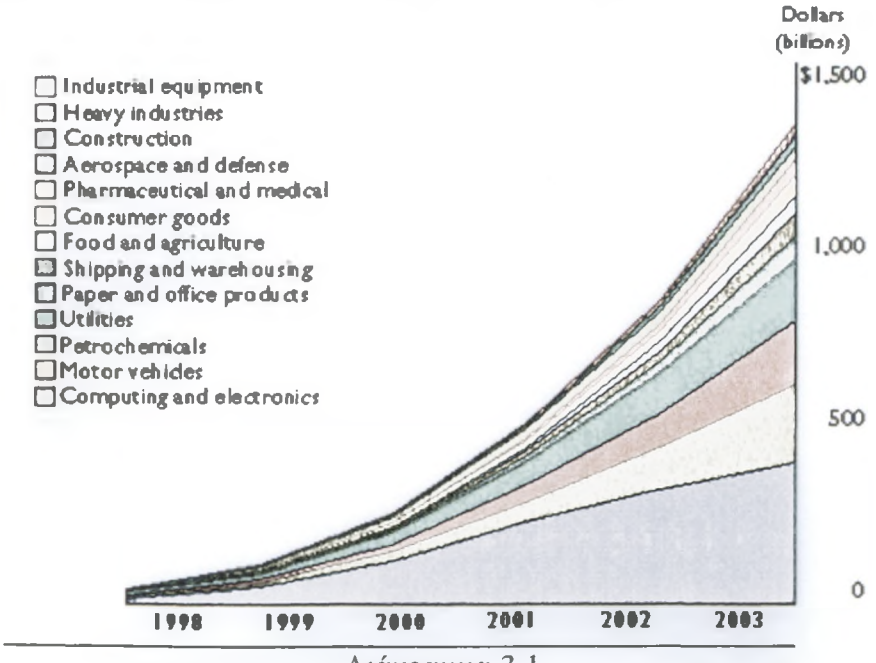
χρήση εφαρμογών ηλεκτρονικού εμπορίου σε διεθνή κλίμακα παρουσιάζουν τα τελευταία χρόνια ραγδαία αύξηση. Όπως φαίνεται και στον πίνακα 3.7 που ακολουθεί μεταξύ των ετών 2001 και 2002 οι διεπιχειρησιακές συναλλαγές που πραγματοποιήθηκαν μέσω Ηλεκτρονικού Εμπορίου έχουν υπερδιπλασιαστεί και στις τρεις σημαντικότερες περιοχές ανάπτυξης και υιοθέτησης νέων τεχνολογιών.

Total B2C Revenues For US, Europe & Asia, 1999 - 2003 (in USD billions)					
Region	1999	2000	2001	2002	2003
US	75	150	250	400	750
Europe	25	30	40	50	60
Japan	25	30	50	75	250
Source: Fortune Magazine					

Πηγή:

Πίνακας 3.8

Οι προβλέψεις της Forrester Research για την πορεία του ηλεκτρονικού εμπορίου είναι ιδιαίτερα αισιόδοξες και τα συνολικά έσοδα για τις Η.Π.Α. προβλέπεται να ανέλθουν στα 1,331 τρισεκατομμύρια δολάρια. Στο παρακάτω διάγραμμα παρουσιάζονται οι προβλέψεις ανά κατηγορία:



Διάγραμμα 3.1

3.2 Έρευνα του eLTRUN

Όσον αφορά στις ελληνικές επιχειρήσεις, από έρευνα του eLTRUN (***Κέντρο Ηλεκτρονικού Επιχειρείν του Οικονομικού Πανεπιστημίου Αθηνών***) για

λογαριασμό της Ε.Α.Σ.Ε. (***Εταιρία Ανώτατων Στελεχών Επιχειρήσεων***), που διεξήχθη το 2001, προέκυψε ότι το 38% των ελληνικών επιχειρήσεων κάνουν χρήση *Εφαρμογών Ηλεκτρονικού Εμπορίου*. Από αυτές το 12,5% έκαναν οργανωμένη χρήση κατά την περίοδο διεξαγωγής της έρευνας, ενώ το 25,5% αποσπασματική. Επιπλέον το 47% των επιχειρήσεων δεν ήταν χρήστες εφαρμογών Ηλεκτρονικού Εμπορίου, αλλά το προγραμμάτιζαν για το άμεσο μέλλον.

Χρήση Εφαρμογών Ηλεκτρονικού Εμπορίου από τις ελληνικές επιχειρήσεις

	%
Χρήστες Ηλεκτρονικού Εμπορίου σε οργανωμένη βάση	12,5
Χρήστες Ηλεκτρονικού Εμπορίου αποσπασματικά	25,5
Δεν είναι χρήστες Ηλεκτρονικού Εμπορίου, αλλά το προγραμματίζουν	47
Δεν είναι χρήστες Ηλεκτρονικού Εμπορίου, ούτε το προγραμματίζουν	15

Στην ίδια έρευνα φαίνεται ότι ορισμένοι κλάδοι της Ελληνικής οικονομίας είναι σαφώς προωθημένοι σε ότι αφορά στην υιοθέτηση Ηλεκτρονικού Εμπορίου σε σχέση με το μέσο όρο στο σύνολο των κλάδων (38% οργανωμένη ή αποσπασματική υιοθέτηση). Ο κλάδος της Πληροφορικής φάνηκε να κυριαρχεί στην οργανωμένη χρήση εφαρμογών Ηλεκτρονικού Εμπορίου σε ποσοστό σχεδόν διπλάσιο του μέσου όρου (22% έναντι 12,5%), ενώ το σύνολο οργανωμένης και αποσπασματικής χρήσης φτάνει το 58%. Ακολουθούσαν οι υπηρεσίες, με τις μισές σχεδόν επιχειρήσεις να δηλώνουν χρήση εφαρμογών Ηλεκτρονικού Εμπορίου και έπονταν τα χρηματοοικονομικά. Το εμπόριο υστερούσε ελαφρά στο ποσοστό υιοθέτησης από το μέσο όρο και ακολουθούσε με ανάλογο ποσοστό η βιομηχανία.

Κλάδος	**%**
Πληροφορική	**58,0**
Υπηρεσίες	**48,5**
Χρηματοοικονομικά	**44,5**
Εμπόριο	**37,0**
Βιομηχανία	**33,5**

4 Ορισμοί και τύποι εγκλημάτων

4.1 Τι είναι το cyber και το computer crime;

Ένας ευρύς ορισμός του όρου **computer crime** θα μπορούσε να είναι ο ακόλουθος:

«οποιοδήποτε έγκλημα που διαπράττεται ή περιλαμβάνει τη χρήση ενός υπολογιστή».

Μέσω της ιστοσελίδας http://www.oxfordreference.com βρίσκουμε για τον ορισμό του **cyber crime**:

«τα εγκλήματα που διαπράττονται μέσω του Διαδικτύου».

Η εγκυκλοπαίδεια Britannica ορίζει ως **cyber crime:**

«οποιοδήποτε έγκλημα που διαπράττεται με τη βοήθεια ειδικών γνώσεων ή της εξειδικευμένης χρήσης των τεχνολογιών που σχετίζονται με υπολογιστές».

Οι παραπάνω ορισμοί αποτελούν απόρροια της προσπάθειας πολλών εμπειρογνωμόνων να οριοθετήσουν το τι ακριβώς αποτελεί ένα έγκλημα στον κυβερνοχώρο («**cyber crime**») ή ένα ηλεκτρονικό έγκλημα (δηλαδή ένα έγκλημα σχετικό με έναν υπολογιστή - «**computer crime**»). Στο παρόν κείμενο όταν αναφερόμαστε στο έγκλημα εννοούμε όλα εκείνα τα εγκλήματα τα οποία μπορούν να πραγματοποιηθούν με τη χρήση της τεχνολογίας της πληροφορικής.

Το cyber crime εύλογα περιλαμβάνει μια ευρεία ποικιλία ποινικών αδικημάτων καθώς και άλλων δραστηριοτήτων. Ένας μεγάλος αριθμός τέτοιων δραστηριοτήτων που θεωρούνται ως cyber crime, μπορούν να βρεθούν στο εγχειρίδιο των **Ηνωμένων Εθνών** «*United Nations Manual on the Prevention and Control of Computer-Related Crime*». Σχετικά αναφέρονται σε αυτό ως παραδείγματα του cyber crime, η απάτη (**fraud**), η παραποίηση (**forgery**), η δολιοφθορά υπολογιστών (**computer sabotage**), η μη εξουσιοδοτημένη πρόσβαση (**unauthorised access**), η κατασκοπεία (**espionage**), η υπεξαίρεση χρημάτων (**embezzlement**), η αντιγραφή προγραμμάτων υπολογιστών καθώς και άλλα.

Συνοψίζοντας τα παραπάνω θα μπορούσαμε να πούμε ότι το έγκλημα που διαπράττεται στον κυβερνοχώρο (**cyber crime**), αποτελεί μια ιδιαίτερη μορφή του ηλεκτρονικού εγκλήματος (**computer crime**), το οποίο με τη σειρά του είναι μια ειδικότερη μορφή του «**κοινού εγκλήματος**», όπως αυτό προσδιορίζεται στο άρθρο 14 του ποινικού κώδικα[1]. Η κακόβουλη χρήση του συνόλου των δυνατοτήτων ενός υπολογιστή μπορεί να χαρακτηριστεί ως «**ηλεκτρονικό έγκλημα**», ενώ κάθε παράνομη, ανήθικη ή χωρίς (την απόκτηση δικαιώματος) δραστηριότητα ή πράξη που σχετίζεται με την αλλοίωση, τροποποίηση, επεξεργασία ή μετάδοση δεδομένων μέσω

[1] Άρθρο 14 - Έννοια της αξιόποινης πράξης (1. Έγκλημα είναι πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο. 2. Στις διατάξεις των ποινικών νόμων ο όρος <<πράξη>> περιλαμβάνει και τις παραλείψεις).

υπολογιστών, μπορεί να χαρακτηριστεί ως έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (**computer related crime ή computer crime**).

4.2 Ταξινόμηση Cyber Crimes

Σύμφωνα με τους ορισμούς της προηγούμενης παραγράφου φαίνεται να επικρατεί η άποψη ότι το έγκλημα στον κυβερνοχώρο (**cyber crime**) αποτελεί τον ίδιο τύπο εγκλήματος με το «κοινό» ή «συμβατικό» έγκλημα με μόνη διαφορά το ότι διαπράττεται σε διαφορετικό περιβάλλον (δηλαδή σε ηλεκτρονικό περιβάλλον). Όπως όμως θα δούμε στις επόμενες παραγράφους αυτό δεν ανταποκρίνεται στην πραγματικότητα.

Αυτό οφείλεται στο γεγονός ότι υπάρχουν εγκλήματα που διαπράττονται τόσο σε κοινό όσο και σε ηλεκτρονικό περιβάλλον ενώ, υπάρχουν εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών χωρίς οι τελευταίοι να συνδέονται με το διαδίκτυο άλλα και εγκλήματα που διαπράττονται αποκλειστικά και μόνο στο περιβάλλον του διαδικτύου. Σύμφωνα με την προηγούμενη διαπίστωση διαφαίνεται μια πρώτη ταξινόμηση των εγκλημάτων ως προς το περιβάλλον στο οποίο πραγματοποιούνται, και είναι η ακόλουθη:

- Εγκλήματα που διαπράττονται τόσο σε «**κοινό**» περιβάλλον, όσο και στο ηλεκτρονικό.
- Εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών χωρίς τη χρήση του διαδικτύου (**computer crimes**).
- Εγκλήματα που διαπράττονται αποκλειστικά και μόνο σε περιβάλλον διαδικτύου (**cyber crimes**).

Οι παραπάνω διαπιστώσεις (σχετικά με τους ορισμούς των εγκλημάτων) δείχνουν τις δυσκολίες τις οποίες αντιμετωπίζει οποιοσδήποτε επιθυμεί να ταξινομήσει τα ηλεκτρονικά εγκλήματα. Πρέπει να σημειωθεί ότι, παρότι υπάρχουν πάρα πολλές σεβαστές προσεγγίσεις, δεν υπάρχει ακόμη μια ευρεία και παγκόσμια αποδεκτή ταξινόμηση των ηλεκτρονικών εγκλημάτων.

Στο παρόν έγγραφο γίνεται μια προσπάθεια ταξινόμησης των ηλεκτρονικών εγκλημάτων με γνώμονα ένα σύνολο παραμέτρων που χρησιμοποιούνται τόσο από την Ελληνική όσο και από την Ευρωπαϊκή Νομοθεσία, καθώς επίσης και με κριτήρια που σχετίζονται με την ασφάλεια ηλεκτρονικών υπολογιστών. Το σύνολο των παραμέτρων που χρησιμοποιούνται για την ταξινόμηση των ηλεκτρονικών εγκλημάτων αναλύεται ως εξής:

- Τύποι Εγκληματιών ανάλογα με το κίνητρό τους
- Τύποι Εγκλημάτων ανάλογα με το επιθυμητό αποτέλεσμα
- Μέσα και εργαλεία που χρησιμοποιούνται από τους εγκληματίες για την επιτυχή έκβαση των εγκληματικών τους ενεργειών
- Μέθοδοι πρόσβασης που χρησιμοποιούνται για την επιτυχή έκβαση των εγκληματικών ενεργειών

Στις ενότητες που ακολουθούν περιγράφονται λεπτομερώς οι παραπάνω κατηγορίες.

4.2.1 *Τύποι Εγκληματιών(ως προς τα Κίνητρα)*

Είναι δύσκολο να αναφερθεί κάποιος με ακρίβεια για το ποια ακριβώς είναι τα κίνητρα εκείνων που πραγματοποιούν ηλεκτρονικά εγκλήματα. Όλοι οι εγκληματίες θέλουν να παραμείνουν ανώνυμοι και για το λόγο αυτό τα κίνητρά τους δεν γίνονται πάντοτε γνωστά, τουλάχιστον στο εύρος που θα επιθυμούσαν οι αρμόδιες αρχές. Τα κίνητρα των εγκληματιών τις περισσότερες φορές παραμένουν ασαφή αλλά όχι άγνωστα. Από συλληφθέντες αλλά και από την εκπόνηση πολλών ερευνών σχετικά με τα cyber crimes εντοπίζονται κίνητρα όπως:

- πρόκληση,
- περιέργεια,
- διασκέδαση,
- ανία,
- εκδίκηση,
- προσωπική φήμη και δόξα,
- διαμαρτυρία,
- αναρχία,
- πολιτικό όφελος
- οικονομικό όφελος,
- βιομηχανική κατασκοπεία,
- κρατική κατασκοπεία,
- δυσφήμιση.

Κατά τα εμβρυακά στάδια του διαδικτύου, το μόνο κίνητρο των ανεξάρτητων hackers ήταν η εξερεύνηση της τεχνολογίας και η απόκτηση γνώσης. Σήμερα οι αυτόνομοι hackers έχουν μετατραπεί, σε μεγάλο βαθμό, σε οργανωμένες ομάδες. Ταυτόχρονα, έχουν εμφανιστεί ομάδες εγκληματιών που έχουν πλέον ως κίνητρα είτε το οικονομικό είτε το πολιτικό κέρδος. Αυτές οι οργανωμένες ομάδες λειτουργούν με τον ελάχιστο δυνατό κίνδυνο, καθώς εκμεταλλεύονται τη συναλλακτική και παγκοσμιοποιημένη φύση του διαδικτύου, και έχουν τη δυνατότητα υλοποίησης ολοένα και μεγαλύτερων εγκλημάτων με σκοπό το κέρδος. Παραδείγματος χάριν, παραδοσιακά εγκλήματα, όπως το ξέπλυμα χρημάτων (money laundering), υλοποιούνται πολύ πιο εύκολα μέσω αγοράς αγαθών που πωλούνται από on-line δημοπρασίες.

Επίσης, φαίνεται ότι οι διεθνείς εξελίξεις διαμορφώνουν τα κίνητρα που σχετίζονται με τα ηλεκτρονικά εγκλήματα. Η κατάσταση έχει αλλάξει άρδην τα τελευταία χρόνια καθώς τα σημαντικά τρομοκρατικά χτυπήματα των τελευταίων ετών αποτελούν ένα κρίσιμο σημείο καμπής των εγκληματικών ενεργειών που παρατηρούνται σε ολόκληρο τον κόσμο, επηρεάζοντας ακόμη και το χώρο του διαδικτύου.

Το οργανωμένο έγκλημα και η τρομοκρατία στο διαδίκτυο αποτελούν ενδείξεις για τη μελλοντική εξέλιξη του cyber crime. Όμως, δεν πρέπει να παραβλέπονται οι αφανείς διαστάσεις του προβλήματος καθώς πλέον η τεχνολογία της πληροφορικής αποτελεί ένα σημαντικό μέσο για την εκπόνηση συμβατικών εγκλημάτων. Για παράδειγμα, το διαδίκτυο χρησιμοποιείται από

εγκληματίες, για την οργάνωσή τους και για την απόκτηση πληροφοριών, με κύριο στόχο την διεξαγωγή συμβατικών εγκλημάτων (πχ. τρομοκρατικές επιθέσεις).

Οι κυριότεροι τύποι εγκληματιών που σχετίζονται με τα εγκλήματα στον κυβερνοχώρο (**cyber crimes**) και με βάση τα διαφορετικά κίνητρα, χωρίζονται συνοπτικά στις παρακάτω κατηγορίες:

- **Εισβολείς (Hackers)** – Εισβάλλουν στους υπολογιστές με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης, γεγονός που το αντιμετωπίζουν ως πρόκληση.
- **Κατάσκοποι (Spies)** - Εισβάλλουν στους υπολογιστές με στόχο την απόκτηση πληροφοριών, ώστε να τις χρησιμοποιήσουν για να κερδίσουν οφέλη τόσο σε πολιτικό όσο και σε οικονομικό επίπεδο.
- **Τρομοκράτες (Terrorists)** - Εισβάλλουν στους υπολογιστές με στόχο την πρόκληση φόβου και με σκοπό να τους βοηθήσει στην επίτευξη πολιτικών ωφελειών.
- **Εταιρικοί Εισβολείς (Corporate raiders)** - Υπάλληλοι μιας επιχείρησης οι οποίοι εισβάλλουν στους υπολογιστές των ανταγωνιστών τους, με κύριο στόχο την επίτευξη εταιρικών οικονομικών ωφελειών (κέρδος).
- **Επαγγελματίες Κακοποιοί (Professional Criminals)** - Εισβάλλουν στους υπολογιστές με στόχο την επίτευξη προσωπικών οικονομικών ωφελειών (σε αντίθεση με τους corporate raiders).
- **Βάνδαλοι (Vandals)** - Εισβάλλουν στους υπολογιστές με στόχο την πρόκληση ζημιών.
- **Συμβατικοί Εγκληματίες (Conventional Criminals)** – Χρησιμοποιούν την τεχνολογία της πληροφορικής ως εργαλείο για την εκπόνηση συμβατικών εγκλημάτων.

4.2.2. Τύποι Εγκλημάτων (ως προς τα αποτελέσματα)

Μια προσπάθεια κατηγοριοποίησης των ηλεκτρονικών εγκλημάτων ως προς τα αποτελέσματα που προξενούν είναι η ακόλουθη (Η κατηγοριοποίηση αυτή έχει γίνει με γνώμονα την αξιόποινη πράξη που τελικά υλοποιείται. Οι κατωτέρω μορφές εγκλημάτων καθορίστηκαν και προσυπογράφηκαν από τα κράτη μέλη της Ευρωπαϊκής Ένωσης που έλαβαν μέρος στην σύνταξη *Σύμβασης για τον Κυβερνοχώρο - CONVENTION ON CYBERCRIME* την 23-11-2001 στην Βουδαπέστη):

- **Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων των ηλεκτρονικών υπολογιστών.**
  - Παράνομη πρόσβαση (Illegal Access): Μη εξουσιοδοτημένη πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών.
  - Αθέμιτη παγίδευση-Υποκλοπή (illegal interception): Παγίδευση – υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων, από, προς ή μέσα σ' ένα σύστημα

υπολογιστών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών.

- Επέμβαση σε δεδομένα (Data interference): Μη εξουσιοδοτημένη καταστροφή (damaging), διαγραφή (deletion), φθορά (deterioration), μεταβολή (alteration), ή απόκρυψη (suppression) δεδομένων.
- Επέμβαση σε σύστημα (System Interference): Μη εξουσιοδοτημένη παρεμπόδιση της λειτουργία ενός συστήματος υπολογιστή, που γίνεται με είσοδο (Inputting), μετάδοση (transmitting), καταστροφή (damaging), διαγραφή (deleting), φθορά (deterioration), μεταβολή (alteration), ή απόκρυψη (suppression) δεδομένων.
- Κακή χρήση συσκευών (misuse of devises): Μη εξουσιοδοτημένη παραγωγή, πώληση, ή προετοιμασία για χρήση εισαγωγή, διανομή ή με οποιαδήποτε άλλο τρόπο διάθεση:
  - μιας συσκευής, συμπεριλαμβανομένου προγράμματος υπολογιστή, που έχει σχεδιαστεί ή προσαρμοστεί πρωτίστως για τους σκοπούς διάπραξης οποιουδήποτε από τα προαναφερθέντα αδικήματα.
  - ενός password, access code, ή παρόμοιων δεδομένων μέσω των οποίων είναι δυνατή η πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών.

- **Εγκλήματα σχετιζόμενα με ηλεκτρονικούς υπολογιστές.**
  - Πλαστογραφία μέσω ηλεκτρονικών υπολογιστών (Computer related Forgery): Μη εξουσιοδοτημένη εισαγωγή, μεταβολή, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικών υπολογιστών με σκοπό τα δεδομένα αυτά να θεωρούνται ή να χρησιμοποιούνται για νόμιμους σκοπούς σαν να ήταν αυθεντικά.
  - Απάτη μέσω ηλεκτρονικών υπολογιστών (Computer related Fraud): Μη εξουσιοδοτημένη πρόκληση απώλειας περιουσίας σε κάποιον άλλον με:
    - οποιαδήποτε εισαγωγή, τροποποίηση, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικού υπολογιστή
    - οποιαδήποτε δόλια επέμβαση στη λειτουργία ενός συστήματος ηλεκτρονικού υπολογιστή.
- **Εγκλήματα σχετιζόμενα με το περιεχόμενο.**
  - Εγκλήματα σχετικά με την παιδική πορνογραφία: Διαπράττει όποιος από πρόθεση και χωρίς δικαίωμα:
    - Παράγει παιδική πορνογραφία δια μέσω συστήματος ηλεκτρονικού υπολογιστή
    - Προσφέρει ή διαθέτει παιδική πορνογραφία δια μέσω συστήματος ηλεκτρονικού υπολογιστή
    - Διανέμει ή μεταδίδει παιδική πορνογραφία δια μέσω συστήματος ηλεκτρονικού υπολογιστή

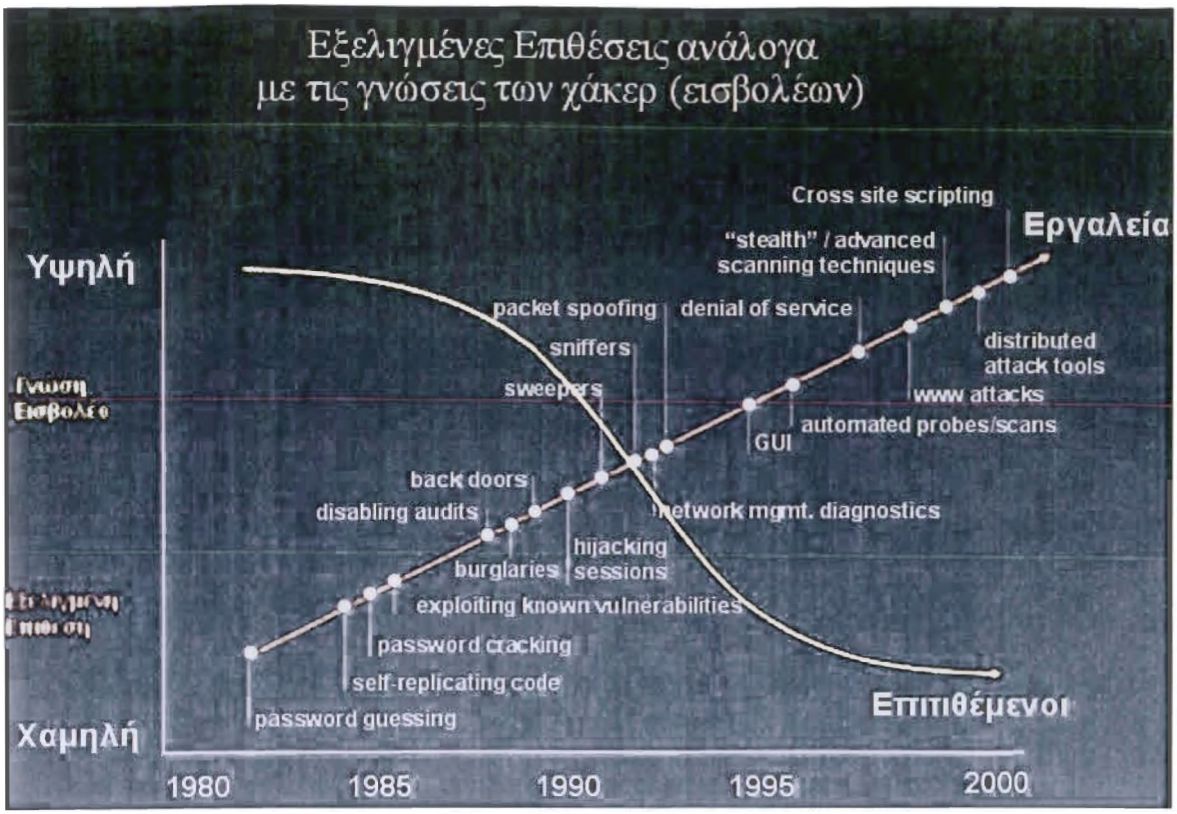
- Προμηθεύει ή προμηθεύεται παιδική πορνογραφία δια μέσω συστήματος ηλεκτρονικού υπολογιστή για τον εαυτό του ή για άλλον
- Κατέχει παιδική πορνογραφία σε σύστημα ηλεκτρονικού υπολογιστή ή σε άλλο μέσο αποθήκευσης δεδομένων ηλεκτρονικού υπολογιστή.

- **Εγκλήματα σχετιζόμενα με την καταπάτηση πνευματικών και αντίστοιχων δικαιωμάτων.**
  - Καταπάτηση πνευματικών δικαιωμάτων: Συμπεριφορά που θεωρείται ως αξιόποινη σύμφωνα με τις διεθνείς συνθήκες όπως την Πράξη των Παρισίων 24-7-1971, τη Σύμβαση της Βέρνης για την προστασία των καλλιτεχνικών δημιουργημάτων, τη Συμφωνία Εμπορίου σχετική με τα δικαιώματα της πνευματικής ιδιοκτησίας, τη Συνθήκη WIPO για τα πνευματικά δικαιώματα και τη Διεθνή σύμβαση για την προστασία των παραγωγών, εκτελεστών Φωνογραφικών Ραδιοφωνικών Οργανισμών που καταρτίσθηκε στη Ρώμη.

4.2.3 Μέσα και Εργαλεία για τη διάπραξη των cyber crimes

Το σύνολο των μέσων ή εργαλείων που έχει στη διάθεσή του ο εγκληματίας είναι πολλά και ο κατάλληλος συνδυασμός τους, προσδίδει σε αυτόν σημαντικά πλεονεκτήματα για την επίτευξη των εγκληματικών του ενεργειών. Τα παρακάτω αποτελούν μια συνοπτική περιγραφή ορισμένων μέσων που χρησιμοποιούνται σήμερα από τους εγκληματίες, για την πραγματοποίηση των στόχων τους.

- Διεξαγωγή Επιθέσεων Social Engineering.
- Χρήση Αυτόνομων Εξειδικευμένων Εργαλείων και Εφαρμογών.
- Χρήση Κατανεμημένων Εξειδικευμένων Εργαλείων (distributed tools).
- Χρήση ειδικών συσκευών παρακολούθησης και καταγραφής δεδομένων (data taps).
- Άμεση εκμετάλλευση αδυναμιών ασφάλειας (πχ. exploit through illegal application input).
- Δημιουργία και αποστολή κακόβουλου κώδικα.
- Συνδυασμός των παραπάνω.



Πηγή: Cyber Crime and Legislation (Carnegie Mellon University)

Διάγραμμα 4.1

4.2.4 Μέθοδοι απόκτησης μη εξουσιοδοτημένης πρόσβασης

Οι μέθοδοι απόκτησης μη εξουσιοδοτημένης πρόσβασης σε ένα πληροφοριακό σύστημα ποικίλλουν ανάλογα με το εκάστοτε τεχνολογικό περιβάλλον στο οποίο χρησιμοποιείται το εκάστοτε σύστημα. Οι γενικές κατηγορίες μεθόδων απόκτησης μη εξουσιοδοτημένης πρόσβασης είναι οι ακόλουθες:

- Αδυναμίες Υλοποίησης (Implementation Vulnerabilities). Οι εγκληματίες εκμεταλλεύονται τις ήδη υπάρχουσες αδυναμίες των διάφορων πληροφοριακών συστημάτων (είτε γιατί έχουν τις εσωτερικές πληροφορίες, είτε γιατί γνωρίζουν πολύ καλά τα συστήματα αυτά). Η εκμετάλλευση των αδυναμιών πραγματοποιείται επειδή τα συστήματα αυτά είτε δεν έχουν ενημερωθεί από τους υπεύθυνους διαχείρισής τους με τις κατάλληλες αναβαθμίσεις ασφάλειας, είτε επειδή δεν έχουν χρησιμοποιηθεί ή δεν έχουν ενεργοποιηθεί σωστά οι κατάλληλοι μηχανισμοί ασφάλειας. Το αποτέλεσμα της εκμετάλλευσης των αδυναμιών αυτών, είναι η μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα.
- Σχεδιασμός Νέων Αδυναμιών (Design Vulnerability). Οι εγκληματίες με τις εξειδικευμένες γνώσεις τους, σε πολλές περιπτώσεις υπερκαλύπτουν ακόμα και εκείνες των κατασκευαστών, ανακαλύπτουν από μόνοι τους αδυναμίες στα συστήματα με διάφορους τρόπους, τις οποίες στη συνέχεια εκμεταλλεύονται για απόκτηση πρόσβασης σε αυτά.
- Αδυναμίες Ρυθμίσεων (Configuration Vulnerability). Όλα τα ηλεκτρονικά και υπολογιστικά συστήματα ρυθμίζονται με συγκεκριμένους τρόπους με σκοπό την απρόσκοπτη και σωστή

5 Ηλεκτρονικό έγκλημα

5.1 Εισαγωγή

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής.

Μαζί όμως με τις αλλαγές αυτές που διευκολύνουν, προάγουν και βοηθούν στην καλυτέρευση της ποιότητας ζωής και στην τάχιστη εξυπηρέτηση των αναγκών που δημιουργεί η σύγχρονη κοινωνίας, οι νέες τεχνολογίες και το Ίντερνετ διευκόλυναν και δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας που συνοψίζονται στον όρο Ηλεκτρονικό έγκλημα.

5.2 Ορισμός

Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων.

Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη , η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων.

Αντίθετα η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο.

5.3 Πλεονεκτήματα και Μειονεκτήματα σχετικά με το ηλεκτρονικό έγκλημα

Στην παρούσα ενότητα παρουσιάζεται ένα σύνολο θεμάτων σχετικά με συστήματα, διαδικασίες για τον εντοπισμό, την πρόβλεψη και τη καταστολή του ηλεκτρονικού εγκλήματος.

5.3.1 Δυσκολίες αντιμετώπισης του ηλεκτρονικού & οικονομικού εγκλήματος

Τα οικονομικά αδικήματα μπορούν να λάβουν πολλές διαφορετικές μορφές και μπορούν να επηρεάσουν τις επιχειρήσεις και ολόκληρα κράτη με πολλούς τρόπους. Έτσι τα οικονομικά αδικήματα περιλαμβάνουν:

- υπεξαιρέσεις
- δωροδοκία
- απάτες επιταγών και πιστωτικών καρτών
- κυβερνοεγκλήματα
- κλοπή ταυτότητας,
- ασφαλιστικές απάτες
- ξέπλυμα χρημάτων

- απάτη προμήθειας
- πλαστογράφηση προϊόντων
- εισόδημα και απάτες με Φ.Π.Α.
- λαθρεμπόριο
- ηλεκτρονική πειρατεία, πλαστογραφία, απάτη, δολιοφθορά κ.λ.π.

Για την αντιμετώπιση των οικονομικών εγκλημάτων και ειδικότερα των εγκλημάτων που πραγματοποιούνται μέσω διαδικτύου, γίνεται ιδιαίτερη προσπάθεια τόσο στην Ευρωπαϊκή Ένωση όσο και στον υπόλοιπο κόσμο για την αντιμετώπισή του. Όμως το έργο αυτό αποδεικνύεται μια δύσκολη υπόθεση, λόγο της πολυπλοκότητας των εγκλημάτων (ηλεκτρονικά ή μη) και των ανισομερών εξελίξεων που παρατηρούνται στους τομείς της τεχνολογίας και των εθνικών ή διεθνών νομοθεσιών. Ειδικότερα μπορούμε να αναφερθούμε στους εξής παράγοντες, όσο αφορά στο θέμα της δυσκολίας αντιμετώπισης των οικονομικών εγκλημάτων κάθε τύπου:

- **Ποικιλία**. Υπάρχει μια ευρεία ποικιλία διαφορετικών τύπων οικονομικών εγκλημάτων που διαπράττονται μέσω μιας ευρείας ποικιλίας συστημάτων λογιστικής (**accounting systems**). Για παράδειγμα, τα εγκλήματα που ερευνώνται (**financial investigations**) περιλαμβάνουν υπεξαιρέσεις (**embezzlements**), διάπραξη εταιρικών αδικημάτων, χρηματιστηριακές απάτες, αδικήματα που σχετίζονται με την ιδιοκτησία καθώς και άλλα όπως αυτά που αναφέρθηκαν στις προηγούμενες παραγράφους.
- **Πολυπλοκότητα**. Το κύριο χαρακτηριστικό των περισσότερων οικονομικών εγκλημάτων που διαπράττονται είναι ότι, η πολυπλοκότητα των οικονομικών συστημάτων επιτρέπει στα άτομα με εξειδικευμένες γνώσεις ενός συστήματος να μπορούν ανά πάσα στιγμή να το χρησιμοποιήσουν εις όφελός τους. Σε περίπτωση που διαπιστωθεί μια απάτη όχι μόνο πρέπει να συλλεχθούν οι αποδείξεις για την απάτη μέσω των κατάλληλων νομικών διαδικασιών, αλλά πρέπει να γίνει κατανοητό και πώς το έγκλημα διαπράχτηκε προτού αυτό να μπορέσει να πάρει τον δρόμο της δικαιοσύνης. Οι έρευνες πρέπει να περιλαμβάνουν συνήθως πολλές συνεντεύξεις, αποσαφηνίσεις σχετικά με την απάτη (τεχνολογικής και οικονομικής φύσεως) και επαλήθευσης του τρόπου με τον οποίο το έγκλημα - απάτη διαπράχτηκε. Το σύνολο των παραπάνω στοιχείων πρέπει να προετοιμαστεί προσεκτικά από τις διωκτικές αρχές που διεξάγουν την έρευνα, ώστε με σαφήνεια να μπορούν να υποστηρίξουν ότι πράγματι μια εγκληματική πράξη έχει πραγματοποιηθεί.
- **Πολυπλοκότητα Περιεχομένου.** Η παραπάνω έρευνα απαιτεί μια σε βάθος κατανόηση των λογιστικών διαδικασιών και των εγκληματικών διερευνητικών τεχνικών (**criminal investigatory techniques**). Οι εγκληματικές πράξεις παραδείγματος χάριν που διαπράττονται μέσα στα σύνθετα εταιρικά συστήματα λογιστικής, απαιτούν την ειδική γνώση εκ μέρους των διωκτικών αρχών των τρόπων λειτουργίας αυτών των συστημάτων.
- **Μεταφερσιμότητα Δεδομένων Υπολογιστών**. Τα δεδομένα υπολογιστών (που μεταφράζονται σε πληροφορίες) που αποτελούν τις περισσότερες φορές τον κύριο στόχο των εγκλημάτων, χαρακτηρίζεται από μια ακραία ικανότητα μεταφοράς, η οποία υπερβαίνει κατά πολύ την οποιαδήποτε ικανότητα μεταφοράς προσώπων, αγαθών ή άλλων υπηρεσιών. Τα παγκόσμια δίκτυα

υπολογιστών μπορούν να μεταφέρουν σήμερα τεράστια ποσά πληροφοριών σε όλη την υδρόγειο σε κλάσματα του δευτερολέπτου, επιτρέποντας έτσι την χρησιμοποίηση ενός υπολογιστή σε μια χώρα, για την επεξεργασία πληροφοριών που προέρχονται από μια άλλη και αντιστρόφως. Αυτή η ικανότητα μεταφοράς των πληροφοριών των υπολογιστών στα διεθνή δίκτυα υπολογιστών δημιουργεί την αναπόφευκτη και αναγκαία υιοθέτηση και εφαρμογή **διεθνών λύσεων**, για την αντιμετώπιση των εγκλημάτων που σχετίζονται με υπολογιστές. Οι εκάστοτε ***εθνικές στρατηγικές*** με στόχο τα εγκλήματα υπολογιστών οδηγούν συνήθως στους περιορισμούς στην αγορά και στην ελεύθερη ροή των πληροφοριών και των παγκόσμιων υπηρεσιών. Κατά συνέπεια οι παραπάνω εθνικές στρατηγικές πρέπει να στραφούν στις ***διεθνείς συνεργασίες*** και στην περίπτωση που αφορά τα οικονομικά και ηλεκτρονικά εγκλήματα, οι τελευταίες αποδεικνύονται ο καλύτερος σύμμαχος στην προσπάθεια για την καταπολέμηση των οικονομικών εγκλημάτων, περισσότερο από κάθε άλλη φορά. Στην κατεύθυνση αυτή θα πρέπει να επισημάνουμε κινείται ολόκληρος ο κόσμος και στην περίπτωση που μας αφορά ειδικότερα (εφόσον είμαστε μέλος της), η Ευρωπαϊκή Ένωση.

- **Καθυστερήσεις στην ΕΕ υιοθέτησης και προσαρμογής σε ένα κοινό ποινικό δίκαιο**. Οι νόμοι των Ευρωπαϊκών Κρατών Μελών καταρχάς περιέχουν ακόμα σημαντικά κενά και διαφορές μεταξύ τους, που παρακωλύουν την αντιμετώπιση του οργανωμένου εγκλήματος και της τρομοκρατίας, καθώς επίσης και τις σοβαρές επιθέσεις ενάντια στα συστήματα πληροφοριών. Η αντιμετώπιση των παραπάνω αδυναμιών καθώς και η επίτευξη της προσέγγισης των εθνικών νομοθεσιών στον τομέα του εγκλήματος υψηλής τεχνολογίας, θα εξασφαλίσει μια κοινή νομοθετική βάση με τη οποία όλες οι μορφές σοβαρών επιθέσεων ενάντια στα συστήματα πληροφοριών θα μπορούν να ερευνηθούν, χρησιμοποιώντας τις τεχνικές και τις μεθόδους που θα επιτρέπει η κοινή νομοθεσία των μελών κρατών της Ευρωπαϊκής Ένωσης. Η κοινή νομοθετική βάση θα επιτρέψει στα εθνικά δικαστήρια να έχουν τα κατάλληλα και ανάλογα ποινικά όπλα για την αντιμετώπιση των εγκληματιών κάθε τύπου. Ειδικά για την **Ελλάδα** παρατηρείται δυστυχώς μια καθυστέρηση στην προσαρμογή της νομοθεσίας στο σύγχρονο ηλεκτρονικό έγκλημα, παράλληλα με την απουσία μιας ολοκληρωμένης πολιτικής αντιμετώπισης του cyber crime. Αυτό οφείλεται και σε ένα βαθμό (εκτός από έναν αριθμό άλλων παραγόντων) και στην καθυστέρηση της διείσδυσης του internet στην Ελλάδα, η οποία σε καμία περίπτωση δεν μπορεί να συγκριθεί με εκείνη αντίστοιχων άλλων Ευρωπαϊκών Κρατών, που σε πολλές περιπτώσεις είναι διπλάσια και τριπλάσια της Ελληνικής ή ακόμα και περισσότερο σε ορισμένες περιπτώσεις[2].

[2] Πρόσφατη Έρευνα (Φύλλο 3 Ιουλίου 2004) της εφημερίδας «**Καθημερινή**», επισημαίνει την μεγάλη καθυστέρηση που παρατηρείται στην Ελλάδα σχετικά με την διείσδυση του Internet στην Ελλάδα και ειδικά στις γραμμές DSL, με άμεσο αποτέλεσμα τις αρνητικές επιπτώσεις στο ηλεκτρονικό εμπόριο όσο και σε κάθε άλλο τομέα που σχετίζεται με το διαδίκτυο.

5.3.2 *Πλεονεκτήματα από την χρήση υπολογιστών (αποκαλύψεις, ανακαλύψεις και αποδείξεις μέσω δεδομένων τους)*

Ένας τεράστιος όγκος επαγγελματικής και ακαδημαϊκής βιβλιογραφίας αναπτύσσεται γύρω από το ζήτημα της χρησιμοποίησης (**evidence**), ανακάλυψης (**discovery**), αποκάλυψης (**disclosure**) των δεδομένων από υπολογιστές. Η απόκτηση – ανάκτηση δεδομένων από υπολογιστές (από τις διωκτικές αρχές ή από ιδιωτικές επιχειρήσεις που ειδικεύονται στο θέμα) αυξάνει το κόστος και την πολυπλοκότητα της αστικής προσφυγής (**civil litigation**) σε ένα δικαστήριο. Από την άλλη η ίδια η φύση των υπολογιστών προσφέρει αναρίθμητα πλεονεκτήματα στις διωκτικές αρχές για την καταπολέμηση των εγκλημάτων, αρκεί να χρησιμοποιείται σωστά και έγκαιρα. Παραδείγματος χάριν μια απλή διαπίστωση σχετικά με τους υπολογιστές επιβεβαιώνει το γεγονός ότι δεν υπάρχει σύγκριση από την διαχείριση δεδομένων με την χρήση υπολογιστών, έναντι της παραδοσιακής χρήσης εγγράφων. Ο χρόνος και το κόστος που απαιτείται για την μελέτη και την οργάνωση των δεδομένων μπορεί να μειωθεί εκθετικά με τη χρησιμοποίηση, μορφών έρευνας, ταξινόμησης και άλλων λειτουργιών με τη χρήση υπολογιστών.

Η χρήση υπολογιστών προσφέρει και άλλα ουσιαστικά πλεονεκτήματα, επίσης. Τα στοιχεία ή δεδομένα που θα ήταν αδύνατα ή εξαιρετικά δύσκολο να ανακαλυφθούν μέσω των παραδοσιακών εγγράφων (τα έγγραφα μπορούν να χαθούν ή να καταστραφούν), τώρα που διατίθενται σε ηλεκτρονική μορφή μπορούν να ανακτηθούν με συγκεκριμένες τεχνικές και μεθόδους. Αυτό οφείλεται στο γεγονός ότι σχεδόν όλες οι πληροφορίες (ανεξάρτητα των μορφών επικοινωνίας που χρησιμοποιούνται) μέσω υπολογιστή, από το γνωστό e-mail μέχρι τις την ψηφιακή τηλεφωνία και τις εικονικές διασκέψεις, καταγράφονται και αποθηκεύονται ως ψηφιακά «**έγγραφα**». Έτσι τεράστια ποσά δεδομένων που θα ήταν αδύνατα να συλλεχθούν και να μελετηθούν εάν προέρχονταν από το συμβατικό χαρτί, σήμερα μπορούν να συγκεντρωθούν, να διαβιβαστούν, να αξιολογηθούν και να αναλυθούν με τη βοήθεια των υπολογιστών. Οι δυνατότητες αυτές με την κατάλληλη στρατηγική από τις διωκτικές αρχές μπορούν να χρησιμοποιηθούν ως σημαντικά όπλα στην καταπολέμηση του διεθνούς οικονομικού – ηλεκτρονικού εγκλήματος.

5.3.3 *Προβλήματα σχετικά με την χρήση δεδομένων υπολογιστών (για αποκαλύψεις, ανακαλύψεις και αποδείξεις)*

Αν και η χρήση υπολογιστών έχει να προσφέρει πολλά πιθανά πλεονεκτήματα (όπως αυτά που περιγράφθηκαν στην προηγούμενη παράγραφο περιληπτικά), μπορεί να δημιουργήσει και μοναδικά ζητήματα που υπό κανονικές συνθήκες δεν εμφανίζονται ή είναι λιγότερο αισθητά στις περιπτώσεις που αφορούν τη χρήση των παραδοσιακών εγγράφων. Μεταξύ των πιο σημαντικών θεμάτων που ανακύπτουν σχετικά με τη χρησιμοποίηση αποδείξεων (**evidence**), ανακάλυψης (**discovery**) και αποκάλυψης (**disclosure**) των δεδομένων από υπολογιστές είναι τα εξής:

- Διατήρηση Δεδομένων Υπολογιστών (**Preservation of data**)

Οι πληροφορίες που αποθηκεύονται σε ένα δίκτυο ή σε ένα υπολογιστή με ηλεκτρονική μορφή αλλάζουν εύκολα, επικαλύπτονται ή εξαλείφονται από τη καθημερινή χρήση του υπολογιστή, είτε αυτός πρόκειται για έναν απλό υπολογιστή γραφείου (προσωπικός υπολογιστής) είτε ένας διακομιστής (server). Οι απλές διαδικασίες που πραγματοποιούνται σε έναν υπολογιστή, όπως η εκκίνησή του, το άνοιγμα ενός αρχείου, η προσθήκη νέων στοιχείων σε έναν σκληρό δίσκο, ή η εκτέλεση πολλών προγραμμάτων μπορούν να αλλάξουν ή να καταστρέψουν δεδομένα και μάλιστα χωρίς τη γνώση του χρήστη του. Στη περίπτωση των παραδοσιακών εγγράφων, οι αποδεικτικές πηγές πληροφοριών είναι τις περισσότερες φορές σταθερές και λιγότερο ευάλωτες γενικά έναντι των ηλεκτρονικών εγγράφων.

- Τοποθεσία και όγκος Δεδομένων Υπολογιστών (**Location and volume of data**)

Σε παλαιότερους καιρούς με χρήση του παραδοσιακού χαρτιού, οι περισσότερες οργανώσεις αποθήκευαν τα έγγραφά τους σε έναν περιορισμένο αριθμό φυσικών θέσεων (ντουλάπια, συρτάρια κ.λ.π.). Στον κόσμο των υπολογιστών, κάθε υπάλληλος μιας επιχείρησης διαθέτει έναν υπολογιστή γραφείου, συν τους δίσκους ή άλλα μετακινούμενα μέσα απομνημόνευσης δεδομένων, έναν φορητό υπολογιστή (**lap-top**) κ.ο.κ. γεγονός που οδηγεί σε υπερβολικές δαπάνες και σε περίπλοκες διαδικασίες, για την ανακάλυψη πληροφοριών (με τη μορφή ηλεκτρονικών δεδομένων), σε ένα σύγχρονο επιχειρησιακό περιβάλλον (με πολλά μέσα αποθήκευσης δεδομένων και τεράστιο όγκο πληροφοριών).

- **E-mail** ένα μοναδικό φαινόμενο

Τα διάφορα χαρακτηριστικά του ηλεκτρονικού ταχυδρομείου το καθιστούν ιδιαίτερα προβληματικό, τουλάχιστον όσο αφορά τη διαχείριση και την ανάκτηση δεδομένων. Ο τρόπος μετάδοσης των πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου και ο όγκος των διακινούμενων πληροφοριών μέσω αυτού αποτελεί τροχοπέδη στην αποτελεσματικότητα των διωκτικών αρχών οικονομικού – ηλεκτρονικού εγκλήματος για τον εντοπισμό και την χρήση των δεδομένων που επιθυμούν.

- Διαγραμμένα Αρχεία (**Deleted documents**)

Αποτελεί σημαντικό στοιχείο το γεγονός ότι η στερεότυπη «**διαγραφή**» ενός βασισμένου σε υπολογιστή ηλεκτρονικού εγγράφου, δεν καταστρέφει στην πραγματικότητα τα δεδομένα που αυτό περιέχει. Εάν ο υπολογιστής για ένα συγκεκριμένο χρονικό διάστημα δεν χρησιμοποιηθεί τα δεδομένα του προς διαγραφή ηλεκτρονικού αρχείου, μπορούν να παραμείνουν στο σκληρό δίσκο ή σε μετακινούμενα μέσα απομνημόνευσης και μπορούν να ανακτηθούν ολικώς ή μερικώς ανάλογα με τη περίπτωση. Πολλές υποθέσεις οικονομικών και ηλεκτρονικών εγκλημάτων έχουν λυθεί, με τη χρησιμοποίηση δεδομένων από αρχεία που «**υποτίθεται**» είχαν διαγραφεί, μετά από σχετικές έρευνες των διωκτικών αρχών

- Backup tapes

Οι περισσότερες επιχειρήσεις, καθώς επίσης και πολλά άτομα, χρησιμοποιούν μεθόδους (αποθήκευσης) **backup** περιοδικά σε ειδικές ταινίες ή δίσκους, για λόγους αποκατάστασης από καταστροφή. Συχνά αυτές οι ταινίες ή οι δίσκοι αποθηκεύονται για μήνες ή ακόμα και για ολόκληρα χρόνια. Τα στοιχεία και τα έγγραφα που έχουν εκδοθεί, έχουν διαγραφεί, ή έχουν γραφτεί στην επιχείρηση, μπορούν να ανακτηθούν από αυτές τις ταινίες ή τους δίσκους. Ειδικά προγράμματα μπορούν να απαιτηθούν για να ανακτήσουν τις συγκεκριμένες πληροφορίες και η διαδικασία μπορεί να αποδειχθεί πολύ δαπανηρή και χρονοβόρα.

6 Οικονομικό έγκλημα

6.1 Εισαγωγή

Οικονομικό έγκλημα, με την ευρύτερη έννοια του όρου, είναι αυτό που βλάπτει ή θέτει σε κίνδυνο τη λειτουργία της οικονομίας (σημαντικών τμημάτων της). Κυριαρχείται από το στοιχείο της απάτης, οι δε εκφραστές του είναι προικισμένοι με ιδιαίτερες γνώσεις (γνωρίζοντας πολύ καλά τις σύγχρονες τεχνολογίες), που τους δίνουν το δικαίωμα να τις χρησιμοποιούν με ιδιαίτερη ευχέρεια στα δίκτυα υπολογιστών και στο Internet.

Το ηλεκτρονικό έγκλημα αποτελεί μια φυσική επέκταση του οικονομικού εγκλήματος, αποτέλεσμα της συστηματικής και παγκόσμιας δικτύωσης του σημερινού κόσμου για την ανταλλαγή πληροφοριών, σε όλες τις δραστηριότητες της καθημερινής ζωής του σύγχρονου ανθρώπου. Τα θύματα των ηλεκτρονικών εγκλημάτων ποικίλουν και μπορεί να είναι τόσο φυσικά πρόσωπα, όσο εταιρείες, τράπεζες, εθνικοί οργανισμοί, δημόσιοι κρατικοί φορείς, και διεθνείς οργανισμοί Το συνηθέστερο ηλεκτρονικό έγκλημα που παρουσιάζει τα τελευταία χρόνια υπέρμετρη έξαρση, είναι σαφώς οι απάτες με τη χρήση πιστωτικών καρτών και κάθε άλλη απάτη που πραγματοποιείται με την χρήση υπολογιστών. Σε αυτά έρχονται με την σειρά τους να προστεθούν και άλλα οικονομικά εγκλήματα, όπως:

- Νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες (ξέπλυμα χρημάτων).
- Παραχάραξη νομισμάτων.
- Πλαστογραφία και η κυκλοφορία των πλαστών νομισμάτων.
- Ακάλυπτες Επιταγές.
- Μεταφορές χρημάτων από και σε τράπεζες του εξωτερικού, με τη χρήση πλαστών εγγράφων.
- Η φοροδιαφυγή (εικονικές μεταβιβάσεις κεφαλαίων από την Ελλάδα σε θυγατρικές εταιρείες του εξώτερικού και αντίστροφα) κ.λ.π.

Σε ολόκληρη την Ευρώπη πολλές έρευνες (**economic crime survey 2003 Price waterhouse Coopers**) δείχνουν ότι σε μεγάλο αριθμό επιχειρήσεων οι επιπτώσεις από οικονομικά αδίκηματα όλων των τύπων, είναι πάρα πολλές. Τα οικονομικά εγκλήματα αποτελούν ολοένα και περισσότερο ένα συνεχώς αυξανόμενο πρόβλημα στη Ευρώπη συνολικά: Για την Δυτική Ευρώπη συγκεκριμένα, οι σχετικές επιθεωρήσεις σε διάφορους οργανισμούς (σε περισσότερους από 1500) ανέδειξε ότι το 34% από αυτές έπεσαν θύματα οικονομικών εγκλημάτων τα τελευταία δύο χρόνια. Αυτό συγκρινόμενο με το ποσοστό του 29% πριν δύο έτη επιβεβαιώνει την σημασία του προβλήματος. Το αντίστοιχο ποσοστό για την Κεντρική και Ανατολική Ευρώπη δείχνει ακόμα υψηλότερο (37%) σε δείγμα 370 οργανισμών.

6.2 Πληροφορίες, Κίνητρο για το Οικονομικό και οργανωμένο έγκλημα;

Οι έρευνες τόσο στην Ευρώπη όσο και στον υπόλοιπο κόσμο δείχνουν ότι το οικονομικό έγκλημα διαπράττεται όλο και περισσότερο σε οργανωμένη βάση. Ο καθοριστικός παράγοντας που επηρεάζει την οργάνωση των εγκλημάτων,

αποτελεί η κάθε μορφή τεχνολογικής πληροφορίας. Οι πληροφορίες, που ορίζονται γενικά ως ένα σύνολο συναφών στοιχείων, διαδραματίζουν έναν βασικό ρόλο στη σύγχρονη κοινωνία. Η αγορά σήμερα όλο και περισσότερο βασίζεται σε οικονομικά πρότυπα που δεν υποστηρίζουν τα «μετρητά» και οι νέοι τύποι χρημάτων και συστημάτων συναλλαγής, έχουν αναπτυχθεί βασιζόμενα στις τεχνολογίες μετάδοσης πληροφοριών. Οι πληροφορίες έχουν γίνει ένας ουσιαστικός παράγοντας της παραγωγής και η διαχείρισή της έχει γίνει το σημαντικότερο στοιχείο σε κάθε διαδικασία απόφασης και σε κάθε στρατηγική επιχειρησιακής ανάπτυξης.

Το οικονομικό αδίκημα επηρεάζεται από την πληροφορία με δύο τρόπους.

- Οι πληροφορίες πρώτα από όλα αποτελούν οι ίδιες ένα άμεσο ή έμμεσο αντικείμενο των εγκλημάτων που διαπράττονται από τους εγκληματίες. Οι πληροφορίες σημαίνουν κέρδος. Μπορούν να αποτελούν έναν άμεσο στόχο όταν αντιπροσωπεύουν τον αρχικό στόχο ενός οικονομικού αδικήματος (παραδείγματος χάριν όπως συμβαίνει στη βιομηχανική κατασκοπεία). Από την άλλη οι πληροφορίες μπορούν να αποτελούν έναν έμμεσο στόχο όταν αυτές διαδραματίζουν έναν ουσιαστικό ρόλο στη ίδια την οργάνωση των εγκληματικών ομάδων. Παραδείγματος χάριν, ας φανταστούμε το μεγάλο ποσό πληροφοριών που απαιτείται για την οργάνωση σε μεγάλη κλίμακα μιας απάτης, ενάντια στα οικονομικά συμφέροντα της Ευρωπαϊκής Ένωσης ή σε οργανισμούς που ανήκουν σε αυτήν. Οι πληροφορίες αυτές θα πρέπει να περιλαμβάνουν γνώσεις: των διαφορετικών περιοχών της, των φορολογικών δομών, των τελωνειακών κανονισμών, των βιομηχανικών κανονισμών, των νομοθετικών ρυθμίσεων κ.ο.κ. Δηλαδή γενικότερα, όταν πρέπει να οργανώσουν οι εγκληματίες τα σύνθετα εγκληματικά σχέδιά τους, πρέπει συνήθως να αποκτήσουν πρόσβαση σε ποικίλες πληροφορίες.
- Οι σημερινές μορφές διάδοσης και προστασίας των πληροφοριών έχουν μια σημαντική επιρροή στα οικονομικά αδικήματα. Προκειμένου να μπορούν αυτά να διαπραχθούν, οι εγκληματίες πρέπει να υιοθετήσουν νέα συστήματα και νέες μορφές οργάνωσης. Οι πληροφορίες σήμερα είναι ακριβές και καλά προστατευμένες. Δεδομένου λοιπόν ότι οι πολύτιμες πληροφορίες γίνονται πιο τεχνικές, συγκεκριμένες και διεσπαρμένες σε όλο τον κόσμο, οι οικονομικοί εγκληματίες στρέφονται στην ανάπτυξη δικών τους δικτύων, προκειμένου να τα χρησιμοποιήσουν για την αποκάλυψη, μετάδοση και μεταπώληση των πληροφοριών, για την συνεργασία και την επικοινωνία τους ανά τον κόσμο.

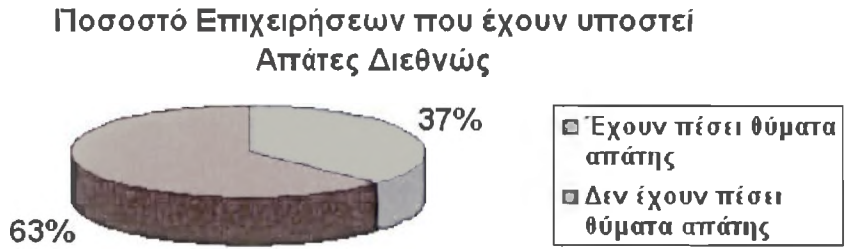
7.1 Παγκόσμια Έρευνα για Οικονομικά Εγκλήματα το έτος 2003

Στην παρούσα ενότητα παρουσιάζονται τα αποτελέσματα της έρευνας σχετικά με το **οικονομικό έγκλημα** το έτος 2003, από την **PricewaterhouseCoopers "economic crime survey 2003"**. Για την ολοκλήρωση της έρευνας πραγματοποιήθηκαν συνεντεύξεις με τους αντιπροσώπους περισσότερων από 3,600 επιχειρήσεων σε 50 χώρες. Τα αποτελέσματα της έρευνας έχουν ως στόχο τη συνειδητοποίηση και την ενημέρωση των επιχειρήσεων, σχετικά με τα οικονομικά εγκλήματα που διαπράττονται ανά τον κόσμο.

7.1.1 Συμπεράσματα από την Έρευνα

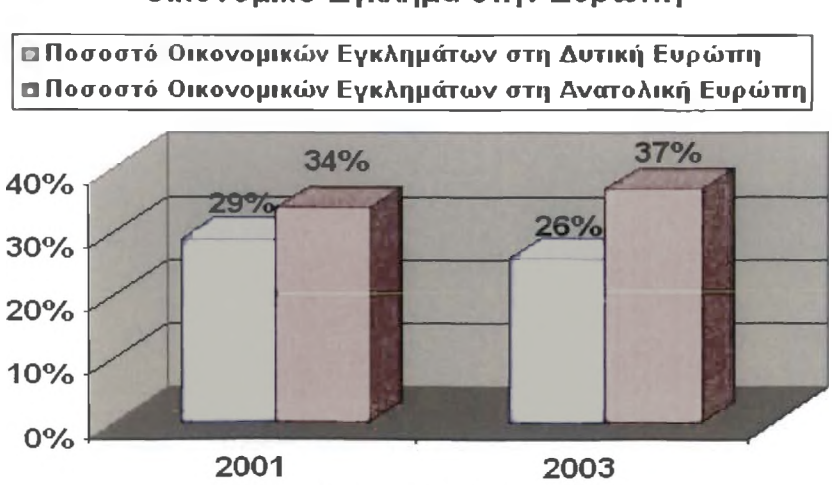
Τα πρώτα συμπεράσματα από την έρευνα που διεξήχθη από την **PricewaterhouseCoopers** δείχνουν ότι:

- **Το οικονομικό έγκλημα παραμένει μια σημαντική απειλή**: Το 37% των ερωτηθέντων εκθέτουν σημαντικά οικονομικά αδικήματα που σχετίζονται με απάτη κατά τη διάρκεια των προηγούμενων δύο ετών όπως απεικονίζεται στον σχέδιο 7.1 που ακολουθεί.



Σχέδιο 7.1

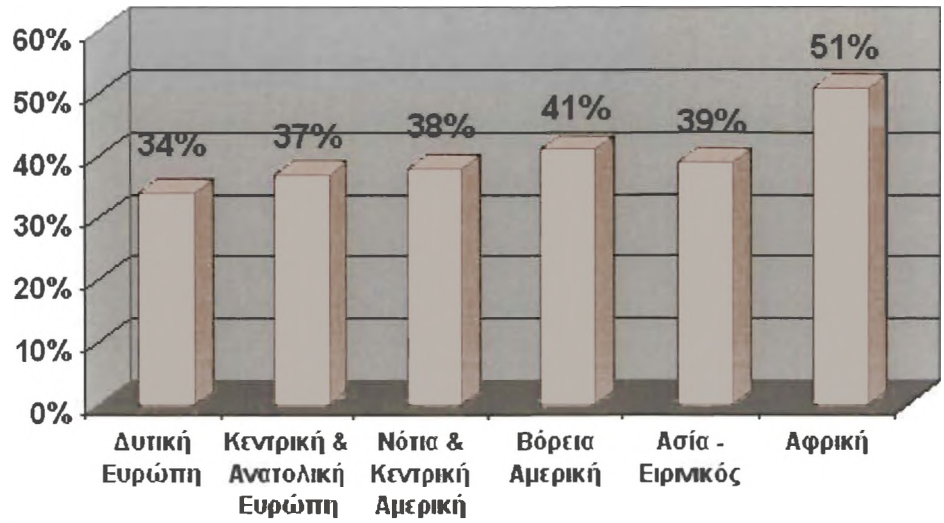
Το ποσοστό των επιχειρήσεων που έχουν υποστεί απάτες είναι σημαντικά υψηλότερο από ότι στην προηγούμενη ευρωπαϊκή έρευνα που διεξήχθη επίσης από την **PricewaterhouseCoopers** το 2001. Συγκεκριμένα ο αριθμός των επιχειρήσεων που αναφέρουν απάτες στη Δυτική Ευρώπη έχει αυξηθεί από 29 % σε 34 % (2001 και 2003 αντίστοιχα) και στην Κεντρική και Ανατολική Ευρώπη από 26 % σε 37 % ((2001 και 2003 αντίστοιχα), όπως φαίνεται και στο διάγραμμα που ακολουθεί.



Διάγραμμα 7.1

Τα πιο υψηλά επίπεδα οικονομικού εγκλήματος αναφέρθηκαν από τους ερωτηθέντες στην Αφρική (51%) και τη Βόρεια Αμερική (41%), όπως φαίνεται και στο διάγραμμα 7.2 που ακολουθεί. Αντίθετα, οι στη Ρωσία και την Τουρκία δεν εξέθεσαν κανένα οικονομικό αδίκημα καθόλου (γεγονός που δεν συνάγει με την πραγματικότητα).

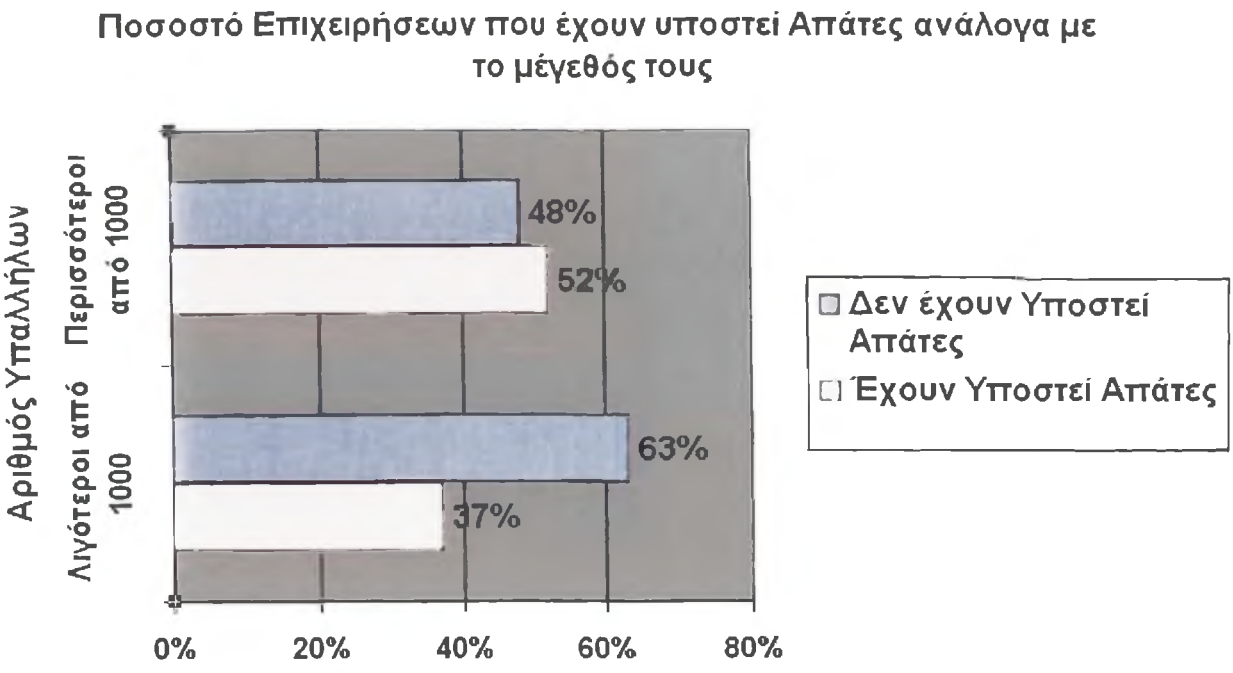
Ποσοστό Επιχειρήσεων που έχουν υποστεί Απάτες ανά Περιοχή



Διάγραμμα 7.2

- **Το οικονομικό έγκλημα είναι συνάρτηση του μεγέθους των επιχειρήσεων: Οι** επιχειρήσεις με περισσότερους υπαλλήλους έχουν μεγαλύτερες πιθανότητες να αποτελέσουν θύματα οικονομικών εγκλημάτων. Τα συμπεράσματα από την έρευνα προτείνουν μια άμεση σχέση μεταξύ του μεγέθους επιχείρησης και της πιθανότητας του οικονομικού αδικήματος. Έτσι μόνο το 37% των μικρότερων επιχειρήσεων (με λιγότερο από 1,000 υπάλληλους) ανέφερε οικονομικό αδίκημα, έναντι του 52% που αναφέρθηκε από μεγαλύτερες επιχειρήσεις (με πάνω από 1,000 υπαλλήλους), όπως φαίνεται και στο διάγραμμα 7.3 που ακολουθεί. Οι πιθανοί λόγοι για αυτήν την υψηλότερη συχνότητα εμφάνισης οικονομικών αδικημάτων μεταξύ των μεγαλύτερων επιχειρήσεων θα μπορούσαν να είναι:

- Η αδυναμία αποκέντρωσης των λειτουργικών ευθυνών
- Η τάσεις διείσδυσής τους σε άγνωστες αγορές
- Η πολυπλοκότητα των συναλλαγών τους
- Οι αυξημένες πιθανότητες διάπραξης οικονομικών εγκλημάτων από το πολυπληθές τους προσωπικό
- Τα μεγάλα ποσοστά που επενδύονται από τις μεγαλύτερες επιχειρήσεις, στα συστήματα διαχείρισης κινδύνων. Αυτά τα ποσοστά ανίχνευσης οδηγούν στον εντοπισμό περισσοτέρων οικονομικών εγκλημάτων.

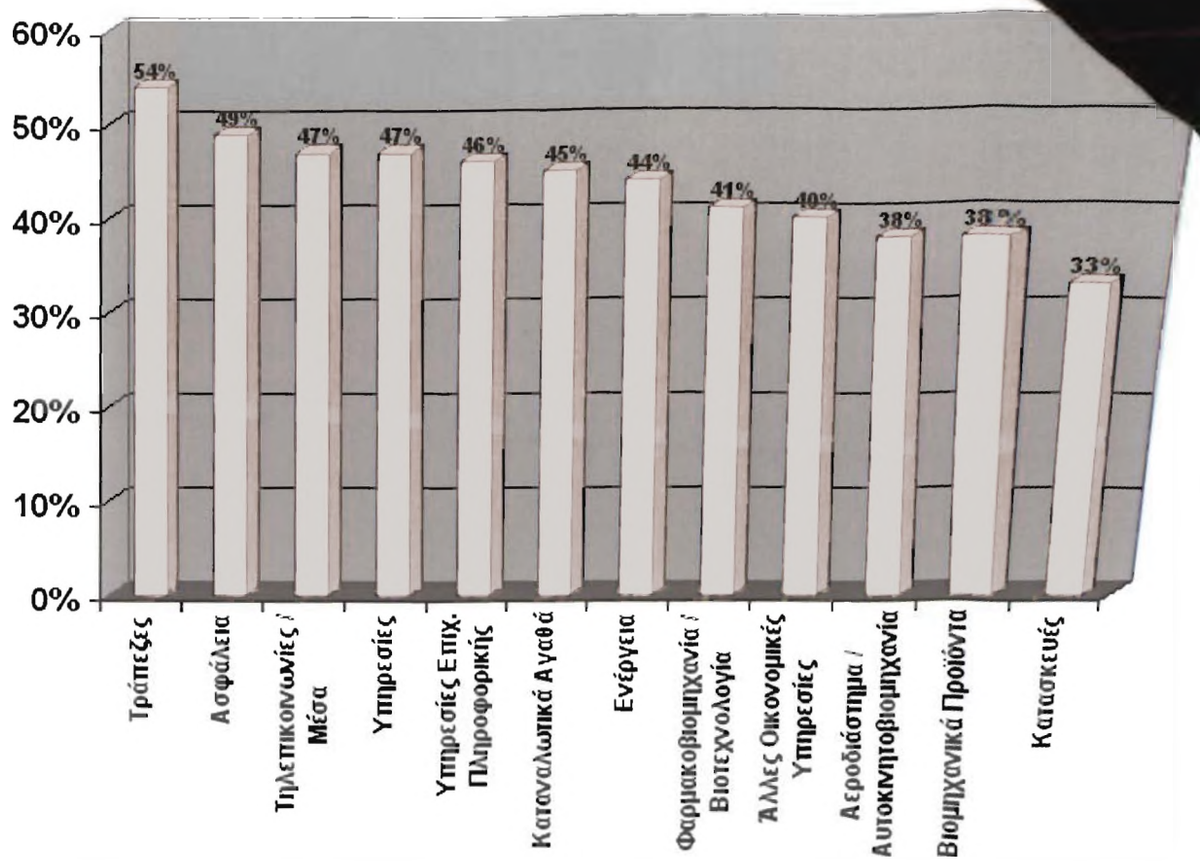


Διάγραμμα 7.3

- **Καμία βιομηχανία δεν είναι ασφαλής**: Πάνω από το 30% των ερωτηθέντων (σε κάθε μια από τις βιομηχανίες που συμμετείχαν στην έρευνα) ανέφεραν ότι έπεσαν θύματα απάτης (fraud). Ενώ όλη η εμπορική δραστηριότητα ανά τον κόσμο είναι ευάλωτη στο οικονομικό έγκλημα, οι επιπτώσεις από αυτό ποικίλλουν μεταξύ των διαφορετικών βιομηχανιών. Τα αποτελέσματα της σχετικής έρευνας δείχνουν ότι οι «**οικονομικές υπηρεσίες**» (τραπεζικές εργασίες, ασφάλεια) εκτίθενται σε μεγαλύτερο βαθμό σε οικονομικά εγκλήματα σε σχέση με άλλες βιομηχανίες και άρα ο βαθμός επιπτώσεων από την δράση των τελευταίων είναι πολύ μεγαλύτερος σε αυτές. Η βιομηχανία οικονομικών υπηρεσιών αποτελεί αδιαμφισβήτητα έναν προφανή στόχο για οποιονδήποτε απατεώνα, λαμβάνοντας υπόψη τις σημαντικές ποσότητες περιουσιακών στοιχείων που αυτές διαχειρίζονται και του μεγάλου αριθμού των οικονομικών συναλλαγών που πραγματοποιούν (οι οποίες αποτελούν και πολύπλοκες διαδικασίες). Είναι επίσης αξιοσημείωτο ότι άλλες ιδιαίτερα προστατευμένες βιομηχανίες (λόγω του ειδικού καθεστώτος που χαρακτηρίζει αυτές τις επιχειρήσεις οι τελευταίες έχουν αναπτύξει συνήθως περίπλοκα συστήματα ελέγχου και συμμόρφωσης - **regulated industries**), όπως οι τηλεπικοινωνίες εμφανίζονται στην κορυφή αυτού του πίνακα σχετικά με τις απάτες, όπως φαίνεται και στο διάγραμμα που ακολουθεί. Η θέση των οικονομικών υπηρεσιών στο σχετικό διάγραμμα 7.4 αποτελεί επίσης και ένδειξη του υψηλότερου βαθμού ανίχνευσης και εντοπισμού του οικονομικού εγκλήματος που διαθέτουν, εφόσον αυτές γνωρίζουν σε μεγαλύτερο βαθμό την απειλή από το οικονομικό έγκλημα. Το χαμηλότερο επίπεδο του διαγράμματος βλέπουμε ότι περιέχει τις λιγότερο προστατευμένες βιομηχανίες (**less regulated industries**), όπως η παραγωγή βιομηχανικών προϊόντων (**manufacturing industrial products**) και οι κατασκευές (**construction**). Ενώ αυτές οι βιομηχανίες είναι επιρρεπείς σε οικονομικά αδικήματα που κυμαίνονται από τις υπεξαιρέσεις ως την πειρατεία προϊόντων, συχνά έχουν τους λιγότερο περίπλοκους μηχανισμούς ελέγχου και ανίχνευσης οικονομικών εγκλημάτων και σε πολλές περιπτώσεις μπορούν να δεχτούν τις απώλειες μέσω της απάτης, ως μια αναγκαία και αναπόφευκτη κατάσταση.

με τον κλάδο

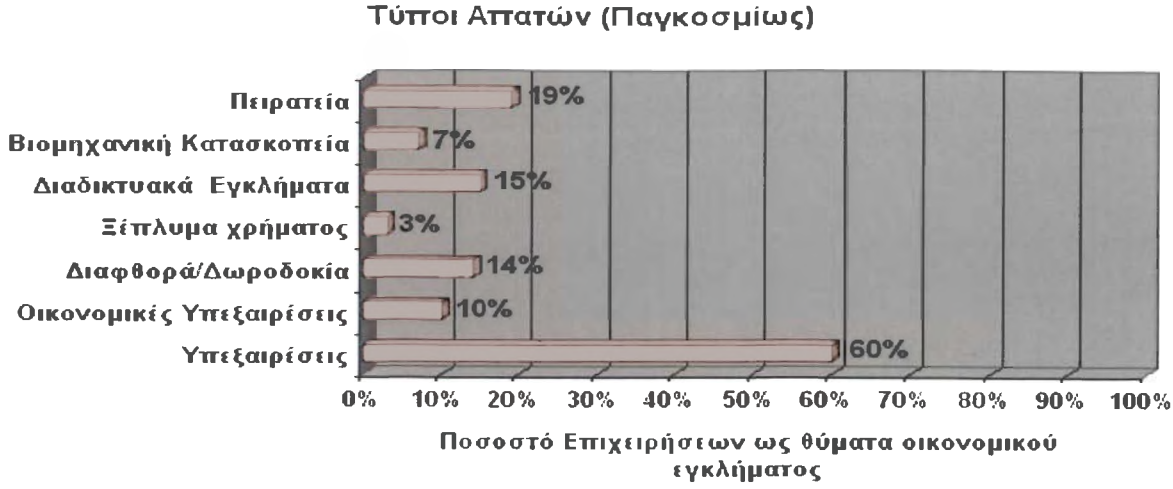
Ποσοστό Επιχειρήσεων που έχουν υποστεί Απάτες, ανάλογα
στον οποίο ανήκουν



Διάγραμμα 7.4

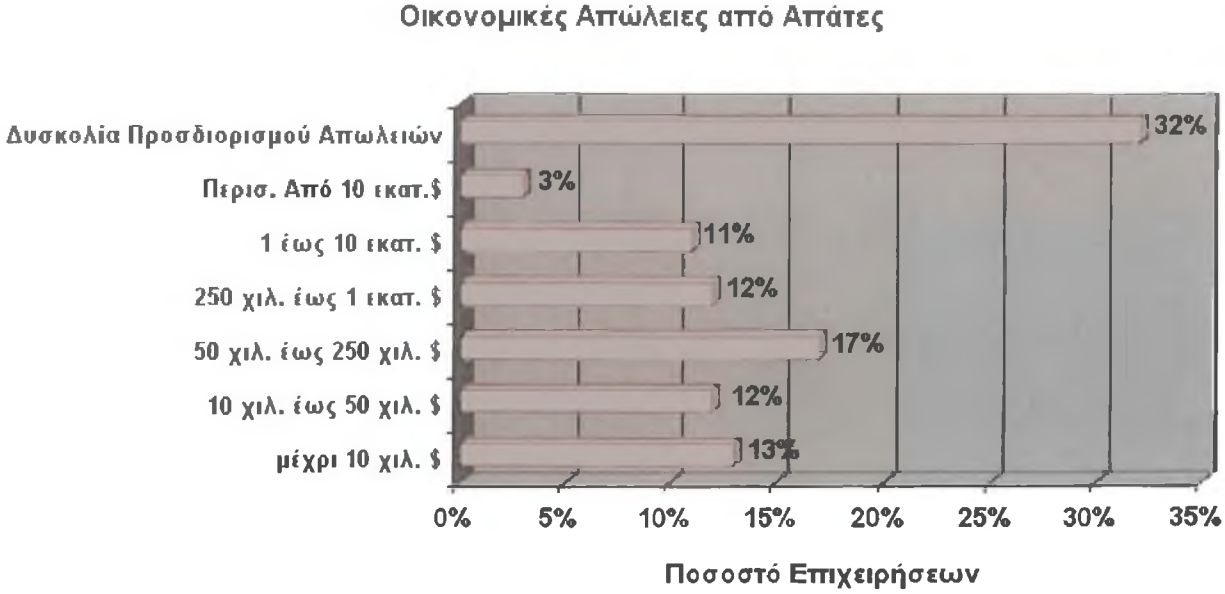
- **Η υπεξαίρεση (asset misappropriation) είναι ευρέως το πιο διαδεδομένο έγκλημα**: Είναι επίσης το ευκολότερο έγκλημα που ανιχνεύεται και χαρακτηριστικό είναι ότι αναφέρεται από το 60% των θυμάτων, ως μια από τις απάτες που αυτά έχουν υποστεί. Άλλοι τύποι απάτης εκτός από τις υπεξαιρέσεις[3], όπως αυτές αναφέρθηκαν από τις επιχειρήσεις που συμμετείχαν στην παρούσα έρευνα, φαίνονται αναλυτικά στο διάγραμμα 7.5 που ακολουθεί.

[3] Οικονομικές Υπεξαιρέσεις. Όταν οι επιχειρήσεις αλλάζουν ή παρουσιάζουν κατά τέτοιο τρόπο τους λογαριασμούς τους (company accounts) ώστε αυτοί να μην απεικονίζουν την αληθινή αξία ή τις αληθινές οικονομικές δραστηριότητες της επιχείρησης.



Διάγραμμα 7.5

- **Μέση απώλεια ανά επιχείρηση**: Πάνω από 1284 επιχειρήσεις που συμμετείχαν στην έρευνα ανέφεραν σημαντικές απώλειες λόγω οικονομικών εγκλημάτων τα τελευταία 2 χρόνια. Από αυτές τις επιχειρήσεις, οι 813 ήταν σε θέση να υπολογίσουν τις απώλειές τους. Ένα σημαντικό χαρακτηριστικό που προκύπτει επίσης από την έρευνα είναι και το γεγονός ότι, ενώ πολλές επιχειρήσεις γνωρίζουν ότι έχουν υποστεί οικονομικά αδικήματα δεν μπορούν να προσδιορίσουν με ακρίβεια τον οικονομικό αντίκτυπο στην επιχείρησή τους. Έτσι σχεδόν το ένα τρίτο των παραπάνω επιχειρήσεων δεν μπορεί ακόμη να κάνει εκτιμήσεις για το ύψος των ζημιών από τη διάπραξη οικονομικών εγκλημάτων, όπως φαίνεται και από το διάγραμμα 7.6 που ακολουθεί. Είναι σαφές επίσης ότι το οικονομικό κόστος από τα λιγότερο απτά οικονομικά αδικήματα, όπως η δωροδοκία η διαφθορά και τα εγκλήματα μέσω διαδικτύου, είναι ιδιαίτερα δύσκολο να υπολογιστούν. Ακόμη και με ένα θεωρητικά εύκολο στον προσδιορισμό του έγκλημα όπως η υπεξαίρεση, το 22% των επιχειρήσεων - θυμάτων δεν στάθηκε δυνατό να υπολογίσει τις σχετικές απώλειες ως προς αυτό το έγκλημα. Μεταξύ των υπόλοιπων δύο τρίτων του συνολικού αριθμού των επιχειρήσεων (συγκεκριμένα 813 επιχειρήσεις), υπολογίστηκε σύμφωνα με την έρευνα ότι η μέση απώλεια από απάτες για κάθε μια από αυτές κυμαίνεται στα 2.199.930 δολάρια ΗΠΑ.



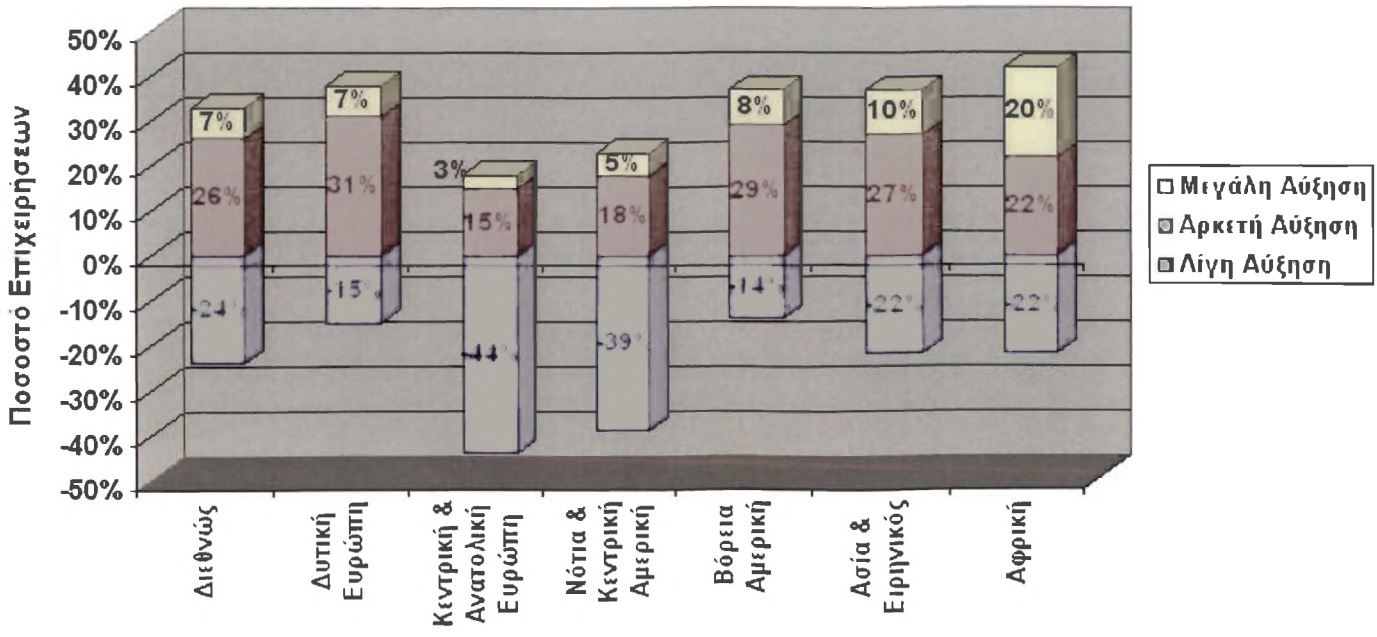
Διάγραμμα 7.6

- **Ο αντίκτυπος των οικονομικών εγκλημάτων** στη φήμη και στην εικόνα των επιχειρήσεων καθώς και στο ηθικό του προσωπικού τους, αποδεικνύεται ότι μπορεί να είναι σημαντικότερος από τις άμεσες οικονομικές απώλειες.
- Το ένα τρίτο των ερωτηθέντων τόνισε ότι η **διοίκηση της επιχείρησης** είχε τελικά την ευθύνη για την παρεμπόδιση ή την διαχείριση των οικονομικών αδικημάτων και μόνο το ένα τέταρτο είχε παράσχει στους διοικούντες οποιεσδήποτε σπουδές σχετικά με τη **διαχείριση κινδύνων**.
- **Η εφαρμογή διοικητικών μέτρων για την αντιμετώπιση πιθανών κινδύνων** εφαρμόζεται από τις επιχειρήσεις που έχουν υποστεί απάτες, ενώ οι επιχειρήσεις που δεν έχουν αντιμετωπίσει ακόμα τέτοιου είδους προβλήματα στηρίζονται ακόμα σε παθητικά μέτρα και όχι ενεργητικά μέτρα.
- **Σχεδόν τα τρία τέταρτα των θυμάτων οικονομικών εγκλημάτων ανάκτησαν λιγότερο από το 20% των απωλειών τους:** Από το σύνολο των θυμάτων μόνο οι μισοί από τους ερωτηθέντες είχαν ασφάλεια ενάντια σε οικονομικά αδικήματα και μέσω αυτής ανάκτησαν τις περισσότερες από τις απώλειές τους.
- Οι μεγαλύτερες ανησυχίες για το μέλλον αποτελούν τα φαινόμενα υπεξαίρεσης (στο σύνολο των ερωτηθέντων).

7.1.2 *Μελλοντικές Προβλέψεις από την Έρευνα*

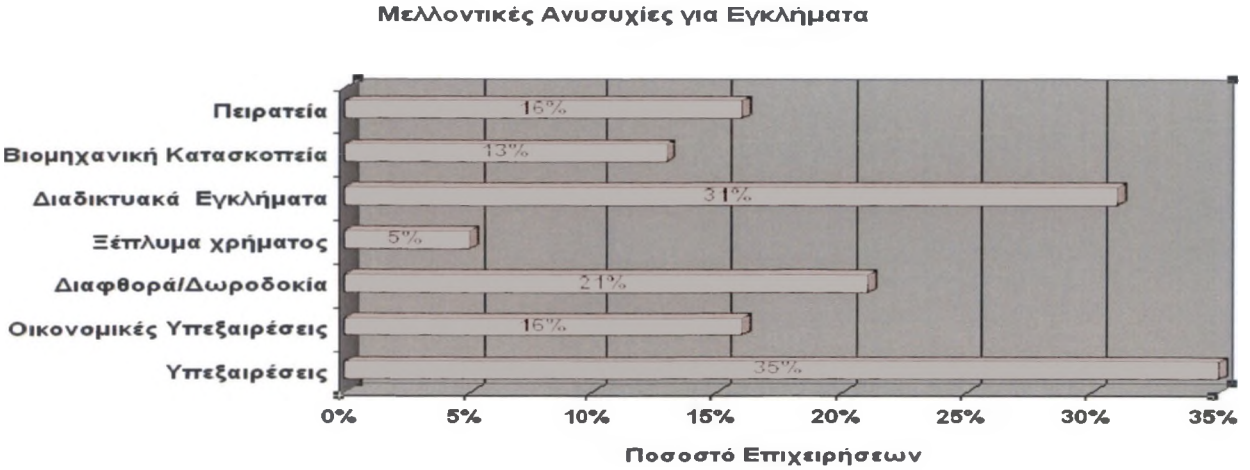
Οι περισσότερες επιχειρήσεις σύμφωνα με την έρευνα της **PricewaterhouseCoopers** αναμένουν την αύξηση των οικονομικών εγκλημάτων κατά τη διάρκεια των επόμενων πέντε ετών, με τις επιχειρήσεις στην ο Αφρική να είναι ιδιαίτερα απαισιόδοξες στο θέμα αυτό. Τα συμπεράσματά της έρευνας έρχονται να υποστηρίξουν την γενική αντίληψη που επικρατεί παγκοσμίως στον επιχειρηματικό κόσμο για την αύξηση των κινδύνων, όπως φαίνεται και στο διάγραμμα 7.7 που ακολουθεί. Εντούτοις, οι επιχειρήσεις στην Κεντρική και την Ανατολική Ευρώπη όπως και στην Νότια και Κεντρική Αμερική ευελπιστούν στην μείωση των οικονομικών εγκλημάτων και στους κινδύνους που απορρέουν από αυτά. Οι απαντήσεις που συλλέχθηκαν από την Κεντρική και την Ανατολική Ευρώπη (στην παρούσα έρευνα) συμφωνούν και με την ευρωπαϊκή έρευνά της **PricewaterhouseCoopers** για το 2001 η οποία είχε να παρουσιάσει στοιχεία που συνηγορούσαν στην αισιοδοξία πολλών επιχειρήσεων των παραπάνω περιοχών της Ευρώπης, για μια πτώση στους οικονομικούς κινδύνους από τα οικονομικά εγκλήματα.

Προβλέψεις Αύξησης Οικονομικών Εγκλημάτων Διεθνώς



Διάγραμμα 7.7

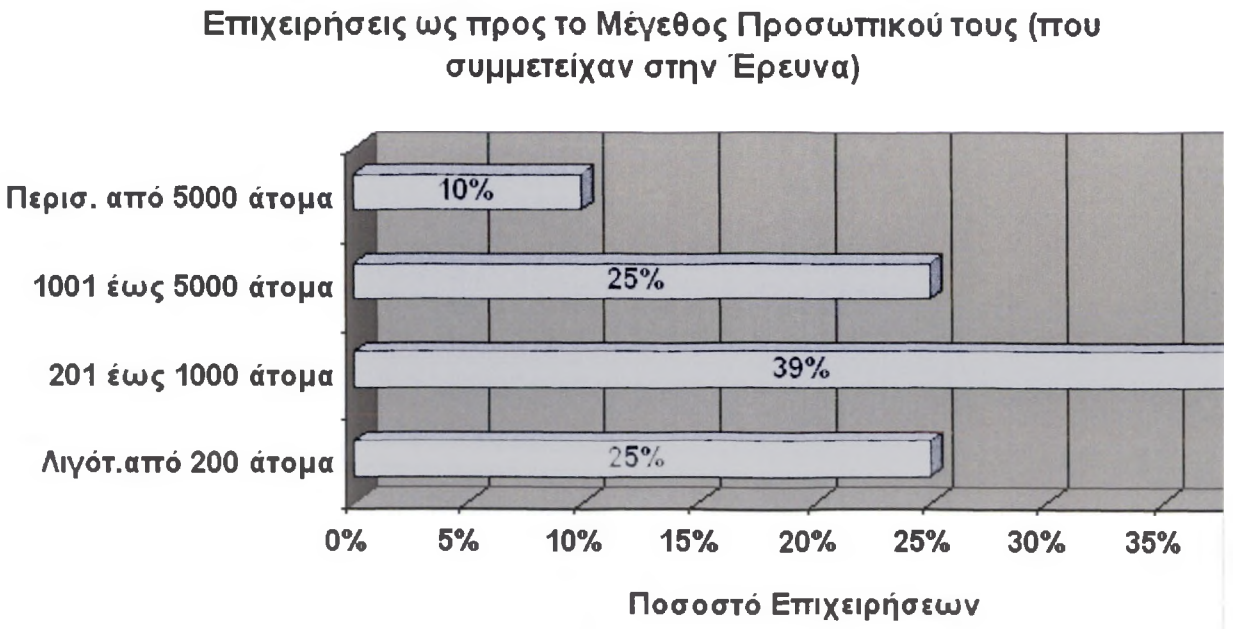
Παρόλο όμως την αισιοδοξία των επιχειρήσεων από την Κεντρική και την Ανατολική Ευρώπη και το 2001 αλλά και το 2003, για τη μείωση των οικονομικών εγκλημάτων οι ίδιες επιχειρήσεις τα τελευταία δύο χρόνια ανέφεραν σημαντικά περισσότερα οικονομικά αδικήματα (**το 2003: 37% έναντι του 2001: 26%**). Κατά την άποψή μας είναι μη ρεαλιστικό σήμερα να αναμένονται σημαντικές μειώσεις στους οικονομικούς κινδύνους από εγκλήματα κάθε τύπου, όταν δεν υλοποιούνται ουσιαστικές ενέργειες για την αντιμετώπιση των ουσιαστικών αιτιών παραγωγής τους, πέρα από την πρόσθετη αδυναμία προσαρμογής της εκάστοτε νομοθεσίας στην οικονομική εγκληματική πραγματικότητα του σήμερα. Κοιτάζοντας προς τα εμπρός κατά τη διάρκεια των επόμενων πέντε ετών, το 35% των επιχειρήσεων αναμένει ως σημαντικότερους κινδύνους εκείνους που προέρχονται από τις κλοπές ή υπεξαιρέσεις καθώς επίσης και κάθε τύπο εγκλήματος που σχετίζεται με το διαδίκτυο (cyber crimes), όπως φαίνεται και στο διάγραμμα 7.8 που ακολουθεί.



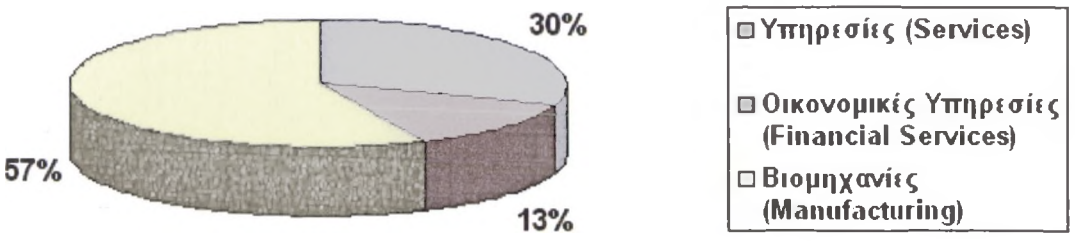
Διάγραμμα 7.8

7.1.3 Δημογραφικά Έρευνας

Για την ολοκλήρωση της έρευνας πραγματοποιήθηκαν συνεντεύξεις σε 3.623 CEOs, CFOs ή υπεύθυνους για την ανίχνευση ή την παρεμπόδιση των οικονομικών εγκλημάτων. Ο αριθμός στόχος των συμμετεχόντων για κάθε χώρα καθορίστηκε σύμφωνα με το ΑΕΠ της εκάστοτε χώρας. Στον παρακάτω πίνακα 7.1 ,διαγράμματα 7.9 και σχέδιο 7.2 αναφέρονται αναλυτικά το σύνολο των χωρών, ο αριθμός των επιχειρήσεων ανά χώρα και ανά περιοχή καθώς και το μέγεθος των επιχειρήσεων ως προς τον αριθμό του προσωπικού τους, που συμμετείχαν στην έρευνα.



Διάγραμμα 7.9



Σχέδιο 7.2

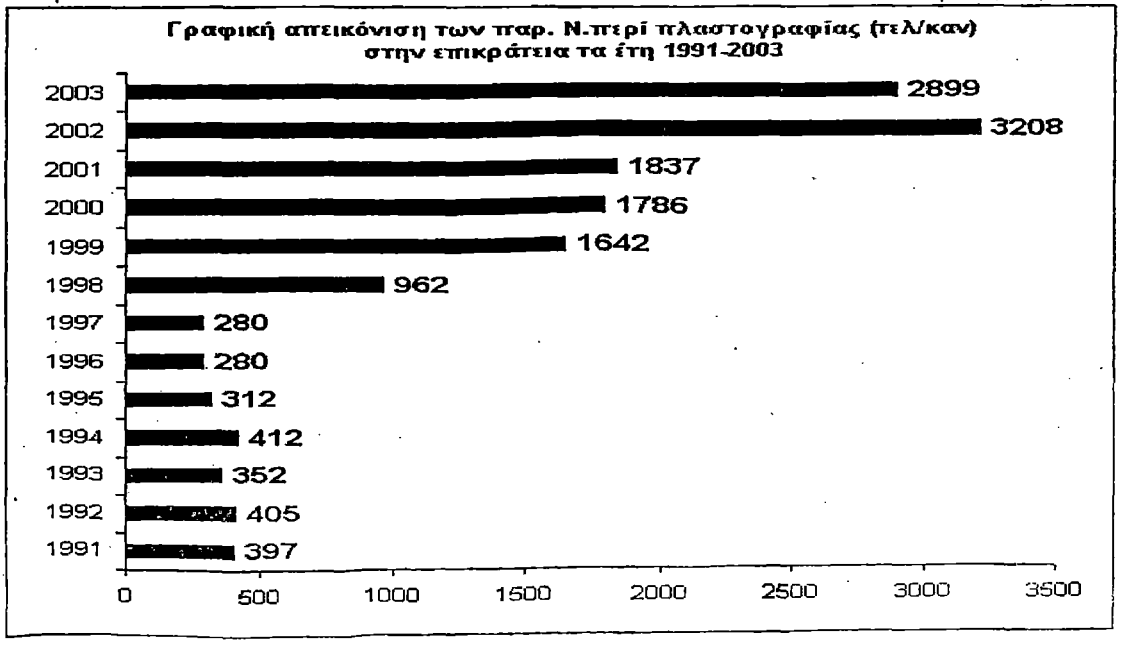
Western Europe	1476	South & Central America	554
Austria	83	Argentina	96
Belgium	90	Brazil	86
Denmark	88	Chile	53
France	156	Colombia	48
Germany	150	Dominican Republic	31
Greece	59	Guatemala	30
Italy	159	Mexico	87
Netherlands	103	Peru	51
Norway	90	Uruguay	36
Portugal	50	Venezuela	36
Spain	106		
Sweden	91	North America	194
Switzerland	89	Canada	103
UK/Ireland	162	USA	91*
Central & Eastern Europe	378	Asia & Pacific	873
Baltics: Estonia/Lithuania/Latvia	25	Australia	100
Bulgaria	25	Hong Kong	85
Czech Republic	50	India	85
Hungary	25	Indonesia	85
Poland	85	Japan	423*
Romania	29	Singapore	50
Russia	29	Thailand	50
Slovak Republic	31		
Slovenia	27	Africa	143
Turkey	52	Algeria	21
		Morocco	17
		South Africa	91
		Tunisia	14

* = weighted in the statistics to reflect a base of 150 respondents – the target number according to the country's GDP.

Πίνακας 7.1

7.2 Στατιστικά Ελληνικής Αστυνομίας

Στους παρακάτω πίνακες 7.2 και 7.3 και στο διάγραμμα 7.10 παρουσιάζονται αναλυτικά οι εξακριβωθείσες υποθέσεις από την Ελληνική Αστυνομία στις περιπτώσεις των παραβάσεων του Ν. 2121/93περί πνευματικής. ιδιοκτησίας στην επικράτεια 1998 – 2003.



Διάγραμμα 7.10

ΠΙΝΑΚΑΣ

κατασχεθέντων προϊόντων παράνομης αντιγραφής (Ν.2121/93) κατά είδος για τα έτη 1995-2003

ΕΙΔΟΣ	1995	1996	1997	1998	1999	2000	2001	2002	2003
Κασσέτες Ήχου	8.345	12.869	23.255	3.151	8.365	9.992	8.712	8.850	14.898
Κασσέτες εικόνας	8.658	616	3.937	433	711	964	5.868	4.625	8.468
CD'S				20.646	214.256	147.512	459.513	754.096	1.737.433
Εξώφυλλα CD'S				13.558	5.442	5.156	27.191	503.637	511.536
CD-R					5.771	3.476	20.142	30.325	425
Θήκες CD							13.968	5.520	6.951
DVD							959	1.189	2.640
PC GAMES									3.192
CD-PLAY STATION								17.589	24.583
CD-PROGRAMMS									1.122

ΣΗΜΕΙΩΣΗ: Για τα έτη 1995,1996,1997 στα παραπάνω νούμερα στις κασσέτες ήχου συμπεριλαμβάνονται και τα CD'S.

ΠΙΝΑΚΑΣ

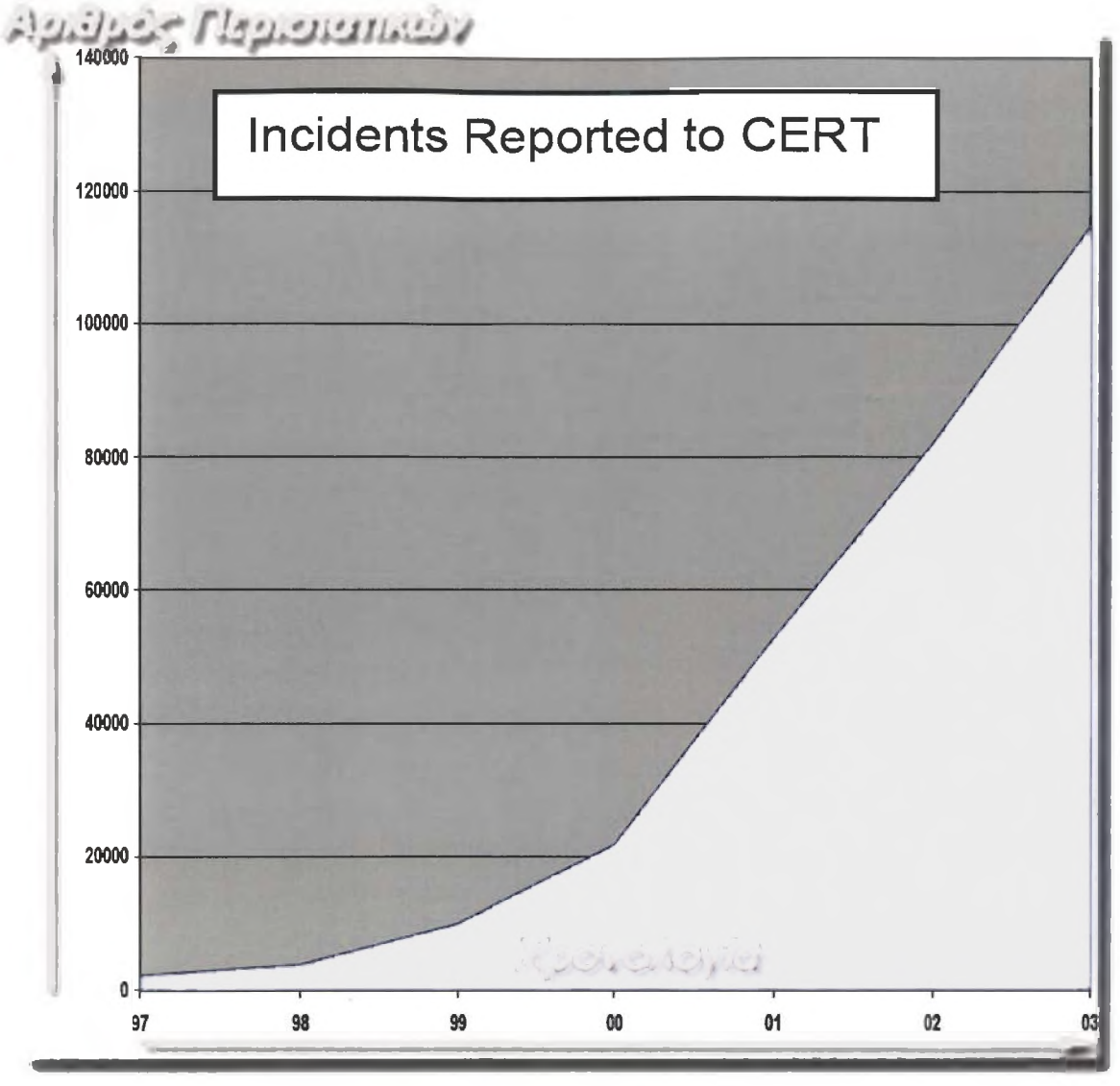
παραβάσεων παράνομης αντιγραφής (Ν.2121/93) για τα έτη 1998-2003

	ΕΤΗ								
	1995	1996	1997	1998	1999	2000	2001	2002	2003
ΠΑΡΑΒΑΣΕΙΣ				115	617	817	1234	2002	2219
ΕΞΙΧΝΙΑΣΘΗΚΑΝ				106	557	602	943	1609	1825
ΑΠΟΠΕΙΡΕΣ					1	6	10	2	6

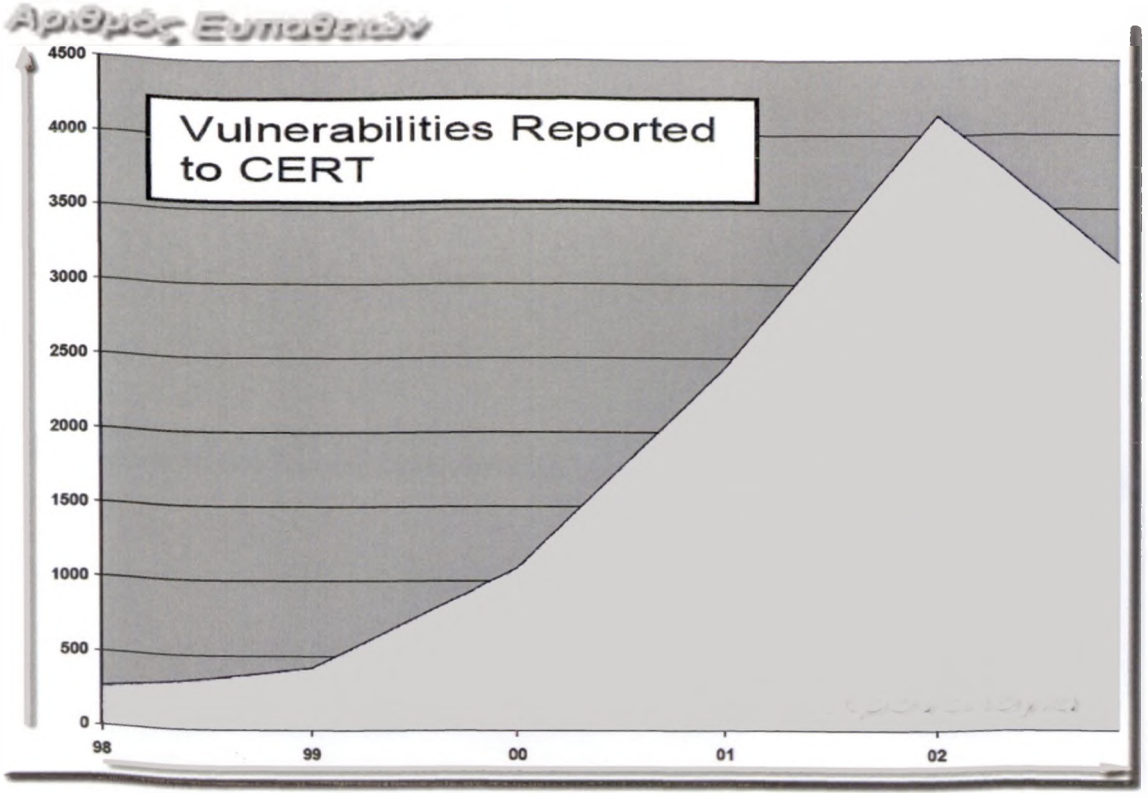
Πίνακες 7.2 και 7.3

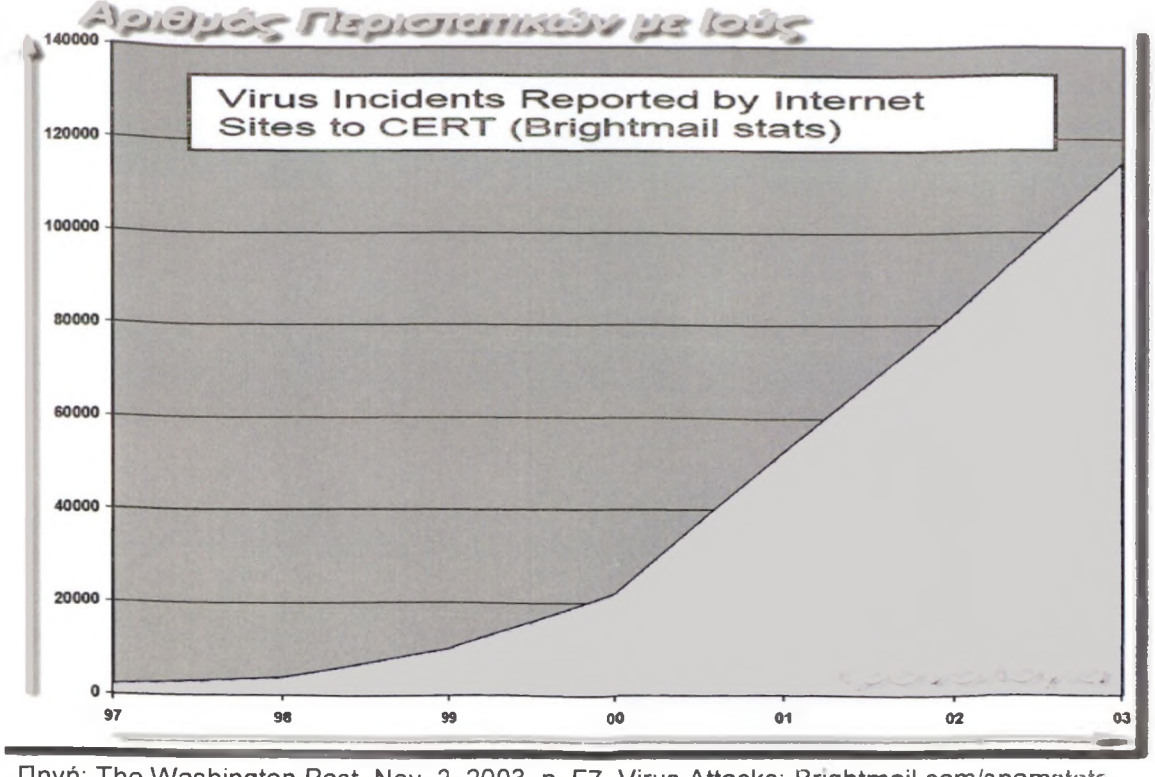
7.3 Έρευνες εγκλημάτων σχετικά με υπολογιστές (Computer-Related Crime)

Τα ποσοστά αύξησης των περιστατικών ασφάλειας που σχετίζεται με υπολογιστές, των ευπαθειών (συστημάτων, λογισμικού) που ανακαλύπτονται και του αριθμού μεμονωμένων διευθύνσεων πρωτοκόλλου (IP addresses) του διαδικτύου φαίνονται να έχουν πολύ υψηλές καμπύλες αύξησης. Το κέντρο συντονισμού CERT (www.cert.org) του πανεπιστημίου Mellon Carnegie (**Carnegie Mellon University's CERT Coordination Center**) υπολογίζει ότι τα περιστατικά που αναφέρονται αντιπροσωπεύσουν μόνο το 5% των πραγματικών περιστατικών. Τα ποσοστά αύξησης (σχετικά με τα παραπάνω) μπορεί να αντιμετωπισθούν ως δείκτες της γενικής με τους υπολογιστές, αύξησης των εγκλημάτων. Στα διαγράμματα που ακολουθούν παρουσιάζονται τα παραπάνω ποσοστά αύξησης:



Πηγή: The Washington Post, Nov. 2, 2003, p. F7, Virus Attacks; Brightmail.com/spamstats, CERT
Coordination Center (charts)
Διάγραμμα 7.11





Πηγή: The Washington Post, Nov. 2, 2003, p. F7, Virus Attacks; Brightmail.com/spamstats, CERT
Coordination Center (charts)
Διαγράμματα 7.12 και 7.13

Σημειώνουμ την ομοιότητα μεταξύ της καμπύλης αύξησης που παρουσιάζεται σε αυτό το διάγραμμα με εκείνων των προηγούμενων διαγραμμάτων, που παρουσιάζει την αύξηση του περιστατικών ασφάλειας και των ευπαθειών.

8 Κατηγορίες οικονομικού εγκλήματος

8.1 Εισαγωγή

Όλα τα οικονομικά τμήματα και οι αρμόδιες επιτροπές τόσο της Αμερικάνικης όσο και της Ευρωπαϊκής οικονομίας εκθέτουν συνεχώς (όπως δείχνουν και οι έρευνες που παρατίθενται στο παρόν κείμενο), τις σημαντικές απώλειες ως αποτέλεσμα των οικονομικών – ηλεκτρονικών εγκλημάτων που διαπράττονται. Στη παρούσα ενότητα παρέχονται οι πιο πρόσφατες πληροφορίες που αφορούν τις εξής βασικές κατηγορίες οικονομικών εγκλημάτων: τράπεζες (**banking**), πιστωτικές κάρτες (**credit card**), υγειονομική περίθαλψη (**health care**), ασφάλεια (**insurance**), τηλεπικοινωνίες (**telecommunications**), πνευματικές ιδιοκτησίες (**intellectual property**), computer crimes, ξέπλυμα χρημάτων (**money laundering**), απάτες (**frauds**) και κλοπή ταυτότητας (**identity theft**).

8.2 Banking

Σχετικά πρόσφατες εκθέσεις[4] στις ΗΠΑ δείχνουν ότι περισσότερες από 500 εκατομμύρια επιταγές είναι πλαστές ετησίως. Το 1997, η αμερικανική ένωση τραπεζών ανέφερε ότι οι τράπεζες έχασαν συνολικά 512 εκατομμύρια δολάρια, για τον έλεγχο σχετικά με απάτες αυτού του τύπου. Άλλες έρευνες προβλέπουν ότι θα υπάρξει μια αύξηση τουλάχιστον 25% σχετικά με τις επιταγές κατά τη διάρκεια του επόμενου έτους. Το ξέπλυμα χρημάτων επίσης έχει αυξηθεί κατά τη διάρκεια των τελευταίων δέκα ετών (περισσότερα για το ξέπλυμα χρήματος σε επόμενη ενότητα) και εκτιμάται ότι το 1998 ήταν της τάξης των 2,85 τρισεκατομμύρια δολαρίων.

Η αύξηση επίσης των online τραπεζικών εργασιών παρουσιάζει πολλές ευκαιρίες για τους δράστες του οικονομικού – ηλεκτρονικού εγκλήματος. Οι υπεξαιρέσεις σημαντικών ποσών επίσης μέσω λογαριασμών ή άλλων μεθόδων δείχνει να έχει ανοδική πορεία. Οι εγκληματίες μπορούν να χρησιμοποιήσουν ψευδείς εφαρμογές ανοικτής γραμμής (online) για την απόκτηση δανείων και οι χάκερ είναι σε θέση να αναστατώνουν το e-commerce με τη διάπραξη εγκληματικών επιθέσεων (denial of service attacks) και με την απόκτηση πρόσβασης σε απευθείας τραπεζικά συστήματα πληρωμών. Η κλοπή ταυτότητας (identity theft) μπορεί επίσης να έχει σημαντικές επιπτώσεις στις online τραπεζικές εργασίες κ.ο.κ. Όλα μαζί τα προαναφερόμενα περιστατικά απατών, δείχνουν ότι ο τραπεζικός χώρος πραγματικά κατακλύζεται από οικονομικά και οικονομικά εγκλήματα κάθε τύπου.

Σύμφωνα με τα παραπάνω η προσαρμογή της νομοθεσίας (του εκάστοτε κράτους) για την αντιμετώπιση του οικονομικού – ηλεκτρονικού εγκλήματος και ειδικότερα για τις απάτες που σχετίζονται με τις online τραπεζικές εργασίες, παρουσιάζει δυσκολίες τόσο σε διεθνές επίπεδό όσο και σε Ευρωπαϊκό που αφορά την Ελλάδα ιδιαίτερα. Δυστυχώς το διαδίκτυο παρέχει πρόσφορο έδαφος για εκείνους που σκοπεύουν να εγκληματούν εις βάρος των χρηματοδοτικούς οργανισμών. Δεδομένου ότι η ανωνυμία είναι εύκολο να

[4] http://www.ckfraud.org/statistics.html (August 2, 2000)

διατηρηθεί με διάφορα μέσα και τρόπους, ο κίνδυνος απάτης μέσω διαδικτύου γίνεται πιθανότερος.

Για την αντιμετώπιση παρόμοιων προβλημάτων όπως αυτά αναφέρθηκαν παραπάνω απαιτείται η συμμετοχή ενός τρίτου παράγοντα με το όνομα «**Έμπιστη Τρίτη Οντότητα**» (**Trusted Third Party**) η οποία να εγγυάται πως οι δύο πλευρές (που συμμετέχουν σε online συναλλαγές ή άλλες τραπεζικές εργασίες)) είναι πράγματι εκείνες που ισχυρίζονται και δεν έχει γίνει κάποια «**πλαστοπροσωπία**» (π.χ. το web site ανήκει πράγματι στην εταιρεία Α και ο πελάτης δεν έχει δρομολογηθεί εν αγνοία του σε ένα «**πειρατικό**» site το οποίο θα τον χρεώσει, αλλά δεν θα του παραδώσει ποτέ τα προϊόντα). Η έμπιστη τρίτη οντότητα πιστοποιεί την ταυτότητα του server με τη χρήση ενός ψηφιακού πιστοποιητικού (**digital certificate**). Το πιστοποιητικό αυτό αποτελεί ένα είδος ηλεκτρονικής κάρτας αναγνώρισης η οποία περιέχει έναν ειδικό αναγνωριστικό αριθμό, μια ημερομηνία λήξεως, το δημόσιο κρυπτογραφικό κλειδί του καταστήματος (για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων και ηλεκτρονικών υπογραφών), καθώς και την ηλεκτρονική υπογραφή της έμπιστης τρίτης οντότητας.

Σήμερα, υπάρχουν πολλές εταιρείες οι οποίες παρέχουν αυτή την υπηρεσία. Ενδεικτικά αναφέρουμε τις:

- Belsign (http://www.belsign.com)
- CyberTrust (http://www.cybertrust.com)
- Entrust (http://www.entrust.com) και
- Verisign (http://www.verisign.com).

Δυστυχώς, μέχρι σήμερα οι χρήστες του διαδικτύου έχουν αποδειχθεί απρόθυμοι να αποκτήσουν πιστοποιητικά αυτής της μορφής (για διάφορους λόγους που δεν είναι του παρόντος να αναλυθούν). Έτσι, ενώ ο πελάτης μπορεί να είναι σίγουρος για την ταυτότητα του πωλητή, ο πωλητής δεν γνωρίζει ποιος είναι αυτός με τον οποίο συναλλάσσεται (το SSL πιστοποιεί μόνο την ταυτότητα του server). Αυτό σημαίνει πως αν κάποιος τρίτος γνωρίζει τα στοιχεία της κάρτας ενός χρήστη μπορεί να επισκεφθεί οποιοδήποτε ηλεκτρονικό κατάστημα και να αγοράσει ότι επιθυμεί, χρεώνοντας το λογαριασμό του πραγματικού κατόχου της κάρτας. Η υιοθέτηση και η ενημέρωση του κοινού για τα ψηφιακά πιστοποιητικά, θα πρέπει να αποτελεί προτεραιότητα για κάθε κυβερνητική αρχή με στόχο την μείωση όσο το δυνατόν, των απατών που συνοδεύουν τον τραπεζικό κόσμο.

8.3 Υγειονομική περίθαλψη

Η απάτες που σχετίζονται με την υγειονομική περίθαλψη περιλαμβάνουν εκείνες, που διαπράττονται σε κυβερνητικά και ιδιωτικά υποστηριζόμενα προγράμματα υγειονομικής περίθαλψης από τα μέλη και τους υπεύθυνους που τα διαχειρίζονται, τους ίδιους τους ασφαλισμένους αλλά και τους διάφορους προμηθευτές. Οι απώλειες για το 1999 υπολογίστηκαν να είναι περίπου το δέκα τοις εκατό όλων των χρημάτων, που ξοδεύτηκαν στην υγειονομική περίθαλψη, στις ΗΠΑ το οποίο μεταφράζεται σε μια απώλεια περίπου 100 δισεκατομμυρίων δολαρίων. Σχετικά με τα cyber εγκλήματα στην υγειονομική

περίθαλψη περιλαμβάνονται, η λήψη φαρμακευτικών ειδών από χώρους του διαδικτύου με την παροχή ψεύτικων πληροφοριών και από ιστοχώρους που υποστηρίζουν ότι παρέχουν ειδικές ιατρικές συμβουλές, αλλά στην πραγματικότητα δεν έχουν καμία επιστημονική ή επαγγελματική υπόσταση.

8.4 Ασφάλεια (insurance)

Σύμφωνα με μια έκθεση του FBI σχετικά με την ασφαλιστική απάτη, που δημοσιεύεται στον ιστοχώρο της και στο πλαίσιο του τμήματος «**των οικονομικών εγκλημάτων**», η συνολική απάτη στην βιομηχανία ασφαλίσεων είναι 27,6 δισεκατομμύρια δολάρια ετησίως. Συγκεκριμένα ο φορέας «**Coalition Against Insurance Fraud**» στις ΗΠΑ εκτιμά τις ζημίες ανά κατηγορία ως εξής:

- Ασφάλεια Αυτοκινήτων - 12,3 δισεκατομμύρια δολάρια
- Ιδιοκτήτες σπιτιών - 1,8 δισεκατομμύρια δολάρια
- Επιχειρήσεις / Εμπορικά καταστήματα - 12 δισεκατομμύρια δολάρια
- Ασφάλειες Ζωής / Σωματικές Αναπηρίες - 1,5 δισεκατομμύρια δολάρια
- Συνολικά όλα τα παραπάνω - 27,6 δισεκατομμύρια δολάρια

Τα οικονομικά αδικήματα σε όλους τους παραπάνω τομείς ασφάλειας, πραγματοποιούνται τόσο εσωτερικά όσο και εξωτερικά σε αυτούς. Ως εσωτερική απάτη μπορούμε να αναφέρουμε ενδεικτικά τη δωροδοκία των στελεχών μιας επιχείρησης, την υπεξαίρεση (**misrepresentation**) των πληροφοριών για προσωπικό κέρδος και άλλα συναφή. Οι υποψήφιοι, οι ασφαλισμένοι, οι ενάγοντες τρίτων, ή οι ασφαλιστικοί πράκτορες που παρέχουν την υπηρεσία στους ενάγοντες, μπορούν να διαπράξουν εξωτερική απάτη. Η απάτη μπορεί να λάβει τη μορφή διογκωμένων αξιώσεων, ψεύτικων εφαρμογών με συνέπεια την έκδοση ψευδών στοιχείων, ή κατάλληλου χειρισμού πληροφοριών προκειμένου να χαμηλώσουν τα ασφάλιστρα.

8.5 Τηλεπικοινωνίες

Το U.S. Secret Service υπολογίζει ότι οι απώλειες από απάτες στις τηλεπικοινωνίες υπερβαίνουν το 1 δισεκατομμύριο δολάρια ετησίως. Άλλες εκτιμήσεις από τις ΗΠΑ κυμαίνονται από 3 δισεκατομμύρια έως 12 δισεκατομμύρια δολάρια. Η συνδρομή, ή η απάτη ταυτότητας περιλαμβάνει τη χρησιμοποίηση πλαστών ή κλεμμένων IDs ή πιστωτικών καρτών για την απόκτηση υπηρεσιών δωρεάν και την διατήρηση της ανωνυμίας. Επίσης από την απάτη τηλεαγοράς (**Telemarketing**), οι απώλειες των θυμάτων ξεπερνούν τα 40 δισεκατομμύρια δολάρια μόνο το 1998. Συγκεκριμένα με στοιχεία του FBI το 1996 υπολογίστηκε ότι υπήρξαν πάνω από 14.000 εταιρίες τηλεαγοράς, οι οποίες συμμετείχαν σε πλαστές πράξεις και στη πλειοψηφία των θυμάτων ανήκουν οι υ ηλικιωμένοι.

8.6 Απάτες και κλοπές στο διαδίκτυο με χρήση Υπολογιστών

Το διαδίκτυο ξεφεύγοντας από τα στενά ακαδημαϊκά και ερευνητικά πλαίσια του παρελθόντος, άρχισε να αυξάνει με γοργό ρυθμό την πολυπλοκότητα του

(ως συστήματος, με την ευρύτερη έννοια). Όπως όμως συμβαίνει και με το σύνολο των συστημάτων που χρησιμοποιούνται κατά κόρον στις ανθρώπινες κοινωνίες, από την αύξηση της πολυπλοκότητας δεν προέκυψαν μόνον επιθυμητά «πλεονεκτήματα». Όταν το σύστημα διαβεί ένα συγκεκριμένο κρίσιμο σημείο, δύσκολα μπορεί κάποιος να διακρίνει το σύνολο των δυνατοτήτων και ιδιοτήτων του και σύντομα αυτές μετατρέπονται από πλεονεκτήματα σε μειονεκτήματα, επιβλαβή τόσο για τους συμμετέχοντες (ή μη) σε αυτό, όσο και για το ίδιο το σύστημα.

Η σημερινή μορφή του διαδικτύου που καθορίζεται σε μεγάλο βαθμό από τις σημερινές τεχνολογίες που χρησιμοποιούνται σε αυτό (και που του προσφέρουν μεγαλύτερες δυνατότητες σε σχέση με το παρελθόν σε θέματα όπως: η ταχύτητα, η αύξηση του συνολικού όγκου μεταφοράς δεδομένων κ.λ.π.), παρέχει στις επιχειρήσεις και σε άτομα την ευκαιρία να προωθούν και να πουλούν τα προϊόντα τους μέσω αυτού. Αυτό οδήγησε στην δημιουργία του ηλεκτρονικού εμπορίου το οποίο αποτελεί ένα σύνολο ολοκληρωμένων συναλλαγών, που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι δηλαδή, οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση, για αγορά και πώληση αγαθών ή υπηρεσιών.

Με τη γέννηση του ηλεκτρονικού εμπορίου άρχισαν ταυτόχρονα να αυξάνονται και οι απάτες ή οι κλοπές στο διαδίκτυο (που αποτελούν κοινά εγκλήματα) ολοένα και περισσότερο, καθώς το τελευταίο εξαπλώνεται αντίστοιχα με ραγδαίους ρυθμούς. Στοχεύοντας κυρίως σε επιχειρήσεις ή άτομα, πραγματοποιούνται πλήθος από εγκληματικές ενέργειες στο διαδίκτυο με σκοπό την εξαπάτησή τους, όπως παραδείγματος χάριν:

- Ψευδή ενημερωτικά δελτία (online newsletters, bulletin boards), που παραπληροφορούν επενδυτές, απλούς χρήστες του διαδικτύου, αγοραστές κ.α.
- Χρήση του ηλεκτρονικού ταχυδρομείου (E-mail) για τη διάδοση ψευδών πληροφοριών που αφορούν μια επιχείρηση (π.χ. σχετικά με επενδύσεις).
- Απάτη πιστωτικών καρτών (Credit card fraud). Περισσότερα για αυτό στις παραγράφους που ακολουθούν.
- Τεχνάσματα εμπιστοσύνης (Cnfidence tricks). Ένα τέχνασμα εμπιστοσύνης, είναι μια προσπάθεια να παραπλανηθεί σκόπιμα ένα πρόσωπο ή τα πρόσωπα συνήθως με το στόχο του οικονομικού ή άλλου κέρδους.
- Κλοπή ταυτότητας (Identity theft). Η κλοπή ταυτότητας είναι η σκόπιμη χρησιμοποίηση της ταυτότητας (ηλεκτρονική ή μη) ενός άλλου προσώπου, συνήθως για να αποκτήσει παράνομη πρόσβαση σε δεδομένα ηλεκτρονικών υπολογιστών (ή συσκευές), με σκοπό το οικονομικό όφελος ή η πραγματοποίηση κάποιου εγκλήματος. Λιγότερο σύνηθες η κλοπή ταυτότητας μπορεί να χρησιμοποιηθεί με άλλα κίνητρα, όπως την τρομοκρατία, την κατασκοπεία ή ως μέσω εκβιασμού.

8.6.1 Παράγοντες που επηρεάζουν τις απάτες

Σε αυτή την ενότητα αναφέρεται ο βαθμός επιρροής της παγκοσμιοποίησης, της τεχνολογίας, των οικονομικών και κοινωνικών αλλαγών όσο αφορά στο θέμα «το μέλλον της απάτης».

8.6.1.1 Παγκοσμιοποίηση

Η παγκοσμιοποίηση είναι η ανάπτυξη και η συγχώνευση των διεθνών επικοινωνιών, των οικονομικών, πολιτικών και κοινωνικών συστημάτων για την διαμόρφωση παγκόσμιων συστημάτων (**global systems**). Η διαμόρφωση αυτή διευκολύνεται από διάφορους παράγοντες συμπεριλαμβανομένης της γρήγορης εξέλιξης των νέων τεχνολογιών, της διάδοσης των τηλεπικοινωνιών υποδομών στο Διαδίκτυο, της άρσης των ελέγχων στις χρηματιστηριακές αγορές, της αύξησης του εμπορίου και των ταξιδιών και των δραστηριοτήτων των πολυεθνικών εταιριών.

Ενώ η δικαιοδοσίες των δικαστηρίων καθορίζονται σε στενά γεωγραφικά πλαίσια, τα εθνικά σύνορα αποτελούν ολοένα και λιγότερο εμπόδιο στη διάπραξη απατών. Η παγκοσμιοποίηση επηρεάζει τις απάτες:

- Επεκτείνοντας την σφαίρα επιρροής των απατεώνων
- Δημιουργώντας προβλήματα δικαιοδοσιών
- Ελαττώνοντας τις δυνατότητες του υπάρχοντος διεθνούς ρυθμιστικού και νομοθετικού περιβάλλοντος
- Ελαττώνοντας τις δυνατότητες των υπαρχόντων συστημάτων εσωτερικού ελέγχου, με την αναγκαστική αλλαγή του σχεδιασμού επιχειρησιακών κινδύνων των οργανισμών.

8.6.1.2 Τεχνολογικές επιρροές

8.6.1.2.1 Εξέλιξη του Διαδικτύου

Οι περισσότερες χώρες στον κόσμο σήμερα παρουσιάζουν μεγάλα ποσοστά διείσδυσης προσωπικών υπολογιστών και πρόσβασης στο διαδίκτυο. Οι εκτιμήσεις παγκοσμίως προβλέπουν σχετικά με την επέκταση του Διαδικτύου, ότι οι συνολικές συνδέσεις σε αυτό θα αυξηθούν τουλάχιστον δέκα φορές κατά τη διάρκεια των επόμενων ετών και ο όγκος των παγκόσμιων συναλλαγών μέσω αυτού εκτιμάται ότι μπορεί να ξεπεράσει και το 40 με 60% από αυτό που είναι σήμερα.

Η πραγματοποίηση απατών στο διαδίκτυο περιλαμβάνει:

- Κλοπή κεφαλαίων μέσω παράνομων μεταφορών
- Κλοπή πιστωτικών καρτών ή στοιχείων τους
- Παράνομη χρήση πιστωτικών καρτών
- Εκβιασμούς
- Πωλήσεις προϊόντων που δεν υπάρχουν στην πραγματικότητα
- Καθώς και πολλά άλλα

Το διαδίκτυο παρέχει στους εγκληματίες την πρόσβαση σε έναν μεγάλο αριθμό θυμάτων συμπεριλαμβανομένων των εμπόρων, των καταναλωτών αλλά και στον καθένα που το χρησιμοποιεί όχι μόνο μέσα σε μια χώρα αλλά διεθνώς. Οι

φοροφυγάδες ωφελούνται επίσης από την ικανότητα να μεταφερθούν τα κεφάλαια σε off-shore τράπεζες εύκολα και ανώνυμα, με αυτόν τον τρόπο αποφεύγοντας τους ελέγχους από τις αρμόδιες αρχές του εκάστοτε κράτους.

8.6.1.2.2 E-commerce

Η ανάπτυξη σήμερα (σχεδόν;) ασφαλών μηχανισμών ανταλλαγής πληροφοριών βασισμένων στο διαδίκτυο, μπορεί να συνδέσει τους αγοραστές, τους προμηθευτές και τους διανομείς on-line. Αυτό δημιουργεί αποτελεσματικότερες αλυσίδων ανεφοδιασμού μεταξύ όλων των παραπάνω και επιτρέπει την χρήση λύσεων βασισμένες στο διαδίκτυο (με αφανείς διαδικασίες), χωρίς την ανάγκη παρουσίας χωριστής υποδομής ηλεκτρονικής ανταλλαγής δεδομένων (EDI), η οποία είναι ακριβή και απαιτεί εξειδικευμένα συστήματα από όλους τους χρήστες του. Οι εφαρμογές που βασίζονται στο διαδίκτυο είναι γενικά φτηνότερες και πιο ευέλικτες από τα συστήματα EDI, αλλά από την άλλη επιταχύνουν τις αλλαγές στην ηλεκτρονική επεξεργασία, η οποία όμως στη συνέχεια έχει επίδραση στη φύση και το επίπεδο κινδύνου των απατών.

8.6.1.2.3 Το νέο επιχειρησιακό πρότυπο

Το παραδοσιακό και επιχειρησιακό πρότυπο αποτελούσε μια απλή μορφή προσφοράς και ζήτησης, με ένα τμήμα που απασχολούνταν με την αγορά των προμηθειών και ένα άλλο τμήμα που απασχολούνταν με την πώληση των προϊόντων στους καταναλωτές. Στο νέο (**ηλεκτρονικό**) επιχειρησιακό πρότυπο, τα πράγματα είναι διαφορετικά και όλες οι πτυχές μιας επιχείρησης διασυνδέονται (**interconnected**) με μεγάλες ταχύτητες (στις επικοινωνίες και στη μεταφορά πληροφοριών) και επίσης ενσωματώνουν και αυτοματοποιούν τις διάφορες επιχειρηματικές λειτουργίες έτσι ώστε όλες να μπορούν να πραγματοποιούνται ταυτόχρονα και γρηγορότερα από ότι πριν. Το νέο επιχειρησιακό μοντέλο ανάπτυξης και λειτουργίας των σύγχρονων επιχειρήσεων απαιτεί την προσαρμογή της νομοθεσίας, για να εξασφαλίσει την διαφανή λειτουργία τους αλλά και να εμποδίσει την κακή χρήση των ηλεκτρονικών επικοινωνιών, που τόσο ραγδαία τα τελευταία χρόνια χρησιμοποιούν οι επιχειρήσεις.

8.6.1.2.4 M-commerce

Το εμπόριο μέσω κινητών συσκευών (**m-commerce**), είναι απλά το ηλεκτρονικό εμπόριο που διευθύνεται από ένα κινητό τηλέφωνο, από συσκευές **palms**, ή από ασύρματες συσκευές πρόσβασης στο διαδίκτυο. Οι ασύρματες συσκευές διαδικτύου προβλέπεται να αλλάξουν σημαντικά τον τρόπο που το διαδίκτυο χρησιμοποιείται, παρέχοντας ευκολότερη πρόσβαση σε αυτό για ολοένα και περισσότερους ανθρώπους και χώρες. Το i-mode που πρόσφατα έκανε την είσοδό του και στην ελληνική αγορά κινητής τηλεφωνίας (**Cosmote**), επισημαίνει με τον πιο χαρακτηριστικό τρόπο την τάση της αγοράς για πιο ενεργή συμμετοχή του κόσμου στο ηλεκτρονικό εμπόριο, εφόσον προσφέρει έναν μεγάλο αριθμό επιλογών για κάθε είδους συναλλαγή μέσω κινητών συσκευών που το υποστηρίζουν. Όπως είναι φυσικό η εξέλιξη του **m-commerce**, δημιουργεί ένα ακόμα πρόσφορο πεδίο για την πραγματοποίηση

των απατών και επίσης πολλά νομικά θέματα σχετικά με την αντιμετώπισή τους.

8.6.1.2.5 Ρυθμιστικό πλαίσιο για το e-commerce

Μια από τις σημαντικότερες δυσκολίες που συναντά οποιοσδήποτε μελετά την μεταβαλλόμενη φύση της απάτης στο νέο παγκόσμιο ηλεκτρονικό και οικονομικό περιβάλλον αποτελεί η εκάστοτε νομοθεσία ή οι κανονισμοί που εφαρμόζονται. Η πρόκληση στο συγκεκριμένο θέμα έχει να κάνει με τον προσδιορισμό των ορίων ανάμεσα στην ικανοποίηση των αναγκών των σύγχρονων επιχειρήσεων (παραδείγματος χάριν την ελαχιστοποίηση ή κατάργηση διεθνών εμπορικών περιορισμών) και στην αποτελεσματική εφαρμογή της νομοθεσίας για την προστασία των καταναλωτικών συμφερόντων, αλλά και των ίδιων των επιχειρήσεων.

Η (**UNCITRAL**), Επιτροπή Ηνωμένων Εθνών (**United Nations Commission**) για τον διεθνή εμπορικό νόμο (**International Trade Law**), εργάζεται συνεχώς με κατεύθυνση την διαμόρφωση διεθνών κανόνων, για την διευκόλυνση των διεθνών συναλλαγών. Η Ευρωπαϊκή Ένωση (**ΕΕ**), ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (**ΟΟΣΑ**), τα Ηνωμένα Έθνη (**Ο.Η.Ε**), η οικονομική συνεργασία Ασίας (**APEC**) και η Ένωση των Χωρών Νοτιοανατολικής Ασίας (**ASEAN**), επεξεργάζονται επίσης τους κανονισμούς που θα πρέπει να διέπουν το σύγχρονο σημερινό ηλεκτρονικό εμπόριο και τη χρήση του διαδικτύου και λειτουργούν με σκοπό την δημιουργία διεθνών προτύπων για τη λειτουργία του e-commerce, καθώς επίσης και των προτύπων που αφορούν τις ηλεκτρονικές συναλλαγές και τις ηλεκτρονικές υπογραφές.

8.7 Κλοπή (Theft)

Στην κατηγορία αυτή των εγκλημάτων που πραγματοποιούνται επίσης με την βοήθεια υπολογιστών προκύπτει μια ενδιαφέρουσα άποψη, σύμφωνα με την οποία τα συνηθέστερα προϊόντα κλοπής είναι οι πληροφορίες. Οι κλέφτες στοχεύουν πολύ συχνά στην πνευματική ιδιοκτησία, όπως τα σχέδια νέων προϊόντων, περιγραφές νέων προϊόντων, την έρευνα, τα σχέδια μάρκετινγκ, τους καταλόγους πελατών και άλλα πολλά. Σχετικές έρευνες στον τομέα αυτό δείχνουν, ότι η αξία των εμπορικών μυστικών και της πνευματικής ιδιοκτησίας είναι υψηλή. Επίσης τα πρόσωπα που διαπράττουν αυτόν τον τύπο εγκλήματος έχουν πραγματοποιήσει και στο παρελθόν παρόμοιες δραστηριότητες, όπως, παράνομες φωτοαντιγραφές εγγράφων, διαρρήξεις κ.λ.π.

Τώρα, οι κλέφτες κλέβουν πολύ πιο συχνά από τους υπολογιστές, επειδή οι πολύτιμες πληροφορίες είναι πιο προσιτές σε αυτούς. Επιπλέον οι μέθοδοι που χρησιμοποιούνται από τους σύγχρονους κλέφτες είναι ευκολότερες και πιο αξιόπιστες από τις παραδοσιακές μεθόδους και παρουσιάζουν τον μικρότερο κίνδυνο για την ανίχνευση και σύλληψή τους. Επίσης οι ίδιες έρευνες δείχνουν ότι υπάρχει μια σημαντική σχέση μεταξύ της προσωπικής χρήσης των υπολογιστών μιας επιχείρησης και των υπαλλήλων που κλέβουν ή που προσπαθούν να κλέψουν χρήματα από αυτήν. Για την αποφυγή των παραπάνω

φαινομένων, πολλές επιχειρήσεις για την προστασία τους τοποθέτησαν πρόσθετους εσωτερικούς ελέγχους ασφάλειας για τα κρίσιμα αρχεία πληροφοριών τους. Όμως παρά τα πρόσθετα μέτρα προστασίας που εφαρμόζονται από πολλές επιχειρήσεις, οι κλοπές δεν δείχνουν να έχουν εξαλειφθεί και οι κλοπές άλλοτε σε λιγότερο και άλλοτε σε περισσότερο βαθμό δείχνουν να συνεχίζουν αποτελούν ένα σημαντικό πρόβλημα για τις επιχειρήσεις του σήμερα σε ολόκληρο τον κόσμο.

8.8 Κλοπή ταυτότητας (Identity theft)

Η κλοπή ταυτότητας (identity theft) αποτελεί στην πραγματικότητα τον καταλύτη, για διάφορους τύπους οικονομικών εγκλημάτων, που σχετίζονται με την τρομοκρατία, εμπορία ναρκωτικών, καθώς και άλλων εγκλημάτων. Στην περίπτωση των τρομοκρατικών επιθέσεων της 11 Σεπτεμβρίου στις ΗΠΑ, αρκετοί από τους τρομοκράτες φαίνονταν να έχουν στη διάθεσή τους κάθε είδους πλαστά έγγραφα όπως: άδειες κυκλοφορίας αυτοκινήτων, κλεμμένες πιστωτικές κάρτες, πλαστά διαβατήρια και άλλα πλαστά ταξιδιωτικά έγγραφα, καθώς ακόμη και ψευδείς αριθμούς κοινωνικής ασφάλισης.

Με την κλοπή μιας ταυτότητας ή με τη δημιουργία πλαστών εγγράφων αναγνώρισης οι εγκληματίες είναι σε θέση να δημιουργήσουν μια πλαστή ταυτότητα (**fraudulent identity**), για να διασχίσουν τα σύνορα, να αποκτήσουνε επιπλέον πρόσβαση σε άλλα έγγραφα προσδιορισμού της ταυτότητας, όπως τα πιστοποιητικά γέννησης, τις άδειες οδήγησης και τις κάρτες κοινωνικής ασφάλισης. Αυτά τα έγγραφα, στη συνέχεια, δημιουργούν ακόμα μεγαλύτερη πρόσβαση για να προμηθευτούν άλλες χρήσιμες για αυτούς, πιστωτικές και πράσινες κάρτες, πρόσβαση σε τραπεζικούς λογαριασμούς και πολλά άλλα. Έχοντας εξασφαλίσει με τα παραπάνω μια «αξιόπιστη ταυτότητα» αυτή τους επιτρέπει να συμμετάσχουν σε οικονομικά εγκλήματα, όπως το ξέπλυμα χρημάτων για το κέρδος, ή την υποστήριξη της τρομοκρατίας.

8.8.1 Έρευνα στις ΗΠΑ.

Στα παρακάτω δυο διαγράμματα (8.1 &8.2) παρουσιάζονται τα αποτελέσματα από έρευνα στις ΗΠΑ (**Identity Theft: the FTC's Response, March 12, 2002**), σχετικά με την ηλικία των θυμάτων από κλοπή ταυτότητας καθώς και των ποικίλων τρόπων με τους οποίους η κλεμμένη ταυτότητα χρησιμοποιήθηκε, συμπεριλαμβανομένης της απάτης πιστωτικών καρτών.

FTC Identity Theft Clearinghouse Report Data – Age

Age of Victim	Percentage
Under 18	2
18-29	26
30-39	28
40-49	22
50-59	13
60 and over	9

Πηγή: FTC Identity Theft Clearinghouse report data (Identity Theft: the FTC's Response, March 12, 2002)

Διάγραμμα 8.1

FTC Identity Theft Clearinghouse Report Data – Uses of Stolen Identity

Crimes Where ID Used	Percentage
Credit card fraud	42
Unauthorized telecommunications or utility services	20
Bank fraud	13
Personal information for employment purposes	9
Fraudulent loans	7
Procurement of government documents or benefits	6
Other identity theft	19
Used for multiple crimes	20

Πηγή: FTC Identity Theft Clearinghouse report data (Identity Theft: the FTC's Response, March 12, 2002)

Διάγραμμα 8.2

8.8.2 Έρευνα στην Ευρώπη (της Europol)

Σύμφωνα με έρευνες της Europol όλοι οι τύποι απατών όχι μόνο συνεχίζουν να επικρατούν στους χώρους της Ευρωπαϊκής ένωσης, αλλά και αναμένεται να αυξηθούν ακόμη περισσότερο στο μέλλον. Συγκεκριμένα αναφέρεται ότι:

- Τα τρέχοντα μέλη της ΕΕ αντιμετωπίζουν μια αύξηση στον αριθμό εγκληματικών ομάδων που λαμβάνουν παράνομα κρατικές επιχορηγήσεις **(state subsidies)** στον τομέα των μισθώσεων, της

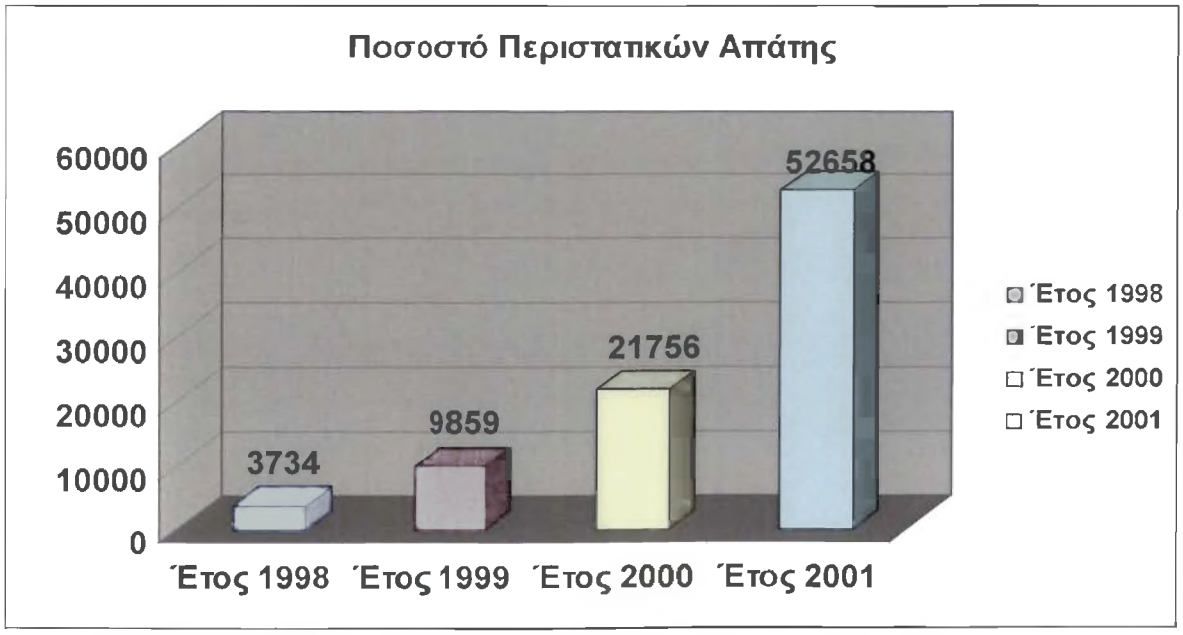
ασφάλειας και της υγείας. Υπάρχει επίσης διαδεδομένη φοροδιαφυγή και απάτες σχετικά με το **Φ.Π.Α**, με αγαθά που αγοράζονται στα κράτη μέλη της Ευρωπαϊκής Ένωσης και που στη συνέχεια πωλούνται σε χαμηλότερες τιμές στη μαύρη αγορά. Από την άλλη πλευρά προϊόντα που είναι αγορασμένα στις ίδιες χώρες χωρίς Φ.Π.Α, πωλούνται στη συνέχεια σε ανυποψίαστα θύματα με τιμές που συμπεριλαμβάνουν το Φ.Π.Α.

- Τα στοιχεία της Europol επιβεβαιώνουν επίσης και τα αποτελέσματα άλλων ερευνών, που δείχνουν ότι η κλοπή ταυτότητας (identity theft) και η απάτη πιστωτικών καρτών αυξάνονται συνεχώς.
- Υπάρχει επίσης ένας αυξανόμενος αριθμός εγκληματικών ομάδων που συμμετέχουν στην πλαστογράφηση χαρτονομισμάτων, ειδικά από την Λιθουανία και την Βουλγαρία. Αυτό όπως είναι φυσικό έχει επιπτώσεις στα κράτη μέλη της ΕΕ, δεδομένου ότι περιλαμβάνει τις περισσότερες φορές το ευρώ-νόμισμα. Επίσης ολοένα και περιπλοκότερες μέθοδοι εκτύπωσης χρησιμοποιούνται από τους επαγγελματίες παραχαράκτες, οι οποίες έχουν βελτιώσει εντυπωσιακά την ποιότητα και την ποσότητα των πλαστογραφιών που εμφανίστηκαν στην Ευρώπη, κατά τη διάρκεια του 2002.
- Το ξέπλυμα χρημάτων αποτελεί μια βασική δραστηριότητα για την πλειοψηφία των εγκληματικών ομάδων που δρουν στην ΕΕ. Τα μέσα που υιοθετούνται από αυτές τις ομάδες, για να καλύπτουν την παράνομη προέλευση των κεφαλαίων τους είναι όλο και περισσότερο περίπλοκα και συχνά περιλαμβάνουν τη στρατολόγηση και άλλων επαγγελματιών, όπως: οι λογιστές και οι δικηγόροι που χρησιμοποιούνται για να προσδώσουν στο παράνομο χρήμα μια νόμιμη νομική προέλευση. Ο κυριότερος τρόπος που επινοείται για το ξέπλυμα του παράνομου χρήματος, αποτελεί η κοινή ύπαρξη η χρήση των (**legal front companies**) νομικών επιχειρήσεων. Η χρήση των **legal front companies** αποτελεί ένα σημαντικό πρόβλημα, δεδομένου ότι παρέχουν στις εγκληματικές ομάδες ένα πρόσθετο νομικό εισόδημα, το οποίο μπορεί στη συνέχεια να επανεπενδυθεί στις εγκληματικές επιχειρήσεις. Αυτό το γεγονός όχι μόνο έχει μια αποσταθεροποιητική επίδραση στις δραστηριότητες γενικά της αγοράς και στις δυνάμεις ανταγωνισμού, αλλά είναι επίσης και ένας κρίσιμος πόρος που συνεχίζει να προωθεί την αύξηση και την επέκταση του οργανωμένου εγκλήματος. Μια νέα προοπτική έρχεται επίσης στο προσκήνιο μέσω επενδύσεων στην ιδιοκτησία, ως μέσο διάθεσης των παράνομων κεφαλαίων. Αυτό απεικονίζει συνήθως εκείνες τις εγκληματικές ομάδες που μεταφέρουν τα παράνομα κέρδη τους πίσω στην χώρα τους, για την επένδυσή τους στην ιδιοκτησία. Τα περισσότερα παραδείγματα σχετικά με τα παραπάνω, έχουν αναφερθεί σε σχέση με το Μαρόκο την Τουρκία και πρόσφατα στην Ελλάδα.
- Τα εγκλήματα με χρήση της υψηλής τεχνολογίας σύμφωνα με την Europol αναμένεται να συνεχίσουν να αντιπροσωπεύουν έναν από τους σημαντικότερους τομείς του εγκλήματος στο μέλλον, παράλληλα με την ανάπτυξη του ηλεκτρονικού εμπορίου και των τραπεζικών εργασιών μέσω διαδικτύου. Σε αυτά συγκαταλέγονται σε μεγάλο βαθμό οι απάτες πιστωτικών καρτών και η κλοπή ταυτότητας (**identity theft**).

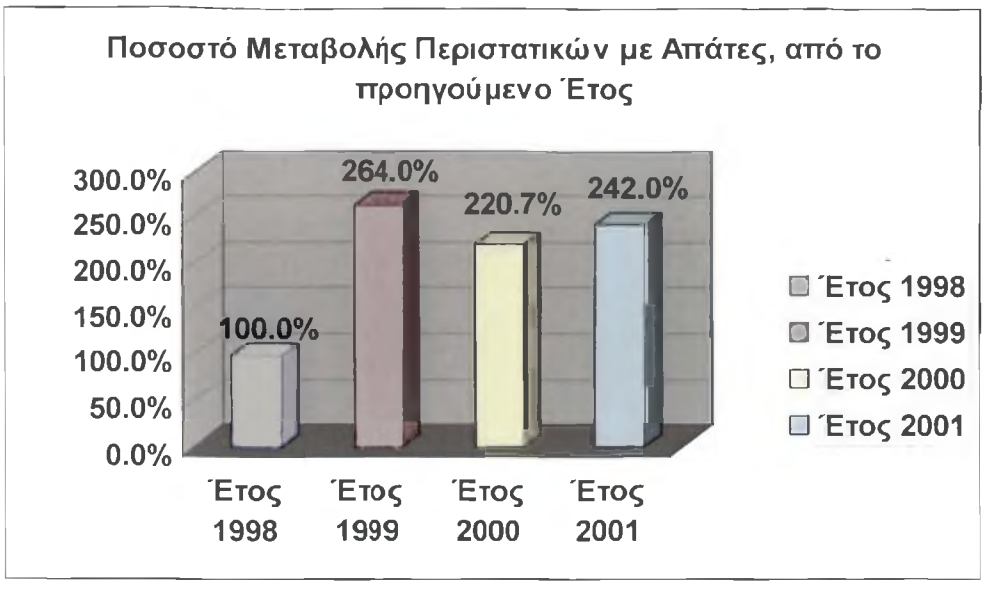
Παραδείγματος χάριν, έχει προσδιοριστεί ότι πολλές Αφρικανικές χώρες χρησιμοποιούν παράνομους αριθμούς λογαριασμών από τις Ηνωμένες Πολιτείες, για να αγοράσουν αγαθά υψηλής αξίας μέσω του διαδικτύου που στη συνέχεια τα πουλούν για μετρητά.

8.8.3 Έρευνα στην Αυστραλία

Από το ινστιτούτο Internal Auditors της Αυστραλίας (τον Μάρτιο του 2003) προκύπτουν τα στοιχεία που παρουσιάζονται στο διάγραμμα που ακολουθεί, για τα γεγονότα που σχετίζονται με απάτες (fraud). Όπως μπορούμε να δούμε από το επόμενο διάγραμμα 8.3 επίσης οι απάτες αυξάνονται σχεδόν με σταθερό ρυθμό κάθε χρόνο (σε σχέση με το προηγούμενο έτος), που κυμαίνεται από 220% έως και 264% (ποσοστό μεταβολής το 1999 έναντι του 1998, που όπως δείχνει και το διάγραμμα 8.4 ήταν το μεγαλύτερο για το χρονικό διάστημα 1998-2001).



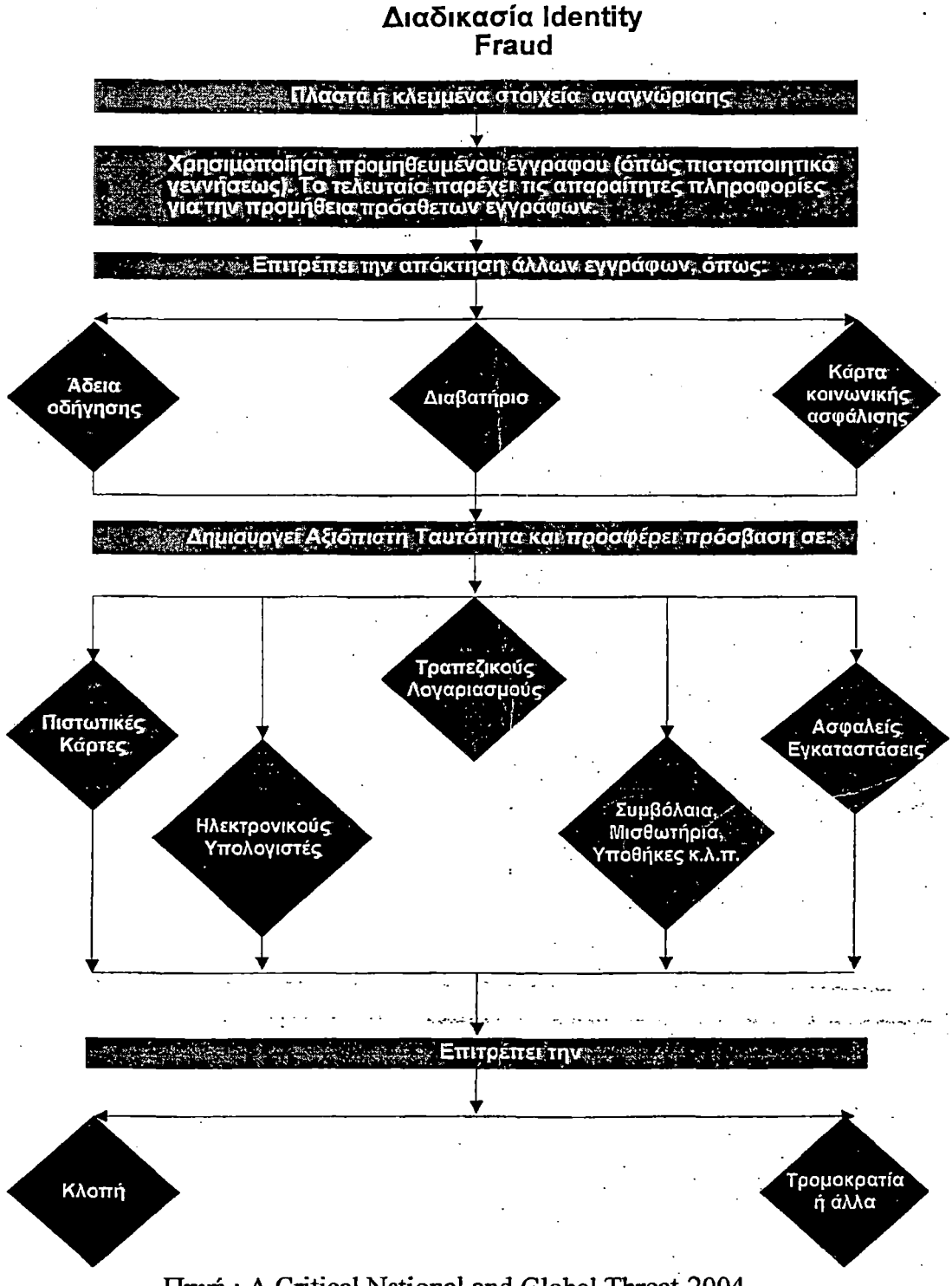
Πηγή: Institute of Internal Auditors Australia / Tasmania Police
Διάγραμμα 8.3



Πηγή: Institute of Internal Auditors Australia / Tasmania Police
Διάγραμμα 8.4

8.8.4 Διάγραμμα Διαδικασίας Κλοπή ταυτότητας (Identity theft)

Το διάγραμμα 8.5 που ακολουθεί απεικονίζει τον τρόπο με τον οποίο συνολικά πραγματοποιείται μια απάτη (**τύπου Identity theft**) από εγκληματίες ή τρομοκράτες, παρουσιάζοντας ολόκληρη τη διαδικασία, από την προμήθεια των πλαστών ή κλεμμένων εγγράφων – στοιχείων αναγνώρισης, ως το τελικό αποτέλεσμα από την πραγματοποίησή της.



Πηγή : A Critical National and Global Threat-2004.
Διάγραμμα 8.5

8.9 Απάτη με πιστωτικές κάρτες

Με το ηλεκτρονικό εμπόριο να έχει αποκτήσει σημαντική θέση και δύναμη στις εθνικές οικονομίες όλων σχεδόν των χωρών του κόσμου σήμερα, είναι φυσικό να προσφέρεται ως ένα νέο και προσοδοφόρο πεδίο δράσης για τους απανταχού εγκληματίες. Στις ΗΠΑ οι δέκα συχνότεροι τύποι απάτης

σχετίζονται με το ηλεκτρονικό εμπόριο (οι απάτες αυτές προκαλούν προβλήματα σε υπηρεσίες, εμπορεύματα, πωλήσεις, δημοπρασίες κ.λ.π.) και στην κορυφή όλων αυτών βρίσκεται αδιαφιλονίκητα πρώτη η απάτη με πιστωτικές κάρτες. Το ύψος της ζημίας σε δολάρια από αυτές τις απάτες στις ΗΠΑ ξεπερνά κατά πολύ το ποσό του μισού δισεκατομμυρίου, εφόσον το τελευταίο προέρχεται από την απάτη των καρτών και μόνο. Στο Ηνωμένο Βασίλειο το ύψος της οικονομικής ζημίας από απάτες με πιστωτικές κάρτες ξεπερνά το ποσό των 411 εκατομμυρίων λιρών για το 2001 όπως αναλυτικά παρουσιάζεται ανάλογα με τον τύπο της στον παρακάτω πίνακα 8.1

Εντυπωσιακά είναι τα στοιχεία της **VISA** για τις περιπτώσεις απάτης στην **Ελλάδα** με πιστωτικές κάρτες, που έχουν ως εξής:

- Το 16% αφορά περιπτώσεις με πλαστές κάρτες. Μεγάλο μέρος του ποσοστού αυτού σχετίζεται με αντιγραφές της μαγνητικής ταινίας που υπάρχει στο πίσω μέρος της πιστωτικής κάρτας.
- Το 39% αφορά συναλλαγές που έγιναν χωρίς την παρουσία του κατόχου της κάρτας. Πρόκειται για περιπτώσεις αγορών που κάνουν οι πελάτες των πιστωτικών καρτών, κατά τις οποίες δίνουν τον αριθμό της κάρτας τους είτε τηλεφωνικώς, είτε μέσω ταχυδρομείου, είτε μέσω Ίντερνετ.
- Το 13% αφορά συναλλαγές με κλεμμένες κάρτες.
- Το 12% αφορά συναλλαγές με χαμένες κάρτες (ο κάτοχος δεν κατάλαβε ότι την έχασε ή δεν ειδοποίησε εγκαίρως για την απώλεια ή δεν την μπλόκαρε κ.λ.π.).
- Το 20% αφορά διάφορες άλλες μη νόμιμες συναλλαγές. Για παράδειγμα, ο κάτοχος της κάρτας δεν πήγε εγκαίρως στο ταχυδρομείο να παραλάβει την κάρτα του, αλλά την πήρε και τη χρησιμοποίησε κάποιος άλλος.

Τα στοιχεία αυτά προκύπτουν για απάτες με πιστωτικές κάρτες που εκδόθηκαν από ελληνικές τράπεζες. Σύμφωνα με τη VISA, στην Ελλάδα οι περιπτώσεις απάτης με κάρτες είναι λιγότερες από εκείνες στο εξωτερικό. Πρόκειται για περιπτώσεις μη νόμιμης χρήσης πιστωτικής κάρτας τουριστών, επισκεπτών κ.λ.π. στην Ελλάδα. Από στοιχεία προκύπτει ότι οι περισσότερες περιπτώσεις αφορούν πιστωτικές κάρτες που εκδόθηκαν στην Αγγλία, τις ΗΠΑ, τον Καναδά, τη Γερμανία και τη Γαλλία.

8.9.1 Τύποι απάτης με πιστωτικές κάρτες

- Η εγκληματική χρήση των πιστωτικών καρτών μπορεί να διαιρεθεί στις ακόλουθες κατηγορίες:
- Πλαστή χρήση πιστωτικών καρτών (**Counterfeit**[5])
- Κάρτες που χάνονται ή που κλέβονται από τον κάτοχο κάρτας
- Απάτη που πραγματοποιείται χωρίς την πραγματική χρήση μιας κάρτας (**no-card fraud**)
- Απάτη που πραγματοποιείται στις κάρτες που δεν παραλαμβάνονται από το νόμιμο κάτοχο κάρτας (**non-receipt fraud**)

[5] **Counterfeit** - Διαδικασία όπου τα στοιχεία της μαγνητικής λωρίδας μιας πιστωτικής κάρτας, αντιγράφονται ηλεκτρονικά επάνω σε άλλη, χωρίς φυσικά να είναι ενήμερος ο νόμιμος κάτοχός της.

- Κάρτες που λαμβάνονται ψευδώς από τους εγκληματίες, που έχουν υποβάλει πλαστές αιτήσεις.

Απώλειες από απάτες (Fraud losses) στο Ηνωμένο Βασίλειο ανάλογα με τον τύπο απάτης (με πιστωτικές κάρτες)

	Σε εκατ. Λίρες Αγγλίας /2000	Σε εκατ. Λίρες Αγγλίας / 2001	% Ποσοστό Μεταβολής
Από πλαστές πιστωτικές κάρτες	107.1	160.3	50%
Από κλεμμένες ή χαμένες πιστωτικές κάρτες	101.9	114.0	12%
Από χρήση πιστωτικών καρτών χωρίς την παρουσία τους (μέσω mail, τηλεφώνων, Ίντερνετ)	72.9	95.7	31%
Από κλεμμένες κάρτες (μέσω ταχυδρομείου)	17.7	26.7	51%
Fraudulent applications	10.5	6.6	-37%
Άλλες Περιπτώσεις	6.9	8.0	15%
ΣΥΝΟΛΟ	**317.0**	**411.4**	**30%**
Απώλειες σε σχέση με τον κύκλο εργασιών (Fraud losses against turnover)	0.162	0.183	13%

Πηγή: Association for Payment Clearing Services (APACS)

Πίνακας 8.1

8.9.2 Νέο σύστημα πρόληψης απατών με πιστωτικές κάρτες

«Παγίδα» στις απάτες με πιστωτικές κάρτες βάζει ένα νέο ηλεκτρονικό σύστημα παρακολούθησης των συναλλαγών με κάρτες παγκοσμίως, το οποίο «υποψιάζεται» το ενδεχόμενο απάτης και σημαίνει συναγερμό στην τράπεζα.

Ήδη, το νέο σύστημα εγκαταστάθηκε στις τράπεζες **Εμπορική, Eurobank** και **Probank** από τη **Visa** και σύντομα θα εγκατασταθεί και στις υπόλοιπες τράπεζες. Το όνομα του νέου συστήματος είναι **VISOR** (Visa Intelligent Scoring of Risk). Ελέγχει διεξοδικά όλες τις συναλλαγές με κάρτες. Βαθμολογεί τις συναλλαγές ανάλογα με το ρίσκο, έχοντας υπόψη του την μέχρι σήμερα καταναλωτική συμπεριφορά του κατόχου της κάρτας και το είδος του εμπορικού καταστήματος. Σημειώνεται ότι το ποσοστό απάτης από κάρτες στην Ελλάδα είναι 0,035% των συναλλαγών, έναντι 0,06% που είναι στην Ευρώπη και 0,07% παγκοσμίως.

8.9.3 Η κατάσταση στην Ελλάδα

Αν και δεν υπάρχουν συγκεκριμένα στοιχεία εκτιμάται ότι το πρόβλημα των συναλλαγών με κλεμμένα στοιχεία πιστωτικών καρτών «**προς το παρόν**» δεν πρέπει να είναι ιδιαίτερα σημαντικό στη χώρα μας για τους ακόλουθους λόγους:

- Τα περισσότερα ηλεκτρονικά καταστήματα παρέχουν τις υπηρεσίες τους μόνο στην ελληνική γλώσσα. Έτσι, μπορούν να αποτελέσουν στόχο μόνο για όσους μιλούν ελληνικά δηλαδή για τους κατοίκους Ελλάδας και Κύπρου (όπου όμως βρίσκονται και τα ίδια τα καταστήματα, άρα η δίωξη είναι πιο εύκολη), καθώς και για τους Έλληνες του εξωτερικού (το υψηλό μορφωτικό και οικονομικό επίπεδο των οποίων όμως δεν ευνοεί την ευρεία εμφάνιση ανάλογων μορφών δράσης).
- Πολλά καταστήματα πωλούν εξειδικευμένα προϊόντα ελληνικού χαρακτήρα (π.χ. www.grproducts.gr), τα οποία σίγουρα δεν ενδιαφέρουν ιδιαίτερα τους διεθνείς "δικτυοαπατεώνες".
- Συνήθως, τα ελληνικά ηλεκτρονικά καταστήματα έχουν μικρό μέγεθος και δεν διαχειρίζονται αυτόματα δικτυακές συναλλαγές

Για τους παραπάνω λόγους οι υπεύθυνοι παρακολούθησης των διαδικτυακών παραγγελιών είναι αρκετά πιθανό να αναγνωρίσουν εύκολα, ότι υπάρχει κάτι περίεργο σε ορισμένες από αυτές.

8.10 Απάτες Δημοπρασιών μέσω διαδικτύου (Auctions Fraud)

Η επανάσταση και οι πρόοδοι που έχουν σημειωθεί τελευταία στις τεχνολογίες που αφορούν το διαδίκτυο, έχουν προκαλέσει μια ραγδαία αύξηση στις συναλλαγές του ηλεκτρονικού εμπορίου, οι οποίες αντιπροσωπεύουν ένα τα πιο εξελισσόμενα πεδία οικονομικής δραστηριότητας σε 24ωρη βάση, μέσω των 24άωρων on-line αγορών. Υπολογίζεται από σχετικές έρευνες ότι το 63% του πληθυσμού (που έχουν πρόσβαση στο διαδίκτυο) μέχρι τα τέλη του 2006 θα συμμετάσχουν ενεργά σε δραστηριότητες που αφορούν το ηλεκτρονικό εμπόριο. Επιπλέον, εκτιμάται ότι η συνολική αξία των συναλλαγών που σχετίζονται με το ηλεκτρονικό εμπόριο σε ολόκληρο τον κόσμο αναμένεται να εκτοξευτεί πάνω από το ποσό των 9 τρισεκατομμυρίων δολαρίων το 2005, έναντι των περίπου 3,8 τρισεκατομμύρια δολαρίων που ήταν το 2003.

Οι on-line δημοπρασίες αποτελούν ένα σημαντικό μερίδιο της αγοράς, που σχετίζεται με τις εμπορικές συναλλαγές του ηλεκτρονικού εμπορίου. Υπάρχουν περισσότερες από 200 on-line site δημοπρασιών σήμερα ανά τον κόσμο, όπως παραδείγματος χάριν είναι τα: eBay, Yahoo και Amazon. Αξίζει να σημειωθεί ότι στο σύνολο των παραπάνω sites πραγματοποιούνται πάνω από 1,3 εκατομμύρια συναλλαγές ημερησίως. Όπως ήταν αναμενόμενο και στον χώρο αυτό του διαδικτύου (από την πρώτη εμφάνισή τους το 1995), οι σε απευθείας σύνδεση δημοπρασίες (που έχουν επιταχύνει σημαντικά σήμερα το ρυθμό του Business-to-Consumer και Consumer-to-Consumer ηλεκτρονικού εμπορίου), λόγω του ότι στερούνται τη διαπροσωπική αλληλεπίδραση και δεδομένου ότι οι συναλλαγές μέσω αυτών ολοκληρώνονται on-line, ενέχουν πολλούς κινδύνους όσον αφορά στην ασφάλεια των πληρωμών, στη προστασία των δεδομένων και στις πιθανές απάτες.

Όσον αφορά τις τελευταίες, θα μπορούσαμε να τις κατατάξουμε στις εξής κατηγορίες (όσο αυτό είναι εφικτό):

- **Non-delivery**. Στις απάτες αυτού του τύπου ο πωλητής διαθέτει ένα προϊόν για πώληση που στην πραγματικότητα, δεν υπάρχει. Ως άμεση συνέπεια τούτου το προϊόν δεν παραδίδεται ποτέ στον αγοραστή, ο οποίος όμως το έχει ήδη αγοράσει.
- **Misrepresentation**. Εμφανίζεται όταν ο σκοπός του πωλητή είναι να εξαπατήσει τον αγοραστή, ως προς την αληθινή αξία ενός προϊόντος με την παράθεση ψεύτικων πληροφοριών ή τη χρησιμοποίηση πλαστών εικόνων του προϊόντος.
- **Non-payment**: Εμφανίζεται όταν ένας αγοραστής κερδίζει μια δημοπρασία έχοντας πραγματοποιήσει την υψηλότερη προσφορά, όμως καθώς το προϊόν παραδίδεται σε αυτόν δεν πληρώνει τον πωλητή του.
- **Triangulation**. Στην περίπτωση αυτή διαπλέκονται τρία συμβαλλόμενα μέρη: ο δράστης, ένας καταναλωτής, και ένας on-line έμπορος. Ο δράστης αγοράζει τα προϊόντα από έναν on-line έμπορο, χρησιμοποιώντας κλεμμένες ταυτότητες και αριθμούς πιστωτικών καρτών. Στη συνέχεια ο δράστης πωλεί τα προϊόντα σε on-line δικτυακούς τόπους δημοπρασιών στους ανυποψίαστους αγοραστές. Στη περίπτωση που ανακαλυφθεί η απάτη τα κλεμμένα προϊόντα κατάσχονται και ζημιώνονται προφανώς ο on-line έμπορος και οι αγοραστές.
- **Fee stacking**. Περιλαμβάνει την προσθήκη πρόσθετων (παράνομων) δαπανών στο προϊόν αντικείμενο μιας δημοπρασίας αφότου η τελευταία έχει ολοκληρωθεί επιτυχώς και από τα δυο συμβαλλόμενα μέρη (πωλητής, αγοραστής), με σκοπό να ληφθούν περισσότερα χρήματα. Παραδείγματος χάριν αντί ενός προκαθορισμένου ποσοστού για τα ταχυδρομικά τέλη μόνο, ο πωλητής προσθέτει χωριστές δαπάνες εξαπατώντας τον αγοραστή ο οποίος πληρώνει τελικά περισσότερο από το προσδοκώμενο.
- **Black-market goods**. Στη περίπτωση αυτή μέσω των δημοπρασιών πωλούνται προϊόντα λογισμικού τα οποία έχουν αντιγραφτεί όπως: λειτουργικά συστήματα, MP3, CD μουσικής, DIVX κινηματογραφικών ταινιών, προγράμματα, παιχνίδια κ.λ.π. Για την αποτελεσματική αντιμετώπιση φαινομένων παράνομης πώλησης λογισμικού οι περισσότεροι δικτυακοί τόποι δημοπρασιών, εφαρμόζουν πολιτικές αναστολής των λογαριασμών των χρηστών τους που συμμετέχουν σε τέτοιου είδους δημοπρασίες.
- **Multiple bidding και Shill bidding**: Με την μέθοδο αυτή ο αγοραστής προσπαθεί να εξαπατήσει έναν ή περισσότερους άλλους αγοραστές προκαλώντας ψευδείς εντυπώσεις, σχετικά με ένα διαθέσιμο προϊόν. Ο τελευταίος για να επιτύχει τον στόχο του χρησιμοποιεί πολλούς λογαριασμούς (ή φίλους του), τους οποίους και χρησιμοποιεί ο ίδιος για τη δημιουργία πολλαπλών προσφορών που αφορούν το εν λόγω προϊόν. Οι προσφορές αυτές διαμορφώνουν αρχικά την τιμή σε υψηλά επίπεδα, για τον εκφοβισμό των άλλων αγοραστών. Λίγο πριν το τέλος όμως της δημοπρασίας ο ίδιος αγοραστής (χρησιμοποιώντας τους

παραπάνω λογαριασμούς του), αποσύρει τις υψηλές προσφορές τους, για να αγοράσει τελικά το προϊόν με τη χαμηλότερη προσφορά.

Αν και οι περισσότερες από τις παραπάνω απάτες μπορούν να αποτραπούν από τους δικτυακούς τόπους δημοπρασιών, με την εφαρμογή και υλοποίηση κατάλληλων πολιτικών και μέτρων για την αποτροπή τους, οι περιπτώσεις της μη παράδοσης, παράδοσης ελαττωματικών αγαθών ή των καθυστερημένων παραδόσεων προϊόντων και της αποτυχίας αποκάλυψης όλων των σχετικών πληροφοριών με αυτές, αποτελεί μια αδυναμία των δημοπρασιών και ένα σημαντικό πλήγμα για το ηλεκτρονικό εμπόριο.

8.11 Ξέπλυμα χρημάτων μέσω διαδικτύου (Money Laundering)

Στο διαδίκτυο σήμερα ανθεί η παραοικονομία (όσο παράδοξο και εάν φαίνεται εκ πρώτης άποψης) και ταυτόχρονα το τελευταίο αποτελεί έναν από τους πιο διαδεδομένους και σίγουρους τρόπους, για το ξέπλυμα μαύρου χρήματος. Το διαδίκτυο άρχισε να κεντρίζει το ενδιαφέρον των απανταχού εγκληματιών, από τη στιγμή που πολλές τράπεζες διεθνώς εισήγαγαν τις υπηρεσίες τους σε αυτό ή έγιναν εξ ολοκλήρου on-line (όπως συμβαίνει και στη χώρα μας με τις περισσότερες τράπεζες). Μέσω αυτών των προσφερόμενων τραπεζικών δικτυακών υπηρεσιών, ο οποιοσδήποτε σήμερα (πόσο μάλιστα οι εγκληματίες) έχει τη δυνατότητα δημιουργίας ενός ή περισσοτέρων λογαριασμών, χωρίς να είναι υποχρεωμένος να έχει οποιαδήποτε επαφή με κάποιον εκπρόσωπο της τράπεζας. Το μόνο που χρειάζεται κάποιος για την δημιουργία αυτών των λογαριασμών είναι ένας απλός υπολογιστής ή ένα κινητό τηλέφωνο. Με αυτό τον τρόπο οι εγκληματίες βασικά εξασφαλίζουν τα εξής:

- Ανωνυμία κατά τη δημιουργία λογαριασμών,
- Ταχύτητα στις οποιεσδήποτε συναλλαγές,
- Μεταφορά μαύρου χρήματος (αρχικά ένα μεγάλο αρχικό ποσό διασπάται σε μικρότερα ποσά, τα οποία με τη σειρά τους διανέμονται- καταθέτονται στους παραπάνω τραπεζικούς λογαριασμούς)

Όπως αναφέρθηκε και στις προηγούμενες παραγράφους του παρόντος κειμένου ο κύριος στόχος ενός μεγάλου αριθμού εγκληματικών πράξεων (όπως identity theft, credit card fraud καθώς και άλλες), είναι το οικονομικό όφελος για ένα άτομο ή την ομάδα, που πραγματοποιεί την εγκληματική πράξη (εις). Στη περίπτωση που μας αφορά, του παράνομου ξεπλύματος χρημάτων (δηλαδή την επεξεργασία κερδών από παράνομες δραστηριότητες και την μετατροπή τους σε νόμιμων), απαιτούνται μια σειρά από διαδικασίες εκ μέρους των εγκληματιών, ώστε οι τελευταίοι να μπορούν να χρησιμοποιήσουν αυτά τα κέρδη νόμιμα, αλλά και να εμποδίσουν την αποκάλυψη της πηγής προέλευσής τους. Οι διαδικασίες αυτές βρίσκουν εύκολα εφαρμογή σήμερα με την χρήση του διαδικτύου, το οποίο χρησιμοποιείται αφειδώς από τους εγκληματίες (μεγαλέμπορους ναρκωτικών, εμπόρους όπλων, κυκλωμάτων πορνείας κ.ο.κ.), για την πραγματοποίηση και συγκάλυψη των παράνομων δραστηριοτήτων τους.

Για την σύλληψη των οικονομικών μεγεθών που αφορούν το ξέπλυμα μαύρου χρήματος, ενδεικτικά αναφέρουμε αποτελέσματα προερχόμενα από έρευνες

του Διεθνές Νομισματικού Ταμείου, το οποίο έχει δηλώσει ότι το συνολικό μέγεθος του ξεπλύματος χρημάτων στον κόσμο εκτιμάται να είναι κάπου μεταξύ 2 και 5% τοις εκατό του παγκόσμιου ακαθάριστου εγχώριου προϊόντος. Χρησιμοποιώντας τις στατιστικές του 1996, αυτά τα ποσοστά δείχνουν ότι το ξέπλυμα χρημάτων κυμαίνεται προσεγγιστικά διεθνώς, μεταξύ των 590 δισεκατομμυρίων και 1,5 τρισεκατομμυρίων δολαρίων. Το μέγεθος της μικρότερης εκτίμησης από τα παραπάνω ποσά από μόνο του είναι αρκετά εντυπωσιακό, εάν σκεφτεί κανείς αυτό ότι αυτό είναι κατά προσέγγιση ισοδύναμο με την αξία της συνολικής εγχώριας παραγωγής μιας οικονομίας, που αντιστοιχεί στο μέγεθος της Ισπανίας.

Η Ευρωπαϊκή Επιτροπή εξέδωσε πρόσφατα ανακοίνωση (22/04/2004) σχετικά με την καταπολέμηση του οικονομικού εγκλήματος στην ΕΕ. Στην ανακοίνωση αυτή, γίνεται ανασκόπηση των μέτρων που έχουν ήδη ληφθεί και παρουσιάζονται τα νέα μέτρα που στοχεύουν κυρίως στην παρεμπόδιση των εγκληματιών να νομιμοποιούν τα έσοδα από παράνομες δραστηριότητες («ξέπλυμα χρήματος»). Ιδιαίτερη έμφαση δίνεται στην ενίσχυση των μηχανισμών εντοπισμού, κατάσχεσης και δήμευσης των προϊόντων του εγκλήματος, καθώς και των μεθόδων έρευνας του οικονομικού εγκλήματος.

Ο αρμόδιος για τη δικαιοσύνη και τις εσωτερικές υποθέσεις Επίτροπος, **Antonio Vitorino** δήλωσε σχετικά: «***Το οργανωμένο οικονομικό έγκλημα βλάπτει τους νομοταγείς παράγοντες της οικονομίας και ενισχύει την παραοικονομία, με αποτέλεσμα να αποδυναμώνονται η οικονομική ανάπτυξη και οι κρατικοί πόροι. Συνεπώς, η καταπολέμηση του οργανωμένου εγκλήματος πρέπει να αποτελεί κορυφαία πολιτική προτεραιότητα της ΕΕ κατά τα επόμενα χρόνια***». Ο αρμόδιος για την εσωτερική αγορά Επίτροπος, **Frits Bolkestein** πρόσθεσε: «***Το οικονομικό έγκλημα αποτελεί παγκόσμιο φαινόμενο. Δεν σταματά στα σύνορα και, αν υπάρχουν αδύναμοι κρίκοι, οι οργανωμένοι κακοποιοί θα τους αξιοποιήσουν. Με το σχέδιο δράσης για τις χρηματοπιστωτικές υπηρεσίες, ενισχύουμε το κανονιστικό πλαίσιο της Ευρώπης, ούτως ώστε να μπορεί να αμυνθεί έναντι αυτών που προσπαθούν να υπονομεύσουν τις επενδυτικές της δραστηριότητες***».

Ωστόσο, χρειαζόμαστε ένα αποτελεσματικό σύστημα καταπολέμησης του οργανωμένου εγκλήματος σε ευρωπαϊκό και διεθνές επίπεδο, περιλαμβανομένης της θέσπισης της κατάλληλης νομοθεσίας για την καταπολέμηση του ξεπλύματος χρήματος στο πλαίσιο ενός ολοένα και πιο εξελιγμένου διεθνούς χρηματοοικονομικού συστήματος».

Η παραπάνω ανακοίνωση της Ευρωπαϊκής Επιτροπής επικεντρώνεται στην πρόληψη και την πάταξη του ξεπλύματος του χρήματος, λαμβάνοντας υπόψη ότι οι μέθοδοι που χρησιμοποιούνται για τη νομιμοποίηση εσόδων από παράνομες ή εγκληματικές δραστηριότητες είναι ολοένα και πιο εξελιγμένες. Στην ανακοίνωση τονίζεται επίσης η ανάγκη εφαρμογής αποτελεσματικών μηχανισμών εντοπισμού και δήμευσης των προϊόντων εγκληματικών πράξεων, καθώς και ενίσχυσης της συνεργασίας μεταξύ του δημοσίου και του ιδιωτικού τομέα στην προσπάθεια καταπολέμησης των εγκληματικών πράξεων αυτού

του είδους. Η ανακοίνωση προβάλλει επίσης την ανάγκη βελτίωσης της διαφάνειας του χρηματοοικονομικού συστήματος, ως καθοριστικό στοιχείο στην προσπάθεια περιορισμού των δυνατοτήτων διάπραξης οργανωμένου οικονομικού εγκλήματος. Από την άποψη αυτή, τονίζεται η σκοπιμότητα ανάπτυξης, σε εθνικό και ευρωπαϊκό επίπεδο, των κατάλληλων τεχνικών έρευνας του οικονομικού εγκλήματος. Με τον τρόπο αυτό θα διευκολυνθεί η συγκέντρωση απόρρητων πληροφοριών σχετικά με τη συμπεριφορά υπόπτων, καθώς και ο εντοπισμός και η κατάσχεση των προϊόντων εγκληματικών πράξεων.

Η σπουδαιότητα της καταπολέμησης του οργανωμένου οικονομικού εγκλήματος υπερβαίνει σε εμβέλεια τα μεμονωμένα αδικήματα αυτά καθαυτά, υπό την έννοια ότι, σε περίπτωση που επιτύχει, καταπολεμά τη ρίζα των δικτύων οργανωμένου εγκλήματος, δηλαδή τη μεγιστοποίηση του κέρδους με αθέμιτα μέσα. Η αφαίρεση από τους οργανωμένους κακοποιούς της δυνατότητας να νομιμοποιούν έσοδα από παράνομες δραστηριότητες («ξέπλυμα χρήματος») ή να χρηματοδοτούν εγκληματικές δραστηριότητες αποδυναμώνει σε μεγάλο βαθμό τα κίνητρά τους και την ικανότητά τους να δρουν. Επίσης, είναι αναγκαία η διασφάλιση της ύπαρξης οργάνων επιβολής το νόμου που θα διαθέτουν τις κατάλληλες ικανότητες και γνώσεις για την αντιμετώπιση του οργανωμένου εγκλήματος σε επίπεδο ΕΕ.

8.12 Η πειρατεία στη μουσική

Στο χώρο της μουσικής βιομηχανίας σαν πειρατεία ορίζεται η παράνομη αντιγραφή και διάθεση μουσικών έργων. Σύμφωνα με τα στοιχεία της Ε.Ε.Π.Η / IFPI, τα πειρατικά δισκογραφικά προϊόντα ανάλογα με το περιεχόμενό τους κατατάσσονται σε τρεις κατηγορίες:

- **Πειρατικά**: Αφορά την αναπαραγωγή πρωτότυπου ηχογραφήματος με σκοπό το κέρδος, χωρίς τη συγκατάθεση του δικαιούχου. Η συσκευασία των πειρατικών αντιτύπων διαφέρει από αυτή των γνήσιων. Συνήθως πρόκειται για συλλογές τραγουδιών ενός καλλιτέχνη ή συγκροτήματος (π.χ. "greatest hits") ή συλλογές με τραγούδια συγκεκριμένου είδους (π.χ. "dance tracks").
- **Παραχαραγμένα δισκογραφικά προϊόντα**: Πρόκειται για αντίγραφα συσκευασμένα κατά τρόπο ώστε να μοιάζουν όσο το δυνατόν περισσότερο με τα γνήσια. Τα λογότυπα και τα εμπορικά σήματα των παραγωγών εταιριών τοποθετούνται στη συσκευασία, έτσι ώστε ο αγοραστής να παραπλανάται από τον πωλητή και να νομίζει ότι αγοράζει το γνήσιο και νόμιμο προϊόν.
- **Bootlegs**: Αναφέρεται σε παράνομες ηχογραφήσεις χωρίς τη σχετική άδεια των δικαιούχων ζωντανών εκτελέσεων ραδιοτηλεοπτικού ή άλλου προγράμματος.

Η πειρατεία αποτελεί τη μεγαλύτερη απειλή που αντιμετωπίζει ο κλάδος της δισκογραφίας σε όλο τον κόσμο σήμερα. Η σημαντική πτώση των πωλήσεων των δισκογραφικών εταιριών διεθνώς, αλλά και όλων των επιχειρηματικών φορέων που ασχολούνται με την εμπορία μουσικών CD, οφείλεται κατά κύριο λόγο στη δράση της πειρατείας. Η Ε.Ε.Π.Η / IFPI αλλά και η διεθνής βιομηχανία ηχογραφημάτων προσπαθούν συνεχώς μέσα από μια σειρά

ενεργειών να καταπολεμήσουν το συγκεκριμένο πρόβλημα απώλειας πωλήσεων , το οποίο υπολογίζεται ότι ανέρχεται ετησίως σε 4.3 δισ. Δολάρια σε παγκόσμια βάση.

Από την πειρατεία δεν πλήττονται μόνο οι καλλιτέχνες και οι δισκογραφικές εταιρίες, που χάνουν σημαντικά έσοδα, τα οποία καρπώνονται τα παράνομα κυκλώματα διανομής πειρατικών CD με ελάχιστο κόστος, αλλά ζημιώνεται και το κράτος από διαφυγόντα έσοδα φορολογίας. Επίσης, οι καταναλωτές χάνουν σε θέματα ποιότητας, συχνά είναι δε τα φαινόμενα πειρατικών προϊόντων που δεν "παίζουν" στα CD players.
Τα τελευταία χρόνια η πειρατεία της μουσικής έχει εξαπλωθεί και στο Internet. Η διάδοση της πειρατείας μέσω του internet διευκολύνθηκε α) από την ανακάλυψη νέων τρόπων συμπίεσης και διαχείρισης ψηφιακών δεδομένων και β) από την αύξηση της διαθέσιμης ταχύτητας μεταφοράς δεδομένων στο διαδίκτυο.
Υπάρχουν δύο τρόποι με τους οποίους διατίθενται μουσικά κομμάτια μέσω του Internet:

- **Downloads**: Η συγκεκριμένη κατηγορία αναφέρεται στη διάθεση των τραγουδιών υπό τη μορφή αρχείων ηλεκτρονικού υπολογιστή (π.χ. mp3, wma κλπ), τα οποία μπορούν να αποθηκευθούν στο σκληρό δίσκο του υπολογιστή, σε CD ή δισκέτες. Ο αποδέκτης μπορεί να επιλέξει και να ακούσει μουσικά κομμάτια οποιαδήποτε στιγμή με τη χρήση του κατάλληλου λογισμικού και μηχανήματος.
- **Streaming audio**: Αφορά τη διαδικτυακή έκδοση του ραδιοφώνου, όπου ο χρήστης μπορεί να ακούσει τα τραγούδια, μόνο όταν είναι συνδεδεμένος στο internet. Η δυνατότητα αποθήκευσης του τραγουδιού δεν είναι εφικτή. Η ποιότητα του ήχου είναι σκόπιμα μειωμένη, ώστε το αρχείο να καταλαμβάνει μικρότερη έκταση αποθηκευμένης μνήμης και να είναι δυνατή η ταχύτερη μεταφορά των κατάλληλων πληροφοριών και η on-line ακρόαση του τραγουδιού.

Η γνωστότερη μορφή ηλεκτρονικής μουσικής πειρατείας, σύμφωνα με τα στοιχεία της **IFPI** είναι η συμπίεση των τραγουδιών σε αρχεία μορφής **MP3** και η διάθεσή τους μέσω του internet, χωρίς την πληρωμή των δικαιωμάτων εκμετάλλευσης στους δημιουργούς.
Εξετάζοντας την παγκόσμια μουσική πειρατεία ανά είδος (CD, CD-R και κασέτες), σύμφωνα με τα στοιχεία της Διεθνούς οργάνωσης IFPI, οι πωλήσεις των πειρατικών CD ανήλθαν σε 500 εκ. τεμάχια το 2001 από 475 εκ. το 2000. Περίπου 450 εκ. τεμάχια πειρατικά CD-R πουλήθηκαν το 2001 από 165 εκ. το 2000. Επίσης εκτιμάται ότι οι πωλήσεις των πειρατικών κασετών μειώθηκαν το 2001 και διαμορφώθηκαν στα 900 εκ. τεμάχια από 1,2 δισ. τεμάχια το 2000. Για την καλύτερη κατανόηση των παραπάνω στοιχείων σημειώνεται ότι ο όρος CD αναφέρεται στους οπτικούς δίσκους που κατασκευάζονται από εργοστάσια, με τη χρήση ειδικών μηχανημάτων μαζικής παραγωγής, ενώ τα CD-R είναι οι οπτικοί δίσκοι που κατασκευάζονται για χρήση από ηλεκτρονικό υπολογιστή. Η ανάπτυξη των CD-R το 2001 οφείλεται κυρίως στο γεγονός ότι το αντίστοιχο μηχάνημα αντιγραφής (burner) είναι αρκετά φθηνό και διαδεδομένο παγκοσμίως. Επιπλέον, η αντιγραφή μουσικών

αρχείων γίνεται σχετικά γρήγορα. Η παραγωγή των CD-R είναι μικρότερης κλίμακας, απαιτεί μικρότερη επένδυση και συνήθως έχει τοπικό χαρακτήρα, δηλαδή η παραγωγή των CD-R και η διάθεσή τους περιορίζεται στα πλαίσια μιας πόλης ή μιας χώρας. Οι προαναφερθέντες παράγοντες αλλά και η διάδοση των προσωπικών ηλεκτρονικών υπολογιστών στο ευρύ κοινό, διευκόλυναν την ανάπτυξη των συγκεκριμένων πειρατικών προϊόντων. Σύμφωνα με δημοσιεύματα της Ε.Ε.Π.Η., τα CD-R αποτελούν το 80% των παράνομων μουσικών προϊόντων στην Ελλάδα και ακολουθούν τα CD και οι κασέτες με 15% και 5% αντίστοιχα.

Στην Ελλάδα η πειρατεία διώκεται σύμφωνα με τον προαναφερθέντα Νόμο 2121/93 περί Προστασίας Πνευματικής Ιδιοκτησίας. Περαιτέρω, το Τμήμα Δίωξης Πειρατείας της Ε.Ε.Π.Η έχει αναλάβει ορισμένες δραστηριότητες στην προσπάθεια πάταξης αυτού του φαινομένου. Το συγκεκριμένο τμήμα ενημερώνει το κοινό για τα προβλήματα και τις επιπτώσεις της μουσικής πειρατείας. Επιπλέον, παρέχει πληροφορίες αλλά και δέχεται καταγγελίες για παράνομες ενέργειες, ενώ παράλληλα επιτελεί επικουρικό έργο στις αρμόδιες Αστυνομικές και Δικαστικές Αρχές με την παροχή εκθέσεων πραγματογνωμοσύνης και την υποβολή μηνύσεων.
Για την καταπολέμηση της ηλεκτρονικής πειρατείας (μέσω internet), η Ε.Ε.Π.Η ακολουθεί τις παρακάτω διαδικασίες.

- Ειδοποιήσεις προς τους **service providers** του internet, ζητώντας τους να "κλείσουν" τις παράνομες ιστοσελίδες.
- Αστικά και ποινικά μέτρα κατά των **service providers** που αρνούνται να συμμορφωθούν με τις ειδοποιήσεις.
- Αστικά και ποινικά μέτρα κατά των ιδιοκτητών των σελίδων, στις περιπτώσεις που μπορούν να **εντοπιστούν**.
- Αστικά και ποινικά μέτρα κατά των συνεργών των παραβατών, π.χ. όποιων προσφέρουν links προς δικτυακούς τόπους με παράνομα αρχεία, ή κατά των υπευθύνων μηχανών ανεύρεσης (**search engines**) που παρέχουν τη δυνατότητα εντοπισμού τέτοιων αρχείων.

Επίσης, η Ε.Ε.Π.Η σε συνεργασία με άλλους οργανισμούς διαχείρισης δικαιωμάτων επενδύει στην ανάπτυξη λογισμικού, το οποίο να είναι ικανό να ανιχνεύει με αυτοματοποιημένες διαδικασίες το σύνολο του διαδικτύου. Το λογισμικό αυτό εντοπίζει τις ιστοσελίδες με παράνομο περιεχόμενο, έτσι ώστε να απαιτείται λιγότερος χρόνος από το ανθρώπινο δυναμικό της IFPI και να μπορεί αυτό να ασχοληθεί αποτελεσματικότερα με τις νομικές ενέργειες κατά των παραβατών.
Οι δισκογραφικές εταιρίες ενσωματώνουν στα μουσικά CD διάφορους μηχανισμούς προστασίας οι οποίοι, ενώ επιτρέπουν την αναπαραγωγή τους σε ένα κανονικό CD-Player, καθιστούν αδύνατη την ακρόαση του ίδιου CD από ηλεκτρονικό υπολογιστή. Με αυτό το τρόπο οι εταιρίες αφενός εμποδίζουν την αντιγραφή των μουσικών CD από ένα CD-R και αφετέρου αποτρέπουν την ψηφιακή μετατροπή των τραγουδιών σε MP3 και την επακόλουθη διακίνησή τους μέσω του διαδικτύου. Εντούτοις, εκφράζονται ορισμένες απόψεις που αμφισβητούν ότι η συγκεκριμένη μέθοδος είναι αποτελεσματική και ισχυρίζονται ότι υπάρχουν τρόποι με τους οποίους οι παραπάνω μηχανισμοί προστασίας μπορούν να εξουδετερωθούν.

8.13 Παραδείγματα σχετικά με οικονομικά – ηλεκτρονικά εγκλήματα

Παράδειγμα -1 (Προσωπικά στοιχεία και κλοπή ταυτότητας)

1. Τεχνικές λεπτομέρειες (βασικά χαρακτηριστικά της απάτης του παραδείγματος)

- Δεν πραγματοποιήθηκε καμία παραβίαση σε οποιοδήποτε πληροφοριακό σύστημα του οργανισμού, από έναν άγνωστο χάκερ
- Δεν απαιτήθηκε ιδιαίτερη τεχνική δεξιότητα εκ μέρους του δράστη
- Η απάτη δεν οφείλεται σε αμέλεια εκ μέρους των θυμάτων
- Απαιτήθηκε η συμμετοχή συνεργάτη που δεν ανήκε στον οργανισμό

Ένας υπάλληλος (Philip Cummings) που εργαζόταν ως εξωτερικός συνεργάτης σε μια επιχείρηση, η οποία παρείχε (μέσω σύμβασης) σε τράπεζες προγράμματα υπολογιστών για την παρακολούθηση και καταχώρηση του ιστορικού των πιστωτικών καρτών, απόκτησε πρόσβαση σε στοιχεία πολλών από αυτές. Χρησιμοποιώντας κωδικούς που ανήκαν σε άλλη (πιστωτική) επιχείρηση (Ford MotorCredit), αλλά και άλλους κωδικούς που ανήκουν σε διάφορες άλλες επιχειρήσεις, ήταν σε θέση να έχει πρόσβαση στις βάσεις δεδομένων (με τα στοιχεία των πιστωτικών καρτών). Χρησιμοποιώντας αυτές τις βάσεις δεδομένων αντέγραφε τα προσωπικά στοιχεία χιλιάδων ανθρώπων και στη συνέχεια τα μεταπωλούσε σε ειδικευμένους απατεώνες, για 30 έως 60 δολάρια. Η παραπάνω διαδικασία αποδείχτηκε στη συνέχεια ότι, πραγματοποιούνταν για σχεδόν δυο ολόκληρα χρόνια και ο εν λόγω υπάλληλος ανήκε σε μια μεγαλύτερη οργανωμένη ομάδα.

2. Συνέπειες

Οι συνέπειες από την παραπάνω απάτη εις βάρος χιλιάδων κατόχων πιστωτικών καρτών, θα μπορούσε να επικεντρωθεί στα παρακάτω σημεία:

- Παράνομη χρήση των προσωπικών στοιχείων πιστωτικών καρτών χιλιάδων ανθρώπων (30.000)
- Παραβίαση τραπεζικών λογαριασμών
- Αναρμόδια χρήση πιστωτικών καρτών
- Αναρμόδια παραγγελία νέων πιστωτικών καρτών
- Αναρμόδιο άνοιγμα γραμμών πίστωσης (opening of lines of credit)
- Αναρμόδιες αποσύρσεις μετρητών από τους απατεώνες (2.7 εκατ. Δολάρια)
- Αναρμόδιες αλλαγές διευθύνσεων.
- Αναρμόδια πρόσβαση σε προσωπικά στοιχεία
- Αποκάλυψη προσωπικών στοιχείων
- Αναρμόδια λήψη προσωπικών πληροφοριών για παράνομη χρήση τους
- Οικονομική απάτη
- Κλοπή ταυτότητας.

Παράδειγμα -2 (Εκβιασμός)

(Αύγουστος 2002 – ΙΑΠΩΝΙΑ). Η ιαπωνική επιχείρηση **Fujitsu** παραδέχθηκε δημοσίως ότι έπεσε θύμα εκβιασμού. Εμπιστευτικά στοιχεία που αναφέρονταν

σε ένα σύστημα για την άμυνα υπολογιστών, έπεσαν στα χέρια ενός προγραμματιστή με τον οποίο συνεργάζονταν η **Fujitsu**. Η απόδειξη για την απόκτηση αυτών των πληροφοριών χορηγήθηκε από τον ίδιο τον εκβιαστή στην Fujitsu, σε ένα έγγραφο 10-σελίδων που περιείχε τις πληροφορίες για τον τρόπο με τον οποίο συνδέονταν οι υπολογιστές του συστήματος «**Ground Self Defense Force**», καθώς επίσης και άλλες λεπτομερείς πληροφορίες για αυτό, που διακύβευαν την ασφάλειά του. Η απειλή εκ μέρους του εκβιαστή ήταν, ότι οι παραπάνω πληροφορίες θα πωλούνταν στη βόρεια Κορέα. Η εταιρεία Fujitsu δεν ενέδωσε στον εκβιασμό, ενημέρωσε την αστυνομία και τελικά υπέβαλε και τις σχετικές μηνύσεις για τον αποπειραθέντα εκβιασμό.

Παράδειγμα -3 (Εκβιασμός)

(Οκτώβριος 2002: Ρουμανία – ΗΠΑ). Στη Ρουμανία, ένας νεαρός ονόματι Nicolae Mircea Harapu, καταδικάστηκε σε φυλάκιση τριών ετών για τη παραβίαση ηλεκτρονικών υπολογιστών μιας αμερικανικής επιχείρησης (**Zwirl.com**). Τα στοιχεία πελατών που κλάπηκαν από τον νεαρό περιλαμβάνανε κυρίως αριθμούς πιστωτικών καρτών. Για την επιστροφή τους και τη μη δημοσίευση των στοιχείων, ο νεαρός απαίτησε το ποσό των 5.000 δολαρίων. Ο νεαρός χάκερ έδωσε το όνομα μιας τράπεζας στην οποία η επιχείρηση θα μπορούσε να στείλει μια πληρωμή 500 δολαρίων. Στη συνέχεια έστειλε έναν φίλο του για να εισπράξει το ποσό, όμως σε μια κοινή και καλά οργανωμένη επιχείρηση του FBI και της Ρουμανικής αστυνομίας συνελήφθηκε τόσο ο νεαρός χάκερ όσο και ο φίλος του.

Παράδειγμα -3 (Hacking & Εκβιασμός)

(Μάιος 2002: η υπόθεση Bloomberg – Kazakhstan-USA-GB). Οι Oleg Zevov και Igor Yarimaka εκδόθηκαν στις ΗΠΑ, υπεύθυνοι για hacking και εκβιασμό. Το 2000, τα δύο παραπάνω άτομα παραβίασαν ηλεκτρονικούς υπολογιστές της εταιρείας Bloomberg. Μετά από αυτό ο Zevov ήρθε σε επαφή με την Bloomberg μέσω ηλεκτρονικού ταχυδρομείου και απαίτησε 200.000 δολάρια, με αντάλλαγμα να δώσει λεπτομέρειες σχετικά με τη μέθοδο που χρησιμοποίησαν για την διείσδυσή τους στους υπολογιστές της εταιρείας. Ο Zvevov ήταν υπάλληλος μιας εταιρείας (Kazcommerts) από το Καζακστάν, που είχε σύμβαση με την εταιρία Bloomberg. Η εταιρεία Bloomberg άνοιξε έναν τραπεζικό λογαριασμό στο Λονδίνο στον οποίο και κατέθεσε τα 200.000 δολάρια. Οι δύο χάκερ ταξίδεψαν στη συνέχεια στο Λονδίνο για να συναντηθούν με εκπροσώπους της Bloomberg. Η εταιρεία όμως είχε έρθει σε επαφή με το FBI, το οποίο συνέλαβε τους ενόχους. Τα δύο άτομα εκδόθηκαν στη συνέχεια από την Αγγλία όπου και στη συνέχεια καταδικάστηκαν στις ΗΠΑ.

Παράδειγμα -4 (Hacking & Skimming & Pin Numbers)

Το συγκεκριμένο παράδειγμα δείχνει ότι το οργανωμένο έγκλημα έχει ενεργή παρουσία στην Ευρωπαϊκή Ένωση: Τον Σεπτέμβριο του 2002, διάφοροι Βούλγαροι συνελήφθηκαν στην περιοχή της Λυών για την κατασκευή πλαστών πιστωτικών καρτών σε συνεργασία με άλλους συνεργάτες τους στην

Βουλγαρία. Τα στοιχεία τα οποία χρησιμοποιούσαν για την κατασκευή των πλαστών πιστωτικών καρτών, είχαν κλαπεί από ATMS με την παράνομη παρακολούθηση πελατών Τραπεζών. Παρόμοια υπόθεση εξιχνιάστηκε από την Αστυνομική Διεύθυνσης Θεσσαλονίκης τον Μάιο του 2004 με εμπνευστές και αυτουργούς Βούλγαρους

9 Νομοθεσία – Νομολογία - Συνθήκες

9.1 Εισαγωγή

Η αντιμετώπιση των κοινών εγκλημάτων όσο και εκείνων που συνδέονται με το διαδίκτυο (με τη χρήση υπολογιστών), δεν αποτελεί μόνο έργο και ευθύνη των αστυνομικών αρχών, αλλά και της κοινωνίας μέσα στην οποία το έγκλημα αναπτύσσεται. Ο αγώνας κατά του εγκλήματος είναι έργο και υπόθεση όλων και ειδικότερα της Δικαιοσύνης που με την εκάστοτε Νομοθεσία προσπαθεί να αντιμετωπίσει τη λαίλαπα όλων των τύπων εγκλημάτων, που χαρακτηρίζει την εποχή μας. Η όποια επιτυχία ή αποτυχία εξαρτάται σημαντικά από το βαθμό προσαρμοστικότητας της Δικαιοσύνης στην παγκοσμιοποίηση του σύγχρονου εγκλήματος.

Ενώ στη περίπτωση αντιμετώπισης των κοινών εγκλημάτων, τόσο στην *Ελληνική Νομοθεσία* όσο και στη *Ευρωπαϊκή* έχουν γίνει σημαντικά βήματα τα τελευταία χρόνια, δε μπορεί κάποιος να ισχυριστεί ότι έχει γίνει το ίδιο και στα θέματα που αφορούν τα ηλεκτρονικά εγκλήματα. Σε αυτήν την παγιωμένη κατάσταση της μη έγκαιρης υιοθέτησης, εναρμόνισης και προσαρμογής της *Ελληνικής και Ευρωπαϊκής Νομοθεσίας* έναντι των *cyber και computer crimes*, συντελούν ένα πλήθος ανασταλτικών παραγόντων, αποτέλεσμα της πολυπλοκότητάς τους. Ενδεικτικά θα μπορούσαμε να αναφέρουμε τους παρακάτω παράγοντες, που στοιχειοθετούν την παγίωση αυτής της κατάστασης:

- Η βελτιστοποίηση των νομικών θεμάτων που αφορούν το διαδίκτυο ή κυβερνοχώρο ενέχει τη δυσκολία ότι προϋποθέτει όχι μόνο τη χρήση νομικών αλλά και τεχνικών γνώσεων σε θέματα που αφορούν τόσο τους ηλεκτρονικούς υπολογιστές, όσο και το ίδιο το διαδίκτυο. Το τεχνολογικό πεδίο μεταβάλλεται και εξελίσσεται ραγδαία στους χώρους αυτούς και είναι φανερό ότι η αδυναμία κατανόησής του, δημιουργεί ανυπέρβλητες δυσκολίες στη δημιουργία και προσαρμογή ενός κατάλληλου και ικανού *Νομοθετικού* πλαισίου, στο πεδίο του σύγχρονου εγκλήματος.
- Σε Νομοθετικό επίπεδο και ειδικότερα στην Ελλάδα δεν έχει γίνει μια συνολική και εκτεταμένη «εκκαθάριση» της ποινικής νομοθεσίας και εκσυγχρονισμός αυτής, ώστε να προσαρμοσθεί έναντι των σύγχρονων εγκληματικών δεδομένων.
- Ένας εξίσου σημαντικός παράγοντας που συμβάλλει στην αύξηση των δυσκολιών για την αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί και η σοβαρή έλλειψη επαρκούς βιβλιογραφίας και σχετικών επιστημονικών άρθρων. Αυτό οφείλεται κυρίως στο γεγονός ότι το ηλεκτρονικό έγκλημα αποτελεί μια νέα και εξειδικευμένη μορφή εγκλήματος.
- Ένας άλλος παράγοντας που επηρεάζει αρνητικά την υπάρχουσα κατάσταση, αποτελεί το γεγονός ότι η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα (ηλεκτρονικά εγκλήματα) είναι διατυπωμένη κατά κανόνα στην Αγγλική γλώσσα. Η αντίστοιχη μεταφορά των όρων αυτών στα Ελληνικά, έχει αποδειχθεί ότι δεν αποτελεί μια εύκολη διαδικασία με

ότι αυτό συνεπάγεται για την ομαλή προσαρμογή τους όχι μόνο στην Ελλάδα αλλά και σε άλλες Ευρωπαϊκές χώρες.

Για τη νομική επιστήμη οι έννοιες έχουν το περιεχόμενο που ρητώς τους προσδίδει ο νόμος. Σε περίπτωση δε, που δεν υπάρχει σχετικός νόμος, ο νομικός ανατρέχει στη **Νομολογία**, δηλαδή, στις υπάρχουσες δικαστικές αποφάσεις. Για την ύπαρξη όμως σχετικής νομολογίας, είναι απαραίτητο να έχει "**φθάσει**" η υπόθεση ή άλλη παρόμοια στο δικαστήριο. Δυστυχώς όμως ο αριθμός των υποθέσεων που φθάνουν στα Ελληνικά Δικαστήρια σχετικά με τα ηλεκτρονικά εγκλήματα, είναι πάρα πολύ μικρός και έτσι, σε πολλές περιπτώσεις, δεν υπάρχει νομικό προηγούμενο. επίσης, οι σχετικοί νόμοι που υπάρχουν, δεν επαρκούν από μόνοι τους για να καλύψουν τα εγκλήματα που έχουν παρουσιαστεί, από τη χρήση της πληροφορικής και του διαδικτύου.

Στους πίνακες που ακολουθούν παρουσιάζεται η σημερινή ισχύουσα **Νομοθεσία, Νομολογία** και **Συνθήκες** στην Ελλάδα, σχετικά με το έγκλημα στο διαδίκτυο (ή κυβερνοχώρο). Ο κάθε πίνακας περιλαμβάνει τον **Τίτλο** του σχετικού εγγράφου, την **Ημερομηνία** έκδοσής του και τέλος μια σύντομη **Περιγραφή** του.

9.2 Οδηγίες ανάγνωσης νομικών αφιερωμάτων

Για την πιο εύκολη ανάγνωση και τελικά την ουσιαστική προσέγγιση των νομικών κειμένων που παρατίθενται στη συγκεκριμένη ενότητα σας παρέχουμε τις ακόλουθες οδηγίες - διευκρινίσεις. Τα βασικότερα έγγραφα που παρατίθενται ανήκουν στις κατηγορίες: **Νομοθεσία** και **Νομολογία**.

- **Νομοθεσία** είναι το σύνολο των νομικών διατάξεων που ορίζουν και ρυθμίζουν ένα θέμα. Λαμβάνουν αυτή τη μορφή μέσα από τη νομοθετική διαδικασία η οποία και προβλέπεται στο ελληνικό Σύνταγμα. Στη χώρα μας το νομοθετικό σώμα είναι η Βουλή των Ελλήνων.
- **Νομολογία** αποτελούν το σύνολο των δικαστικών αποφάσεων. Είναι οι αποφάσεις των δικαστηρίων οι οποίες και βασίζονται στις σχετικές νομοθετικές διατάξεις ερμηνεύοντας έτσι ταυτόχρονα τα περιεχόμενά τους και το πνεύμα του νομοθέτη.

9.3 Η νομοθεσία διακρίνεται σε εθνική, ευρωπαϊκή και διεθνή.

Εθνική νομοθεσία αποτελεί η εσωτερική νομοθεσία ενός κράτους π.χ. η νομοθεσία της Ελλάδας. Η ελληνική νομοθεσία αποτελείται από:

- Νόμους π.χ. Ν.3012.2003 ή Ν.3012/03 δηλαδή ο νόμος με αριθμό 3012 του έτους 2003.
- Προεδρικά Διατάγματα π.χ. Π.Δ.52.1985 ή Π.Δ.52/85 , δηλαδή προεδρικό διάταγμα με αριθμό 52 του έτους 1985.
- Υπουργικές αποφάσεις π.χ. Υ.Α.102587.1999 ή Υ.Α. 102587/99 δηλαδή υπουργική απόφαση με αριθμό 102587 του έτους 1999.
- Επίσης νομοθετική ισχύ λαμβάνουν και οι Αποφάσεις επιτροπών όπως της Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), της

Επιτροπής Ανταγωνισμού, της Επιτροπής Κεφαλαιαγοράς κ.α. ή κάποιων αρχών όπως της Αρχής προστασίας προσωπικών δεδομένων κ.α.

Ευρωπαϊκή νομοθεσία είναι η νομοθεσία της Ευρωπαϊκής Ένωσης. Με την ίδρυση της Ευρωπαϊκής Κοινότητας τα κράτη μέλη περιόρισαν τη νομοθετική κυριαρχία τους και δημιούργησαν ένα αυτοτελές σύστημα κανόνων δικαίου που είναι υποχρεωτικά γι' αυτά τα ίδια και για τους πολίτες τους και πρέπει να εφαρμόζονται από τα δικαστήριά τους. Η Ευρωπαϊκή νομοθεσία αποτελείται από:

- Κανονισμούς π.χ. Κανονισμός 792/2002 δηλαδή κανονισμός με αριθμό 792 του έτους 2002.
- Οδηγίες π.χ. Οδηγία 90/88/ΕΟΚ, δηλαδή οδηγία του έτους 1990 με αριθμό 88 της Ευρωπαϊκής Οικονομικής Κοινότητας ή Οδηγία 2000/35/ΕΚ, δηλαδή οδηγία του έτους 2000 με αριθμό 35 της Ευρωπαϊκής Κοινότητας. Οι Οδηγίες σε αντίθεση με την υπόλοιπη νομοθεσία διαβάζονται πρώτα με το έτος και μετά με τον αριθμό τους.
- Αποφάσεις π.χ. Απόφαση 1999/169/ΕΚ δηλαδή απόφαση του έτους 1999 με αριθμό 169 της Ευρωπαϊκής Κοινότητας. Οι αποφάσεις διαβάζονται όπως οι Οδηγίες.
- Επίσης περιλαμβάνει Συστάσεις επιτροπών π.χ. σύσταση 92/295/ΕΟΚ δηλαδή σύσταση του έτους 1992 με αριθμό 295 της Ευρωπαϊκής Οικονομικής Κοινότητας, Ψηφίσματα π.χ. "ΨΗΦΙΣΜΑ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΚΑΙ ΤΩΝ ΑΝΤΙΠΡΟΣΩΠΩΝ ΤΩΝ ΚΥΒΕΡΝΗΣΕΩΝ ΤΩΝ ΚΡΑΤΩΝ ΜΕΛΩΝ, ΣΥΝΕΡΧΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Δεκεμβρίου 1999 για το μέγεθος της απασχόλησης και την κοινωνική της διάσταση στην κοινωνία της πληροφορίας (2000/ C 8/01)" όπου ο αριθμός 2000/ C 8/01 αποτελεί τον κωδικό δημοσίευσης του ψηφίσματος στην Ευρωπαϊκή Εφημερίδα δηλαδή του έτους 2000 το τεύχος C 8 της Εφημερίδας με αριθμό θέματος 01.

Διεθνής είναι η νομοθεσία που υιοθετείται από τα κράτη εφόσον έχουν προσχωρήσει (υπογράψει) τα σχετικά κείμενα και αναφέρεται συνήθως σε Συνθήκες ή/και Συμβάσεις μεταξύ των κρατών.

9.4 Η νομολογία διακρίνεται σε εθνική, ευρωπαϊκή και διεθνή.

Εθνική νομολογία αποτελεί η εσωτερική νομολογία ενός κράτους π.χ. η νομολογία της Ελλάδας, της Βρετανίας, Γαλλίας. Η ελληνική νομολογία αποτελείται από:

- Αποφάσεις του Συμβουλίου της Επικρατείας και του Αρείου Πάγου που αποτελούν τα ανώτατα δικαστήρια της χώρας. Π.χ. ΣτΕ 657.2002 είναι η απόφαση 657 του 2002 του Συμβουλίου της Επικρατείας και Α.Π. 784.1999 είναι η απόφαση 784 του 1999 του Αρείου Πάγου.
- Αποφάσεις Εφετείου π.χ. ΕφΑθ 1239.2002 δηλαδή Εφετείο Αθηνών απόφαση 1239 του έτους 2002 ή ΕφΛαρ 125.1999, δηλαδή Εφετείο Λάρισας απόφαση 125 του 1999.

- Αποφάσεις Πρωτοδικείου π.χ. ΜΠρΑθ 23105/1998 δηλαδή Μονομελές Πρωτοδικείο Αθηνών απόφαση 23105/1998 ή ΠολΠρΘες 14638 . 2001 δηλαδή Πολυμελές Πρωτοδικείο Θεσσαλονίκης απόφαση 14638 του έτους 2001.
- Αποφάσεις Ειρηνοδικείου π.χ. ΕιρΒολ 71/1982 δηλαδή Ειρηνοδικείο Βόλου απόφαση 71 του 1982.
- Γνωμοδοτήσεις του Νομικού Συμβουλίου του Κράτους ή κάποιας Αρχής όπως η Αρχή Προστασίας Προσωπικών Δεδομένων που εκτελούν ρόλο ερμηνευτικό ενός κανόνα δικαίου.
- Ευρωπαϊκή νομολογία αποτελούν οι αποφάσεις του Δικαστηρίου των Ευρωπαϊκών Κοινοτήτων (ΔΕΚ) και του Πρωτοδικείου των Ευρωπαϊκών Κοινοτήτων.

Διεθνή νομολογία αποτελούν οι αποφάσεις των Δικαστηρίων τα οποία εδρεύουν εκτός Ελλάδας και ΕΕ, με βασικότερη αυτή των ΗΠΑ ειδικότερα στα σχετικά με τις νέες τεχνολογίες θέματα.

9.5 Ηλεκτρονικό Εμπόριο: Λίστα νομικών κειμένων

- **Νόμοι**

Ν.2251.1994
Προστασία Καταναλωτή

Ν.2854.2000
Δικαστική προστασία κατά το στάδιο που προηγείται της σύναψης συμβάσεων φορέων οι οποίοι λειτουργούν στους τομείς του ύδατος, της ενέργειας, των μεταφορών και των τηλεπικοινωνιών.

- **Προεδρικά Διατάγματα**

Π.Δ. 39.2001
Για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της Κοινωνίας των Πληροφοριών

Π.Δ. 150.2001
Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

Π.Δ. 131.2003
Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο).

- **Υπουργικές Αποφάσεις**

Υ.Α. Ζ1-496/2000

Υπουργική απόφαση Ζ1-496/2000: Πωλήσεις από απόσταση - Συγκριτική διαφήμιση - Προσαρμογή του Νόμου 2251/1994 για την "Προστασία των καταναλωτών".

Υ.Α. 1023404/2001
Υπουργική απόφαση 1023404/1363/0016 του 2001 για την είσπραξη του Φόρου Προστιθέμενης Αξίας (Φ.Π.Α.), που υποβάλλεται ηλεκτρονικά, με χρέωση Τραπεζικών λογαριασμών των υποκειμένων.

- **Κοινοτικές Οδηγίες**

Οδηγία 87/102/ΕΟΚ
Οδηγία 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη

Οδηγία 90/88/ΕΟΚ
Οδηγία 90/88/ΕΟΚ για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη

Οδηγία 93/13/ΕΟΚ
Οδηγία 93/13/ΕΟΚ του Συμβουλίου σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές

Οδηγία 97/7/ΕΚ
Οδηγία 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις

Οδηγία 2000/31/ΕΚ
Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου στην εσωτερική αγορά.

Οδηγία 2000/35/ΕΚ
Οδηγία 2000/35/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την καταπολέμηση των καθυστερήσεων πληρωμών στις εμπορικές συναλλαγές

Οδηγία 2000/46/ΕΚ
Οδηγία 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος

Οδηγία 2002/38/ΕΚ
Οδηγία 2002/38/ΕΚ όσον αφορά το σύστημα φόρου προστιθεμένης αξίας που εφαρμόζεται στις ραδιοφωνικές και τηλεοπτικές υπηρεσίες και σε ορισμένες υπηρεσίες που παρέχονται ηλεκτρονικά

Οδηγία 2002/58/ΕΚ

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

Οδηγία 2002/65/ΕΚ
Οδηγία 2002/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές

- **Κοινοτικές Συστάσεις**

Σύσταση 92/295/ΕΟΚ
Σύσταση επιτροπής με αριθμό 92/295/ΕΟΚ σχετικά με τους κώδικες δεοντολογίας για την προστασία των καταναλωτών όσον αφορά συμβάσεις διαπραγματευόμενες από απόσταση

Σύσταση 97/489/ΕΚ
Σύσταση 97/489/ΕΚ σχετικά με τις συναλλαγές που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά στις σχέσεις μεταξύ του εκδότη και του κατόχου

- **Κοινοτικοί Κανονισμοί**

Κανονισμός 733/2002
Κανονισμός (ΕΚ) αριθ. 733/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την υλοποίηση του τομέα ανωτάτου επιπέδου

Κανονισμός 792/2002
Κανονισμός (ΕΚ) αριθ. 792/2002 του Συμβουλίου σχετικά με τη διοικητική συνεργασία στον τομέα των έμμεσων φόρων (ΦΠΑ) όσον αφορά πρόσθετα μέτρα για το ηλεκτρονικό εμπόριο

- **Συγκροτήσεις**

Συγκρότηση Αριθ. 536/ΔΠΛ8/Φ19Α
Συγκρότηση γνωμοδοτικής επιτροπής των αιτήσεων που υπεβλήθησαν για το Μητρώο Αξιολογητών για τη δράση «Επιχειρείτε Ηλεκτρονικά» του Μέτρου 3.2 του Επιχειρησιακού Προγράμματος «Κοινωνία της Πληροφορίας».

Συγκρότηση Αριθ. 4708/ΔΠΛ 159/Φ19Α
Συγκρότηση Μητρώου Αξιολογητών για τη δράση «Επιχειρείτε Ηλεκτρονικά» του Μέτρου 3.2 του Επιχειρησιακού Προγράμματος «Κοινωνία της Πληροφορίας».

9.6 Νομοθεσία

Τίτλος	Χρόνος	Περιγραφή
Ψήφισμα του Συμβουλίου της 18ης Φεβρουαρίου 2003	2003	Για την ευρωπαϊκή αντίληψη για την ασφάλεια των δικτύων και των πληροφοριών
ΟΔΗΓΙΑ 9/66/ΕΚ	1999	ΟΔΗΓΙΑ 9/66/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 15ης Δεκεμβρίου 1999 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα
EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC)	2001	FINAL ACTIVITY REPORT
Απόφαση αριθ. 1151/2003/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.	2003	Περί τροποποίησης της απόφασης αριθ. 276/1999/ΕΚ για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου.
Απόφαση του Συμβουλίου με αριθμό 1999/C 362/06	1999	Σχετικά με την καταπολέμηση της παιδικής πορνογραφίας στο Ίντερνετ
Κανονισμός (ΕΚ) αριθ. 1383/2003	2003	Για την παρέμβαση των τελωνειακών αρχών έναντι εμπορευμάτων που είναι ύποπτα ότι παραβιάζουν ορισμένα δικαιώματα πνευματικής ιδιοκτησίας
Απόφαση 2003/490/ΕΚ	2003	Σχετικά με την επάρκεια προστασίας δεδομένων προσωπικού χαρακτήρα στην Αργεντινή
Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΥ	2000	Για την καταπολέμηση της παιδικής πορνογραφίας στο Ίντερνετ
Απόφαση του Συμβουλίου με αριθμό 2001/C 213/0301	2001	Σχετικά με την έκθεση αξιολόγησης της Επιτροπής για την εφαρμογή της σύστασης για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας
Κανονισμός 460	2004	Για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών
Fraud and Related Activity in Connection with Computers	2000	Ηλεκτρονική απάτη
Cyberspace Electronic Security	1999	Ηλεκτρονική ασφάλεια στον κυβερνοχώρο
Information and Readiness Disclosure Act	2000	Αποκάλυψη πληροφοριών
EUROPEAN COMMITTEE ON CRIME PROBLEMS	2001	Part1
EUROPEAN COMMITTEE ON CRIME PROBLEMS	2001	Part3
Draft Explanatory Report	2001	Part1
Draft Explanatory Report	2001	Part2
Draft Explanatory Report	2001	Part3
Draft Explanatory Report	2001	Part4
Draft Explanatory Report	2001	Part5

Τίτλος	Χρόνος	Περιγραφή
Draft Explanatory Report	2001	Part6
N.2928	2001	Τροποποίηση διατάξεων του Ποινικού Κώδικα και του Κώδικα Ποινικής Δικονομίας και άλλες διατάξεις για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων
Απόφαση του Συμβουλίου με αριθμό 2000/C 8/06	2000	Σχετικά με την προστασία των ανηλίκων σε ένα περιβάλλον ψηφιακών οπτικοακουστικών υπηρεσιών
Απόφαση 2256	2003	Σχετικά με την έγκριση πολυετούς προγράμματος (2003-2005) για την παρακολούθηση του σχεδίου δράσης eEurope 2005, τη διάδοση ορθής πρακτικής και τη βελτίωση της ασφάλειας των δικτύων και των πληροφοριών (MODINIS)
ΠεντΕφΑθ 678,751/1998	1998	Απάτη κατά τράπεζας με υπολογιστή
Anticybersquatting Consumer Protection Act	1999	Προστασία του κυβερνοχώρου από καταπατητές
N.1805 (COMPUTER SECURITY ACT)	1988	Ηλεκτρονική ασφάλεια και Εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές
Y2K Act	2000	Ηλεκτρονική ασφάλεια

9.7 Νομολογία

Τίτλος	Χρόνος	Περιγραφή
ΣΤΕ 280/2002	2002	Απόφαση του Συμβουλίου της Επικρατείας σχετικά με διαφημιστικά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου.
ΜΠρΑθ 2110/2002	2002	Απόφαση του Μονομελούς Πρωτοδικείου Αθηνών σχετικά με τη μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου.
Ηλεκτρονικό Έγκλημα - Δικαστική Απόφαση	2002	Απόφαση Αμερικανικού Δικαστηρίου για ηλεκτρονικό σαμποτάζ
ΜΟΝΟΜΕΛΕΣ ΠΡΩΤΟΔΙΚΕΙΟ ΤΡΙΚΑΛΩΝ 1129 . 2001	2001	Προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα.
Mark B. ARONSON, v.BRIGHT-TEETH NOW, LLC.	2003	Απόφαση Αμερικανικού Δικαστηρίου για spam
ΑΡΕΙΟΣ ΠΑΓΟΣ 1152/1999	1999	Έγκλημα της απάτης με υπολογιστή του άρθρου 386Α ΠΚ
ΑΡΕΙΟΣ ΠΑΓΟΣ 1277/1998	1998	Απάτη και απάτη με υπολογιστή
United States v. $734,578.82 in United States Currency	2002	Απόφαση Αμερικανικού Δικαστηρίου για στοιχήματα μέσω Ιντερνετ
Brian P. Corcoran v. Michael Sullivan	1997	Απόφαση Αμερικανικού Δικαστηρίου για ψηφιακά εγκλήματα

9.8 Συνθήκες

Τίτλος	Χρόνος	Περιγραφή
Ευρωπαϊκή συνθήκη για την καταπολέμηση του ηλεκτρονικού εγκλήματος	2001	Ηλεκτρονικό έγκλημα
EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC)	2001	FINAL ACTIVITY REPORT

9.9 Άλλες Χώρες και Σχετική Νομοθεσία

Στον πίνακα 9.1 που ακολουθεί παρουσιάζεται η ισχύουσα νομοθεσία σε πολλές χώρες του κόσμου, όσο αφορά στα εγκλήματα δεδομένων (**data crimes**), δικτύων (**network crimes**), πρόσβασης (**access crimes**) και στα εγκλήματα μέσω υπολογιστών (**computer related crimes**).

Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	✔	✔	✔	✔		✔			✔	✔
Brazil		✔			✔	✔		✔		
Canada	✔	✔	✔	✔	✔	✔	✔			✔
Chile	✔	✔	✔	✔	✔					
China		✔		✔			✔			
Czech Republic		✔	✔		✔	✔				✔
Denmark		✔		✔						✔
Estonia		✔	✔	✔	✔	✔	✔	✔		✔
India		✔	✔	✔	✔	✔	✔	✔		✔
Japan	✔	✔	✔	✔	✔	✔		✔	✔	✔
Malaysia		✔				✔		✔		✔
Mauritius	✔	✔		✔	✔	✔	✔	✔	✔	
Peru	✔	✔	✔	✔	✔	✔				✔
Philippines	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Poland		✔	✔	✔				✔		
Spain	✔	✔	✔					✔		✔
Turkey		✔	✔	✔	✔		✔	✔	✔	✔
United Kingdom		✔		✔	✔	✔		✔		
United States	✔	✔	✔	✔	✔	✔	✔	✔		✔

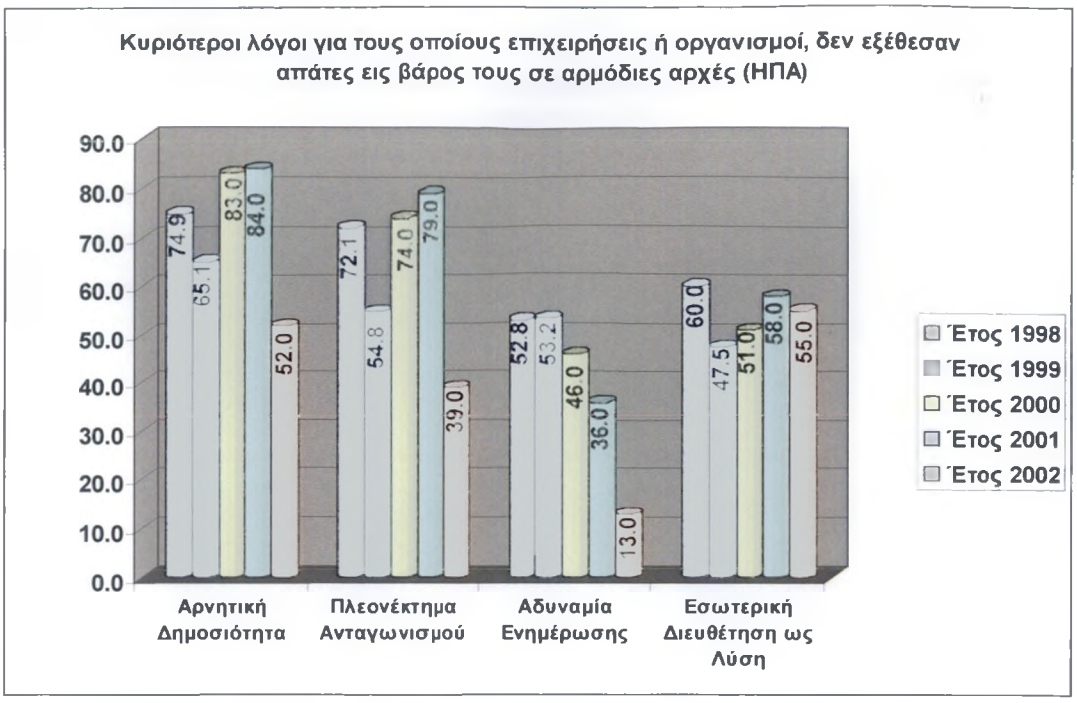
Πηγή: McConnell International LLC
Πίνακας 9.1

10.1.1 Συνεργασία με μεγάλους οργανισμούς & επιχειρήσεις (σε εθνικό και διεθνές επίπεδο)

Η συνεργασία με μεγάλους οργανισμούς και επιχειρήσεις στην Ελλάδα όσο και στο εξωτερικό μπορεί να βοηθήσει στην ενημέρωση και καταγραφή περιστατικών ασφάλειας και απατών, που έχουν πραγματοποιηθεί. Σε αντίθετη περίπτωση χάνονται πολύτιμα στοιχεία σχετικά με τα οικονομικά ή ηλεκτρονικά εγκλήματα, τα οποία δυστυχώς δεν βλέπουν τη δημοσιότητα λόγω του τρόπου με τον οποίο κάθε επιχείρηση αντιμετωπίζει το συγκεκριμένο θέμα, αλλά και των παρακάτω παραγόντων:

- **Αρνητική Δημοσιότητα.** Οι επιχειρήσεις φοβούνται τον επιχειρησιακό αντίκτυπο από τη δημοσιοποίηση περιστατικών διακύβευσης της ασφάλειάς τους ή την πραγματοποίηση απατών που σχετίζονται με αυτές (εσωτερικές ή εξωτερικές)
- **Ανταγωνισμός.** Η δημοσιοποίηση απατών ή θεμάτων που σχετίζεται με την ασφάλεια των επιχειρήσεων, δημιουργεί τον φόβο του πλεονεκτήματος που δίνεται στον «**αντίπαλο**», ο οποίος μπορεί να το χρησιμοποιήσει εις όφελός του
- **Αδυναμία Ενημέρωσης.** Οι επιχειρήσεις πολλές φορές δεν γνωρίζουν που θα μπορούσαν να απευθυνθούν για την υποβολή σχετικών εκθέσεων με εγκλήματα ή περιστατικά ασφάλειας
- **Εσωτερική Διευθέτηση.** Η αντιμετώπιση των οποιονδήποτε προβλημάτων με εσωτερικούς μηχανισμούς των επιχειρήσεων, φαίνεται σε πολλές από αυτές ικανοποιητική λύση

Οι παραπάνω παράγοντες όσο παράξενο και εάν φαίνεται, αποτελούν τον κυριότερο λόγο για τον οποίο δεν υπάρχουν εκτεταμένα στοιχεία για εγκληματικές ενέργειες οικονομικού ή ηλεκτρονικού περιεχομένου, σε πολλές Ευρωπαϊκές χώρες αλλά και σε άλλες χώρες του κόσμου. Σχετικά παρατίθεται το διάγραμμα 10.1 που ακολουθεί, το οποίο επισημαίνει σε μεγάλο βαθμό αυτά που μόλις αναφέραμε παραπάνω. Τα αποτελέσματα του διαγράμματος αποτελούν προϊόν έρευνας του FBI και δείχνει τους κυριότερους λόγους για τους οποίους οι επιχειρήσεις ή οργανισμοί, δεν εξέθεσαν απάτες εις βάρος τους στις αρμόδιες αρχές.



Πηγή: CSI/FBI 2000 Computer Crime and Security Survey

Διάγραμμα 10.1

Οι διωκτικές αρχές οικονομικού εγκλήματος θα πρέπει να προσανατολιστούν στην άμεση συνεργασία με τον επιχειρηματικό κόσμο ή το δημόσιο, με στόχο την συλλογή και ανταλλαγή στοιχείων, ενημέρωσης των επιχειρήσεων για τα οφέλη από την συνεργασία μαζί τους και την διεξαγωγή ερευνών σχετικά με το ηλεκτρονικό έγκλημα. Η συνεργασία των αρχών οικονομικού εγκλήματος θα πρέπει επίσης να επεκταθεί και να ενταθεί σε μεγαλύτερο βαθμό με την Ευρωπαϊκή Ένωση και τους αρμόδιους οργανισμούς της ή τις επιτροπές της, οι οποίες σαφώς μπορούν να προσφέρουν με τον καλύτερο τρόπο ενημέρωση και τεχνογνωσία σε πολλούς τομείς που αφορούν άμεσα το ηλεκτρονικό ή το οικονομικό έγκλημα.

10.1.2 Προσφυγή σε Στατιστικές (για cyber crimes, internet κ.λ.π.)

Η υιοθέτηση χρήσης στατιστικών για τα εγκλήματα όλων των ειδών σε εθνικό ή διεθνές επίπεδο (κυρίως από τις διωκτικές αρχές) είναι σημαντική διότι:

- Οι στατιστικές περί οικονομικού εγκλήματος εξυπηρετούν έναν σημαντικό ρόλο στην εφαρμογή της νομοθεσίας και της επιβολής του νόμου. Κατ' αρχάς, επιτρέπουν την κατάλληλη κατανομή των συνήθως περιορισμένων πόρων, που διαθέτουν οι υπηρεσίες δίωξης του οικονομικού – ηλεκτρονικού εγκλήματος. Παραδείγματος χάριν, εάν μια ή περισσότερες έρευνες επισημαίνουν την σημαντική αύξηση σε μια συγκεκριμένη κατηγορία εγκλημάτων, οι διοικήσεις των διωκτικών αρχών μπορούν να ελίσσονται δυναμικά και να λαμβάνουν μέτρα για την αντιμετώπιση αυτών των εγκλημάτων, χωρίς την σπατάλη πολύτιμου χρόνου και την σπατάλη πόρων και προσωπικού. Η διαπίστωση σε μικρότερο ή μεγαλύτερο βαθμό για την παρουσία και διάπραξη συγκεκριμένων οικονομικών – ηλεκτρονικών εγκλημάτων, επιτρέπει στις διωκτικές αρχές να διαμορφώνουν γρήγορα και αποτελεσματικά λύσεις για την αντιμετώπισή τους.

- Οι διωκτικές αρχές πρέπει να δικαιολογούν σε μόνιμη βάση τον βαθμό κατάρτισης, τον εξοπλισμό και τις δαπάνες του προσωπικού τους, στοιχεία που είναι απαραίτητα για την αποτελεσματικότητά τους στην καταπολέμηση του οικονομικού – ηλεκτρονικού εγκλήματος. Έτσι πολύ συχνά οι διευθυντές των διωκτικών αρχών πρέπει να δικαιολογούν τις δαπάνες τους στους αρμόδιους υπουργούς των εκάστοτε κυβερνήσεων. Με την χρήση των αποτελεσμάτων από ποικίλες στατιστικές η διωκτική αρχή μπορεί να τεκμηριώσει το πρόβλημα βασισμένη σε πραγματικά στοιχεία και όχι σε υποθέσεις.
- Τα οικονομικά ηλεκτρονικά εγκλήματα έχουν επιπτώσεις σε πολλούς τομείς της ανθρώπινης δραστηριότητας. Οι επιχειρήσεις αλλά και πολλοί άνθρωποι στηρίζονται στις στατιστικές εγκλήματος για τη λήψη σημαντικών αποφάσεων που αφορούν την ασφάλειά τους και τις στρατηγικές τους στο παγκόσμιο εμπόριο. Οι παραπάνω χρησιμοποιούν τα στατιστικά στοιχεία περί εγκλημάτων για να αξιολογήσουν τα επιχειρησιακά επίπεδα κινδύνου τους, να καθορίσουν τρόπους αντιμετώπισής τους και να υπολογίζουν τις πιθανές δαπάνες αποκατάστασης από την διάπραξή τους, εις βάρος τους.

11 Στρατηγική αντιμετώπισης οικονομικών ηλεκτρονικών εγκλημάτων (Hi-Tech Crime Strategy)

11.1 Εισαγωγή

Όπως έχει αναφερθεί εκτενέστερα στις προηγούμενες ενότητες του παρόντος κειμένου, οι περισσότερες κυβερνήσεις και οι σχετικοί αρμόδιοι οργανισμοί έχουν επισημάνει τους κινδύνους που διατρέχει το e-commerce παγκοσμίως και του βαθμού που το τελευταίο διαμορφώνει το πεδίο εγκληματικότητας (οικονομικό ή ηλεκτρονικό). Η αυξανόμενη μάλιστα συμμετοχή ολοένα και περισσότερων επιχειρήσεων στο ηλεκτρονικό εμπόριο καθώς και η ηλεκτρονική παροχή δημόσιων υπηρεσιών αποτελούν βασικούς στρατηγικούς στόχους, για κάθε σύγχρονη επιχείρηση ιδιωτικού ή δημόσιου χαρακτήρα.

Οι στόχοι αυτοί των επιχειρήσεων δεν μπορούν παρά να αποτελούν και έναν ρυθμιστικό παράγοντα, για τον τρόπο με τον οποίο οι διωκτικές αρχές (οικονομικών ή μη εγκλημάτων) πρέπει να ικανοποιούν τόσο τις ανάγκες των εκάστοτε κυβερνήσεων, όσο και του ιδιωτικού ή δημόσιου τομέα, ώστε να παρέχουν αποτελεσματικότητα στην καταπολέμηση των οικονομικών και ηλεκτρονικών εγκλημάτων, στην πρόληψή τους και στην επιβολή του νόμου (όταν και όποτε αυτή χρειάζεται) στην νέα αυτή ηλεκτρονική εποχή. Επίσης θα πρέπει να λαμβάνονται υπόψη από τις διωκτικές αρχές και η υπάρχουσα νομοθεσία, ώστε να διατηρείται μια σωστή ισορροπία μεταξύ της επιβολής νόμου και των ανθρώπινων δικαιωμάτων.

Σε ένα μη ηλεκτρονικό περιβάλλον, η επιβολή του νόμου και η πρόληψη των εγκλημάτων δεν αποτελούν αποκλειστική αρμοδιότητα μόνο των διωκτικών αρχών, αλλά και των ιδιωτικών, δημόσιων και μη κυβερνητικών οργανώσεων (άμεσα ή έμμεσα). Με τις νέες προκλήσεις των cybercrimes που έχουν προκύψει με τη δικτύωση των υπολογιστών, οι παραπάνω οργανώσεις έχουν να αντιμετωπίσουν μια νέα πρόκληση, η οποία προκύπτει από την στροφή του παραδοσιακού εγκλήματος στο ηλεκτρονικό περιβάλλον. Αντιμέτωποι με αυτή τη νέα πραγματικότητα οι διωκτικές αρχές (οικονομικού και ηλεκτρονικού εγκλήματος) θα πρέπει να διαμορφώσουν τις πρακτικές και τις μεθόδους τους με τέτοιο τρόπο ώστε αυτές να συνάδουν με τις εξελίξεις της τεχνολογίας και τον χαρακτήρα της παγκοσμιότητας.

Οι προκλήσεις που ενδέχεται να αντιμετωπίσουν οι ήδη υπάρχουσες διωκτικές αρχές του οικονομικού ή ηλεκτρονικού εγκλήματος, όπως δηλώνονται και από τις σχετικές έρευνες που παρατίθενται σε προηγούμενες ενότητες του παρόντος κειμένου (τόσο στον Ευρωπαϊκό όσο και στον παγκόσμιο χώρο), είναι τεράστιες και άμεσες και αποδεικνύουν περίτρανα ότι κανένα έθνος αυτόβουλα δεν μπορεί να αντιμετωπίσει από μόνο του το πρόβλημα. Κατά συνέπεια, ο ρόλος για τις διωκτικές αρχές οικονομικού εγκλήματος στην Ελλάδα πρέπει να συνδεθεί μέσα στο πλαίσιο των ενεργειών που πραγματοποιούνται από την Ελληνική Δικαιοσύνη, των διεθνών πρωτοβουλιών για την καταπολέμηση του εγκλήματος, των σχέσεων με τις ιδιωτικές βιομηχανίες και γενικά με την ιδιωτική πρωτοβουλία, για να μπορεί να προστατευθεί η υποδομή του εμπορίου και της αγοράς.

Δηλαδή απαιτείται μια μακροπρόθεσμη στρατηγική εκ μέρους των διωκτικών αρχών, για την αντιμετώπιση του οικονομικού ή ηλεκτρονικού εγκλήματος. Μέσω της στρατηγικής αυτής θα πρέπει να αναπτυχθεί μια δομή για την μεγιστοποίηση των σχέσεων και την ελαχιστοποίηση των επαναλαμβανόμενων προσπαθειών, μεταξύ του δημόσιου και ιδιωτικού τομέα αλλά και ειδικότερα μεταξύ των διωκτικών αρχών και άλλων δημόσιων υπηρεσιών. Η δημιουργία της στρατηγικής θα πρέπει επίσης να αναγνωρίσει ένα τετελεσμένο γεγονός, ότι καθώς η τεχνολογία της πληροφορίας γίνεται ολοένα πιο κυρίαρχη παγκοσμίως, το ευρέως κοινό έγκλημα θα περιλαμβάνει όλο και περισσότερο το σύνολο των πτυχών του ηλεκτρονικού εγκλήματος (και ως επακόλουθο και του οικονομικού).

11.2 Αρχές Στρατηγικής

Η παραπάνω στρατηγική θα πρέπει να καθοδηγείται και να βασίζεται στις ακόλουθες αρχές:

- Δομημένος συντονισμός υψηλού επιπέδου για το ηλεκτρονικό οικονομικό έγκλημα σε εθνικό επίπεδο, για την κεφαλαιοποίηση του συνόλου των υπαρχόντων δεδομένων και δυνατοτήτων από όπου και εάν αυτά προέρχονται (ιδιωτικός ή δημόσιος τομέας)
- Το ηλεκτρονικό έγκλημα είναι παγκόσμιο και απαιτεί τη λήψη αποτελεσματικών και αμοιβαίων πρωτοβουλιών, για την ενθάρρυνση διεθνών συνεργασιών, τη διαλειτουργικότητα και το συντονισμό τους
- Η πρόληψη είναι καλύτερη από τη θεραπεία και οι διωκτικές αρχές οικονομικού εγκλήματος στην Ελλάδα θα πρέπει να συνεργάζονται στενά με επιλεγμένους συνεργάτες, για την αποτροπή, ανίχνευση και μείωση του ηλεκτρονικού οικονομικού εγκλήματος
- Απαιτείται η εκπαίδευση του προσωπικού (δεξιότητες), δεδομένου ότι οι νέες μορφές ηλεκτρονικού εγκλήματος αναπτύσσονται με ραγδαίους ρυθμούς
- Η αποτελεσματικότητα των διωκτικών αρχών οικονομικού εγκλήματος, απαιτεί την παράλληλη ρυθμιστική και νομοθετική μεταρρύθμιση, τόσο σε εθνικό όσο και σε διεθνή επίπεδο
- Απαιτείται η ανάπτυξη της υποδομής των διωκτικών αρχών οικονομικού εγκλήματος, σχετικά με την τεχνολογία
- Χρειάζεται συνεχής και αποτελεσματικός έλεγχος όσο και αξιολόγηση, για να εξασφαλίζεται η αποτελεσματικότητα της στρατηγικής.

11.2.1 Κρίσιμοι παράγοντες για την επίτευξη των στόχων

Οι παραπάνω αρχές της στρατηγικής που πρέπει να ακολουθούνται από τις διωκτικές αρχές του οικονομικού και ηλεκτρονικού εγκλήματος, δεν αποτελούν από μόνες τους αναγκαία και ικανή συνθήκη για την επίτευξη της στρατηγικής. Επιπλέον απαιτείται η υποστήριξή της μέσω:

- **Της διαρκούς δέσμευσης** και προσήλωσης στις αρχές της στρατηγικής από την εκάστοτε κυβέρνηση, τις αντιπροσωπείες συνεργατών και το ίδιο το προσωπικό των διωκτικών αρχών
- **Της διεθνούς συνεργασίας** και συντονισμού σε σχέση με τους διαθέσιμους πόρους, τις διαδικασίες και τα νομοθετικά πλαίσια

- **Της νομοθετικής μεταρρύθμισης** από την εκάστοτε κυβέρνηση (όταν και όποτε απαιτείται από τις υπάρχουσες συνθήκες), ώστε να επιτρέπεται στις διωκτικές αρχές απερίσπαστα να διεξάγουν αποτελεσματικά και γρήγορα ηλεκτρονικές έρευνες εγκλήματος και ταχεία εξέταση ή διαχείριση ηλεκτρονικών δεδομένων
- **Της αναγνώρισης από την κυβέρνηση,** ότι η επιβολή νόμου αντιμετωπίζει με νέα προοπτική τη επιχείρηση του σήμερα, η οποία χαρακτηρίζεται από νέους τύπους εγκλημάτων, νέους εγκληματίες, νέες δημογραφικές παραμέτρους και νέες πολυπλοκότητες
- **Της παροχή επαρκών πόρων,** από την εκάστοτε κυβέρνηση που φροντίζει για:

- *Την κάλυψη των αυξανόμενων απαιτήσεων* για την καταπολέμηση του οικονομικού και ηλεκτρονικού εγκλήματος, που προέρχονται λόγω της αυξανόμενης χρήσης της σύγχρονης τεχνολογίας από τους απανταχού εγκληματίες
- *Ζητήματα σχετικά με το ανθρώπινο δυναμικό*, που προκύπτουν με τη αναγκαία στρατολόγηση και τη διατήρηση, του τεχνικά εξειδικευμένου προσωπικού και
- *Δαπάνες κατάρτισης, έρευνας και ανάπτυξης*, που συνδέονται με τη βελτίωση της ικανότητας των διωκτικών αρχών στην καταπολέμηση του οικονομικού και ηλεκτρονικού εγκλήματος

11.2.2 Ζητήματα προτεραιότητας

Η χρήση της τεχνολογίας πληροφοριών από τους εγκληματίες, καθιερώνεται πια ως μια κοινή πραγματικότητα όπως δείχνει ένας μεγάλος αριθμός ερευνών παγκοσμίως. Η πραγματικότητα αυτή όπως είναι φανερό επηρεάζει σε μεγάλο βαθμό την οποιαδήποτε στρατηγική ακολουθείται ή που επιθυμεί να ακολουθήσει η εκάστοτε διωκτική αρχή ενός κράτους. Η αναγνώριση αυτής της πραγματικότητας οδηγεί στην ανάγκη για μια ισορροπημένη προσέγγιση, για την ταχεία ανάπτυξη των διωκτικών αρχών να ανταποκριθούν στα παραδοσιακά ζητήματα αστυνόμευσης, που δείχνουν ολοένα και περισσότερο ότι συνδυάζονται με τις σύγχρονες μορφές της τεχνολογίας, καθώς επίσης στην εύρεση μεθόδων και πρακτικών άμεσης εφαρμογής, για την αντιμετώπιση του αναδυόμενου τομέα του cybercrime. Η διαδικασία ανάπτυξης στρατηγικής θα πρέπει να δώσει έμφαση στους τομείς πρώτης προτεραιότητας, οι οποίοι προσδιορίζονται ως εξής:

- **Ευθυγράμμιση** των στρατηγικών αστυνόμευσης οικονομικού και ηλεκτρονικού εγκλήματος, με εκείνες άλλων κυβερνητικών υπηρεσιών σχετικά με το ηλεκτρονικό περιβάλλον
- **Διαμόρφωση** συνεργασιών (με ή χωρίς την παρουσία κυβερνητικών υπηρεσιών)
- **Ανάπτυξη των τεχνικών δυνατοτήτων,** για την αντιμετώπιση των τρεχουσών αλλά και των μελλοντικών αναγκών στις έρευνες των εγκλημάτων
- **Συμμετοχή και συνεργασία** με τον ιδιωτικό τομέα, ο οποίος μπορεί να παρέχει σε συγκεκριμένα ζητήματα λύσεις και πρακτικές, με στόχο την πρόληψη και τη μείωση του ηλεκτρονικού ή οικονομικού εγκλήματος (ειδικά σε θέματα τεχνογνωσίας) και

- **Ενεργή Συμβολή και συμμετοχή** στις νομοθετικές μεταρρυθμίσεις, για την διαμόρφωση του κατάλληλου πλαισίου αρμοδιοτήτων των διωκτικών αρχών σχετικά με τις ηλεκτρονικές έρευνες εγκλήματος και για την γενική βελτιστοποίηση της νομοθεσίας, ώστε να είναι αποτελεσματικότερη και γρήγορα προσαρμόσιμη, έναντι των εξελίξεων

11.3 Περιοχές εστίασης στρατηγικής

Η στρατηγική αντιμετώπισης του σύγχρονου εγκλήματος θα πρέπει να έχει περιοχές δράσης, οι οποίες θα πρέπει να προσδιορίζουν τους κύριους στόχους των διωκτικών αρχών, κατά τη διάρκεια εφαρμογής της στρατηγικής (που διαμορφώνεται προφανώς από την εκάστοτε διωκτική αρχή ανάλογα με τις δυνατότητές της και τις αποφάσεις των υπεύθυνων της διοίκησής της). Οι περιοχές δράσης θα πρέπει να περιέχουν ένα σύνολο δραστηριοτήτων που να λειτουργούν προς την επίτευξη μιας ισορροπίας, μεταξύ της δυναμικής πρόληψης και των αποτελεσματικών λύσεων έναντι του ηλεκτρονικού ή οικονομικού εγκλήματος. Αυτές οι περιοχές δράσης θα πρέπει επίσης να είναι, αλληλοσυνδεόμενες και αλληλοσυνεργαζόμενες, ώστε να οδηγήσουν στο μεγαλύτερο δυνατό ποσοστό επιτυχίας. Οι περιοχές δράσης (και οι στόχοι τους) θα πρέπει να είναι:

11.3.1.1 Πρόληψη.

- **Στόχος Α. Μείωση των επιπτώσεων των αποτελεσμάτων του ηλεκτρονικού ή οικονομικού εγκλήματος.** Η παρεμπόδιση του ηλεκτρονικού εγκλήματος (όταν και όποτε επιτυγχάνεται) διευκολύνει το έργο των διωκτικών αρχών, εφόσον βοηθά στην καλύτερη διαχείριση των διαθέσιμων πόρων των διωκτικών αρχών (οι οποίοι δεν είναι φυσικά απεριόριστοι) και στην καλύτερη κατανομή τους για την αντιμετώπιση των πιο σημαντικών οικονομικών και ηλεκτρονικών εγκλημάτων. Οι στρατηγικές πρόληψης συνδέονται στενά με τις στρατηγικές εκπαίδευσης και τις στρατηγικές διαχείρισης κινδύνου και διαχείρισης ασφάλειας πληροφοριών, που στοχεύουν στην μείωση του όγκου και της σοβαρότητας των εγκλημάτων που παρατηρούνται.
- **Στόχος Β: Διεξαγωγή ερευνών και διατήρηση στατιστικών σχετικά με το ηλεκτρονικό οικονομικό έγκλημα.** Η πρόσβαση σε ακριβείς στατιστικές και η διεξαγωγή ερευνών (σχετικά με το ηλεκτρονικό οικονομικό έγκλημα), είναι απαραίτητες για την παροχή πολύτιμων πληροφοριών που οδηγούν σε ποιοτικές επιλογές, τόσο την εκάστοτε κυβέρνηση όσο και τις διωκτικές αρχές, σε θέματα που αφορούν την αντιμετώπιση της εγκληματικότητας. Στη παρούσα φάση με το αναδυόμενο νέο φαινόμενο, όπως το cybercrime όπου υπάρχουν περιορισμένα ιστορικά δεδομένα, η διεξαγωγή ερευνών τόσο από τις ίδιες τις διωκτικές αρχές όσο και από τρίτους (κυβερνητικοί οργανισμοί, ιδιωτικές επιχειρήσεις, Ευρωπαϊκή ένωση κ.λ.π.), μπορούν να οδηγήσουν σε σωστές στρατηγικές προβλέψεων και πρόληψης.

11.3.1.2 Συνεργασίες

- **Στόχος Α: Καθιέρωση και διατήρηση αποτελεσματικών συνεργασιών.** Αυτός ο στόχος επικεντρώνεται κυρίως στη συνεργασία με άλλους οργανισμούς, συμπεριλαμβανομένων των οργανισμών εθνικής ασφάλειας όπου απαιτείται , για την μεγιστοποίηση και την αποτελεσματικότητα των

ερευνών ηλεκτρονικού οικονομικού εγκλήματος και την προστασία των υποδομών. Μια βασική κατεύθυνση αυτού του στόχου είναι και η αποτροπή της επανάληψης παρόμοιων προσπαθειών από άλλους οργανισμούς, λόγω της έλλειψης συνεργασίας μεταξύ των.

- **Στόχος Β: Προώθηση συνεργασίας με τον ιδιωτικό τομέα.** Αυτός ο στόχος θα πρέπει να εξασφαλίσει την ουσιαστική συνεργασία των διωκτικών αρχών με τον ιδιωτικό τομέα (επιχειρήσεις, οργανισμούς). Οι επιχειρήσεις θα πρέπει να γνωρίζουν ότι όταν παρατηρούνται εγκληματικές ενέργειες (οικονομικής ή ηλεκτρονικής μορφής), οι διωκτικές αρχές είναι σε θέση να ενημερώνονται γρήγορα σχετικά με αυτές και ότι μπορούν να δώσουν κατάλληλες και έγκαιρες απαντήσεις. Περαιτέρω, οι διωκτικές αρχές θα πρέπει να έχουν και να διατηρούν αποτελεσματικές σχέσεις, με τη βιομηχανία πληροφοριών και τα ερευνητικά ιδρύματα, που γνωρίζουν σε μεγαλύτερο βαθμό τις νέες τεχνολογίες.

11.3.1.3 Εκπαίδευση Προσωπικού

- **Στόχος Α. Απόκτηση ειδικευμένου προσωπικού.** Για να μπορούν οι διωκτικές αρχές να ανταποκριθούν στην ανάγκη αντιμετώπισης των εγκλημάτων, αλλά και στην έρευνα σχετικά με αυτά, απαιτείται η τεχνολογική, νομική και διαδικαστική γνώση καθώς επίσης και πρακτικές δεξιότητες, που θα πρέπει να επιδεικνύουν οι υποψήφιοι για την είσοδό τους στις διωκτικές αρχές. Για την υλοποίηση του εν λόγω στόχου, απαιτούνται τα εξής:

- **Δημιουργία ή Εκσυγχρονισμός Εκπαιδευτικού Τμήματος.** Η παρουσία ειδικού τμήματος για την εκπαίδευση του προσωπικού, θεωρείται από μόνος του ως ένας κρίσιμος παράγοντας, για την επιτυχία ή όχι μιας διωκτικής αρχής οικονομικού ή ηλεκτρονικού εγκλήματος. Είτε πρόκειται για ένα νέο τμήμα ή για ένα ήδη υπάρχον, ο εκσυγχρονισμός του με σύγχρονα συστήματα και έμπειρους εκπαιδευτές, αποτελεί μονόδρομο για την βελτίωση των ικανοτήτων και δεξιοτήτων ολόκληρου του προσωπικού μιας διωκτικής αρχής.
- **Επανεκπαίδευση Υπάρχοντος Προσωπικού στις νέες τεχνολογίες.** Το εκπαιδευτικό τμήμα, επιμερίζεται επίσης με την ευθύνη της επανεκπαίδευσης του προσωπικού ανά τακτά χρονικά διαστήματα, ώστε να είναι ενήμερο για τις τεχνολογικές εξελίξεις όσο αφορά στο θέμα του οικονομικού και ηλεκτρονικού εγκλήματος
- **Σεμινάρια.** Η ενημέρωση του προσωπικού μπορεί να πραγματοποιείται με την μορφή σεμιναρίων από ειδικούς, σε θέματα που αφορούν αποκλειστικά την διωκτική αρχή ή με την μορφή ειδικών προγραμμάτων που καθορίζονται από την διοίκησή της.
- **Βασική Εκπαίδευση.** Θα πρέπει να ακολουθείται στην εκπαίδευση συγκεκριμένη πολιτική, η οποία θα οδηγεί σε μια κοινή βάση γνώσεων για όλο το προσωπικό, αποφεύγοντας έτσι τα προβλήματα που δημιουργούνται εσωτερικά από την ελλιπή κατάρτιση σε ορισμένα καίρια θέματα.
- **Εξειδικευμένη Εκπαίδευση.** Κύριος στόχος της εκπαίδευσης θα πρέπει να είναι η δημιουργία σημαντικού ποσοστού του προσωπικού με άριστη γνώση, όχι μόνο στα θέματα που αφορούν αποκλειστικά την υπηρεσία αλλά και σε τεχνολογικά θέματα (πληροφοριακά συστήματα, διαδίκτυο κ.λ.π.).

- **Συνολικοί Στόχοι Εκπαίδευσης και Τεχνολογικού Εξοπλισμού**

- Σύγκλιση τεχνικών δεξιοτήτων με την ανακριτική εμπειρία
- Εθνική και σφαιρική κάλυψη
- Βελτίωση τεχνικών ανάκρισης - ερευνών
- Αξιοποίηση των διαθέσιμων πόρων
- Προσαρμογή στην νομοθεσία και βελτίωση στους τρόπους επιβολής νόμου
- Καλύτερη Ανάλυση των διαθέσιμων στοιχείων
- Καθιέρωση σχέσεων συνεργασίας με εταιρείες παροχής ασφάλειας πληροφοριακών συστημάτων
- Ενεργή Συμμετοχή στα φόρουμ ασφάλειας υπολογιστών
- Οικονομικές γνώσεις (μεθοδολογίες ελέγχου)

11.4 Κατάρτιση Ειδικής Ομάδας Μονάδας Τεχνολογικού Εγκλήματος (Creation of Hi-Tech Crime Unit)

Για την πραγματοποίηση των στόχων μιας διωκτικής αρχής απαιτείται η δημιουργία ειδικών μονάδων *Ερευνητών Τεχνολογικού Οικονομικού Ηλεκτρονικού εγκλήματος*, που θα πρέπει να έχει την ακόλουθη δομή:

- Επόπτη (**Supervisor**). Ο επόπτης συντονίζει την ομάδα ως προς τον τρόπο λειτουργίας της και αξιολόγησης των αποτελεσμάτων από τις πραγματοποιηθείσες έρευνες.
- Ανακριτές (**Investigators**). Οι ανακριτές – ερευνητές επωμίζονται με την διερεύνηση και συλλογή στοιχείων και πρέπει να είναι ειδικά εκπαιδευμένοι ώστε να πραγματοποιούν με ακρίβεια και ταχύτητα την συγκομιδή πολύτιμων στοιχείων, για την επιτυχή ολοκλήρωση μιας έρευνας και ίσως απαιτείται η κατοχή ειδικών τεχνολογικών γνώσεων για την αποτελεσματικότερη δράση τους.
- Αναλυτές (**Analysts**). Οι αναλυτές θα πρέπει να είναι σε θέση να αναλύουν με σύγχρονες μεθόδους και πρακτικές το σύνολο των αποτελεσμάτων από τις έρευνες των ανακριτών και θα πρέπει να είναι ειδικά εκπαιδευμένοι και μάλιστα σε υψηλότερο επίπεδο από ότι οι ανακριτές στις σύγχρονες τεχνολογίες πληροφοριών, ώστε να μπορούν να εκμεταλλευτούν στο έπακρο τα δεδομένα που διαθέτουν.

11.4.1 Πόροι και ικανότητες.

Με τον στόχο αυτό θα πρέπει να καθοριστούν οι απαραίτητοι πόροι, που απαιτούνται γενικά για την αντιμετώπιση του ηλεκτρονικού οικονομικού εγκλήματος. Οι προηγούμενες περιοχές εστίασης (που αναφέρονται σε προηγούμενες παραγράφους) για μια διωκτική αρχή, χρησιμοποιούνται επίσης για την σωστή αξιολόγηση των μελλοντικών αναγκών ή για την σωστότερη κατανομή τους, ως προς ορισμένες κατηγορίες εγκλημάτων.

11.4.2 Κανονισμοί και νομοθεσία.

Στόχος. Παρακολούθηση της εκάστοτε νομοθεσίας και συνδρομή στην βελτίωσή της, ώστε να συνάδει με τις πραγματικές ανάγκες των διωκτικών αρχών.

11.4.3 Πληροφόρηση, επικοινωνία και βάση δεδομένων

Στόχος Α. Η υπηρεσία δίωξης οικονομικού ηλεκτρονικού εγκλήματος θα πρέπει να διαθέτει σύστημα διαχείρισης των πληροφοριών που συλλέγει από τις επιχειρησιακές της δραστηριότητες, των πληροφοριών που κοινοποιούνται από κράτη μέλη της Ευρωπαϊκής Ένωσης, καθώς και των πληροφοριών που προέρχονται από συγκεκριμένα Ευρωπαϊκά Θεσμικά Όργανα ή από άλλα τρίτα μέρη.

Στόχος Β. Η υπηρεσία δίωξης οικονομικού ηλεκτρονικού εγκλήματος θα πρέπει να εκπονήσει ειδικό σχέδιο εργασίας με στόχο να αναπτύξει την υποδομή, να διασφαλίσει τη συγκέντρωση και την αξιοποίηση των πληροφοριών και να παράσχει τεχνική συνδρομή στα θεσμικά όργανα και τα λοιπά όργανα ή οργανισμούς, καθώς και στις αρμόδιες εθνικές αρχές. Το σχέδιο εργασίας θα πρέπει να έχει σαν στόχους επίσης, την οργάνωση των συστημάτων ελέγχου της εσωτερικής λειτουργίας της υπηρεσίας και αφετέρου το σχεδιασμό συστημάτων στήριξης για εξωτερική χρήση (υπηρεσίες και όργανα της Ευρωπαϊκής Ένωσης, Εθνικές Αρχές,).

Στόχος Γ. Η υπηρεσία δίωξης οικονομικού ηλεκτρονικού εγκλήματος θα πρέπει να διαθέτει μια σύγχρονη **βάση δεδομένων**, ώστε να αντιμετωπίζονται οι ακόλουθες ανάγκες:

- να υπάρχει ένα σύστημα διαχείρισης υποθέσεων προσαρμοσμένο στις διαδικασίες που καθορίζονται από τις «**πολιτικές**» της υπηρεσίας
- να διασφαλίζεται η ομοιογενής και συνεκτική καταχώρηση των πληροφοριών (εσωτερικά και εξωτερικά) που αφορούν το σύνολο των υποθέσεων της υπηρεσίας, μέχρι να ολοκληρώνεται ο κύκλος διεκπεραίωσής τους (αλλά και μετά)
- να διασφαλίζεται η καλύτερη παρακολούθηση της προόδου που σημειώνεται στις υποθέσεις, από αυτούς που διενεργούν τις έρευνες
- να διασφαλίζεται η χρησιμοποίηση της βάσης ως μέσο ενημέρωσης και διαχείρισης εκ μέρους της ιεραρχίας
- να επιτυγχάνεται η συνεχής προσαρμογή της βάσης δεδομένων στις όποιες απαιτήσεις επέκτασης της Υπηρεσίας

11.4.4 Άλλοι στόχοι

Στους παραπάνω στόχους θα πρέπει να πλαισιωθούν και με τα παρακάτω για την καλύτερη και αποδοτικότερη εφαρμογή τους:

- Συνεργασία και Συντονισμός Υπηρεσιών (Collaborative and Coordinated Services)
- Διασπορά και Ανταλλαγή Πληροφοριών (Dissemination of Information)
- Επικοινωνία και Συντονισμός Υπηρεσιακών μονάδων (Liaison)

12 Συμπεράσματα

Για την αποτελεσματική αντιμετώπιση του οικονομικού – ηλεκτρονικού εγκλήματος θα πρέπει να επιστηθεί η προσοχή στα ακόλουθα:

- Βελτίωση των νόμων και των κανονισμών, καθώς και των μεθόδων που χρησιμοποιούνται για την επεξεργασία των αναφορών, σχετικά με τα εγκλήματα κάθε τύπου. Υπάρχουν πολυάριθμες υποθέσεις που εκκρεμούν στα δικαστήρια, που εξετάζουν τις απάτες που διαπράττονται στο διαδίκτυο, την κλοπή ταυτότητας και τα ζητήματα που αναφέρονται στην ασφάλεια και στις επιθέσεις στο διαδίκτυο. Η εκάστοτε νομοθεσία θα πρέπει να χρησιμοποιεί κατάλληλη γλώσσα που να είναι εύκολα προσαρμόσιμη στις μελλοντικές τεχνολογικές αλλαγές, ώστε να μπορεί να βοηθήσει αποτελεσματικά στην αποτροπή των οικονομικών και ηλεκτρονικών αδικημάτων.
- Απαιτούνται λεπτομερείς υποβολές εκθέσεων για την εμπεριστατωμένη μελέτη του οργανωμένου οικονομικού ηλεκτρονικού εγκλήματος. Το αποτέλεσμα της επιτυχής έκβασης των εκθέσεων και ερευνών θα οδηγήσει αναπόφευκτα στην διάθεση των κατάλληλων πόρων για την πρόληψη, την έρευνα, την εκπαίδευση και τη ετοιμότητα που χρειάζονται απαραίτητα προκειμένου να αντιμετωπιστεί το πρόβλημα.
- Οι δημόσιες και ιδιωτικές συνεργασίες πρέπει να ενθαρρυνθούν και να δρομολογηθούν το συντομότερο δυνατό, προκειμένου να αποτραπούν και να καταπολεμηθούν τα οικονομικά και cyber εγκλήματα. Οι στρατηγικές που θα υιοθετηθούν και θα αναπτυχθούν από τις διωκτικές αρχές θα πρέπει να ενσωματώνουν επιπλέον ως βασικές διαδικασίες, εξειδικευμένα εργαλεία και βάσεις δεδομένων για τη διαχείριση όλων των πληροφοριών που σχετίζονται με τις απάτες.
- Η αύξηση στους προϋπολογισμούς των διωκτικών αρχών θα πρέπει να κατανέμεται ισορροπημένα μεταξύ του προσωπικού τους, του υλικού υπολογιστών και του λογισμικού για να βοηθήσει στην καλύτερη οργάνωση των ερευνών, στην ορθότερη κατάρτιση και στην εξειδικευμένη εκπαίδευση του προσωπικού, με στόχο την αντιμετώπιση του εγκλήματος. Οι ειδικές τεχνολογικές μονάδες οικονομικού ηλεκτρονικού εγκλήματος θα πρέπει να εκπαιδευθούν στην ανίχνευση, την έρευνα και την αποτροπή του οικονομικού ηλεκτρονικού εγκλήματος, με διεθνείς και κυβερνητικές συνεργασίες, δεδομένου του γεγονότος ότι τα τελευταία αποτελούν αδιαμφισβήτητα ένα παγκόσμιο φαινόμενο.
- Τέλος θα πρέπει να υπάρχει βούληση από κάθε Ελληνική κυβέρνηση η αναγκαιότητα της ενεργού ύπαρξης ελεγκτικού μηχανισμού που θα έχει ως προσανατολισμό τον έλεγχο και την πάταξη του οικονομικού ηλεκτρονικού εγκλήματος και δεν θα παραμείνει μόνο στον σχεδιασμό γιατί τότε το διαδικτυακό οικονομικό θα είναι πολύ επιζήμιο για την Εθνική Οικονομία μιας και το ηλεκτρονικό εμπόριο γνωρίζει τεράστια εξάπλωση και κατέχει σημαντικό μερίδιο στην αγορά.

13 Αναφορές

1. **Ηλεκτρονικό Εμπόριο**, ΠΑΣΧΟΠΟΥΛΟΣ Α.- ΣΚΑΛΤΣΑΣ Π., Εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ
2. Turban, E et al, **Electronic Commerce**: a Managerial Perspective (2000), Prentice Hall, New York
3. Θωμόπουλος Ν., **Στρατηγικές για την είσοδο μιας εταιρείας στο Διαδίκτυο**, ANUBIS, 2002.
4. Δουκίδης Γ. Ι. Θεμιστοκλέους Μ., Δράκος Β. Σ., Παπαζαφειροπούλου Α., **Ηλεκτρονικό εμπόριο**, Εκδ. Νέων Τεχνολογιών, 1998.
5. Kalakota R. and Whinston A, **Electronic Commerce: A Managers Guide**, (1996),Addison Wesley, New York.
6. Dien D. Phan, **"E-business development for competitive advantages: a case study"**, Information & Management, (2002)
7. Δουκίδης Γ., Α. Πουλυμενάκου, Ν. Γεωργόπουλος, Θ. Μότσιος, «**Το Ηλεκτρονικό Επιχειρείν στις μεγάλες ελληνικές επιχειρήσεις: Θέματα και Προοπτικές**», 2001
8. **Computer-Related Crime Impact** (Measuring the Incidence and Cost January 2004)
9. **Identity Fraud: A Critical National and Global Threat** (Dr. Gary R. Gordon & Mr. Norman A. Willox, Jr.)
10. **Europol, 2003 European Union organized crime report** (Section - Technology and crime)
11. **Use of cash payments for money laundering purposes** (COMPARATIVE STUDY INTO THE CURRENT LEGISLATIVE CONTROLS ON LARGE-SCALE CASH PAYMENTS WITHIN THE EU MEMBER STATES)
12. **COMPUTER-RELATED CRIME IMPACT: Measuring the Incidence and Cost** (Edward J. Appel, by By the Joint Council on Information Age Crime)
13. **E-Business και Προστασία Προσωπικών Δεδομένων**: σεβασμός του πολίτη στην Ψηφιακή Εποχή (Κωνσταντίνος Μουλίνος , Κωνσταντίνα Καμπουράκη)
14. Ραχανιώτου Ελένη, Ατζάμπου Ισιδώρα «**Ηλεκτρονικά Καταστήματα στο Internet**», 1998
15. **CyberSecurityBrochure2004** (DG JRC and Cyber-Security DG JRC and Cyber-Security)
16. **JRC Multi-Annual WΣφάλμα! Δεν βρέθηκαν καταχωρίσεις ευρετηρίου.ork programme 2003-2006.** (JRC Multi-Annual Workprogramme 2003-2006)
17. **McConnell-cybercrime.** (Cyber Crime . . . and Punishment - Archaic Laws Threaten Global Information)
18. **Evaluation of the activities.** (Evaluation of the activities of the European Anti-fraud Office - OLAF)
19. **FIGHT AGAINST FRAUD.** (PROTECTION OF THE FINANCIAL INTERESTS OF THE COMMUNITY AND FIGHT AGAINST FRAUD - COMMISSION OF THE EUROPEAN COMMUNITY)
20. **IFCC Referred 48000 - Fraud Complaints in 2002.** (IFCC 2002 Internet Fraud Report)

14 Ιστοσελίδες (Economic, Computer & Cyber Crime)

1. http://www.aic.gov.au/publications/tandi (Trends & Issues in Crime and Criminal Justice)
2. http://www.crimereduction.gov.uk (Resources for people working to reduce crime)
3. http://www.dcpcu.org.uk (The Dedicated Cheque and Plastic Crime Unit - DCPCU)
4. http://www.homeoffice.gov.uk/rds/adhocpubs1.html
5. http://www.heuni.fi/?sfgdata=4 (The European Institute for Crime Prevention and Control)
6. http://www.gcn.com/vol20_no9/news/4082-1.html (On the trail of cybersmugglers)
7. http://talkjustice.com/search.asp (The world's Criminal Justice Directory)
8. http://www.4law.co.il/6.html (CYBER CRIME UNITS AROUND THE GLOBE)
9. http://www.4law.co.il/hackingcases.htm (Computer Crime and Intellectual Property Section – CCIPS - Computer Intrusion Cases)
10. http://www.secretservice.gov/electronic_evidence.shtml (BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE)
11. http://www.interpol.int/Public/TechnologyCrime (Interpol's contribution to combating Information Technology Crime)
12. http://www.4law.co.il/Lea410.htm (ELECTRONIC EVIDENCE AND THE LAW)
13. http://www.sgrm.com/art24.htm (Forensic Computing)
14. http://www.britsoccrim.org/bccsp/vol04/alvesalo_tombs.html (Economic Crime Control Program in Finland)
15. http://www.chips.navy.mil/archives/96_jul/file3.htm (FIRST EVER COMPUTER WIRETAP ORDER)
16. http://www.epaynews.com (Payments News & Resource Center)
17. http://www.tnsofres.com ή http://www.tns-global.com (Welcome to TNS - A leading market information group)
18. http://europa.eu.int/comm/anti_fraud/index_el.html (Ευρωπαϊκή Υπηρεσία Καταπολέμησης της απάτης)
19. http://www.jrc.cec.eu.int (Joint Research Centre is a research based policy support organization and an integral part of the European Commission, providing the scientific advice and technical know-how to support EU policies)
20. http://www.jrc.cec.eu.int/langtech/AIM.html (Anti-fraud Information Management Sector)
21. http://www.jrc.cec.eu.int/langtech/AIM_2003.html (FP6 - Action n°4312 - Information Management to support Intelligence and Analysis in Anti-Fraud practice - IMIA)
22. http://www.jrc.cec.eu.int/langtech/index.html (Language Technology Activities in the AIM Sector)

14.1 Εναλλακτικές Ιστοσελίδες

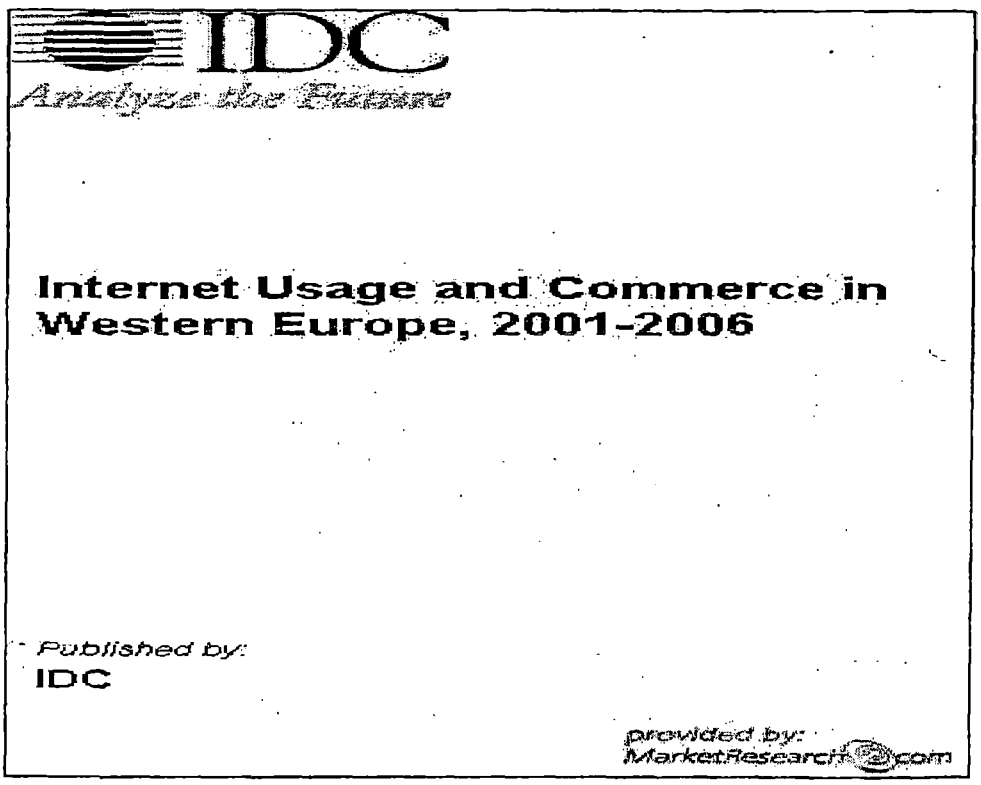
1. http://www.semper.org/sirene/outsideworld/ecommerce.html (Electronic Commerce, Payment Systems, and Security)
2. http://home.att.net/~s-prasad/ecsc.htm (Prasad's Electronic Commerce & Smart Cards Page)
3. http://www.batnet.com/oikoumene/ec_contracts.html (Electronic Commerce: On-line Contract Issues)
4. http://www.theregister.co.uk/2003/03/10/lawyer_cleared_in_bloomberg_extortion (Bloomberg extortion case)
5. http://www.theregister.co.uk/2003/02/06/bloomberg_extortion_hacking_case_opens (Bloomberg extortion, hacking case opens in New York)
6. http://www.cnn.com/2002/TECH/11/26/hln.wired.id.theft (Tackling identity theft)
7. http://www.cardcops.com (Πληροφορίες για απάτες σχετικά με πιστωτικές κάρτες και για την προστασία των κατόχων τους)

14.2 Ιστοσελίδες σχετικά με hi-tech crime

1. Interpol (http://www.interpol.int/Public/TechnologyCrime/default.asp)
2. Information Security and Forensics Society (http://www.isfs.org.hk)
3. Society for the Policing of Cyberspace (http://www.polcyb.org)
4. Hi-tech Crime Investigators Association (http://www.htcia.org)
5. United Nations (http://www.un.org)
6. UNAFEI (http://www.unafei.or.jp/)
7. Council of Europe (http://conventions.coe.int/)
8. Europol (http://www.europol.eu.int/home.htm)
9. Internet Engineering Task Force (http://ietf.org)
10. Scientific Working Group on Digital Evidence (SWGDE) (http://www.for-swg.org/swgdehm.htm)
11. International Organization on Computer Evidence (IOCE) (http://www.ioce.org)
12. APEC (http://www.apecsec.org.sg/)
13. OECD (http://www.oecd.org)

14.3 Ιστοσελίδες e-commerce

1. http://www.go-online.gr/goonline/programme/results/index.html
2. http://www.cosmo-one.gr/ebusiness_old/old_ecom016.htm
3. http://www.ebusinesslex.net
4. http://europa.eu.int/ISPO/ecommerce/research/Welcome.html
5. http://europa.eu.int/information_society/topics/ebusiness/ecommerce/11statistics/index_en.htm
6. http://ecommerce.internet.com/research/stats/article/0,3371,10371_157001,00.html
7. http://www.iobe.gr/meletes.php?ID=GK6
8. http://www.marketing-net.gr

9. http://www.electronicmarkets.org/modules/pub/view.php/electronicmarkets-462 (registered users only)
10. http://www.inlandrevenue.gov.uk/taxagenda/ecom1.htm#n5 (Growth of e-commerce in Europe – 1998)
11. http://www.marketresearch.com/map/prod/763662.html (Internet Usage and Commerce in Western Europe, 2001-2006 - This report sizes and forecasts the market for Internet usage and commerce in Western Europe per country - The 16 Western European countries covered are: Austria, Belgium, Denmark, Finland, France, Germany, **Greece**, Ireland, Italy, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom – **Buy Report**)
12. 

13. http://www.marketresearch.com/product/display.asp?productid=929915&SID=12146483-295267731-287324832&kw=e%2Dcommerce%09sales%09Western%09Europe (Jupiter Research Executive Survey, European Commerce, 2003: Taking the Pulse of E-commerce in Europe- **Buy Report**) http://www.exploit-lib.org/issue3/ecommerce/#ref-01 (e-commerce in Europe – 1999)
14. http://www.eubusiness.com/guides/e-commerce
15. http://www.emarketer.com/Article.aspx?1002328 (Europe E-Commerce to Grow Fourfold to 2006)
16. http://www.crm2day.com/news/crm/EpVZkEZFkpunOFVxee.php (Europe B2C E-Commerce Revenues to Top $240 Billion in Three Years)