ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Π.Μ.Σ. "ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ"

Διπλωματική Εργασία

Η Ασφάλεια της Πληροφορίας ως Επιχειρηματικό Μοντέλο

Γ. Τσιατούρας

Επιβλέπων: Επίκουρος Καθηγητής κ. Κ. Λαμπρινουδάκης

Πειραιάς, Μάιος 2014

Περιεχόμενα

Ευρετήριο Εικόνων

Αντιστοιχίσεις Όρων

Αγγλικά	Ελληνικά
Accountability	Λογοδοσία
Annual Loss Exposure (ALE)	Ετήσια έκθεση σε πιθανές απώλειες από περιστατικά ασφάλειας
Annual Rate of Occurrence (ARO)	Ετήσια συχνότητα εμφάνισης περιστατικών ασφάλειας
Architecture DI (BMIS term)	Σύνδεσμος που αντιπροσωπεύει την αρχιτεκτονική των υποδομών
Automated Teller machine (ATM)	Μηχάνημα Αυτόματης Ανάληψης
Automatic Database Diagnostic Monitor (ADDM)	Διαγνωστικό εργαλείο ανίχνευσης πληροφοριακών συστατικών
Build-in security	Ενσωματωμένη ασφάλεια
Business processes	Επιχειρηματικές διεργασίες
Business requirements	Επιχειρηματικές απαιτήσεις
Change Management	Διαχείριση Αλλαγών
Chief Information Security Officer (CISO)	Επικεφαλής Ασφάλειας Πληροφοριών
Configuration Item (CI)	Στοιχείο Διαμόρφωσης
Configuration Management Data Base (CMDB)	Σύστημα Διαχείρισης Στοιχείων Διαμόρφωσης
Control environment	Περιβάλλον ελέγχου
Culture DI (BMIS term)	Σύνδεσμος που αντιπροσωπεύει την συλλογική κουλτούρα
Day-to-day operations	Καθημερινή ροή εργασιών
Data Loss Prevention (DLP)	Σύστημα Αποτροπής Διαρροής Δεδομένων
Dynamic Interconnections – DIs (BMIS term)	Οι σύνδεσμοι του BMIS
Elements (BMIS term)	Τα στοιχεία του BMIS
Emergence DI (BMIS term)	Σύνδεσμος που αντιπροσωπεύει την ανάδειξη αναγκών
Emergency changes	Επείγουσες αλλαγές
Enabling and Support DI (BMIS term)	Σύνδεσμος που αντιπροσωπεύει την υποστήριξη της τεχνολογίας
Event correlation	Συσχετισμός γεγονότων
False positive	Ψευδώς αληθές
Firewall	Τοίχος προστασίας
Gap analysis	Ανάλυση αποκλίσεων από τις αρχικές απαιτήσεις
Governing DI (BMIS term)	Σύνδεσμος που αντιπροσωπεύει τη διακυβέρνηση των διεργασιών πληροφορικής
Human error	Ανθρώπινο σφάλμα
Human Factors DI (BMIS term)	Σύνδεσμος που αντιπροσωπεύει το απρόβλεπτο του ανθρώπινου παράγοντα
Human - Computer Interface (HCI)	Διεπαφή ανθρώπου - υπολογιστή
Incident escalation	Κλιμάκωση περιστατικών
Information Security Management System (ISMS)	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
Intrusion Detection System (IDS)	Σύστημα Εντοπισμού Εισβολών
Intrusion Prevention System (IPS)	Σύστημα Αποτροπής Εισβολών
IT Management Suite (ITMS)	Πλατφόρμα Διαχείρισης Υπηρεσιών Πληροφορικής
IT Quality Management System (ITQMS)	Σύστημα Παρακολούθησης Ποιότητας Πληροφορικής

Αγγλικά	Ελληνικά
IT Service Management System (ITSMS)	Σύστημα Διαχείρισης Υπηρεσιών Πληροφορικής
IT silos	Μηχανογραφικές νησίδες
Lessons learned (PMBOK term)	Στάδιο διαχείρισης έργων για την καταγραφή των διδαγμάτων
Logical security	Λογική ασφάλεια
Low-level Risk Assessment	Ανάλυση επικινδυνότητας σε κάθε πληροφοριακό αγαθό
Network Management System (NMS)	Σύστημα Διαχείρισης Δικτύου
Organization (BMIS element)	Στοιχείο που αντιπροσωπεύει τους επιχειρησιακούς στόχους του οργανισμού
Organizational silos	Οργανωτικές νησίδες
Outsourcing	Εξωτερική ανάθεση εργασίας
Ownership	Κυριότητα
People (BMIS element)	Στοιχείο που αντιπροσωπεύει τους ανθρώπους που απαρτίζουν τον οργανισμό
Performance monitoring tool	Εργαλείο για την παρακολούθησης των επιδόσεων των συστημάτων
Physical security	Φυσική ασφάλεια
Prioritization	Προτεραιοποίηση
Process (BMIS element)	Στοιχείο που αντιπροσωπεύει τις διεργασίες ασφάλειας
Reasonable assurance	Εύλογη διασφάλιση
Release	Έκδοση
Responsibility	Ευθύνη
Risk assessment	Ανάλυση επικινδυνότητας
Risk exposure	Έκθεση σε κίνδυνο
Risk mitigation	Μετρίαση επικινδυνότητας
Security best practices	Βέλτιστες πρακτικές ασφάλειας
Security breach	Παραβίαση της ασφάλειας
Security control	Δικλείδα ασφάλειας
Security framework	Πλαίσιο ασφάλειας
Security Incident Management	Διαχείριση Περιστατικών Ασφάλειας
Security Information and Event Management (SIEM)	Σύστημα Συλλογής Πληροφοριών από Γεγονότα Ασφάλειας
Security Office	Υπηρεσία Εποπτείας των Επιπέδων Ασφάλειας
Security programme	Πρόγραμμα ασφάλειας
Security standard	Πρότυπο ασφάλειας
Service Desk	Υπηρεσία Εξυπηρέτησης
Service Level Agreement (SLA)	Συμβόλαιο Διασφάλισης Επιπέδου Ποιότητας
Single Loss Exposure (SLE)	Έκθεση σε απώλεια μεμονωμένου περιστατικού
Technology (BMIS element)	Στοιχείο που αντιπροσωπεύει την εφαρμοζόμενη τεχνολογία
User acceptance	Αποδοχή των χρηστών
User friendliness	Φιλικότητα της τεχνολογίας προς το χρήστη
Version control	Έλεγχος έκδοσης εντύπων
Vulnerability	Ευπάθεια

Περίληψη

Σε έναν οργανισμό, ανάμεσα στα στελέχη του *business* και στα όργανα της Ασφάλειας της Πληροφορίας, βρίσκονται πάντα οι λειτουργίες της Πληροφορικής. Το μεν *business* έχει ως αποστολή την επίτευξη των επιχειρηματικών του στόχων με ευκολία και αποδοτικότητα ενώ το *Security Office* έχει ως αποστολή την διασφάλιση της επίτευξης των στόχων αυτών με ασφάλεια. Τις περισσότερες φορές οι δύο αυτές μονάδες έχουν αντικρουόμενες προτεραιότητες, δημιουργώντας λειτουργικά προβλήματα στη ροή εργασιών της Πληροφορικής τα οποία ξεκινούν από το έλλειμμα επικοινωνίας μεταξύ των τριών οντοτήτων.

Στα πλαίσια αυτά πραγματοποιείται έρευνα πάνω στα Οικονομικά της Ασφάλειας με σκοπό την εξεύρεση μεθόδων υπολογισμού της βέλτιστης επενδυτικής απόδοσης των *security controls*. Ωστόσο, το συγκεκριμένο πεδίο αντιμετωπίζεται με σκεπτικισμό αναφορικά με την αξιοπιστία των μελετών που παράγει. Μία άλλη άποψη, με εξίσου μεγάλο ενδιαφέρον, είναι αυτή που προσεγγίζει την Ασφάλεια της Πληροφορίας ως έναν επιπλέον επιχειρηματικό στόχο και όχι ως μία παράλληλη λειτουργία της Πληροφορικής, θέτοντάς την στα χέρια της υψηλής Διοίκησης. Βασική προϋπόθεση ωστόσο είναι η υψηλή Διοίκηση να αντιλαμβάνεται πλήρως τις απαιτήσεις ασφάλειας και τις πιθανές επιπτώσεις από τη μη επίτευξη αυτών. Με βάση αυτή την προσέγγιση, έχουν ξεκινήσει να αναπτύσσονται επιχειρηματικά μοντέλα τα οποία θέτουν στον πυρήνα τους την Ασφάλεια της Πληροφορίας και που μπορούν να αξιοποιηθούν από κάθε οργανισμό ο οποίος στηρίζεται σε σύνθετα πληροφοριακά αγαθά.

Στην εισαγωγή της υπάρχουσας μελέτης, αναλύεται το επικοινωνιακό πρόβλημα μεταξύ των οργανωτικών οντοτήτων σχετικά με την ασφάλεια ενώ έπειτα γίνεται και μία αναφορά στις προσπάθειες επίλυσής του μέσω των Οικονομικών της Ασφάλειας. Στη συνέχεια παρουσιάζεται μία επίκαιρη εικόνα των περιστατικών ασφάλειας σε παγκόσμια κλίμακα προκειμένου να γίνει αντιληπτή η ανάγκη για περισσότερη συμμετοχή της Διοίκησης στην Ασφάλεια της Πληροφορίας. Έπειτα παρουσιάζεται η πρόταση του *ISACA* για την Ασφάλεια της Πληροφορίας ως επιχειρηματικό μοντέλο και πάνω σε αυτήν την πρόταση πραγματοποιούνται τρεις μελέτες περίπτωσης πάνω σε ελληνικό όμιλο εταιρειών ο οποίος δραστηριοποιείται κυρίως στον τραπεζικό τομέα.

1. Εισαγωγή

Η Ασφάλεια Πληροφοριακών Συστημάτων αποτελεί σήμερα έναν από τους σημαντικότερους κλάδους της Πληροφορικής τόσο στο χώρο της έρευνας και της τεχνολογίας όσο και στο χώρο των επιχειρήσεων. Όντας σε ένα σχετικά καινούργιο επιστημονικό πεδίο, οι Αναλυτές της Ασφάλειας Πληροφοριακών Συστημάτων καλούνται να πλαισιώσουν την ειδικότητά τους με πληθώρα γνώσεων σε *hands-on* αξιολόγηση ασφάλειας, σε θέματα συμμόρφωσης και προτυποποίησης καθώς και σε θέματα αρχιτεκτονικού σχεδιασμού και διακυβέρνησης. Ταυτόχρονα οι ικανότητες στην ανάλυση και τη διαχείριση των κινδύνων Πληροφοριακών Συστημάτων αποτελούν σπουδαία αναγκαιότητα για τον αναλυτή ασφάλειας, μίας αναγκαιότητας που προκύπτει από την ίδια την αγορά της Πληροφορικής. Σε ένα περιβάλλον όπου καθημερινά οι αγοραστικές ανάγκες μεταβάλλονται και που η στρατηγική για την επιτυχία των περισσοτέρων οργανισμών βασίζεται στις καινοτόμες τεχνολογίες, οι νέοι κίνδυνοι αναδύονται με όλο και μεγαλύτερη συχνότητα. Ένας ειδικός σε θέματα Ασφάλειας Πληροφοριακών Συστημάτων οφείλει να διακρίνει τον οποιοδήποτε κίνδυνο εισάγεται από κάθε τάση, ανάγκη ή μεταβολή προκύπτει στο επιχειρησιακό περιβάλλον και να σχεδιάζει ικανοποιητικές δικλείδες ασφάλειας για την αποτροπή των κινδύνων ή τη μετρίαση αυτών.

Παρόλο που η ανάγκη για την Ασφάλεια της Πληροφορίας αποτελεί αποδεδειγμένη ανάγκη είτε μέσω προτύπων κανονιστικής συμμόρφωσης είτε μέσω περιστατικών με ανεπανόρθωτες συνέπειες που έχουν συμβεί κατά καιρούς από κακόβουλους και μη, η Ασφάλεια Πληροφοριακών Συστημάτων εξακολουθεί να αντιμετωπίζεται ως «αναγκαίο κακό» από τις διοικήσεις των οργανισμών, συχνά με το χαρακτηρισμό «κακό» να υπερτερεί του χαρακτηρισμού «αναγκαίο». Ως συνέπεια, οι αναλυτές ασφάλειας, πολύ συχνά αναγκάζονται να επιτελέσουν το έργο τους με χαμηλό προϋπολογισμό, περιορισμένο και ανειδίκευτο προσωπικό και χωρίς τη δέσμευση της Διοίκησης για υποστήριξη. Ωστόσο το καθήκον της απρόσκοπτης λειτουργίας των μηχανογραφικών συστημάτων του οργανισμού βαρύνει αποκλειστικά τους αναλυτές ασφάλειας δημιουργώντας μία σχέση ανισότητας μεταξύ του *business* που έχει τον πρώτο λόγο και του *security* που έχει την αποκλειστική ευθύνη.

Από την πλευρά του *business*, οι πρωταρχικοί στόχοι σε έναν οργανισμό δεν μπορεί να είναι άλλοι από του επιχειρηματικούς στόχους. Συνεπώς ένα πρόγραμμα ασφάλειας το οποίο ορίζεται πάνω στις μηχανογραφικές διεργασίες του οργανισμού μπορεί είτε να έρθει σε πλήρη αντίθεση με τις διοικητικές επιλογές για τους στρατηγικούς στόχους είτε να μη γίνει αντιληπτό στο βαθμό που χρειάζεται ώστε να δοθεί η απαραίτητη δέσμευση για υλοποίηση. Λαμβάνοντας υπόψη και το ότι η ασφάλεια συχνά κοστίζει πολλά χρήματα

καθώς και το γεγονός ότι ποτέ δεν μπορεί να επιτευχθεί απόλυτη ασφάλεια απέναντι στους συνεχώς αναδυόμενους κινδύνους τότε εύκολα μπορεί κάποιος να κατανοήσει τον σκεπτικισμό που διέπει τους ανθρώπους του *business* σχετικά με την αποτελεσματικότητα ενός κοστοβόρου *security programme*.

Ακριβώς αυτό το πρόβλημα «επικοινωνίας» μεταξύ *business* και *security* είναι που έχει απασχολήσει ιδιαίτερα τους ανθρώπους τόσο της Πληροφορικής όσο και της Οργάνωσης και Διοίκησης. Σε αυτό το πλαίσιο, στις αρχές τις προηγούμενης δεκαετίας άρχισε να γίνεται αντιληπτή η ανάγκη για την ένταξη της Ασφάλειας Πληροφοριακών Συστημάτων στις επιχειρηματικές λειτουργίες των οργανισμών. Πράγματι, οι κίνδυνοι Πληροφορικής είναι λειτουργικοί κίνδυνοι συνεπώς και οι κίνδυνοι ασφάλειας δε θα μπορούσε να είναι τίποτα διαφορετικό στο περιβάλλον ενός οργανισμού με σύνθετα και κρίσιμα πληροφοριακά συστήματα. Το πρόβλημα επικοινωνίας όμως παρέμεινε κάνοντας αισθητή την παρουσία του στις καθημερινές λειτουργίες σχεδόν όλων των μεγάλων οργανισμών.

Ωστόσο οφείλει κάποιος να παραδεχτεί ότι η αναγνώριση για την ανάγκη της Ασφάλειας Πληροφοριακών Συστημάτων έχει αυξηθεί σημαντικά. Υπάρχουν πολλά *security standards* τα οποία μπορούν να αξιοποιηθούν τόσο για την αξιολόγηση της ασφάλειας όσο και για το σχεδιασμό *security controls* και άλλα τόσα πλαίσια ασφάλειας *(frameworks)* τα οποία μπορούν να χρησιμοποιηθούν σαν οδηγοί στις μεθόδους υλοποίησης, ωστόσο σε κανένα από αυτά δεν περιγράφονται οι ιδιαιτερότητες που προκύπτουν από χαρακτηριστικά όπως η γεωγραφική θέση, το είδος της βιομηχανίας, το μέγεθος του οργανισμού και τα κανονιστικά πλαίσια και πρωτόκολλα. Πολλοί πιστεύουν ότι εφόσον ο οργανισμός τους είναι απόλυτα συμμορφωμένος με κάποιο διεθνές πρότυπο ή πλαίσιο ασφάλειας τότε δεν υπάρχει τίποτα καλύτερο στο οποίο να μπορούν να επενδύσουν. Παρόλο που τα πρότυπα των βέλτιστων πρακτικών συνθέτουν σίγουρα πολύ καλές στρατηγικές για την προστασία των πληροφοριακών συστημάτων, υπάρχει ένα πολύ σημαντικό στοιχείο το οποίο απουσιάζει από αυτά και αυτός δεν είναι άλλος από το ρόλο του *business* και τους στρατηγικούς εταιρικούς στόχους. Τα πρότυπα έχουν αποδείξει τη χρησιμότητά τους στην ανάδειξη συγκεκριμένων αναγκών ασφάλειας αλλά αποτυγχάνουν στο να παρέχουν ολιστικές λύσεις οι οποίες εξετάζουν το σύνολο των διαδικασιών μιας επιχείρησης και κυρίως το πώς οι επιχειρησιακοί στόχοι επηρεάζουν το *security programme* αλλά και αντιστρόφως.

Το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής, εφεξής *ISACA (Information Systems Audit and Control Association)*, το 2010 εξέδωσε το λεγόμενο *BMIS (Business Model for Information Security)* [1]. Η συγκεκριμένη μελέτη έδωσε μεγαλύτερη έμφαση στο επιχειρησιακό περιβάλλον εντός του οποίου λειτουργούν οι διεργασίες Ασφάλειας Πληροφοριακών Συστημάτων και στις αλληλεπιδράσεις τους με τις υπόλοιπες

επιχειρησιακές διεργασίες. Αυτή η εστίαση της ασφάλειας στους επιχειρησιακούς στόχους, έδωσε διαφορετική διάσταση στην εφαρμογή προτύπων θέτοντας στο επίκεντρο του ενδιαφέροντος όχι τις διεργασίες ασφάλειας αλλά τις διεργασίες του *business*. Το *BMIS* το οποίο αξιοποιείται για τη μελέτη της παρούσας εργασίας, σύντομα εντάχθηκε στο πλαίσιο Διακυβέρνησης Πληροφορικής *COBIT 5* [2] το οποίο σήμερα θεωρείται το πιο ολοκληρωμένο και σύγχρονο εργαλείο διοίκησης και διαχείρισης πληροφοριακών συστημάτων σε εταιρικά περιβάλλοντα.

2. Τα Οικονομικά της Ασφάλειας

Για να είναι κάποιος αναλυτής ασφάλειας σε θέση να κατανοήσει το για πιο λόγο η Ασφάλεια Πληροφοριακών Συστημάτων πρέπει να προσεγγίζεται ως *business* διεργασία, θα πρέπει να βάλει τον εαυτό του στο ρόλο της Διοίκησης και να αναλογιστεί το πώς η ασφάλεια μπορεί να συμβάλει στην επιτυχία της επιχείρησης χωρίς να την επιβαρύνει ανώφελα. Αυτό σημαίνει ότι η ασφάλεια θα πρέπει να αντιμετωπίζεται τόσο από τους αναλυτές της ασφάλειας όσο και από τους ανθρώπους της Διοίκησης ως επένδυση για τη βιωσιμότητα του οργανισμού και όχι ως ανώφελη δαπάνη ή αναγκαίο κακό.

Η πραγματικότητα αυτή είναι που έχει οδηγήσει στην εκπόνηση μεγάλου όγκου μελετών πάνω στα Οικονομικά της Ασφάλειας, με την ανάπτυξη μοντέλων για την ορθή λήψη αποφάσεων στην προστασία την πληροφορίας και της ιδιωτικότητας σε εταιρικά περιβάλλοντα. Πρώτος ο *Ross Anderson* [3] υπέδειξε ότι τα προβλήματα της ασφάλειας μπορούν να εξηγηθούν πιο εύστοχα και κατανοητά αξιοποιώντας την ορολογία της μακροοικονομίας. Σύμφωνα με τη μελέτη του, ένα σημαντικό πρόβλημα για την ασφάλεια είναι η έλλειψη ευθυγράμμισης των κινήτρων με την ίδια την τεχνολογία ώστε να υπάρχει και η κατάλληλη υιοθέτηση της καινοτόμας τεχνολογίας για ανάπτυξη μέτρων ασφάλειας. Επομένως οι οικονομικές προβλέψεις και αποδόσεις θα πρέπει να ενσωματώνονται σε επίπεδο τεχνικού σχεδιασμού για κάθε καινοφανή τεχνολογία ασφάλειας ώστε οι ενδιαφερόμενοι να είναι σε θέση να εξάγουν συμπεράσματα για την αποτελεσματικότητά τους στη μετρίαση των κινδύνων ασφάλειας.

Πολλοί θεωρούν τη μελέτη του *Anderson* ως τη γενεσιουργό των Οικονομικών της Ασφάλειας, ενός τομέα ο οποίος πλέον έχει αποκτήσει ιδιαίτερα έντονη ερευνητική δραστηριότητα τόσο στον ακαδημαϊκό χώρο όσο και στο χώρο των επιχειρήσεων, ειδικά στον τομέα της ασφάλισης *(insurance)*. Ασχέτως όμως του επιχειρηματικού πεδίου εφαρμογής ενός οργανισμού, όπως κάθε επιχειρηματική δραστηριότητα έτσι και η Ασφάλεια των Πληροφοριακών Συστημάτων πρέπει να προσεγγίζεται βάσει των οικονομικών ωφελειών που αυτή μπορεί να προσφέρει και όχι βάσει των τεχνολογικών τάσεων.

“A smart company needs to approach security as it would any other business decision: Costs versus benefits”. Bruce Schneier [4]

2.1 Η Επενδυτική Απόδοση της Ασφάλειας (ROSI)

Δεν είναι λίγες οι φορές όπου η Διοίκηση απαιτεί από την Πληροφορική να γνωστοποιήσει τις οικονομικές ωφέλειες των έργων ασφάλειας χωρίς ωστόσο να είναι άμεσα εφικτή η ποσοτικοποίησή τους σε χρήμα. Σε αυτήν την κατεύθυνση έχουν αναπτυχθεί μοντέλα *ROSI (Return Of Security Investment)* [5], ο δείκτης των οποίων βασίζεται στη σχέση *ROI (Return of Investment)* [6] και έχει ως εξής:

$$\boldsymbol{ROSI} = \frac{(\boldsymbol{Risk\ Exposure} \cdot \boldsymbol{Risk\ Mitigation}\%) - \boldsymbol{Solution\ Cost}}{\boldsymbol{Solution\ Cost}} \quad (1)$$

Για την ποσοτικοποίηση των μεταβλητών *Risk Exposure, Risk Mitigation* της σχέσης υφίσταται πληθώρα μεθοδολογιών ανάγοντας το πρόβλημα στον τρόπο επιλογής της μεθοδολογίας καθώς και στην πραγματογνωμοσύνη του εκάστοτε αναλυτή επικινδυνότητας.

Μία απλή μέθοδος για τον υπολογισμό της έκθεσης στον κίνδυνο *(Risk Exposure)* είναι ο πολλαπλασιασμός του κόστους ζημιάς που προκύπτει από ένα μεμονωμένο περιστατικό *(Single Loss Exposure, SLE)* με την προβλεπόμενη συχνότητα εμφάνισης ανά έτος *(Annual Rate of Occurrence, ARO)*. Το αποτέλεσμα δίνει την ετήσια έκθεση απωλειών *(Annual Loss Exposure, ALE)*, ήτοι:

$$\boldsymbol{Risk\ Exposure} = \boldsymbol{ALE} = \boldsymbol{SLE} \cdot \boldsymbol{ARO} \quad (2)$$

Η συλλογή στοιχείων για τον υπολογισμό του κόστους ζημίας ενός μεμονωμένου περιστατικού *(SLE)* ωστόσο μπορεί να αποδειχθεί εξαιρετικά δύσκολη και περίπλοκη διαδικασία. Αυτό συμβαίνει αφενός μεν λόγω του ότι οι περισσότεροι οργανισμοί συχνά δεν υιοθετούν επαρκείς μηχανισμούς ανίχνευσης περιστατικών ασφάλειας και αφετέρου δε λόγω του ότι τα περιστατικά ασφάλειας τα οποία δεν έχουν άμεσο και εμφανή αντίκτυπο στην καθημερινή ροή εργασιών *(day-to-day operations)* συνήθως περνάνε απαρατήρητα [5]. Τις περισσότερες φορές μάλιστα που τα περιστατικά ασφάλειας γίνονται αντιληπτά ο χρόνος που απομένει από την ορθή αντιμετώπιση του περιστατικού είναι πολύ λίγος ώστε να υπολογιστούν και οι οικονομικές συνέπειες. Επίσης δεν είναι λίγες οι περιπτώσεις όπου περιστατικά ασφάλειας τα οποία γίνονται αντιληπτά, ενώ αντιμετωπίζονται ώστε να μην επαναληφθούν, να μην γνωστοποιούνται πουθενά πέραν του άμεσα αρμοδίου χώρου. Ως εκ τούτου, ο όγκος δεδομένων που παρέχεται από τα καταγεγραμμένα περιστατικά ασφάλειας τις περισσότερες φορές είναι ανεπαρκής ώστε να μπορέσουν να εξαχθούν ορθές *ALE* τιμές για κάθε ομάδα περιστατικών ασφάλειας.

Ο υπολογισμός του κόστους της μετρίασης του κινδύνου *(Risk Mitigation)* είναι εξίσου δύσκολη υπόθεση. Το πρόβλημα έγκειται στο γεγονός ότι η ασφάλεια δεν δημιουργεί «απτά» οφέλη αλλά εμποδίζει την οικονομική απώλεια από εν δυνάμει ζημιές. Η απώλεια

όμως η οποία αποτρέπεται δεν μπορεί και να γίνει γνωστή ώστε να υπολογιστεί με οικονομικούς όρους. Συνεπώς ο υπολογισμός της εν λόγω μεταβλητής εξαρτάται αποκλειστικά από τη μέθοδο εκτίμησης και τους υπολογιστικούς αλγόριθμους που αξιοποιούνται. Τα πλαίσια βέλτιστων πρακτικών που έχουν εκδοθεί από οργανισμούς προτυποποίησης όπως οι *International Security Forum (ISF), National Institute of Standards in Technology (NIST),* και *International Standards Organization (ISO)* μπορούν να αποδειχθούν εξαιρετικά χρήσιμα εργαλεία για τη δημιουργία σχετικά αξιόπιστων μεθόδων εκτίμησης ενώ για τη δημιουργία υπολογιστικών αλγόριθμων, αξίζει να σημειωθεί ότι υπάρχουν όλο και περισσότερες προτάσεις που αξιοποιούν μοντέλα Τεχνητών Νευρωνικών Δικτύων *(Artificial Neural Networks)* [7].

Είναι φανερό ωστόσο ότι όσο αξιόπιστες μεθόδους και να χρησιμοποιήσει κάποιος σε έναν *ROSI* υπολογισμό δεν θα μπορέσει ποτέ να απαλλαγεί από το μεγάλο πλήθος προσεγγίσεων. Το κόστος των περιστατικών ασφάλειας καθώς και η ετήσια συχνότητα εμφάνισής τους είναι δύσκολο να υπολογιστούν ενώ οι τιμές τους μπορούν να έχουν εξαιρετικά μεγάλη απόκλιση σε διαφορετικά περιβάλλοντα. Στα παραπάνω έρχεται να προστεθεί και η διαφοροποίηση της ικανότητας αντίληψης κινδύνου από άνθρωπο σε άνθρωπο (πολιτισμική θεωρία, ψυχομετρικό πρότυπο, *SARF*) [8].

Για έναν ανεξάρτητο αναλυτή, η ακρίβεια των στατιστικών δεδομένων τα οποία χρησιμοποιούνται σε ένα *ROSI* υπολογισμό είναι μεγάλης σημασίας. Τα πραγματικά δεδομένα τα οποία όμως μπορεί να προκύπτουν από υπαρκτά περιστατικά ασφάλειας ενδέχεται να είναι δύσκολο να εντοπιστούν λόγω του το ότι και οι ίδιοι οι οργανισμοί παρουσιάζουν διστακτικότητα στο να παράσχουν στον αναλυτή τις σχετικές πληροφορίες [9]. Πολλές φορές αποδεικνύεται προτιμότερη η έρευνα πάνω στο ιστορικό των περιστατικών του οργανισμού παρά η ανάθεση μιας *ROSI* ανάλυσης σε έναν πάροχο.

2.2 Το μοντέλο Gordon & Loeb

Ένα αρκετά δημοφιλές μοντέλο στο χώρο της έρευνας των Οικονομικών της Ασφάλειας είναι το μοντέλο που παρουσίασαν στη μελέτη τους οι οικονομολόγοι *Lawrence Gordon* και *Martin Loeb* [10]. Βάσει αυτού του μαθηματικού μοντέλου, σε αντίθεση με τα όσα επιτάσσουν οι αρχές της ανάλυσης επικινδυνότητας, ένα πληροφοριακό αγαθό υψηλής αξίας δεν είναι απαραίτητο να προστατευθεί με μία πολύ δαπανηρή επένδυση. Η βέλτιστη δαπάνη για την προστασία ενός πληροφοριακού αγαθού δεν είναι πάντα ανάλογη της αξίας του αφού στην πραγματικότητα υφίσταται ένα σημείο δαπάνης από το οποίο και έπειτα η επένδυση για την ασφάλειας του πληροφοριακού αγαθού κρίνεται ασύμφορη.

Σύμφωνα με τους *Gordon* και *Loeb*, *«η βέλτιστη δαπάνη για την Ασφάλεια Πληροφοριακών Συστημάτων δεν μπορεί ποτέ να ξεπεράσει το 37% της εν δυνάμει οικονομικής απώλειας που μπορεί να προκύψει από ένα περιστατικό ασφάλειας»* [10].

Το εν λόγω μαθηματικό μοντέλο έχει χρησιμοποιηθεί ως αναφορά σε εκατοντάδες δημοσιεύσεις, στην ακαδημαϊκή και επαγγελματική βιβλιογραφία αφού στην ουσία ήταν το πρώτο το οποίο έθεσε απτά όρια στα Οικονομικά της Ασφάλειας τα οποία επιπλέον συνοδεύονταν από μαθηματική θεμελίωση. Επίσης, το μοντέλο έχει δοκιμαστεί σε διάφορα περιβάλλοντα πληροφορικής, σε μελέτες οι οποίες εστιάζουν στην συσχέτιση της βέλτιστης δαπάνης για επένδυση στην ασφάλεια και το βαθμό της ευπάθειας *(vulnerability)* των πληροφοριακών συστημάτων [11].

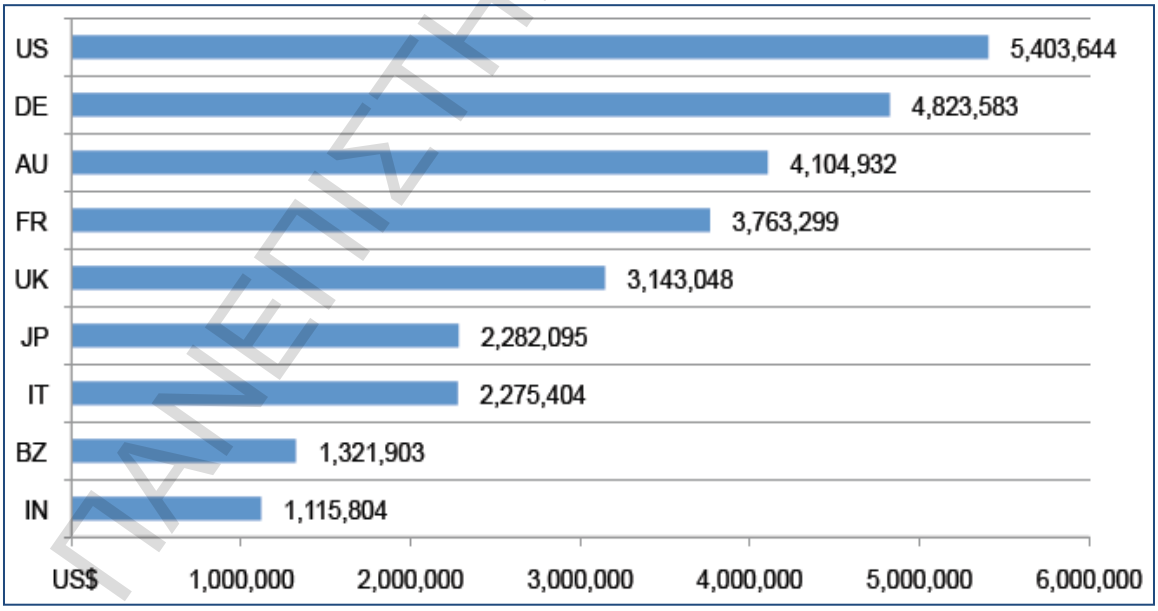
Ωστόσο το μοντέλο *Gordon & Loeb* έχει επικριθεί από μία άλλη μελέτη [12], η οποία αξιοποιώντας τα ίδια σενάρια δείχνει ότι η βέλτιστη επένδυση ασφάλειας ενδέχεται να ξεπεράσει το 50% ενώ μεταβάλλοντας τις αρχικές συνθήκες του περιβάλλοντος που παρουσιάζουν οι *Gordon* και *Loeb,* η περίπτωση κατά την οποία η βέλτιστη δαπάνη μπορεί να φτάσει και το 100% της απώλειας από περιστατικό ασφάλειας δεν είναι καθόλου απίθανη.

Αυτές οι αντικρουόμενες μελέτες αποδεικνύουν ότι οι υπολογισμοί που προκύπτουν από τις διάφορες *ROSI* μεθόδους θα πρέπει να λαμβάνονται υπόψη μόνο ενδεικτικά και όχι ως αυστηροί κανόνες αφού το πιθανότερο είναι ότι ποτέ δεν θα υπάρξει κάποιος *ROSI* υπολογισμός ο οποίος να είναι απόλυτα ακριβής [9].

3. Τα κόστη των περιστατικών Ασφάλειας σε παγκόσμια κλίμακα

Οι ραγδαίες αλλαγές στην τεχνολογία, η παγκόσμια δικτύωση καθώς και η αυξανόμενη αξία της έγκυρης και άμεσης πληροφόρησης έχουν αναδείξει την ανάγκη για αποτελεσματικές μεθόδους διαχείρισης κινδύνων Πληροφοριακών Συστημάτων. Στην προσπάθεια των οργανισμών να διατηρηθούν επικερδείς, είναι εύκολα αναγνωρίσιμο το γεγονός ότι ένα περιστατικό ασφάλειας – ή καλύτερα, ένα «ρήγμα ασφάλειας» *(security breach)*, να έχει καταστροφικές συνέπειες είτε με άμεσο τρόπο (απώλεια χρημάτων) είτε με έμμεσο, βλάπτοντας την αξιοπιστία και τη φήμη του οργανισμού. Οι αναλυτές ασφάλειας βρίσκονται πλέον στη θέση να είναι οι υπεύθυνοι, μεταξύ άλλων, και για την προστασία του *brand* του οργανισμού για τον οποίο εργάζονται.

Την εικόνα της Ασφάλειας της Πληροφορίας καθώς και τις οικονομικές επιπτώσεις που έχουν τα *security breaches* καταγράφει σε ετήσια βάση το *Ponemon Institude* το οποίο διενεργεί ανεξάρτητες και εμπειρικές μελέτες σε παγκόσμιο επίπεδο για την ασφάλεια και την ιδιωτικότητα με σκοπό την βαθύτερη κατανόηση των πρακτικών και των τάσεων που ισχύουν. Σύμφωνα με την τελευταία ετήσια μελέτη για το έτος 2013 [13], το άθροισμα του κόστους των περιστατικών ασφάλειας ξεπερνάει την τάξη του εκατομμυρίου σε αμερικάνικα δολάρια για τις εννέα χώρες με τη μεγαλύτερη δραστηριότητα περιστατικών ασφάλειας (εικόνα 1).

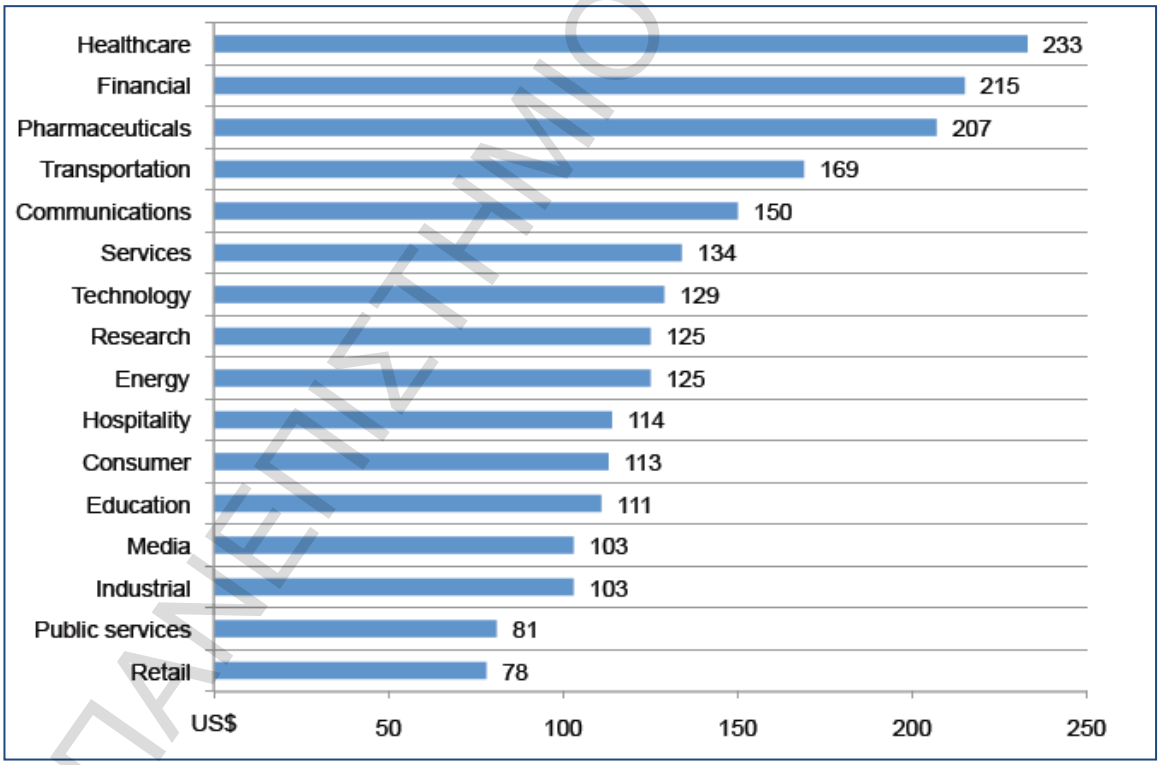


Εικόνα 1: Κόστος περιστατικών ανά χώρα (Ponemon, "2013 Data Breach Study")

Η εικόνα του μεγάλου κόστους των περιστατικών ασφάλειας παραμένει αρκετά μεγάλη παρόλο που τα τελευταία χρόνια έχουν αναπτυχθεί ολοένα και πιο αποτελεσματικές

τεχνολογίες ασφάλειας. Ο λόγος είναι η συνεχώς αυξανόμενη «ανάγκη για πληροφορία» και η μεγάλη εξάρτηση των οργανισμών από τη διαχείριση και τη μηχανογράφησή της. Συνεπώς, ενώ από τη μία αναπτύσσονται τεχνικές υλοποίησης προηγμένων τεχνικών ασφάλειας από την άλλη αυξάνεται και η έκθεση στους κινδύνους Ασφάλειας Πληροφοριακών Συστημάτων.

Το μέσο κατά κεφαλήν κόστος για το κάθε *security breach* υπολογίζεται από την ίδια εμπειρική μελέτη στα $136 [21]. Ωστόσο σε συγκεκριμένους τύπους βιομηχανιών το μέσο κατά κεφαλήν κόστος υπολογίζεται αρκετά μεγαλύτερο. Τομείς όπως αυτοί της υγειονομικής περίθαλψης, των χρηματοοικονομικών και των φαρμακευτικών παρουσιάζουν εμφανώς μεγάλη απόκλιση από τη μέση τιμή του κατά κεφαλήν κόστους ζημιάς. Ο λόγος είναι διότι σε αυτού του τύπου τις βιομηχανίες γίνεται διαχείριση ευαίσθητων προσωπικών δεδομένων όπως ιατρικά ιστορικά και οικονομικά δεδομένα (εικόνα 2). Σημειώνεται ότι με τον όρο «κατά κεφαλήν κόστος» *("per capita cost")* των *security breaches* ορίζεται το συνολικό κόστος ενός μεμονωμένου περιστατικού ασφάλειας διαιρεμένου με το πλήθος των εγγραφών των δεδομένων που διέρρευσαν ή χάθηκαν.

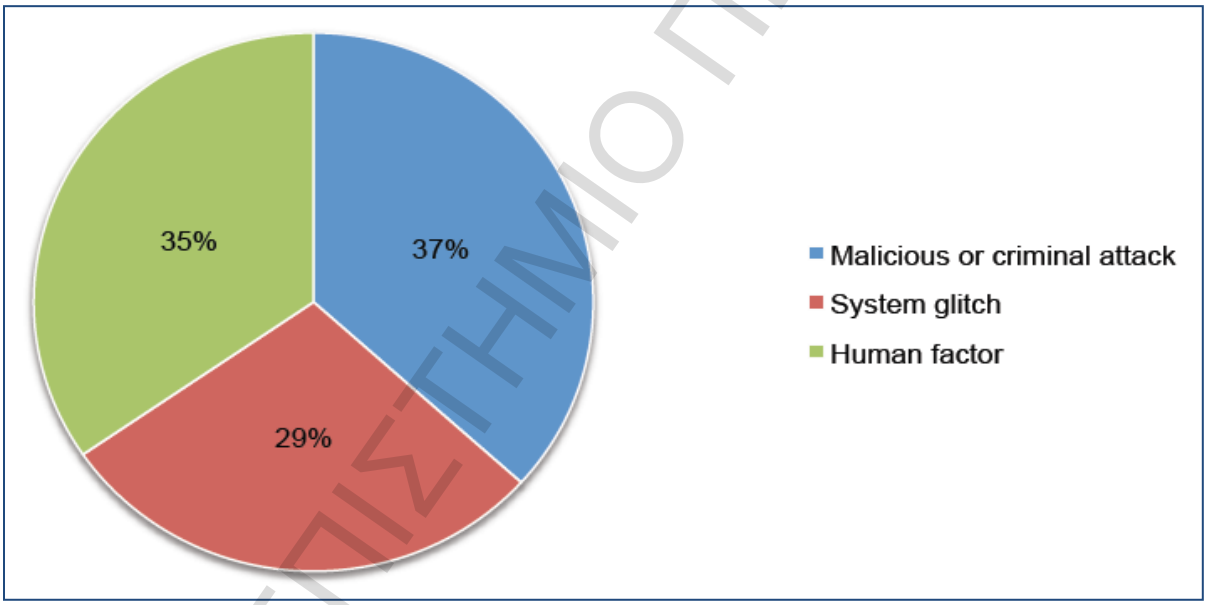


Εικόνα 2: Μέσο κόστος περιστατικών ανά βιομηχανία ($US) (Ponemon, "2013 Data Breach Study")

Τέλος, παρουσιάζει ιδιαίτερο ενδιαφέρον η διερεύνηση των αιτιών των *security breaches* για το εάν αυτά προέρχονται από:

- κακόβουλες ενέργειες όπως την εισαγωγή ιομορφικού λογισμικού *(malware)*, επιθέσεις εκ των έσω *(insider attacks)*, μεθόδων κοινωνικής μηχανικής *(phishing/social engineering)* και δικτυακών επιθέσεων *(SQL injection, XXS),*
- δυσλειτουργία συστημάτων η οποία μπορεί να διακόψει τη ροή εργασιών της μηχανογράφησης και συνεπώς και του *business*,
- ανθρώπινους παράγοντες όπως αμέλεια καθηκόντων ή άγνοια κινδύνου,

Στην εν λόγω μελέτη για το 2013 [21] προκύπτει ότι αν και τα περιστατικά που προέρχονται από κακόβουλες ενέργειες είναι περισσότερα δεν παύουν να διατηρούν ιδιαίτερα μεγάλο ποσοστό και οι άλλες δύο κατηγορίες δίνοντας μία εικόνα ισοκατανομής στα ποσοστά των αιτιών των *security breaches* (εικόνα 3).



Εικόνα 3: Αίτια περιστατικών (Ponemon, "2013 Data Breach Study")

Το αποτέλεσμα της συγκεκριμένης μέτρησης δείχνει την ανάγκη για τη λήψη μέτρων σε καθολικό επίπεδο και όχι την επικέντρωση σε μεμονωμένα σενάρια παραβίασης της ασφάλειας. Ένας οργανισμός ο οποίος θέλει να προστατεύσει επαρκώς τα πληροφοριακά του συστήματα θα πρέπει να «αγκαλιάσει» το θέμα της ασφάλειας με στρατηγικές οι οποίες:

- υλοποιούν μηχανισμούς αποτροπής και ανίχνευσης κακόβουλων ενεργειών (εντός και εκτός οργανισμού),

- ορίζουν Πολιτικές Διαχείρισης Παραμετροποίησης *(Configuration Management)* αλλά και παρακολούθησης της απόδοσης των πληροφοριακών συστημάτων και της ορθής εκτέλεσης των μηχανογραφικών τους ροών,
- περιλαμβάνουν την διενέργεια τακτικών εκπαιδεύσεων του προσωπικού για τη βελτίωση της επίγνωσης των κινδύνων που αφορούν τα πληροφοριακά συστήματα σε κάθε επίπεδο.

Θα μπορούσε εύκολα να θεωρήσει κάποιος ότι με την εισαγωγή προηγμένων τεχνολογιών Ασφάλειας Πληροφοριακών Συστημάτων, την επιβολή θεσμικών πλαισίων καθώς και την έμφυτη τάση του *business* να προστατεύσει την πληροφορία που εκμεταλλεύεται, το πλήθος των περιστατικών ασφάλειας θα πρέπει να μειώνεται με την πάροδο του χρόνου. Ωστόσο *security breaches* συμβαίνουν κατ' εξακολούθηση. Υποθέσεις απατών και επιθέσεων εκ των έσω αναφέρονται σε συνεχή βάση, θέτοντας την ανάγκη για ασφάλεια τόσο απέναντι σε εξωτερικές όσο και απέναντι σε εσωτερικές απειλές. Υφίσταται η άποψη που λέει ότι οι αναλυτές ασφάλειας εξακολουθούν να εστιάζουν στις μεθόδους αντιμετώπισης των περιστατικών και όχι στις προσπάθειες αποτροπής τους. Αυτή η συνεχόμενη προσπάθεια αφήνει λίγο χρόνο για καινοτομία και στρατηγικό σχεδιασμό. Οι τάσεις εξακολουθούν να δείχνουν την υπερβολική εξάρτηση των τεχνολογικών *security controls* για την κάλυψη των προβλημάτων που έχουν ήδη παρουσιαστεί. Το γεγονός αυτό σε συνδυασμό με την έλλειψη ιστορικών στοιχείων για παλαιότερα περιστατικά διαιωνίζει την κατάσταση εμφάνισης προβλημάτων, ασχέτως εάν κάποια από αυτά έχουν αντιμετωπιστεί στο παρελθόν. Η άλλη άποψη λέει ότι, όπως ειπώθηκε νωρίτερα, λόγω της μεγαλύτερης εξάρτησης του *business* στα πληροφοριακά συστήματα η χρήση τους έχει αυξηθεί με ρυθμούς γεωμετρικής προόδου αυξάνοντας αναλόγως και τα περιστατικά ασφάλειας που πηγάζουν τόσο από κακόβουλες ενέργειες όσο και από ανθρώπινα λάθη. Είναι βέβαιο ότι και οι δύο παράγοντες συνεπικουρούν στη διατήρηση του κόστους των *security breaches* σε σχετικά υψηλά επίπεδα.

Πολλές εταιρικές κουλτούρες δυσκολεύονται να αποδεχτούν την Ασφάλεια των Πληροφοριών ενώ ταυτόχρονα οι *Security Officers* κάνουν ότι μπορούν για να αναδείξουν την αξία του *Security*. Σύμφωνα με την πρόταση του *ISACA*, όταν η Διαχείριση Κινδύνων Πληροφοριακών Συστημάτων δεν είναι ενσωματωμένη με το *business* τότε μοιραία δημιουργούνται «οργανωτικές νησίδες» *(organizational silos)* οι οποίες αποτρέπουν την εκμετάλλευση ευκαιριών για στρατηγικές επιλύσεις. Στη γλώσσα του *business* και του *IT business*, με τον όρο *"organizational silos"* εννοούνται οι μονάδες που δημιουργούνται σε έναν οργανισμό οι οποίες χαρακτηρίζονται από την τάση να διαφυλάττουν τα δικά τους συμφέροντα, να διατηρούν εταιρικά δεδομένα για δικούς τους σκοπούς, να επικοινωνούν με μεγαλύτερη ευκολία στο εσωτερικό τους παρά με τις υπόλοιπες οργανωτικές μονάδες και να θέτουν σε προτεραιότητα τους δικούς τους στόχους εις βάρος των στρατηγικών

στόχων του ίδιου του οργανισμού. Αξίζει να σημειωθεί ότι σε ένα περιβάλλον με πολλές οργανωτικές νησίδες, είναι εξαιρετικά πιθανό να υπάρχουν και «μηχανογραφικές νησίδες» *(IT silos)*. Σε αυτές τις περιπτώσεις, οι εν λόγω απομονωμένες μονάδες κάνουν χρήση πληροφοριακών συστημάτων για τα οποία δεν υπάρχει καμία κεντρική εποπτεία για τη λειτουργία και τη διαχείρισή τους από το *IT Management* με συνέπεια την ακόμα μεγαλύτερη δυσλειτουργία της επικοινωνίας και της διάχυσης της πληροφορίας στο εσωτερικό του οργανισμού καθώς και την εισαγωγή επιμέρους κινδύνων. Δεδομένης της κατάστασης της Ασφάλειας της Πληροφορίας σε παγκόσμια κλίμακα, η πρόταση του *ISACA* δίνει έμφαση στην ανάγκη διαχείρισης της ασφάλειας των πληροφοριακών αγαθών ενός οργανισμού σε επίπεδο Διοίκησης.

4. Η Προτυποποίηση της Ασφάλειας της Πληροφορίας

Όπως επισημαίνεται ιδιαίτερα και στη δημοσίευση του *BMIS*, είναι πολύ σημαντικό να γίνουν κατανοητές οι διαφοροποιήσεις μεταξύ των μοντέλων, των πλαισίων και των προτύπων Ασφάλειας της Πληροφορίας. Το *BMIS*, όπως άλλωστε δηλώνει και η ονομασία του, αποτελεί ένα μοντέλο ασφάλειας το οποίο προκειμένου να μπορέσει να εφαρμοστεί, ενδεχομένως να χρειαστεί να υποστηριχθεί από επιμέρους πλαίσια και πρότυπα.

4.1 Μοντέλα

Με τη λέξη «μοντέλο» *(model)* περιγράφουμε ως επί τω πλείστων τη ροή των εργασιών ενός θεωρητικού συστήματος με συγκριμένους πόρους ως *input* και συγκεκριμένους στόχους ως *output*. Στον χώρο του *business*, αυτό σημαίνει ότι ένα μοντέλο για να είναι πετυχημένο θα πρέπει να ορίζει τις επιχειρησιακές διεργασίες, να αναδεικνύει τις όποιες αλληλεπιδράσεις μεταξύ τους και να δοκιμάζεται τακτικά προκειμένου να επιβεβαιώνεται η εφαρμοσιμότητά του. Είναι πολύ μεγάλης σημασίας να γίνει κατανοητό ότι τα μοντέλα αποτελούνται από περιγραφικές σχέσεις και όχι από κανόνες. Στην περίπτωση του *BMIS* όπου το πεδίο δράσης *(scope)* είναι η Ασφάλεια της Πληροφορίας θα πρέπει το ίδιο το μοντέλο να είναι η πηγή από την οποία θα προκύπτουν όλα τα πλαίσια και πρότυπα που βρίσκουν εφαρμογή στην ενίσχυση της ασφάλειας του οργανισμού. Ταυτόχρονα, λόγω της φύσης του αντικειμένου της Πληροφορικής, το μοντέλο θα πρέπει να είναι σε θέση να αφομοιώνει της αλλαγές σε σύντομο χρονικό διάστημα και να αναδεικνύει τις όποιες συνέπειές τους στον οργανισμό.

Η αξία των μοντέλων στο χώρο του *business* έχει να κάνει κυρίως με τον ορισμό των στόχων αλλά και τη χάραξη των στρατηγικών ώστε αυτοί να επιτευχθούν. Δεν είναι λίγες οι περιπτώσεις επιχειρήσεων στις οποίες τα επιχειρησιακά μοντέλα που ακολουθήθηκαν, έπαιξαν σπουδαιότερο ρόλο από ότι η ίδια η τεχνολογία για την επίτευξη των στόχων. Χαρακτηριστικό είναι το παράδειγμα της *Xerox* και το *business model* που αξιοποίησε για την προώθηση της φωτοτυπικής συσκευής *Xerox 914* [14]. Η εν λόγω εταιρεία το 1959 ανέπτυξε μία τεχνολογία η οποία ήταν πολύ ανώτερη αλλά και πολύ ακριβότερη από τις τεχνολογίες άλλων ανταγωνιστικών προϊόντων φωτοτυπίας. Ως εκ τούτου η *Xerox* αντιμετώπισε ουσιαστικές δυσκολίες στην προώθηση της *Xerox 914* συσκευής, εξαιτίας του απαγορευτικού της κόστους. Ωστόσο η εταιρεία αποφάσισε να επενδύσει σε ένα διαφορετικό *business model* διακόπτοντας τις απευθείας πωλήσεις των συσκευών αυτών. Αντί αυτού, η *Xerox* άρχισε να εκμισθώνει τις συσκευές αυτές με σχετικά χαμηλό κόστος ενώ για κάθε φωτοαντίγραφο πλέον των 2000 φωτοαντιγράφων την ημέρα, χρέωνε ένα επιπλέον ποσό. Τον καιρό εκείνο, το μέσο φωτοτυπικό μηχάνημα δεν μπορούσε να παράγει περισσότερα από 20 φωτοαντίγραφα ημερησίως. Συνεπώς οι πελάτες είχαν στη διάθεσή

τους τεχνολογία αιχμής σε χαμηλό κόστος την οποία σύντομα την αξιοποίησαν στο έπακρο παράγοντας πολύ περισσότερα φωτοαντίγραφα από ότι παλαιότερα και γιγαντώνοντας την εταιρεία *Xerox* στο επιχειρηματικό της πεδίο.

Σύμφωνα με την πρόταση του *ISACA*, όπως στο παράδειγμα της *Xerox* αλλά και άλλων οργανισμών οι οποίοι αναθεώρησαν τα *business models* τους προκειμένου να κερδίσουν την αγορά αξιοποιώντας καινοτόμα τεχνολογία έτσι και ένα Επιχειρηματικό Μοντέλο Ασφάλειας όπως το *BMIS* μπορεί να δημιουργήσει ευκαιρίες για το *security programme* ώστε να θεμελιωθεί ως καταλύτης στην προσπάθεια επίτευξης των επιχειρησιακών στόχων.

4.2 Πλαίσια

Η αξιοποίηση των πλαισίων *(frameworks)* μπορεί να παρομοιαστεί με την σκελετό μιας υποδομής πάνω στην οποία μπορεί να υλοποιηθεί ένα πρόγραμμα. Κατά κανόνα, ένα *framework* είναι λειτουργικής αξίας και παρέχει μία αναλυτική περιγραφή για το πώς μπορεί να επιτευχθεί η υλοποίηση και η διαχείριση ενός προγράμματος και των διεργασιών του. Τα *frameworks* βασίζονται σε αρχές οι οποίες όμως πρέπει να παρακολουθούνται για την συνεχιζόμενη βελτίωσή τους. Ως αποτέλεσμα, τα πλαίσια βασίζονται συνήθως σε υφιστάμενα πρότυπα ενώ μπορούν να αξιοποιηθούν και με περαιτέρω οδηγούς υλοποίησης αναλόγως την προτίμηση και τις ανάγκες του οργανισμού.

Στο χώρο της Ασφάλειας της Πληροφορίας, ένα *framework* μπορεί να αποτελέσει σημαντικό εργαλείο τόσο για την ανάπτυξη ολοκληρωμένων *security programmes* όσο και για τη διαρκή βελτίωσή τους. Προς το παρόν το μοναδικό *framework* το οποίο είναι αφιερωμένο αποκλειστικά στο *security* είναι το νεοκδοθέν *"COBIT 5 for Information Security"* [15] ωστόσο παραμένουν δημοφιλή *frameworks* για την υλοποίηση *security programmes* τα *"COBIT 4.1"* η *"OCTAVE"* [16] ως πλαίσιο διαχείρισης κινδύνων Πληροφοριακών Συστημάτων καθώς και οι διεργασίες ασφάλειας του *"ITIL"* οι οποίες πηγάζουν από τις βέλτιστες πρακτικές του *"ISO/IEC 27002"* [17]. Σε αντίθεση με τα όσα ειπώθηκαν για τα *models*, ένα *framework* είναι κανονιστικό και όχι περιγραφικό.

4.3 Πρότυπα

Σύμφωνα με το *British Standards Institute* ένα πρότυπο *(standard)* είναι ένας συμφωνημένος και επαναλαμβανόμενος τρόπος διεκπεραίωσης μιας εργασίας ο οποίος τεκμηριώνεται από ένα δημοσιευμένο κείμενο (διαδικασία, οδηγία εργασίας κλπ) περιγράφοντας τις τεχνικές προδιαγραφές και τα λοιπά κριτήρια τα οποία απαιτούνται για την κατά κανόνα συνεχόμενη χρήση τους [18].

Τα πιο συνηθισμένα πρότυπα που αξιοποιούνται στο χώρο της Ασφάλειας της Πληροφορίας αποτελούνται από το "*ISO/IEC 27001:2005"* και την ευρύτερη σειρά *"ISO/IEC 27000"* [19], από το *"Special Publication 800-53"* του *"National Institute for Standards and Technology (NIST)"* [20] καθώς και από το σύνολο οδηγιών *"Payment Card Industry Data Security Standard (PCI DSS)"* [21].

4.4 Σχέση μεταξύ Μοντέλων, Πλαισίων και Προτύπων

Οι αναλυτές ασφάλειας προσπαθούν εδώ και αρκετά χρόνια να ευθυγραμμίσουν τα *"security programmes"* των εταιρειών για τις οποίες εργάζονται με διάφορα *frameworks, standards* και λοιπούς κανονισμούς οι οποίοι ως επί τω πλείστων επιβάλλονται στους οργανισμούς λόγω κανονιστικής συμμόρφωσης όπως για παράδειγμα τα *PCI DSS* στα χρηματοπιστωτικά ιδρύματα. Ωστόσο η εμπειρία δείχνει ότι ακόμα και με την χρήση γνωστών και διεθνώς αναγνωρισμένων *security frameworks* και *standards*, υφίστανται δυσκολίες στην αξιοποίησή τους οι συνηθέστερες από τις οποίες είναι οι εξής:

- *Ελλιπής κατανόηση της Διοίκησης για την ανάγκη των μέτρων ασφάλειας.*
  Η Διοίκηση συχνά αδυνατεί να κατανοήσει το λόγο υλοποίησης δικλείδων ασφαλείας μόνο και μόνο επειδή αναφέρονται σε ένα γενικευμένο κείμενο.

- *Έλλειψη δέσμευσης από τη Διοίκηση.*
  Η Διοίκηση, ακριβώς επειδή αδυνατεί να κατανοήσει γενικευμένες οδηγίες, αντιμετωπίζει διστακτικά την εφαρμογή ακριβών μεθόδων και πρακτικών ασφαλείας, είτε πρόκειται για την υλοποίηση δικλείδων ασφαλείας είτε για την εκπαίδευση του προσωπικού της σε θέματα ασφάλειας.

- *Προβλήματα επικοινωνίας μεταξύ information security και business.*
  Πρόκειται για το συνηθέστερο πρόβλημα στους μεγάλους οργανισμούς οι οποίοι έχουν στη κατοχή τους σύνθετα και κρίσιμα πληροφοριακά συστήματα. Τις περισσότερες φορές η ροή επικοινωνίας μεταξύ των δύο οντοτήτων γίνεται μέσω τρίτων (Διαχείριση Έργων, Διαχείριση Προμηθευτών κ.α.).

- *Αδυναμία απόδοσης ευθύνης και λογοδοσίας σε θέματα παραβίασης της ασφάλειας τα οποία προέκυψαν από στρατηγικές αποφάσεις.*
  Το πρόβλημα αυτό βρίσκει λύση στο πρόσωπο του *Chief Information Security Officer* οποίος είναι υπεύθυνος για όλα τα θέματα Ασφάλειας Πληροφοριών χωρίς ωστόσο να είναι ο άμεσα αρμόδιος για τη λήψη στρατηγικών αποφάσεων του οργανισμού.

- *Απουσία εμπλοκής του information security πριν από την υλοποίηση νέων τεχνολογιών.*
  Τις περισσότερες φορές, το *business* εισάγει μία καινούργια τεχνολογία στις λειτουργίες του οργανισμού και εκ των υστέρων απαιτεί από το *information security* να την προστατεύσει επαρκώς.

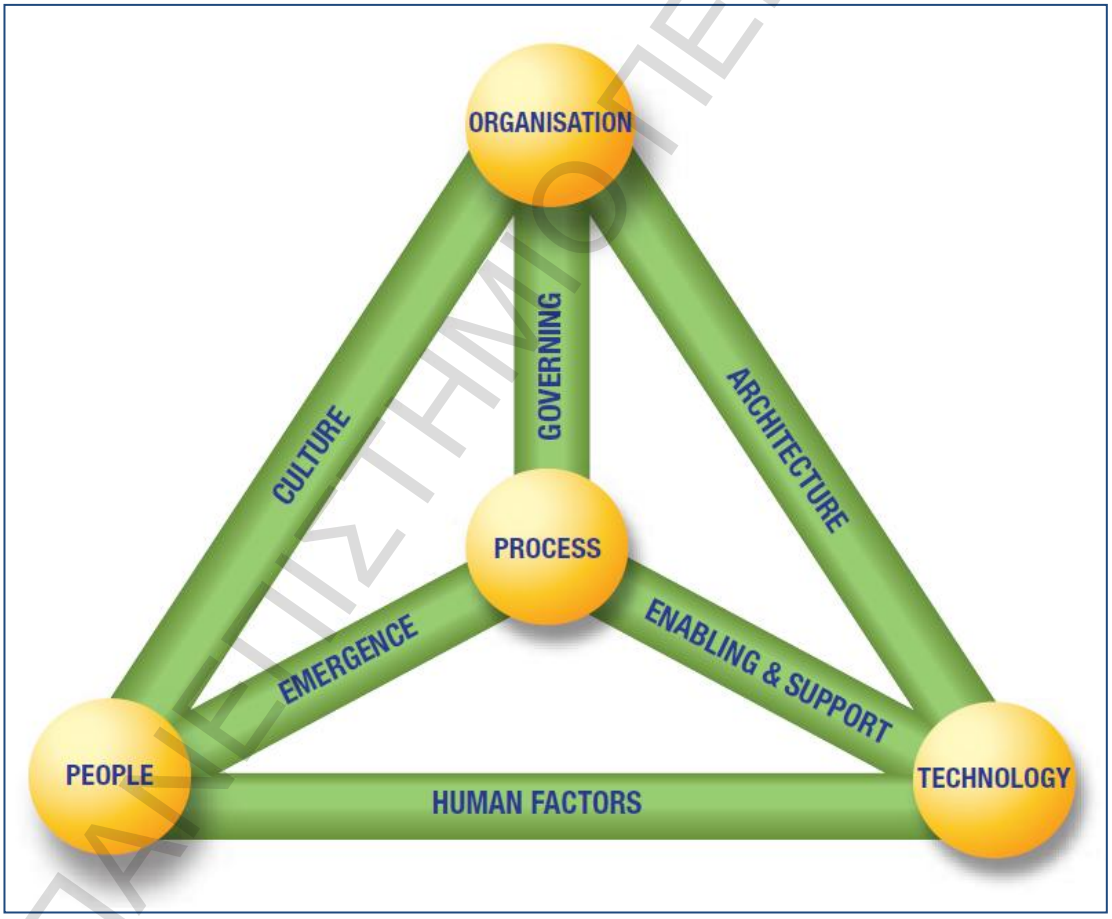
- *Απόρριψη πολιτικών και διαδικασιών ασφάλειας από το προσωπικό του οργανισμού.*
  Η τυφλή εφαρμογή προτύπων χωρίς να έχει γίνει πρώτα ένα *risk assessment* το οποίο να λαμβάνει υπόψη του την εταιρική κουλτούρα μπορεί να οδηγήσει στη δημιουργία μεθόδων και πρακτικών οι οποίες θα καταλήξουν να μην ακολουθούνται από κανένα [8].

- *Ευθυγράμμιση του information security με τους εταιρικούς στόχους.*
  Δεν είναι καθόλου σπάνια η περίπτωση κατά την οποία το *information security* λησμονεί το σκοπό του οργανισμού και το επιχειρησιακό του πεδίο με αποτέλεσμα την τυφλή προσπάθεια υλοποίησης δικλείδων ασφαλείας χωρίς τη μελέτη εναλλακτικών μεθόδων ώστε και να ικανοποιούνται τα όποια *security standards* έχουν επιλεχθεί και να μην δυσχεραίνεται η προσπάθεια υλοποίησης της εταιρικής στρατηγικής.

Η πρόταση του *ISACA* για την εφαρμογή ενός επιχειρηματικού μοντέλου για την Ασφάλεια της Πληροφορίας όπως το *BMIS* η οποία και διερευνάται και στην παρούσα μελέτη υπόσχεται ότι επιτρέπει στους οργανισμούς να συνθέσουν τα δικά τους *frameworks* και *standards* τα οποία ακολουθούν, αξιοποιώντας ένα επίσημο μοντέλο ώστε να δημιουργήσουν ένα ολοκληρωμένο και απόλυτα προσαρμοσμένο στους στρατηγικούς στόχους *security programme*.

5. BMIS (Business Model for Information Security)

Όπως ειπώθηκε στην εισαγωγή, ο *ISACA* εξέδωσε το 2010 το *Business Model for Information Security*, δίνοντας μεγαλύτερη έμφαση στο επιχειρηματικό περιβάλλον εντός του οποίου λειτουργούν οι διεργασίες Ασφάλειας της Πληροφορίας και στις αλληλεπιδράσεις τους με τις υπόλοιπες επιχειρησιακές διεργασίες παρά στα *security best practices* αυτά καθαυτά. Το μοντέλο παρομοιάζεται σχηματικά με μία τετράεδρη πυραμίδα η οποία αποτελείται από τέσσερεις κορυφές και έξι ακμές οι οποίες στο μοντέλο ονομάζονται *Elements* (στοιχεία) και *Dynamic Interconnections – DIs* (σύνδεσμοι) αντίστοιχα (εικόνα 4). Σημειώνεται ότι στα πλαίσια της παρούσας μελέτης, η αναφορά στις περιοχές του *BMIS* γίνεται στην Αγγλική λόγω της αποτελεσματικότερης απόδοσής τους στη γλώσσα που συγγράφηκε το μοντέλο.



Εικόνα 4: Σχηματική παράσταση του BMIS (ISACA, "BMIS", 2010)

Η κεντρική ιδέα είναι ότι αναλόγως την προσέγγιση, το σχηματικό μοντέλο μπορεί να περιστραφεί θέτοντας ως αφετηρία το στοιχείο ή το σύνδεσμο που ενδιαφέρει τον εκάστοτε παρατηρητή. Ως κανόνας ισχύει το ότι τα στοιχεία αλληλεπιδρούν μεταξύ τους μέσω των συνδέσμων. Σε ένα ιδανικό περιβάλλον όπου η διαχείριση της Ασφάλειας της

Πληροφορίας λειτουργεί άψογα, το μοντέλο αυτό θα πρέπει να βρίσκεται σε πλήρη ισορροπία. Συνεπώς, εάν συμβεί κάποια αλλαγή σε ένα τμήμα του μοντέλου τότε θα συμβούν επιμέρους αλλαγές και στα υπόλοιπα τμήματα. Ομοίως, εάν εμφανιστούν αδυναμίες ασφάλειας σε κάποιο τμήμα τότε η ισορροπία του μοντέλου διαταράσσεται. Οι αλληλεξαρτήσεις ανάμεσα στα τμήματα του *BMIS* είναι αποτέλεσμα της ολικής συστημικής προσέγγισης.

Το μοντέλο αναγνωρίζει ως θεμελιώδη τα παρακάτω στοιχεία:

- *People*
- *Process*
- *Technology*

και προσθέτει ως επιπλέον τον ίδιο τον οργανισμό *(Organization).* Σε ένα *information security programme* η βαρύτητα του κάθε στοιχείου και του κάθε συνδέσμου μπορεί να ποικίλει. Κάποιο στοιχείο μπορεί να είναι σχετικά «αδρανές» ωστόσο εξακολουθεί να υφίσταται εντός του συνόλου του οργανισμού. Σε αυτές τις περιπτώσεις, τα στοιχεία αυτά θα πρέπει να θεωρούνται ως «όρια» για τις πρωτοβουλίες της διαχείρισης της ασφάλειας και όχι ως ενεργά τμήματα τα οποία θα μπορούν να παραμετροποιηθούν ή να επηρεάσουν τα επίπεδα της ασφάλειας των υπόλοιπων τμημάτων. Ομοίως, το στοιχείο *“People”,* αποτελεί ένα σπουδαίο τμήμα το οποίο δεν μπορεί να αλλάξει με την πάροδο του χρόνου. Οι ιδιαιτερότητες της ανθρώπινης φύσης θα εξακολουθούν να υφίστανται και ο μόνος τρόπος για προσαρμογή της ανθρώπινης συμπεριφοράς στους στόχους ενός εξειδικευμένου *security programme* είναι με μία θεμελιώδη μεταβολή σε επίπεδο κουλτούρας.

Αντίστοιχα οι σύνδεσμοι *(DIs)* είναι οι εξής:

- *Culture*
- *Governing*
- *Architecture*
- *Emergence*
- *Enabling and Support*
- *Human Factors*

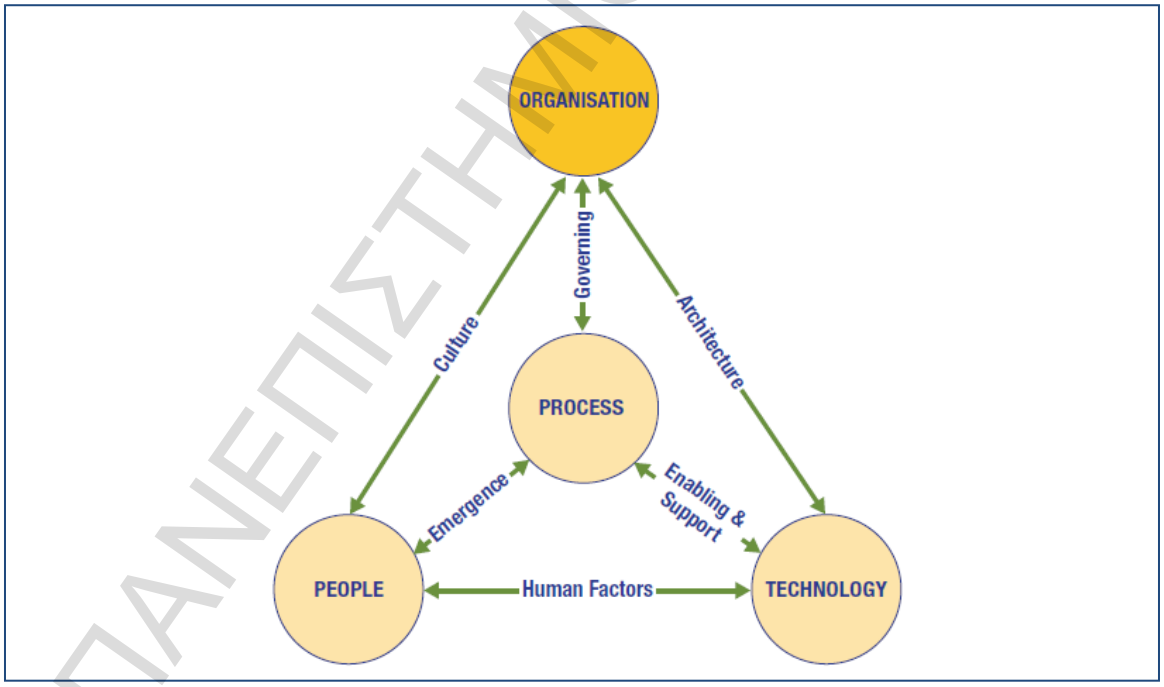
Για τη βέλτιστη αξιοποίηση του μοντέλου, θα πρέπει να γίνει αντιληπτό ότι τα *DIs* επηρεάζονται από οποιαδήποτε αλλαγή συμβεί σε οποιοδήποτε τμήμα του μοντέλου, και όχι μόνο από αλλαγές στα στοιχεία με τα οποία συνδέονται στο σχήμα..

6. Τα στοιχεία του BMIS

Στην παρούσα ενότητα κρίνεται σκόπιμο να γίνει ανάλυση των στοιχείων του μοντέλου ώστε να γίνει αντιληπτή η σημασία τους στους κόλπους ενός οργανισμού μέσω των διεργασιών με τις οποίες αλληλεπιδρούν μεταξύ τους. Τονίζεται ότι το μοντέλο είναι δομημένο με τέτοιο τρόπο ώστε να υφίσταται η δυνατότητα αξιοποίησής του σε κάθε οργανισμό με κρίσιμα πληροφοριακά συστήματα, ανεξαρτήτως πεδίου επιχειρηματικού ενδιαφέροντος.

6.1 Organization

Όπως ειπώθηκε, το *BMIS* προσθέτει στα θεμελιώδη στοιχεία της πληροφορικής και το επιπλέον στοιχείο του «οργανισμού» (εικόνα 5). Με αυτόν τον τρόπο δίνεται η δυνατότητα διερεύνησης του τρόπου με τον οποίο ο σχεδιασμός και η στρατηγική ενός οργανισμού επηρεάζει τα επίπεδα ασφάλειας στα υπόλοιπα θεμελιώδη στοιχεία, *People, Process, Technology*, αναδεικνύοντας περισσότερους κινδύνους, ευκαιρίες και περιοχές για βελτίωση.



Εικόνα 5: Organization element (ISACA, "BMIS", 2010)

Μέσω της εταιρικής στρατηγικής η οποία είναι προαπαιτούμενη για τον καθορισμό του στοιχείου *"Organization"* οι αναλυτές της ασφάλειας μπορούν να κατανοήσουν τους στόχους του οργανισμού και τους τρόπους με τους οποίους το *security programme* θα πρέπει να τους υποστηρίξει. Αυτοί με τη σειρά τους μπορούν να χαρτογραφηθούν με τα

θεμελιώδη στοιχεία της Ασφάλειας της Πληροφορίας: εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα.

Στο *BMIS* γίνεται ο διαχωρισμός του επίσημου *(formal)* και του ανεπίσημου *(informal)* οργανισμού. Ως *Formal Organization* ορίζεται η δομή που απαρτίζεται από τα επίσημα οργανογράμματα, τις έντυπες πολιτικές και τις οδηγίες εργασίας που δίδονται από τη Διοίκηση προς το σύνολο του προσωπικού. Στις καθημερινές λειτουργίες, οι πιο αποτελεσματικές αλλαγές από άποψη πληρότητας ασφάλειας γίνονται όταν ένα διοικητικό στέλεχος αναλαμβάνει την ευθύνη για την ασφάλεια τόσο σε πρακτικό επίπεδο όσο και σε επικοινωνιακό ώστε να μπορέσει να αναδιαμορφωθεί η οργανωτική κουλτούρα βάσει των νέων δεδομένων. Αυτό βοηθάει στη μείωση της «λογικής των νησίδων» με τα παραδείγματα που αναφέρθηκαν νωρίτερα, η οποία συνήθως αναπτύσσεται όταν η ασφάλεια δεν αντιμετωπίζεται ως στρατηγική προτεραιότητα. Στις περιπτώσεις όπου ο σχεδιασμός και η δομή του οργανισμού υποστηρίζουν την ασφάλεια ως στρατηγικό στόχο, όλα τα υφιστάμενα τμήματα και οι μονάδες γίνονται πιο αποτελεσματικά στην επίτευξη του στόχου αυτού.

Παρόλο που δεν συνηθίζεται ο ορισμός του στα περισσότερα πλαίσια ασφάλειας, το στοιχείο του *Formal Organization* αποτελεί ίσως την κρισιμότερη οντότητα για μία εταιρεία. Άλλωστε είναι αποδεδειγμένο ότι η Ασφάλεια της Πληροφορίας δε μπορεί να είναι επιτυχής χωρίς την υποστήριξη και τη δέσμευση της Διοίκησης [22]. Σε πολλούς οργανισμούς, ειδικά στην ελληνική βιομηχανία, επικρατεί το πρότυπο της ιεραρχίας. Συνεπώς, εάν τη Ασφάλεια δεν τεθεί ως προτεραιότητα από την υψηλή Διοίκηση και δεν επικονωνηθεί προς τους υφιστάμενους τομείς και τα στελέχη που τους απαρτίζουν τότε το πιθανότερο είναι να βρεθούν εμπόδια στην αποδοχή των μέτρων ασφάλειας, στην εξασφάλιση επαρκών πόρων για την υλοποίηση του *security programme* και στην επιβολή πολιτικών.

Ένα *security programme* υπάρχει όχι μόνο για να προστατεύσει τις εταιρικές πληροφορίες αλλά κυρίως για να υποστηρίξει το *business* να επιτύχει τους στόχους του. Ο *Formal Organization* (εντός του *BMIS* στοιχείου *Organization*) ενημερώνει τον *security manager* για το τι σκοπούς έχει το *business* σχετικά με την ποιότητα και το είδος των πληροφοριών που διατηρεί η εταιρεία. Η γνώση αυτή είναι υπερπολύτιμη για τους *security managers* διότι τους βοηθάει να εντοπίσουν την κατεύθυνση στην οποία πρέπει να κινηθεί το *security programme* ώστε να επιτύχει τον βασικότερο σκοπό του: Να υποστηρίξει το *business* στο να επικεντρωθεί στα δεδομένα και τις πληροφορίες που αξιοποιεί και όχι στους τρόπους διαφύλαξής τους.

Όπως ειπώθηκε νωρίτερα, εκτός από τον *Formal Organization*, το *BMIS* αναγνωρίζει και τον *Informal Organization*. Δεν είναι λίγες οι φορές όπου, κυρίως σε μεγάλους οργανισμούς, οι στρατηγικοί στόχοι δεν καθορίζονται από ένα επίσημο διοικητικό πρόσωπο αλλά από ένα

σύνολο περιφερειακών μονάδων εντός του οργανισμού χωρίς κατ' ανάγκην την αξιοποίηση γραπτών και επίσημων πολιτικών. Ακόμη συχνότερα συμβαίνει το να υφίστανται επίσημες διαδικασίες επικοινωνίας μεταξύ των οργανωτικών οντοτήτων χωρίς ωστόσο να αποτελούν την κύρια μέθοδο με την οποία μεταδίδεται η πληροφορία εντός του οργανισμού. Ο *Informal Organization* είναι στην ουσία ο παρασκηνιακός παράγον εντός ενός οργανισμού ο οποίος καθορίζει σε μεγάλο βαθμό το «πώς» οι αποφάσεις παίρνονται και που στην ελληνική πραγματικότητα υφίσταται σχεδόν σε κάθε περίπλοκη οργανωτική δομή.

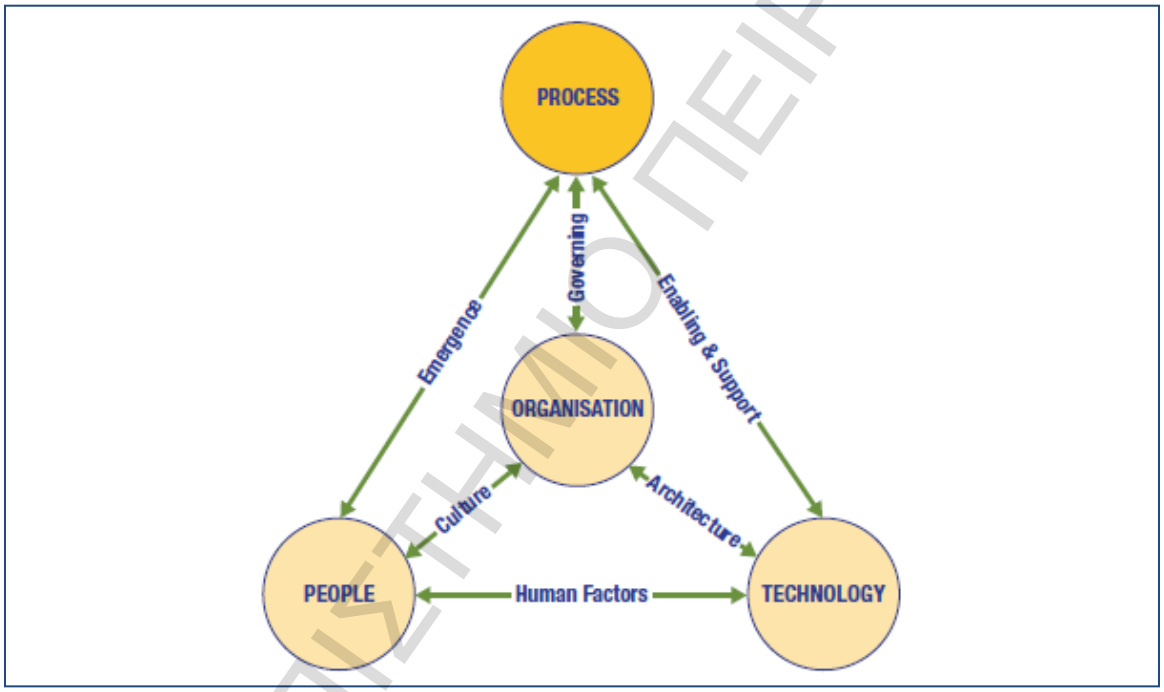
Ο *Informal Organization* εκτείνεται από το σύνολο των νοοτροπιών μεμονωμένων υπαλλήλων έως της συλλογικές τάσεις οι οποίες καθορίζονται από κουλτούρες εντός μονάδων του οργανισμού. Σχηματικά μπορεί κάποιος να αντιληφθεί ότι ο *Formal Organization* είναι στην ουσία το κομμάτι του στοιχείου *Organization* που αλληλεπιδρά μέσω του έσω του *DI "Architecture"* ενώ ο *Informal Organization* είναι το κομμάτι που αλληλεπιδρά μέσω του *DI "Culture"*. Και οι δύο τύποι του στοιχείου *Organization* αλληλεπιδρούν με το σύνδεσμο *"Governing"* (εικόνα 6).

Εικόνα 6: Formal & Informal Organization

Είναι μεγάλης σημασίας για έναν *security manage*r να αναγνωρίσει και να κατανοήσει τόσο τον *Formal Organization* όσο και τον *Informal*. Ένα σημαντικό πρώτο βήμα θα ήταν να μπορέσει να εντάξει τις δύο αυτές περιοχές εντός του *security programme*. Το στοιχείο *Organization* διασυνδέεται μέσω των προαναφερθέντων *DIs* με τα στοιχεία *People, Technology* και *Process* αντίστοιχα. Αλλαγές οι οποίες συμβαίνουν σε οποιοδήποτε από αυτά τα στοιχεία έχουν ως συνέπεια αλλαγές και στο *Organization*.

6.2 Process

Το στοιχείο *Process* το οποίο μεταφράζεται ως οι διεργασίες του οργανισμού, είναι το αμέσως επόμενο στοιχείο από άποψη σπουδαιότητας (εικόνα 7). Οι διεργασίες δημιουργούνται με σκοπό την επίτευξη των στόχων του οργανισμού. Πρόκειται για σύνολα δομημένων ενεργειών τα οποία αποσκοπούν στο να φέρνουν εις πέρας συγκεκριμένα αποτελέσματα. Το *Process* στοιχείο εξηγεί τους λόγους ύπαρξης των πρακτικών και των διαδικασιών που υπάρχουν στο εσωτερικό των μονάδων λειτουργίας του οργανισμού. Είναι θεμελιώδες στοιχείο στο οποίο ορίζονται οι προϋποθέσεις εξέλιξης ενός οργανισμού ένα εξαιρετικό σημείο στο οποίο μπορούν να καθιερωθούν πρακτικές και διαδικασίες ασφάλειας.



Εικόνα 7: Process element (ISACA, "BMIS", 2010)

Οι διεργασίες στο *BMIS* χαρακτηρίζονται ως προς το επίπεδο ωριμότητάς τους ενώ όπως συμβαίνει και στο *Organization element* μπορεί να είναι είτε επίσημες, είτε ανεπίσημες. Μία διεργασία θεωρείται ώριμη όταν είναι σαφώς ορισμένη, διαχειρίσιμη και με δυνατότητες βελτιστοποίησης. Ανεπίσημες διεργασίες συνήθως εκτελούνται από μεμονωμένους ανθρώπους με εμπειρία σε συγκεκριμένες εργασίες και είτε δεν είναι τεκμηριωμένες είτε είναι τεκμηριωμένες ανεπαρκώς. Υπάρχουν σήμερα διαθέσιμα μοντέλα τα οποία ορίζουν και μετρούνε τα επίπεδα ωριμότητας των διεργασιών με πιο αναγνωρισμένο όλων το *CMMI (Capability Maturity Model Integration)* [23].

Όπως φαίνεται και από τη σχηματική παράσταση του *BMIS*, το *Process element* συνδέεται άμεσα με τα *DIs Governing*, *Emergence* και *Enabling and Support* που θα αναλυθούν

αργότερα. Από την οπτική του *Governing*, μία διεργασία ορίζεται ως αποτέλεσμα της στρατηγικής του οργανισμού. Από την οπτική του *Emergence* μία διεργασία χρειάζεται ευελιξία ώστε να προσαρμόζεται σε νέες καταστάσεις και προκλήσεις και να λαμβάνει υπόψη την αντίστοιχη δυνατότητα προσαρμοστικότητας των ανθρώπων από το *People element*. Τέλος από την οπτική του *Enabling and Support* μία διεργασία θα πρέπει να επιτυγχάνεται μέσω της υποστήριξης τεχνολογίας από το *Technology element.* Συνολικά, λοιπόν μία διεργασία θα πρέπει να είναι ευθυγραμμισμένη με την εταιρική στρατηγική η οποία θα υποστηρίζεται από τη τεχνολογία ενώ θα πρέπει να έχει υψηλές δυνατότητες προσαρμοστικότητας και ευελιξίας.

Μία διεργασία συνήθως απαρτίζεται από πολλές υποδιεργασίες. Όπως θα δούμε και στην ενότητα με τις μελέτες περίπτωσης, το γεγονός αυτό σε συνδυασμό με την αλληλεπίδραση με τα *DIs* που αναφέρθηκαν παραπάνω, δημιουργεί την ανάγκη για συστεμικές προσεγγίσεις των όποιων *Information Security Processes* με υποδιεργασίες ανατροφοδότησης και βελτίωσης.

6.3 Technology

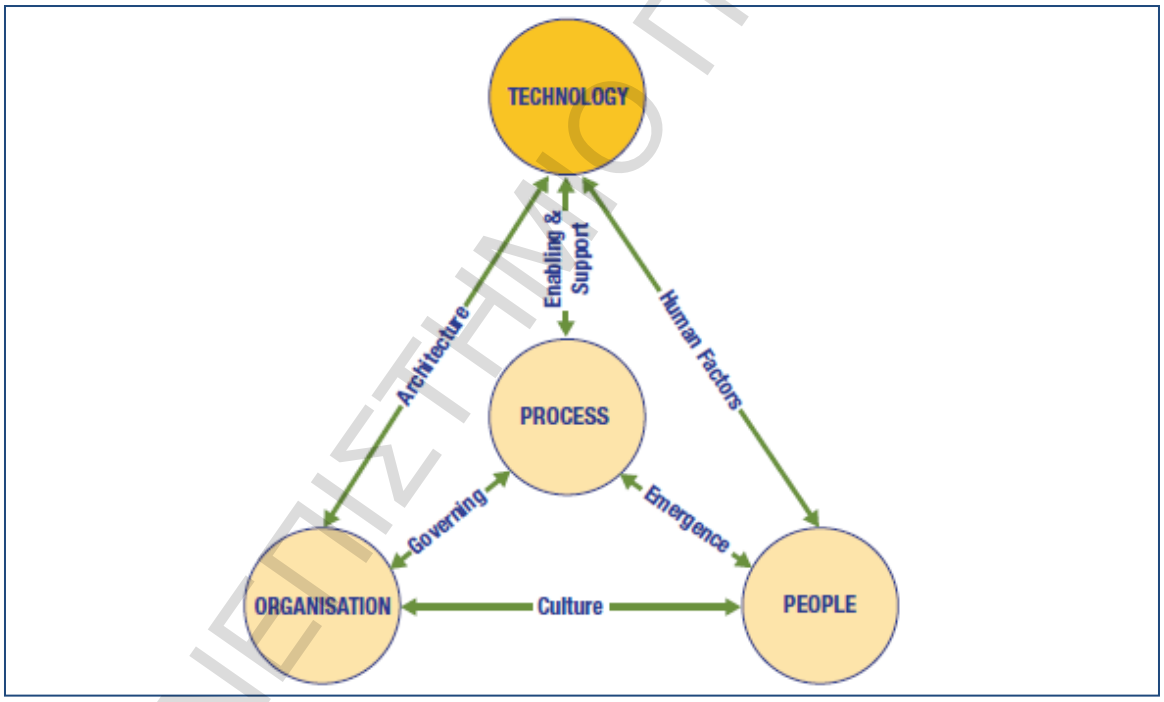
Η τεχνολογία είναι σίγουρα ένα από τα πιο σύνθετα στοιχεία της Ασφάλειας της Πληροφορίας και κατ' επέκταση και του *BMIS* (εικόνα 8). Όλα τα τεχνικά μέσα που διαθέτει ένας οργανισμός για να επιτύχει τους στόχους του σχετικά με την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών εντάσσονται σε αυτό το στοιχείο. Ωστόσο, η Ασφάλεια της Πληροφορίας δεν εξαρτάται αποκλειστικά από την τεχνολογία, σε αντίθεση με την συχνή θεώρηση που λέει ότι η επένδυση στην τεχνολογία θα επιλύσει κάθε πρόβλημα ασφάλειας.

Η Τεχνολογία είναι στην ουσία η αξιοποίηση της επιστημονικής γνώσης για την επίλυση πρακτικών προβλημάτων ή την επίτευξη συγκεκριμένων στόχων με σκοπό τη βελτίωση της ποιότητας ζωής. Για το *BMIS*, το στοιχείο της τεχνολογίας, συμπεριλαμβάνει κάθε τεχνική εφαρμογή η οποία χρησιμοποιείται σε έναν οργανισμό.

Η συστηματική προσέγγιση που προωθεί το *BMIS,* επιτρέπει την ανάλυση του στοιχείου της τεχνολογίας σε κατηγορίες όπως ενδεικτικά είναι οι εξής:

- **Βασικές υποδομές:** Υπηρεσίες ηλεκτρισμού, θέρμανσης, κλιματισμού καθώς και φυσικών υποδομών όπως κτηριακές εγκαταστάσεις ή δρόμοι. Σε ένα συστεμικό πλαίσιο, οι βασικές τεχνολογικές υποδομές επηρεάζουν άμεσα όλες τις διεργασίες καθώς και τους ανθρώπους. Αν και βρίσκονται μακριά από το τελικό στάδιο των υπηρεσιών πληροφορικής, η κατηγορία αυτή θα πρέπει να αντιμετωπίζεται με ιδιαίτερη κρισιμότητα.

- **Υποδομές Πληροφορικής:** Δικτυακές υποδομές και hardware τα οποία μπορεί να είναι είτε *in-house* είτε *outsourced*. Η κατηγορία αυτή αλληλεπιδρά με τις διεργασίες καθώς και με τις υπηρεσίες Πληροφορικής.
- **Υπηρεσίες Πληροφορικής:** Εφαρμογές και επιχειρηματικές υπηρεσίες οι οποίες βασίζονται στις υποδομές. Η κατηγορία αυτή έχει άμεσο αντίκτυπο σε όλα τα άλλα στοιχεία του *BMIS* (Οργανισμό, Διεργασίες, Άνθρωποι).
- **Διάχυτη τεχνολογία Πληροφορικής:** Με τον όρο αυτό *(Pervasive IT)* νοείται η τεχνολογία Πληροφορικής η οποία είναι διασκορπισμένη σε διάφορες περιοχές του οργανισμού. Αποκεντρωμένες εφαρμογές, έξυπνες συσκευές και τάσεις οι οποίες διαμορφώνονται από τις τεχνολογικές εξελίξεις είναι παραδείγματα αυτής της κατηγορίας. Επηρεάζουν επίσης όλα τα στοιχεία του *BMIS* με τη διαφορά ότι έχουν την ιδιότητα να επαναπροσδιορίσουν την εταιρική στρατηγική σε αντίθεση με την προηγούμενη κατηγορία που συνδέεται με την τρέχουσα στρατηγική.



Εικόνα 8: Technology element (ISACA, "BMIS", 2010)

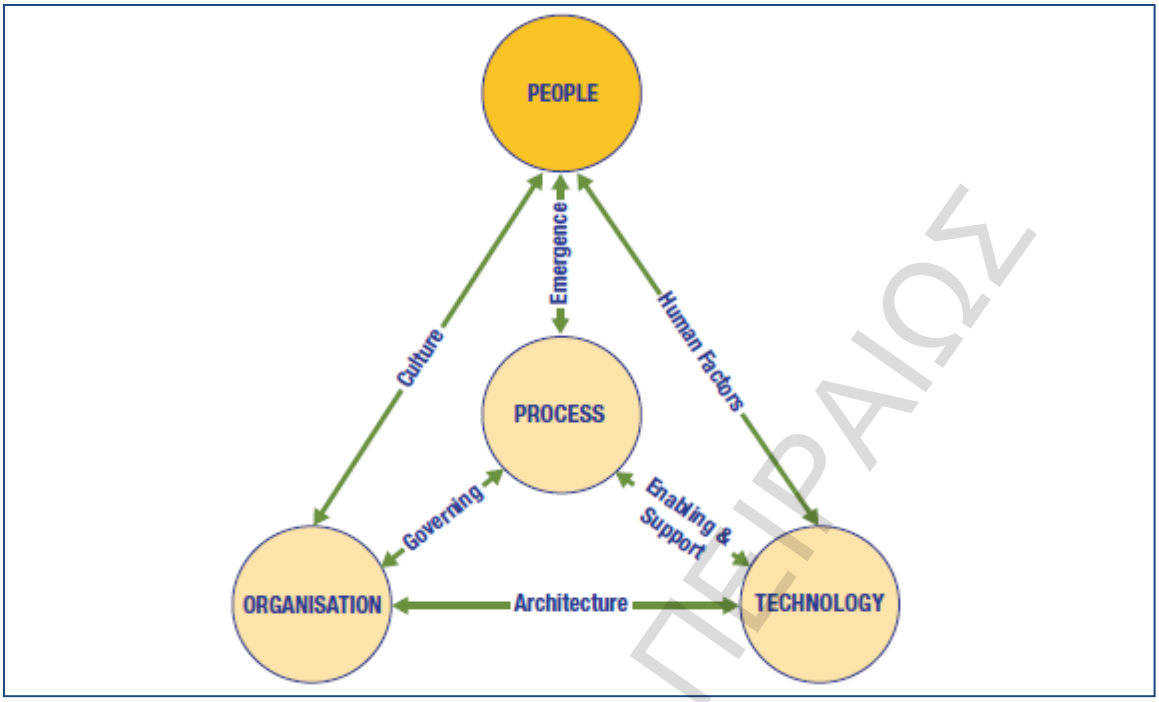
Σίγουρα το στοιχείο της Τεχνολογίας είναι απαραίτητο για τον εντοπισμό αδυναμιών ασφάλειας αλλά και για τον χειρισμό περιστατικών που προέρχονται από αυτές. Πολλές γνωστές αδυναμίες καλύπτονται με την υλοποίηση τεχνολογικών δικλείδων ασφαλείας, είτε αυτές προέρχονται από ακούσιους χειρισμούς *(human errors)* είτε από μεθοδευμένες επιθέσεις είτε από φυσικές και περιβαλλοντικές απειλές.

Με το πέρασμα των ετών και την επιστημονική πρόοδο, η τεχνολογία άρχισε εκτός από το να παρέχει μέτρα φυσικής ασφάλειας, να δίνει λύσεις και σε πιο εξεζητημένα προβλήματα με συστήματα *DLP (Data Loss Prevention)*, *IDS/IPS (Intrusion Detection/Prevention Systems)*, συσχετισμού περιστατικών *(Security Information and Event Management – SIEM)*, διαχείρισης πρόσβασης και άλλα. Παρόλο που υπάρχει πληθώρα επιλογών, ο εταιρικός και επιχειρηματικός κίνδυνος είναι αυτός ο οποίος οδηγεί τις εξελίξει σε ένα περιβάλλον ασφάλειας και διαμορφώνει το *security programme*.

Η τεχνολογία θα πρέπει να διαμορφώνει την ωφέλεια, την αποδοτικότητα και την παραγωγικότητα, με προδιαγραφές ασφάλειας για το σύνολο του οργανισμού. Αφού η τεχνολογία επιλεχθεί και «στηθεί», θα πρέπει να γίνεται και η κατάλληλη εκπαίδευση των ανθρώπων που την αξιοποιούν ώστε αυτή να λειτουργεί αποδοτικά. Εάν η τεχνολογία Ασφάλειας της Πληροφορίας αξιοποιηθεί, υλοποιηθεί και στη συνέχεια αγνοηθεί ως πάγιο στοιχείο του εταιρικού περιβάλλοντος τότε είναι σχεδόν βέβαιο ότι η Διοίκηση θα αποκτήσει λανθασμένη εντύπωση για την πραγματική θωράκιση του οργανισμού απέναντι σε πάσης φύσεως περιστατικών ασφάλειας.

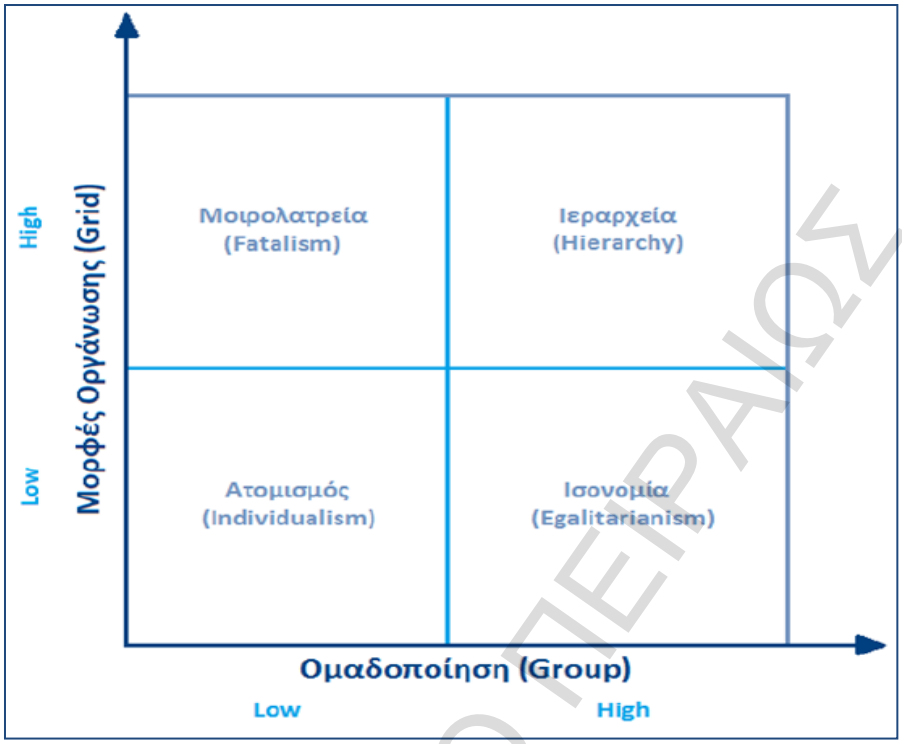
6.4 People

Το στοιχείο των ανθρώπων (εικόνα 9), αποτελεί προφανώς το σύνολο των ανθρώπινων πόρων του οργανισμού. Διοικητικά στελέχη, υπάλληλοι, υπεύθυνοι έργων καθώς και πάροχοι υπηρεσιών (εσωτερικών και εξωτερικών). Το κύριο μέρος του εν λόγω στοιχείου είναι τα πρόσωπα τα οποία έχουν άμεση συμβατική σχέση εργασίας με τον οργανισμό. Ωστόσο σε περιπτώσεις *outsourced* υπηρεσιών το στοιχείο αυτό εμπλουτίζεται και από έναν διευρυμένο κύκλο ανθρώπων που εργάζονται εμμέσως για αυτόν.



Εικόνα 9: People element (ISACA, "BMIS", 2010)

Το στοιχείο των ανθρώπων είναι ιδιαίτερα περίπλοκο για να μελετηθεί μονομερώς. Υφίστανται πάρα πολλές θεωρίες οι οποίες προσπαθούν να προσεγγίσουν την αντίληψη του κινδύνου και την αλληλεπίδρασή τους με την ασφάλεια, άλλοτε βάσει Κοινωνιολογικών και Ανθρωπολογικών προτύπων, άλλοτε βάσει Ψυχολογικών και Ψυχομετρικών [8]. Οι προσεγγίσεις των μεθόδων αυτών έχουν να κάνουν με την ανάλυση των ανθρώπινων συμπεριφορών και την κατάταξή τους σε ομάδες αναλόγως με το πώς κάθε ομάδα αντιλαμβάνεται τον κίνδυνο. Για παράδειγμα, η Πολιτισμική Θεωρεία *(Cultural Theory of Risk)* [24] η οποία και έχει αξιοποιηθεί πολλές φορές για έρευνες πάνω στην αποτελεσματικότερη διεξαγωγή ανάλυσης κινδύνων, λαμβάνει υπόψη της γενικευμένες τάσεις και συμπεριφορές των δομών οργάνωσης των κοινωνιών και της τάσεις ομαδοποίησης που διακρίνουν τους ανθρώπους με σκοπό να τους κατατάξει σε τέσσερις ομάδες (εικόνα 10). Κάθε μία από αυτές τις ομάδες έχει δικά της χαρακτηριστικά ως προς την αντίληψη της πληροφορίας και κατ' επέκταση την αντίληψη του κινδύνου ενώ περαιτέρω μελέτες έχουν προχωρήσει στην εκμετάλλευση των κατηγοριών αυτών για την επιβολή αποτελεσματικών πολιτικών ασφαλείας οι οποίες θα είναι αποδεκτές από την πλειοψηφία των ανθρώπων που στελεχώνουν έναν υπό μελέτη οργανισμό [25].



Εικόνα 10: Grid/Group Diagram, Ομάδες κατάταξης Πολιτισμικής θεωρίας

Από το *BMIS* προκύπτουν επίσης συστεμικές προσεγγίσεις του στοιχείου των ανθρώπων δεδομένου ότι τα στελέχη που απαρτίζουν έναν οργανισμό έχουν ξεχωριστά πιστεύω και συμπεριφορές αναλόγως τις προσωπικότητές τους και τις εμπειρίες τους. Το εταιρικό προφίλ επηρεάζει και επηρεάζεται από τα χαρακτηριστικά αυτά δεδομένου ότι ο οργανισμός «αναμένει» από τους υπαλλήλους του να έχουν συμπεριφορές που συνάδουν με τις πολιτικές και τους στόχους του. Οι υπάλληλοι απεναντίας μπορεί να επιθυμούν διαφορετικά πράγματα από τον οργανισμό διαμορφώνοντας τελικά ένα περίπλοκο περιβάλλον στον τομέα της ασφάλειας. Στο μοντέλο, αυτό απεικονίζεται στο *DI Culture*. Για παράδειγμα, ο τρόπος με τον οποίο οι άνθρωποι ενσωματώνονται μέσα σε έναν οργανισμό εξαρτάται από την εταιρική στρατηγική διαχείρισης ανθρώπινου δυναμικού όπως αυτή ορίζεται στο στοιχείο *Organization* και όπως υλοποιείται μέσω του *Governing* στο στοιχείο του *Process*. Εάν η εταιρική στρατηγική διαχείρισης ανθρώπινου δυναμικού αξιολογεί τη συμμόρφωση των υπαλλήλων στις πολιτικές ασφάλειας τότε ενισχύεται το *DI Culture*. Εάν ο οργανισμός υλοποιήσει τεχνικά *security controls* για την αποφυγή ανθρώπινων λαθών τότε ελαχιστοποιείται το *DI Human Factors*. Ωστόσο όταν αξιολογεί κάποιος μία διεργασία η οποία περιλαμβάνει ανθρώπινους χειρισμούς είναι μοιραίο να εισάγει ένα βαθμό «προσαρμοστικότητας» των ανθρώπων, κάτι το οποίο ερμηνεύεται μέσω του *DI Emergence* μεταξύ των στοιχείων *People* και *Process*.

7. Οι σύνδεσμοι του BMIS (DIs)

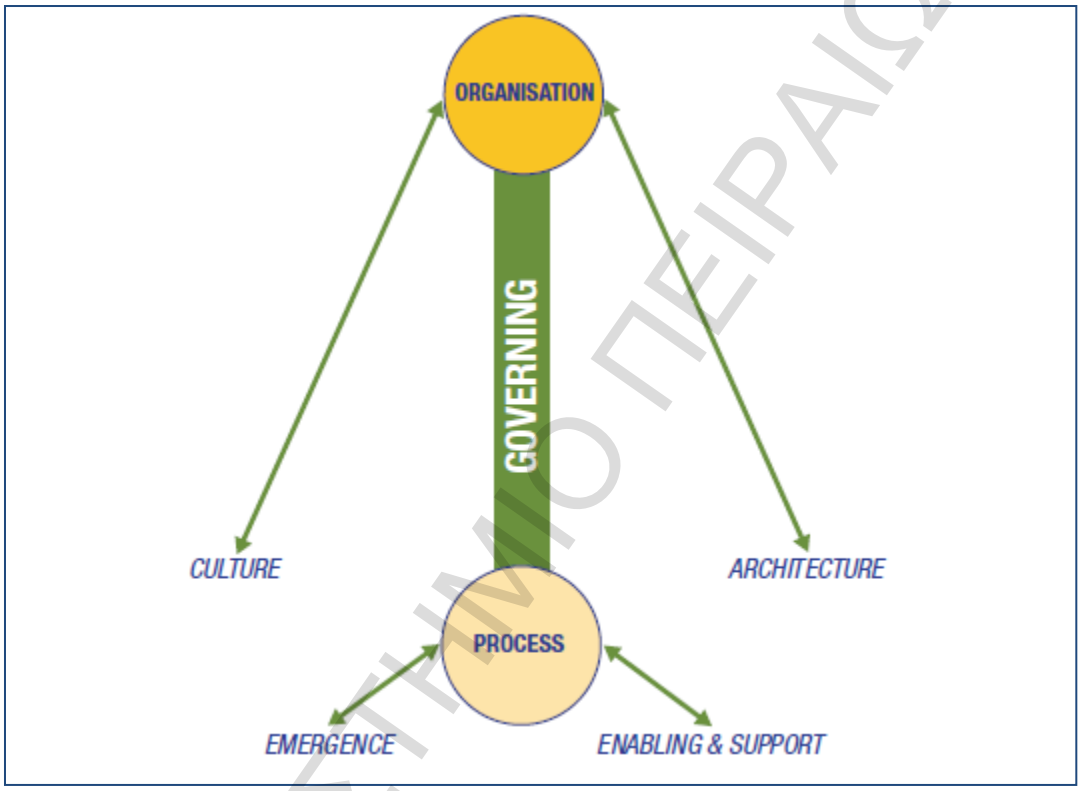
Ένα πολύ συχνό φαινόμενο κατά τη σχεδίαση *security programmes* είναι η παράλειψη των μηχανισμών αλληλεξαρτήσεων μεταξύ των οντοτήτων σε έναν οργανισμό. Το γεγονός αυτό οδηγεί συχνά σε γραμμικές προσεγγίσεις της ασφάλειας χωρίς να επιτυγχάνονται ουσιαστικά βήματα προόδου στην αντιμετώπιση των κινδύνων. Αν και στην πράξη είναι προφανές ότι κάθε φορά που συμβαίνει μία αλλαγή σε ένα στοιχείο του οργανισμού, τα επίπεδα ασφάλειας επηρεάζονται τόσο στο ίδιο το στοιχείο όσο και τα υπόλοιπα στοιχεία, στο σχεδιασμό η πρόβλεψη των επιπτώσεων των κινδύνων στα επιμέρους στοιχεία είναι εξαιρετικά δύσκολη. Στο *BMIS*, η σύνδεση αυτή μεταξύ των στοιχείων του οργανισμού εκφράζεται μέσω των *DIs*.

Κάθε *DI* μεταξύ δύο στοιχείων χαρακτηρίζεται από μία «ελαστικότητα» η οποία στην ουσία συμβολίζει το πόσο «ισχυρή» είναι η σχέση μεταξύ των δύο στοιχείων. Για παράδειγμα τα στοιχεία *Organization* και *People* συνήθως είναι στενά συνδεδεμένα, ωστόσο πολλές από τις καθημερινές δυσκολίες προκύπτουν από το γεγονός ότι η δομή ενός οργανισμού δεν ικανοποιεί τις προσδοκίες των υπαλλήλων που εργάζονται για αυτόν όπως συμβαίνει συχνά σε περιπτώσεις αξιοποίησης ενοικιαζόμενης εργασίας (Μελέτη Περίπτωσης Γ'). Παρομοίως το *DI Enabling and Support* ανάμεσα στα στοιχεία *Process* και *Technology*, αν και πάντα υπάρχει, μπορεί να παρομοιαστεί ως χαλαρός σύνδεσμος στις περιπτώσεις όπου η υφιστάμενη τεχνολογία δεν εξυπηρετεί απόλυτα τις διεργασίες του οργανισμού. Σε αυτή την περίπτωση, συνήθως απαιτούνται παραπάνω ενέργειες από το στοιχείο *People* προς το στοιχείο *Processes* οι οποίες εκφράζονται μέσω του *DI Emergence*. Οι διαφορετικές «τάσεις» μεταξύ των *DIs* γενικώς παραμορφώνουν το μοντέλο της τετράεδρης πυραμίδας, ωστόσο ο σκοπός του *BMIS* είναι η διενέργεια διορθωτικών αλλαγών με σκοπό την επαναφορά του μοντέλου σε ισορροπία.

Οι σύνδεσμοι μεταξύ των στοιχείων δείχνουν και τη δυναμικότητα του μοντέλου *(Dynamic Interconnections)*. Αντιπροσωπεύουν τα δυναμικά μέρη του μοντέλου στα οποία συμβαίνουν γεγονότα και αλλαγές οι οποίες καθορίζουν την κατάσταση της ασφάλειας των στοιχείων του οργανισμού. Οι αλλαγές προκύπτουν αρχικά στα *DIs* όπου εμφανίζεται μεγάλη τάση η οποία παραμορφώνει το μοντέλο, για να επηρεάσουν με τη σειρά τους τα αντίστοιχα στοιχεία. Χρησιμοποιώντας τη λέξη «τάση» μπορούμε να εκφράσουμε και την προβληματική επίδραση μίας αλλαγής στο σύστημα. Ένας βασικός στόχος του *BMIS* είναι η πρόβλεψη των επιπτώσεων των αλλαγών στα επίπεδα της ασφάλειας σε όλα τα στοιχεία του οργανισμού.

7.1 Governing

Ως *Governance* (Διακυβέρνηση) ορίζεται το σύνολο των ευθυνών και των πρακτικών της Διοίκησης για την παροχή στρατηγικής κατεύθυνσης, τη διασφάλιση επίτευξης των επιχειρηματικών στόχων και της αποτελεσματικής διαχείρισης των κινδύνων [26]. Η Εταιρική Διακυβέρνηση και η Διακυβέρνηση Πληροφοριακών Συστημάτων θέτουν τα όρια για το τι είναι εφικτό και τι όχι στην Ασφάλεια της Πληροφορίας.



Εικόνα 11: Governing DI (ISACA, "BMIS", 2010)

Ενεργώντας ως ο φυσικός σύνδεσμος μεταξύ των στοιχείων *Organization* και *Process*, το *Governing DI* (εικόνα 11), στα πλαίσια του *BMIS*, αντιπροσωπεύει το μέσο με το οποίο επιτυγχάνεται η Διακυβέρνηση. Αυτό σημαίνει «διαχείριση των διεργασιών με ταυτόχρονη επίτευξη των στρατηγικών στόχων». Ενώ τα δύο στοιχεία αντιπροσωπεύουν το «τι» και «πως» πρέπει να επιτευχθεί, το *DI* αυτό αντιπροσωπεύει το μέσον διασφάλισης υλοποίησής τους.

Η Διακυβέρνηση περιλαμβάνει το σύνολο των τακτικών ενεργειών που χρειάζονται για την επίτευξη των στρατηγικών στόχων στα πλαίσια ενός οργανισμού. Κάθε ενέργεια η οποία δεν εκπληρώνει αυτό το σκοπό από πλευράς Διακυβέρνησης συνήθως γίνεται αντιπαραγωγική δημιουργώντας δυσκολίες οι οποίες πρέπει να διευθετηθούν μέσω αλλαγών στο *Governing DI*. Η «υπερβολική διακυβέρνηση» πέρα από τα όσα είναι απαραίτητα για την επίτευξη των στόχων του οργανισμού και τον περιορισμό των κινδύνων

σε αποδεκτά επίπεδα, συχνά ανάγεται σε περιοριστική γραφειοκρατία, μειώνοντας τη δυνατότητα του οργανισμού στην υιοθέτηση καινούργιων στρατηγικών, στην προσαρμοστικότητά του στις αλλαγές του επιχειρηματικού περιβάλλοντος καθώς και στις αντοχές του σε περιόδους κρίσης.

Τα βασικά εργαλεία της διακυβέρνησης είναι τα πρότυπα και η έκδοση οδηγιών εργασίας για την εκπλήρωση των πολιτικών. Η εφαρμογή παρωχημένων προτύπων που δεν παρέχουν ολοκληρωμένη καθοδήγηση είναι βέβαιο ότι θα αφήσει τον οργανισμό εκτεθειμένο απέναντι σε σύγχρονους κινδύνους. Από την άλλη η εφαρμογή πολύ «αυστηρών» προτύπων, περισσότερο από όσο χρειάζεται το *control environment* του οργανισμού, περιορίζει την ευελιξία και την αποδοτικότητα των διεργασιών. Ομοίως, κάθε ενέργεια Διακυβέρνησης θα πρέπει να συνδέεται άμεσα με τη στρατηγική του οργανισμού και τους αντίστοιχους στόχους και να έχει σαφή και ξεκάθαρο λόγο ύπαρξης. Αυτό ισχύει στον υπερθετικό βαθμό για τις ενέργειες Διακυβέρνησης που σχετίζονται με τις διεργασίες της Ασφάλειας της Πληροφορίας.

Συνοπτικά η Διακυβέρνηση και κατά συνέπεια το *Governance DI* περιλαμβάνουν τα εξής στοιχεία:

- Πολιτικές
- Πρότυπα, οδηγίες εργασίας και άλλα κανονιστικά κείμενα
- Κανόνες λογοδοσίας *(accountability rules)*
- Διαχείριση πόρων (διανομή και προτεραιοποίηση)
- Διαδικασίες παραγωγής στατιστικών *(metrics)*
- Συμμόρφωση

Η επικοινωνία είναι ζωτικής σημασίας για το *Governing DI*. Ουσιαστικά, η Διακυβέρνηση θα πρέπει να γνωρίζει όλα τα κανάλια επικοινωνίας εντός ενός οργανισμού και για κάθε ενέργεια διακυβέρνησης να αξιοποιεί το κατάλληλο. Όπως ειπώθηκε ήδη, η αποτελεσματική επικοινωνία είναι εξαιρετικά δύσκολο να επιτευχθεί, ειδικά στους κόλπους πολύ μεγάλων οργανισμών. Δεν είναι τυχαίο που στα σύγχρονα πρότυπα διαχείρισης υπηρεσιών πληροφορικής *ITSMS* όπως το *“ISO/IEC 20000:2011”* υπάρχουν αφιερωμένες διατάξεις στη διαχείριση την επικοινωνίας (*ISO/IEC 20000:2011 - clause 4.1.3.b)* [27]. Για να επιτευχθεί η μέγιστη αποτελεσματικότητα στις διαδικασίες επικοινωνίας, αυτές πρέπει να είναι εγγενείς στην κουλτούρα, στις πρακτικές καθώς και στις υπόλοιπες διαδικασίες του οργανισμού.

Οι απαιτήσεις ασφάλειας θα πρέπει να επικοινωνούνται σαφώς σε κάθε επίπεδο και να είναι εξειδικευμένες σε κάθε ρόλο, και ει δυνατόν, σε κάθε θέση εργασίας. Αυτοί οι οποίοι είναι άμεσα υπεύθυνοι θα πρέπει να είναι σε θέση να εκτελούν στο ακέραιο τα καθήκοντά

τους, είτε ως εποπτικά είτε ως εκτελεστικά όργανα, και αυτό θα πρέπει να διασφαλίζεται μέσω προγραμμάτων εκπαίδευσης και συνεχούς προσπάθειας διατήρησης του βαθμού επίγνωσης των κινδύνων σε υψηλά επίπεδα.

Πολλά από τα θέματα Ασφάλειας των Πληροφοριών προκύπτουν απλώς από ανεπαρκείς σχεδιασμούς διεργασιών ή από την αποτυχία της εταιρικής κουλτούρας στο να μεταδώσει την ανάγκη για Ασφάλεια στις συνειδήσεις των ανθρώπων. Και τα δύο συνήθως συμβαίνουν εξαιτίας της προσήλωσης στην απόδοση των εργασιών. Εάν οι διεργασίες της Ασφάλειας αφεθούν έρμαια στις τάσεις της εταιρικής κουλτούρας τότε είναι βέβαιο ότι αυτές θα εξελιχθούν κατά τρόπο που να εξυπηρετεί στόχους οι οποίοι δεν έχουν γίνει κατανοητοί. Η Διακυβέρνηση θα πρέπει να επαναφέρει διαρκώς τα *processes* στην σωστή πορεία μέσω των διαδικασιών και των οδηγιών.

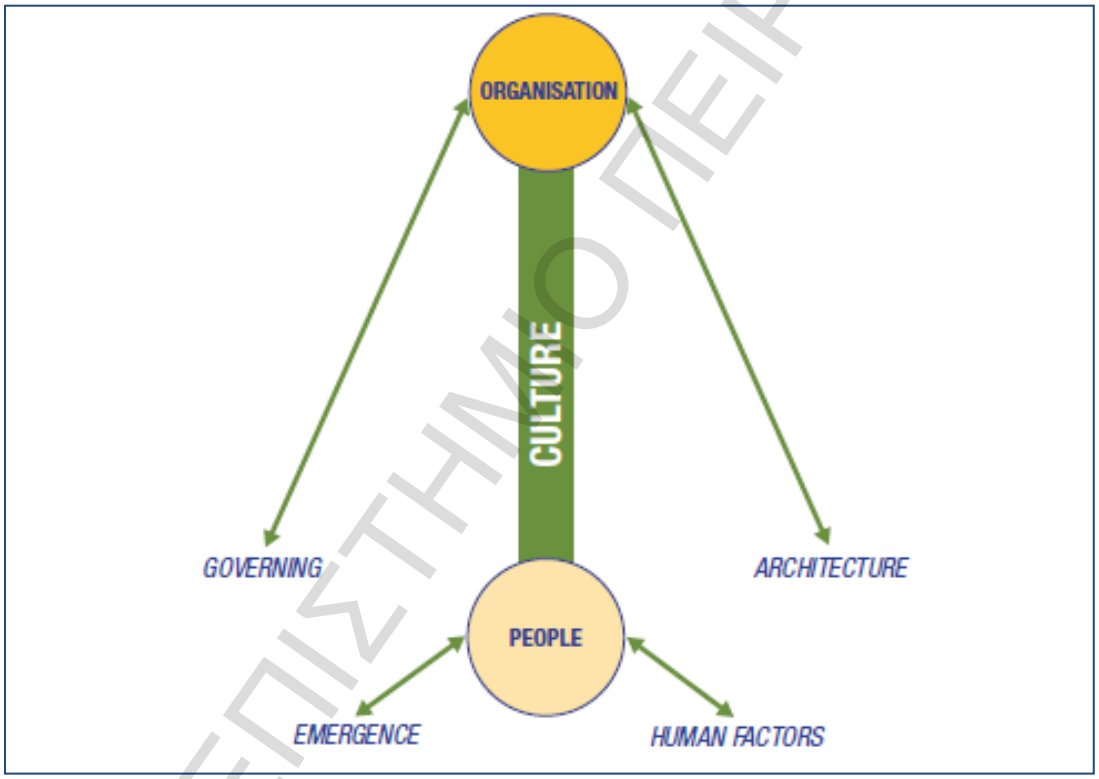
Η Διακυβέρνηση απαιτεί την ευθυγράμμιση όλων των διεργασιών τόσο με τους στρατηγικούς στόχους όσο και με τις μεθόδους μετρίασης ή περιορισμού των κινδύνων που απειλούν την επίτευξη των στρατηγικών στόχων. Είναι ευθύνη της υψηλής Διοίκησης η θέσπιση των διεργασιών, η επίγνωση των κινδύνων καθώς και η επίτευξη των στρατηγικών επιχειρηματικών στόχων.

Η αποτελεσματική διαχείριση κινδύνων απαιτεί στρατηγικό έλεγχο αφού τόσο η ευθύνη όσο και η λογοδοσία σε θέματα Ασφάλειας της Πληροφορίας πρέπει να βρίσκεται σε χέρια ανώτατων διευθυντικών στελεχών. Σε πολλές εταιρείες, η Ασφάλεια αντιμετωπίζεται περισσότερο ως ένα *low-level* τεχνικό ζήτημα παρά ως ένας στρατηγικός στόχος με αποτέλεσμα το ολοένα και μεγαλύτερο πλήθος περιστατικών ασφάλειας ανά τον κόσμο σε μεγάλους οργανισμούς. Στο μοντέλο *BMIS*, σύμφωνα με τα όσα έχουν ειπωθεί για τον τρόπο αλληλεπίδρασης μεταξύ των στοιχείων του, το *Governing DI* είναι ο μηχανισμός ο οποίος αναλαμβάνει να διατηρήσει την ισορροπία ανάμεσα στην επιχειρηματική στρατηγική και τις διεργασίες ασφάλειας. Για παράδειγμα, μία υπερβολικά φιλόδοξη στρατηγική για τον περιορισμό των εξόδων που έχει οριστεί από την υψηλή Διοίκηση μπορούν να επηρεάσουν καθοριστικά τις διεργασίες ασφάλειας. Σε αυτήν την περίπτωση, ο μηχανισμός της Διακυβέρνησης είναι αυτός που θέτει την πράξη του καθορισμού των απαιτούμενων επιπέδων ασφάλειας, των αποδεκτών επιπέδων κινδύνων και του κόστους των μέτρων για την επίτευξη αυτών.

Όλες οι δραστηριότητες της Διακυβέρνησης σχετικά με την Ασφάλεια της Πληροφορίας πρέπει να είναι ρητές και να αποτελούν αναπόσπαστο κομμάτι της οργανωτικής δομής και της στρατηγικής με καθορισμένους δεσμούς μεταξύ του σχεδιασμού , της στρατηγικής και των διεργασιών.

7.2 Culture

Η έννοια της «κουλτούρας» (εικόνα 12) είναι από τα *DIs* του *BMIS* το οποίο το διαφοροποιεί από άλλα μοντέλα ασφάλειας. Αν και ως όρος χρησιμοποιείται ευρέως για να περιγράψει τη συλλογική τάση των συμπεριφορών απέναντι σε διάφορα θέματα, σπανίως λαμβάνεται υπόψη στη μελέτη θεμάτων ασφάλειας, στην ανάλυση κινδύνων και στο σχεδιασμό πολιτικών. Ορίζοντας την κουλτούρα και τις επιπτώσεις της, μπορεί κάποιος να προσδώσει μία πιο ολοκληρωμένη εικόνα για τον οργανισμό. Οι επιπτώσεις της κουλτούρας στους ανθρώπους είναι «σημείο κλειδί» στην Ασφάλεια της Πληροφορίας δεδομένου ότι οι ίδιοι οι άνθρωποι είναι ικανοί στο να συνεισφέρουν τόσο στην προστασία της πληροφορίας όσο και στην διακύβευσή της.



Εικόνα 12: Culture DI (ISACA, "BMIS", 2010)

Το *Cultute DI* έχει άμεση επαφή με τα στοιχεία *Organization* και People, κάτι το οποίο ουσιαστικά σημαίνει ότι η εταιρική κουλτούρα επηρεάζει και επηρεάζεται από τις πολιτισμικές επιρροές του κάθε ανθρώπου – μέλος τους οργανισμού.

Τι είναι όμως ουσιαστικά η «κουλτούρα» και πως μπορεί κάποιος να την εντάξει σε ένα μοντέλο ασφάλειας; Ο ορισμός που αξιοποιείται από τον *ISACA* έχει ως εξής: *«Κουλτούρα είναι ένα μοτίβο συμπεριφορών, πεποιθήσεων, πιστεύω, υποθέσεων, στάσεων και τρόπων εκτέλεσης ενεργειών»* [28]. Η λέξη «μοτίβο» είναι αυτή η οποία έχει τη μεγαλύτερη ουσία σε αυτόν τον ορισμό. Οι κουλτούρες χτίζονται από μεμονωμένους ανθρώπους αλλά δεν

αντιπροσωπεύουν απαραίτητα τις ατομικές συμπεριφορές. Στο συγκεκριμένο μοντέλο, υφίστανται δύο επίπεδα κουλτούρας.

- την εταιρική κουλτούρα η οποία μορφοποιείται στο πέρασμα του χρόνου από τη στρατηγική, τον οργανωτικό σχεδιασμό και τις συμπεριφορές των ανθρώπων κατά την εργασία τους.
- την ατομική κουλτούρα η οποία σχεδόν πάντα ποικίλει ενώ συχνά είναι και ετερόκλητη.

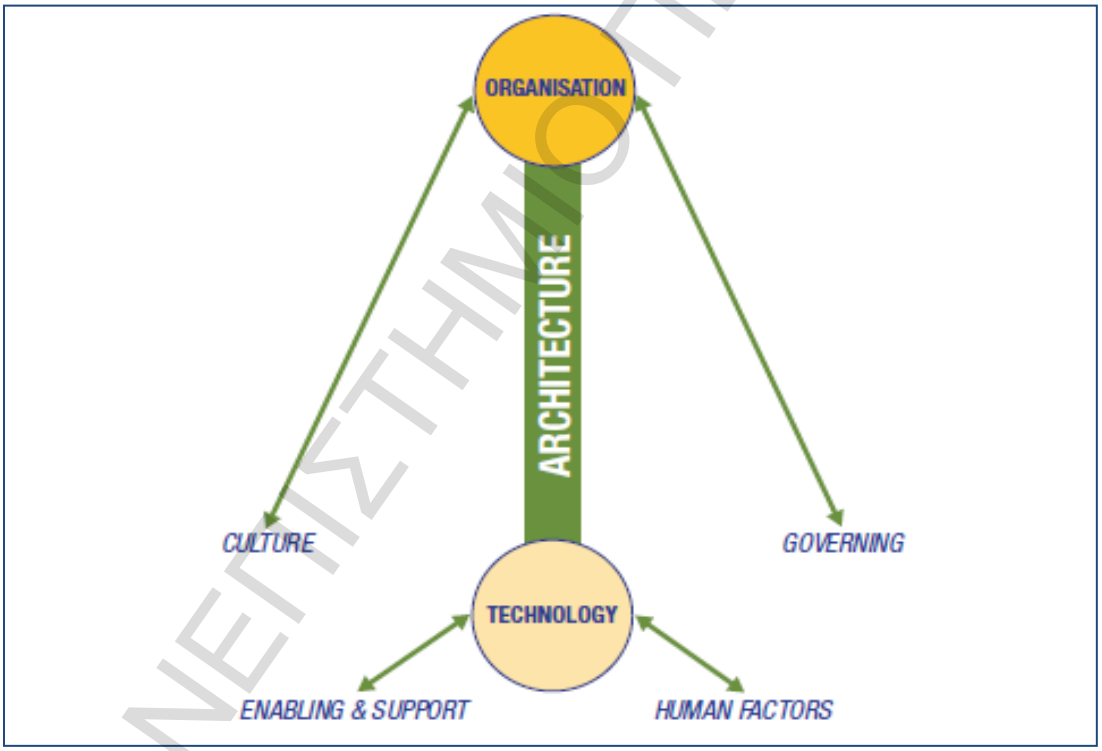
Και τα δύο επίπεδα θα πρέπει να λαμβάνονται υπόψη σε ένα περιβάλλον ελέγχου που περιέχει ανθρώπους. Για να μπορέσει να βελτιωθεί ένα *information security programme*, οι *managers* θα πρέπει να προσπαθούν να κατανοούν την υπάρχουσα κουλτούρα σε όλο το εύρος του οργανισμού και στη συνέχεια να βελτιώνουν τα αδύνατα σημεία αναφορικά με την ασφάλεια.

Το να αλλάξει ή να διαμορφώσει κάποιος την κουλτούρα σε ένα έναν οργανισμό είναι εξ ορισμού πολύ δύσκολο έργο δεδομένου ότι υπάρχουν φυσικοί περιορισμοί αναφορικά με την άμεση επίδραση που μπορεί να έχει κάποιος στην κουλτούρα του κάθε ανθρώπου. Συνεπώς είναι σημαντικό να αναγνωρίσει κανείς τις μεθόδους με τις οποίες μπορεί να επηρεάσει το πρώτο επίπεδο, την εταιρική κουλτούρα, η οποία μεταξύ άλλων αντιπροσωπεύει και την κοινή αντίληψη κινδύνων και τη στάση τους απέναντι σε θέματα ασφάλειας.

Η εταιρική κουλτούρα διαμορφώνεται κυρίως από την υψηλή Διοίκηση μέσω κανονιστικών εφαρμογών και οδηγιών. Κάθε προσέγγιση πρέπει να αξιολογείται άμεσα βάσει της επιχειρηματικής δραστηριότητας, της κρισιμότητας των πληροφοριών, της εξάρτησης της βιωσιμότητας του οργανισμού από τα πληροφοριακά του συστήματα. Ένας ιεραρχικός οργανισμός με σαφείς ρόλους οι οποίοι μεταδίδουν τα πιστεύω τους «από πάνω προς τα κάτω» αλλά και αυστηρούς κανονισμούς οι οποίοι σε πολλές περιπτώσεις προβλέπουν και πειθαρχικές κυρώσεις χαρακτηρίζεται από εν γένει ισχυρές δικλείδες ασφαλείας αλλά και από χαμηλή ευελιξία καθώς το περιβάλλον δεν επιτρέπει την εφαρμογή καινοτόμων ιδεών και πρωτοβουλιών. Αυτή η κουλτούρα σε μία ραγδαίως αναπτυσσόμενη αγορά μπορεί να αποδειχθεί καταστροφική. Από την άλλη, κουλτούρες οι οποίες χαρακτηρίζονται από μεγαλύτερη ισονομία μεταξύ των μονάδων και των στελεχών ενός οργανισμού, βάζουν ως πρώτη προτεραιότητα την παραγωγικότητα και την παρουσίαση γρήγορων και ανταγωνιστικών αποτελεσμάτων. Αυτό επιτυγχάνεται μέσω των δυνατοτήτων λήψης πρωτοβουλίας αλλά πολλές σε βάρος της ασφάλειας η οποία αντιμετωπίζεται ως εμπόδιο στη ροή εργασιών. Και σε αυτή την περίπτωση, εάν δεν έχει προηγηθεί μία αξιολόγηση από τη Διοίκηση για την κουλτούρα που θέλει να δημιουργήσει σχετικά με το περιβάλλον ασφάλειας, οι ενδεχόμενες συνέπειες περιστατικών ασφάλειας μπορεί να είναι ολέθριες.

7.3 Architecture

Η Αρχιτεκτονική είναι το σύνδεσμος που ενώνει τα στοιχεία *Organization* και *Technology* (εικόνα 13). Ενώ συχνά συγχέεται με την «υποδομή», σε ένα περιβάλλον ασφάλειας η Αρχιτεκτονική έχει πολύ μεγαλύτερη σημασία. Η Αρχιτεκτονική στην ουσία θέτει ένα σύνολο από κριτήρια τα οποία θα πρέπει να πληρούνται. Στη συνέχεια θα πρέπει τα κριτήρια αυτά να μεταφράζονται σε στόχους και να τοποθετούνται σε ένα μοντέλο. Έπειτα γίνεται η έρευνα για τις μεθόδους επίτευξης των στόχων και τα εργαλεία τα οποία θα αξιοποιηθούν για την ολοκλήρωση του περιβάλλοντος Ασφάλειας. Σύμφωνα με το *CISM Review Manual* του *ISACA* [29]: *Η ουσία της Αρχιτεκτονικής είναι ο σαφής και συνεκτικός καθορισμός των στόχων πολύπλοκων συστημάτων με ακριβείς προδιαγραφές και δομές οι οποίες έχουν σχεδιαστεί και δοκιμαστεί ως προς τη μορφή, την εφαρμογή και τη λειτουργία τους καθώς και για τις δυνατότητες παρακολούθησης των επιδόσεων τους ώστε να αξιολογούνται για το βαθμό επιτυχίας τους.*

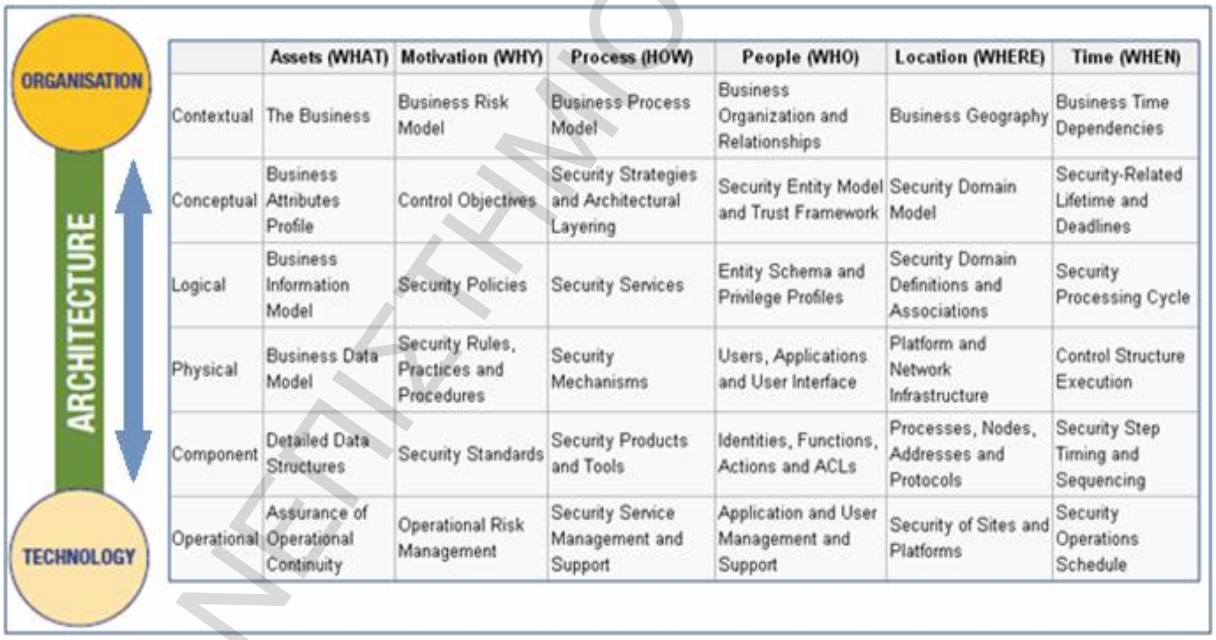


Εικόνα 13: Architecture DI (ISACA, "BMIS", 2010)

Υπάρχει πλήθος διαφορετικών προσεγγίσεων υλοποίησης αρχιτεκτονικών μοντέλων τα οποία εν γένει κατηγοριοποιούνται είτε σε *frameworks* είτε σε *process models*. Εάν η εταιρική Αρχιτεκτονική περιλαμβάνει και στόχους ασφάλειας τότε εύκολα ανάγεται και σε Αρχιτεκτονική ασφάλειας. Ωστόσο, το να διαχωρίζονται τα στοιχεία της ασφάλειας από την υπόλοιπη αρχιτεκτονική, δε βοηθά στην ενσωμάτωσή τους. Ενώ υπάρχουν διαθέσιμες πολλές διαφορετικές προσεγγίσεις, οι πιο διαδεδομένες είναι η *"TOGAF" (The Open Group*

Architecture Framework) [30] και η *"SABSA" (Sherwood Applied Business Security Architecture)* [31] η οποία έχει κοινή δομή με το πλαίσιο εταιρικής αρχιτεκτονικής "*Zachman Enterprise Framework"* [32].

Στα πλαίσια αξιοποίησης του *BMIS*, είναι προτιμότερη η αξιοποίηση μίας απλής και άμεσης προσέγγισης τύπου *Zachman* όπως η *SABSA*. Το εν λόγω *framework*, χωρίζεται σε έξι επίπεδα όπως φαίνεται στον πίνακα της εικόνας 14. Το ανώτερο επίπεδο *(Contextual)* είναι το στάδιο της ανάλυσης των απαιτήσεων των επιχειρήσεων. Για κάθε κατώτερο επίπεδο, ορίζεται και ένα νέο στάδιο ανάλυσης, ξεκινώντας από την σημασία των αρχιτεκτονικών στόχων *(Conceptual)*, την αρχιτεκτονική σε επίπεδο λογικών υπηρεσιών *(Logical)*, την αρχιτεκτονική σε επίπεδο φυσικών υποδομών *(Physical)*, την επιλογή των τεχνολογιών και προϊόντων *(Component)* και τέλος ο καθορισμός των λειτουργιών τους *(Operational)*. Ο πίνακας δείχνει τη σχέση και την αλληλεπίδραση που έχουν τα επίπεδα με τα συστατικά μέρη του οργανισμού. Τα ανώτερα επίπεδα είναι άμεσα συνδεδεμένα με τον στοιχείο *Organization* ενώ τα χαμηλότερα επίπεδα είναι άμεσα συνδεδεμένα με το στοιχείο *Technology*.



	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetime and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites and Platforms	Security Operations Schedule

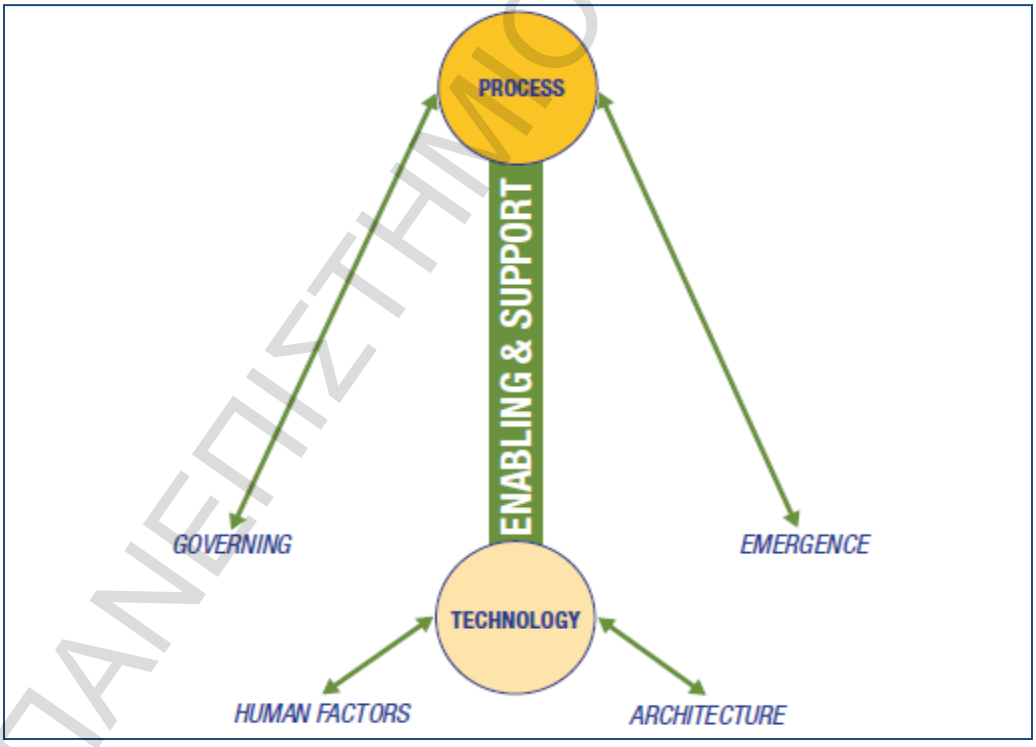
Εικόνα 14: SABSA Matrix Ανάπτυξης Αρχιτεκτονικής Ασφάλειας και Architecture DI

Στο *contextual* επίπεδο, το *Architecture DI* αποσκοπεί στο να διασφαλίσει ότι η ασφάλεια της Εταιρικής Πληροφορίας είναι σε συμφωνία με τα νομικά και κανονιστικά πλαίσια της γεωγραφικής περιοχής αλλά και του επιχειρηματικού πεδίου στο οποίο δραστηριοποιείται ο οργανισμός (τραπεζικός τομέας, ασφαλιστικές εταιρείες, υπηρεσίες υγείας κ.λπ.). Το *conceptual* επίπεδο για την Ασφάλεια της Πληροφορίας είναι αυτό στο οποίο διασφαλίζεται ο σωστός σχεδιασμός των παρακάτω τεχνολογικών επιπέδων *(physical* και *logical)* ώστε να

μην υποστηρίζουν απλώς τους στόχους ασφάλειας αλλά και να τους θέτουν ως προαπαιτούμενη ανάγκη από σχεδιασμού τους *(build-in security)*. Τα επόμενα τα οποία αναφέρονται σε τεχνικό επίπεδο *(logical & physical)* αναφέρονται στον λεπτομερή σχεδιασμό των συστατικών ασφάλειας αξιοποιώντας την τεχνολογία για να διασφαλιστεί η εκπλήρωση των στόχων ασφάλειας που έχουν τεθεί από τα υψηλότερα επίπεδα.

7.4 Enabling and Support

Ο σύνδεσμος *Enabling and Support DI* ο οποίος στα ελληνικά θα μπορούσε να αποδοθεί ως «Ενεργοποίηση και Υποστήριξη», ενώνει τα στοιχεία *Process* και *Technology* (εικόνα 15). Αντιπροσωπεύει την διεργασία με τους οποίους αλληλεπιδρούν οι *business* διεργασίες με την τεχνολογία. Από τη μία, οι διεργασίες αξιοποιούν την τεχνολογία και από την άλλη οι αλλαγές στην τεχνολογία επηρεάζουν τις ροές των διεργασιών. Το εν λόγω *DI* έχει ονομαστεί *"Enabling & Support"* στο *BMIS* διότι οι διεργασίες είναι αυτές που θέτουν σε εφαρμογή την τεχνολογία *(enabling)* και η τεχνολογία είναι αυτή που υποστηρίζει τις *business* διεργασίες *(support)*.



Εικόνα 15: Enabling & Support DI (ISACA, "BMIS", 2010)

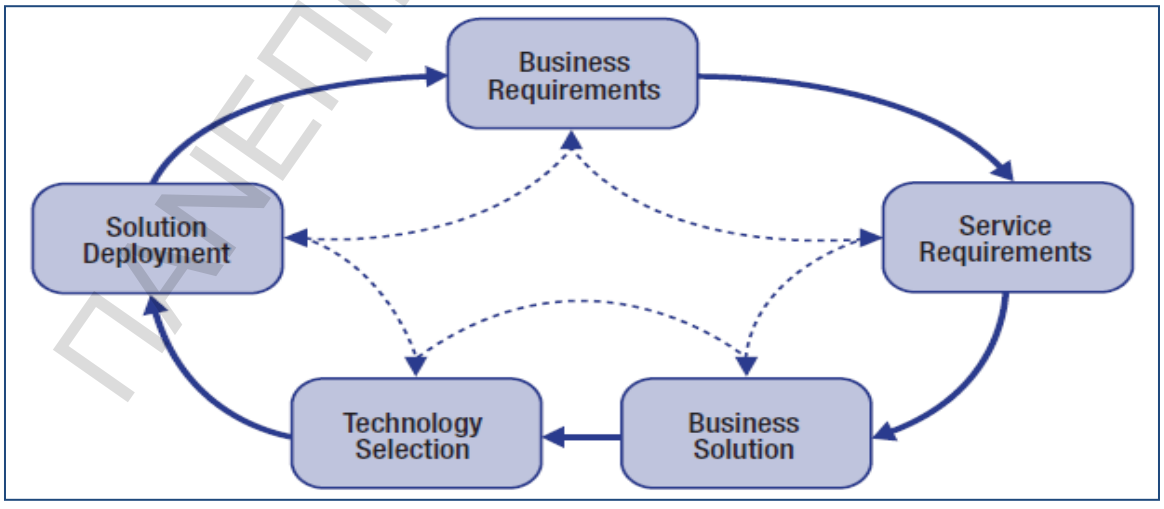
Όπως έχει ήδη ειπωθεί, πολλοί οργανισμοί αντιμετωπίζουν την ασφάλεια ως ένα αποκλειστικά τεχνικό ζήτημα. Αυτό έχει ως επιπλέον παρενέργεια, να διαχωρίζεται η τεχνολογία από τα *business processes* και να αντιμετωπίζεται γραμμικά χωρίς να

λαμβάνεται υπόψη η υποστήριξη που θα προσφέρει στις διεργασίες του οργανισμού βάσει των στρατηγικών στόχων.

Εικόνα 16: Γραμμική ροή αξιοποίησης της Τεχνολογίας (ISACA, "BMIS", 2010)

Η προσέγγιση αυτή οδηγεί ουσιαστικά τους οργανισμούς στο να χρησιμοποιούν την υπάρχουσα τεχνολογική εγκατάσταση ανεξαρτήτως με το αν προκύπτουν διαφορετικές ανάγκες μέσω μηχανισμών ανατροφοδότησης. Συχνά για τα προβλήματα που προκύπτουν, ο οργανισμός καλεί τον πάροχο για συνεχείς βελτιώσεις που ανεβάζουν το κόστος και οι οποίες πολλές φορές δεν αποτελούν ολοκληρωμένες λύσεις. Το προσαυξημένο κόστος οδηγεί τον οργανισμό από το διακόψει την υποστήριξη από τον πάροχο και τελικά να μείνει στην κατοχή του με ένα εργαλείο για το οποίο έχει πληρώσει πολλά χρήματα χωρίς την αναμενόμενη ανταπόδοση.

Αντιθέτως, μία συστεμική λογική η οποία θα αξιοποιούσε μία κυκλική ροή αξιοποίησης της τεχνολογίας (εικόνα 17), θα δίνει αφενός μεν τη δυνατότητα να επιστρέφει κάποιος σε προηγούμενα βήματα και αφετέρου δε θα επιτρέπει τη συνεχή αξιολόγηση *(gap analysis)* της τεχνολογικής υλοποίησης βάσει των επιχειρηματικών απαιτήσεων *(business requirements)*. Για παράδειγμα, εάν η τεχνική εφαρμογή δεν είναι απόλυτα συμβατή με τις δυνατότητες της τεχνολογίας τότε κάποιος θα πρέπει να επαναξιολογήσει την υφιστάμενη τεχνολογία *(technology selection)*. Αν η προς επιλογή τεχνολογική λύση δεν είναι ξεκάθαρη τότε κάποιος θα πρέπει να διερευνήσει ή να επαναπροσδιορίζει την επιχειρηματική λύση *(business solution)*. Το ίδιο ισχύει και για τα υπόλοιπα στάδια.

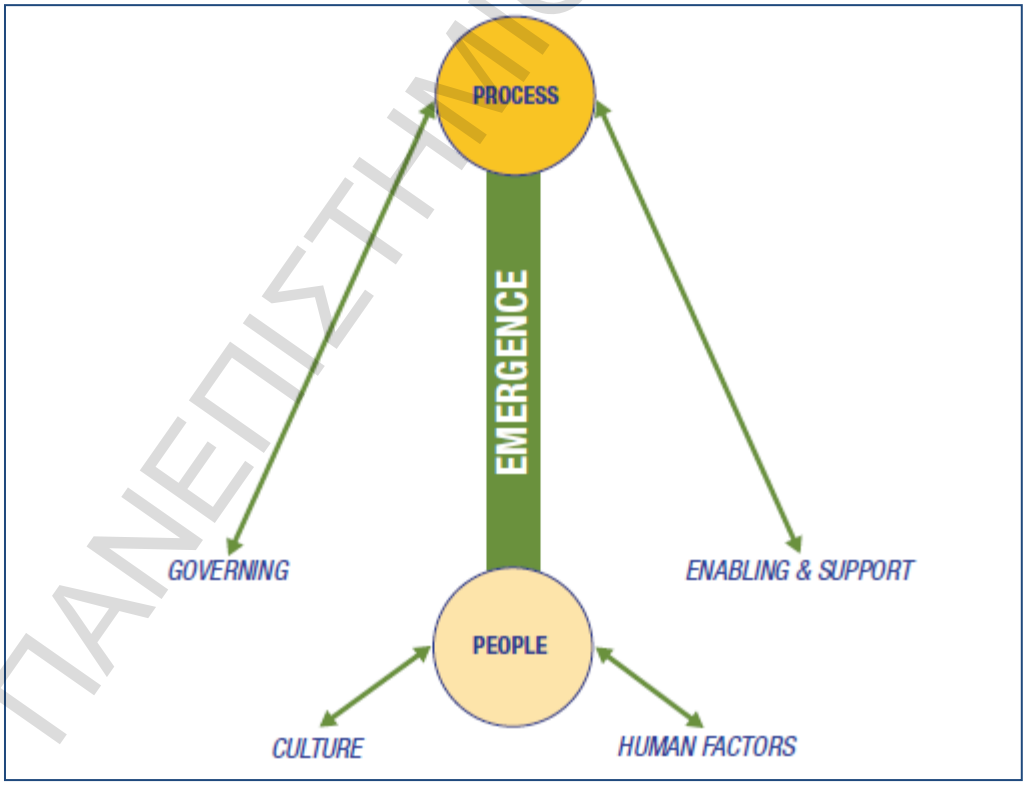


Εικόνα 17: Κυκλική ροή αξιοποίησης της Τεχνολογίας (ISACA, "BMIS", 2010)

Στο *BMIS*, η σχέση των στοιχείων *Process* και *Technology* είναι αυτονόητη. Στην πραγματικότητα είναι πολύ δύσκολο να διαχωρίσει κανείς αυτά τα δύο στοιχεία. Το *Enabling & Support DI* είναι μία αμφίδρομη σχέση η οποία μπορεί να γίνει κατανοητή μόνο μέσω μίας συστεμικής προσέγγισης η οποία θα περιλαμβάνει την ανατροφοδότηση, την ισορροπία μεταξύ των αναγκών και των λύσεων αλλά και την καθυστέρηση της εγκατάστασης μιας τεχνολογικής λύσης από τη στιγμή που θα αναδειχθεί ως ανάγκη.

7.5 Emergence

Με τον όρο *"Emergence"* ο οποίος στα ελληνικά μπορεί να αποδοθεί ως «ανάδειξη αναγκών» εννοούνται οι διαδικασίες με τις οποίες πραγματοποιείται η συνεχής βελτίωση βάσει συνεχών αξιολογήσεων των λειτουργιών ως προς την αποδοτικότητά αλλά και των κινδύνων ή ευκαιριών που αναδεικνύονται στη ροή των καθημερινών εργασιών. Το *BMIS* θέτει το συγκεκριμένο *DI* ανάμεσα στα στοιχεία *Processes* και *People* (εικόνα 18) με τη λογική ότι από τα στοιχεία του μοντέλου, οι άνθρωποι είναι αυτοί με την ικανότητα «μάθησης» και οι διεργασίες είναι αυτές με την δυνατότητα «βελτίωσης» σε ένα συνεχώς μεταβαλλόμενο επιχειρηματικό πεδίο.



Εικόνα 18: Emergence DI (ISACA, "BMIS", 2010)

Δεδομένου λοιπόν ότι το εν λόγω *DI* εκφράζει τον τρόπο με τον οποίο οι άνθρωποι επηρεάζουν τις διεργασίες, το *Emergence* γίνεται αυτομάτως ένα πολύ κρίσιμο σημείο του *BMIS*. Είναι μία περιοχή η οποία εάν διαχειριστεί με σωστό τρόπο, μπορεί να προσφέρει αποδοτικές μεθόδους υψηλής προσαρμοστικότητας σε απότομες και βίαιες αλλαγές, να βελτιώσει σημαντικά τις προοπτικές βιωσιμότητας του οργανισμού απέναντι σε καινοφανείς κινδύνους καθώς και να αναπτύξει τρόπους ανάδειξης καινοτόμων λειτουργιών.

Το *Emergence* μπορεί να διαχωριστεί σε θετικό και αρνητικό. Το θετικό *Emergence* σχετίζεται με τη διαδικασία εκμάθησης και βελτίωσης των διεργασιών και των επιπέδων ασφάλειάς τους. Το αρνητικό *Emergence* σχετίζεται με το φαινόμενο των ανεξήγητων περιστατικών ασφάλειας και της ανεπαρκούς ευθυγράμμισης της Ασφάλειας των Πληροφοριών και των επιχειρησιακών στόχων.

Μία διεργασία μπορεί να είναι σαφώς ορισμένη και κατανοητή στους ανθρώπους που την υλοποιούν. Πολλές φορές ωστόσο το αποτέλεσμα μίας διεργασίας δεν μπορεί να είναι προβλέψιμο, ειδικά όταν αυτή βρίσκεται στα πρώτα στάδια εκτέλεσής της και επομένως σε χαμηλό επίπεδο ωριμότητας [23]. Η εκτέλεση μίας διεργασίας Ασφάλειας Πληροφοριών, μπορεί να προκύπτει από τα εξής:

- **Διαδικασίες Ασφάλειας και Οδηγίες Εργασίας:** Εκπλήρωση καθημερινών εργασιών βασισμένες σε γραπτές, επίσημες και καθορισμένες οδηγίες.
- **Πολιτικές Ασφάλειας:** Εκτέλεση καθηκόντων βασισμένων στη «μετάφραση» των κανόνων που ορίζουν οι Πολιτικές Ασφάλειας.
- **Ad hoc:** Εκτέλεση ενεργειών που προκύπτουν από απρόβλεπτους παράγοντες σε ανύποπτους χρόνους και χωρίς την κάλυψη επίσημων οδηγιών.

Κάθε μία από τις παραπάνω κατηγορίες εισάγει ένα βαθμό αβεβαιότητας ο οποίος δεν μπορεί να εξαλειφθεί πλήρως και ο οποίος πηγάζει από τις ιδιαιτερότητες της ανθρώπινης φύσης. Συγκεκριμένα:

- Αναφορικά με τις επίσημες Διαδικασίες Ασφάλειας, οι άνθρωποι ενδέχεται να παρουσιάζουν συμπεριφορά μη συμμόρφωσης ή να τις ακολουθούν με λανθασμένο τρόπο. Μία Διαδικασία μπορεί, έτσι όπως έχει συνταχθεί, να μην καλύπτει όλες τις πιθανές περιπτώσεις εκτέλεσής της (διαφορετικές τεχνολογικές πλατφόρμες, διαφορετικές κατηγορίες δεδομένων κ.λπ.) ή να παρουσιάζει μεγάλο βαθμό πολυπλοκότητας ώστε η εκτέλεση των εργασιών βάσει αυτής να είναι εξαιρετικά δύσκολη. Συχνά, σε τέτοιες περιπτώσεις, κάποιοι άνθρωποι μπορεί να μεταφράσουν τις Διαδικασίες κατά τρόπο ο οποίος μπορεί να μην είναι συμβατός με τις επίσημες οδηγίες αλλά γίνεται αποδεκτός από το σύνολο των όσων τις ακολουθούν. Σε αυτή

την περίπτωση υφίσταται μία ανάδειξη *(Emergence)* ενός νέου τρόπου χειρισμού μίας Διαδικασίας.

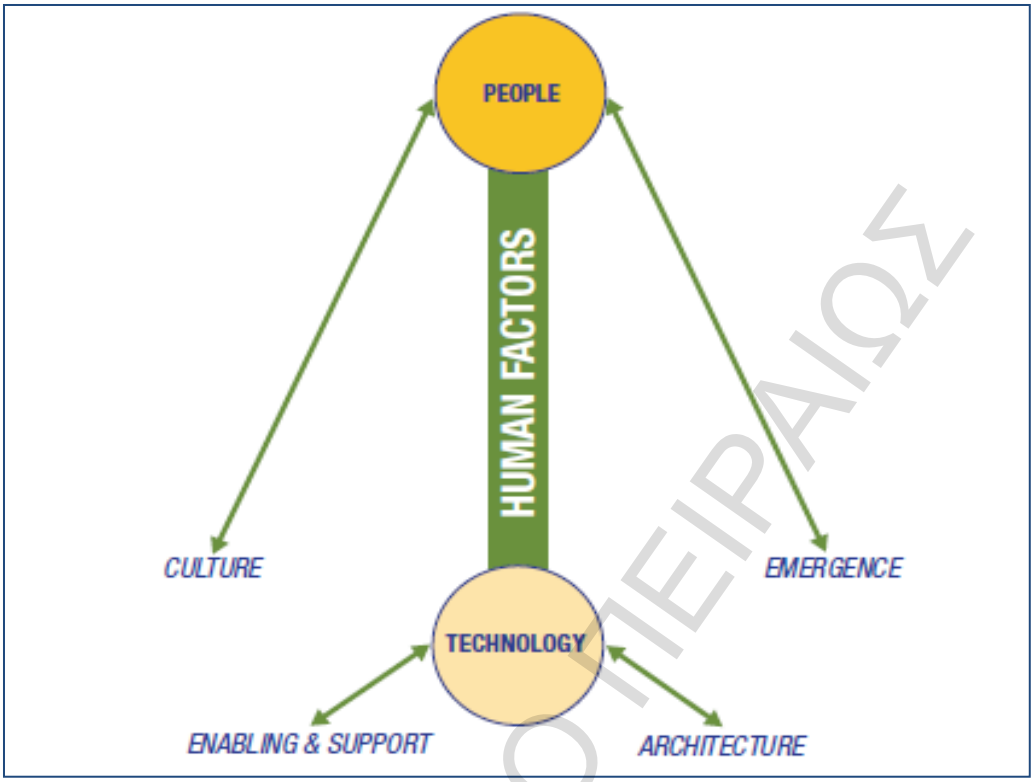
- Οι Πολιτικές Ασφάλειας είναι περισσότερο γενικευμένες από ότι οι Διαδικασίες Ασφάλειας οι οποίες περιγράφουν σε βήματα την εκτέλεση εργασιών και ως εκ τούτου περισσότερο πιθανό να παρερμηνευτούν. Μπορούν επίσης να μεταφραστούν λαθεμένα, κυρίως σε χώρους με πολύ διαφορετικό αντικείμενο εργασίας. Επιπλέον μπορούν να μην εξυπηρετούν καθόλου σε καταστάσεις κρίσης ή να δίνουν τόσο μεγάλο πλήθος εναλλακτικών που να ακυρώνουν την αξία τους ως Πολιτικές Ασφάλειας.

- Όσο για τις ad hoc καταστάσεις, το μόνο που μπορεί να πει κάποιος με σιγουριά είναι ότι σε ένα σύνθετο περιβάλλον με πολλά πληροφοριακά αγαθά, οι καταστάσεις αυτές είναι τόσο συχνές ώστε η προσέγγισή τους στις Πολιτικές και τις Διαδικασίες Ασφάλειας να γίνεται αναγκαιότητα. Δεδομένου ότι η ανθρώπινη συμπεριφορά δεν μπορεί να ενταχθεί σε κανένα πλαίσιο, η αβεβαιότητα αυξάνεται όταν οι άνθρωποι δεν έχουν εντολές να ακολουθήσουν σε απρογραμμάτιστες περιπτώσεις ή δεν έχουν εκπαιδευτεί σε καταστάσεις κρίσης.

Το *Emergence DI*, εκτός από διεργασία εκμάθησης είναι και το εργαλείο με το οποίο η ασφάλεια περνάει από τη θεωρία στην πράξη. Μέσω αυτού, γίνεται η προσαρμογή των ανθρώπων με απόλυτο στόχο τη βέλτιστη απόδοση των διεργασιών ασφάλειας αλλά και αντιστρόφως. Η προσαρμογή και η εκμάθηση απαιτεί χρόνο ενώ είναι απαραίτητη η παροχή ανατροφοδότησης από τους ανθρώπους ώστε το *security* να βελτιώνεται συνεχώς χωρίς ωστόσο αυτό να συμβαίνει εις βάρος της αποδοτικότητας των λειτουργιών.

7.6 Human Factors

Ο ανθρώπινος παράγων *(Human Factors)* αντιπροσωπεύει το *DI* που συνδέει τα στοιχεία *People* και *Technology* (εικόνα 19). Το πεδίο των ανθρώπινων παραγόντων έχει γίνει αντικείμενο μελέτης για πάρα πολλές έρευνες. Το συγκεκριμένο *DI* έχει συσχετιστεί πολλές φορές με το *HCI (human-computer interface)*, το επίπεδο φιλικότητας της τεχνολογίας προς το χρήστη *(user friendliness)* και το βαθμό χρηστικότητας των τεχνολογικών εφαρμογών.



Εικόνα 19: Human Factors DI (ISACA, "BMIS", 2010)

Η σχέση μεταξύ ανθρώπων και τεχνολογίας εισάγει πάγιους κινδύνους ασφάλειας δεδομένου ότι τα επίπεδα κατανόησης τόσο της ασφάλειας όσο και της ίδιας της τεχνολογίας που αξιοποιείται μπορούν να διαφέρουν από άνθρωπο σε άνθρωπο.

Επιπλέον θίγονται και τα θέματα ευκολίας της χρήσης της τεχνολογίας τόσο σε επίπεδο καθημερινής χρήσης όσο και σε επίπεδο διαμόρφωσης *(configuration)* και παραμετροποίησης *(customization)*. Τέτοια θέματα μπορούν να εισάγουν νέους κινδύνους Ασφάλειας Πληροφοριών. Συνήθως οι οργανισμοί με σύνθετα πληροφοριακά συστήματα και κρίσιμα επιχειρησιακά δεδομένα, επενδύουν στην αγορά ακριβού εξοπλισμού για υλοποιήσεις *IPS, DLP, SIEM* κ.λπ. Αν και συνήθως οι συσκευές αυτές διαθέτουν προεπιλεγμένες ρυθμίσεις *(default settings)* οι οποίες είναι σύμφωνες με συνήθεις και βέλτιστες πρακτικές, οι μονάδες που τις διαχειρίζονται συχνά τις διαμορφώνουν με σενάρια τα οποία θεωρούν ότι ενδιαφέρουν τον οργανισμό για τον οποίο λειτουργούν. Οποιαδήποτε λάθη κατά την διαμόρφωση ενδέχεται να κάνουν τον εξοπλισμό να λειτουργεί κατά αναξιόπιστο τρόπο όπως με την παραγωγή χιλιάδων ψευδώς αληθών *(false positives)* δημιουργώντας απρόβλεπτα περιστατικά ασφάλειας τα οποία δε θα μπορέσουν να αξιολογηθούν και να αντιμετωπισθούν έγκαιρα. Αντίστοιχα, είναι πολύ σημαντικό οι υπάλληλοι οι οποίοι διαχειρίζονται και παρακολουθούν τον εξοπλισμό αυτό να είναι κατάλληλα εκπαιδευμένοι ώστε να μπορούν να «διαβάζουν» σωστά τις ενδείξεις που λαμβάνουν. Θα πρέπει λοιπόν, η όποια διαμόρφωση εφαρμόζεται στον εξοπλισμό

ασφάλειας να είναι βασισμένη στα αποτελέσματα μίας ολοκληρωμένης ανάλυσης επικινδυνότητας και να μην είναι υλοποιείται βάσει των προεπιλεγμένων ρυθμίσεων, ούτε να βασίζεται στη διαίσθηση και την εμπειρία των στελεχών που τον διαχειρίζεται. Με αυτόν τον τρόπο οι ενδείξεις των συσκευών μπορούν να γίνουν πιο αξιόπιστες ενώ οποιοδήποτε ψευδώς αληθές, μπορεί να δράσει ως διορθωτικός παράγων σε επόμενες αναλύσεις επικινδυνότητας.

Ένα άλλο σημείο το οποίο χρήζει προσοχής είναι η αποδοχή της τεχνολογίας από τους ίδιους τους χρήστες *(user acceptance)*. Εάν οι τεχνολογίες οι οποίες έχουν επιλεχθεί για την προστασία των εταιρικών δεδομένων φτάσουν στο σημείο να μειώνουν την παραγωγικότητα ή να εμποδίζουν τη φυσιολογική ροή των καθημερινών εργασιών τότε αυτές δε μπορούν να χαρακτηριστούν ως αποδοτικές ή ακόμα και ως αποτελεσματικές. Επομένως, είναι πολύ σημαντικό τα επίπεδα αποδοχής των χρηστών να λαμβάνονται υπόψη κατά την υλοποίηση τεχνικών *security controls*.

Τόσο το *Human Factors DI* όσο και το *Culture DI*, είναι υπεύθυνα για την περιγραφή και αναγνώριση των συμπεριφορών των ανθρώπων σε θέματα ασφάλειας. Η εικόνα των ανθρώπων οι οποίοι διαρκώς παρακάμπτουν τα υφιστάμενα *security controls* δεν είναι καθόλου σπάνια στους μεγάλους οργανισμούς. Δεν είναι λίγες οι εταιρείες που έχουν επενδύσει στην αιχμή της τεχνολογίας στο χώρο του *IT Security* μόνο και μόνο για να δουν τους υπαλλήλους τους είτε να την αγνοούν είτε να εφευρίσκουν τρόπους για να την παρακάμπτουν. Αξίζει να αναφερθεί και το ότι η προμήθεια των ακριβότερων ή πιο σύγχρονων τεχνολογιών δημιουργεί συχνά την ψευδαίσθηση της πλήρους ασφάλειας εισάγοντας επιπλέον κινδύνους.

Όπως είναι προφανές, το *IT* παρέχει λύσεις και απαντήσεις, ωστόσο οι απαντήσεις δεν μπορούν να αντικαταστήσουν τις «σωστές ερωτήσεις», ειδικά στον χώρο της Ασφάλειας της Πληροφορίας. Όταν οι άνθρωποι επαναπαύονται απλώς στην τεχνολογία χωρίς να αντιλαμβάνονται το σκοπό που εξυπηρετεί τότε ακόμα και οι πιο προφανείς αδυναμίες ασφάλειας μπορούν να παραβλεφθούν. Αυτό μπορεί να ισχύσει σε όλα τα επίπεδα ενός οργανισμού:

- Τα ανώτερα στελέχη παρουσιάζουν υπερβολικά μεγάλη εξάρτηση στον τεχνικό εξοπλισμό για να παρέχουν την υποδομή ασφάλειας που απαιτεί το *business*.
- Οι *managers* βασίζονται στην ύπαρξη των *security controls* που προκύπτουν από τις Πολιτικές Ασφάλειας για την κάλυψη όλων των αδυναμιών.
- Το προσωπικό αισθάνεται αναρμόδιο για τα ζητήματα ασφάλειας ενώ πιστεύει ότι όλες οι αδυναμίες ή ακόμα και οι απειλές προέρχονται από κάποιον άλλο χώρο και όχι από το δικό του, εφόσον φυσικά ακολουθεί πιστά τις Πολιτικές και τις Διαδικασίες Ασφάλειας.

Συνεπώς τα πιθανά θέματα τα οποία θα πρέπει να ελέγχονται από αυτό το *DI* περιλαμβάνουν μεταξύ άλλων:

- Αποτυχία κατανόησης, όχι απλώς των απαιτήσεων ασφάλειας αλλά κυρίως των λόγων για τους οποίους αυτές είναι απαραίτητες.
- Αδυναμία αντίληψης των επιχειρηματικών κινδύνων και των πιθανών επιπτώσεων.
- Έλλειψη επαρκούς γνώσης υλοποίησης - ή και ακόμα ύπαρξης – τεχνικών μεθόδων στο περιβάλλον ασφάλειας.
- Ανθρώπινα λάθη υπό τη μορφή αμέλειας.
- Εξωγενείς ανθρώπινοι παράγοντες όπως περιπτώσεις δωροδοκίας, διαφθοράς και κοινωνικών προβλημάτων.
- Φυσικές ανθρώπινες τάσεις οι οποίες οδηγούν τους ανθρώπους να κάνουν κακή χρήση της τεχνολογίας για δικούς τους σκοπούς (π.χ. η χρήση του *internet* για μη υπηρεσιακούς σκοπούς).

Οι επιπτώσεις του *Human Factors DI* στο στοιχείο *People*, όπως και το αντίστροφο, είναι εν γένει εύκολες στην κατανόηση αλλά δύσκολες στο χειρισμό και στην αντιμετώπιση των προβλημάτων που αυτές δημιουργούν. Ωστόσο, η σχέση αυτή μπορεί να αποδειχθεί η πιο κρίσιμη από όλες δεδομένου ότι από την εποχή της κρυπτανάλυσης του *Enigma* έως και σήμερα, σε ολόκληρη τη σχετική βιβλιογραφία, ο ανθρώπινος παράγων είναι γνωστός ως ο πιο αδύναμος κρίκος της Ασφάλειας των Πληροφοριών [33], [34].

8. Αξιοποίηση του Μοντέλου

Η λογική που ακολουθεί το μοντέλο προωθεί την προσέγγιση της ασφάλειας σε φάσεις οι οποίες θα μπορούν να αναλυθούν διακριτά και στη συνέχεια να ενταχθούν σε ένα ολοκληρωμένο *BMIS security programme* το οποίο θα παρακολουθείται διαρκώς για την συνεχή βελτίωσή του. Ωστόσο δεδομένου ότι αναφερόμαστε σε «μοντέλο» και όχι σε κάποιο «αυστηρό πρότυπο», η προσέγγιση μπορεί να ποικίλει κατά την κρίση του εκάστοτε αναλυτή ασφάλειας και αναλόγως τις επιχειρηματικές συνθήκες και ανάγκες. Σε γενικές γραμμές τα βήματα θα μπορούσαν να ακολουθούν την εξής λογική:

- Ενσωμάτωση του υφιστάμενου *security programme*.
- Ανάλυση των υφιστάμενων *controls* που υπάρχουν στο περιβάλλον ασφάλειας.
- Ευθυγράμμιση των απαιτούμενων, προτύπων, πλαισίων και λοιπών κανονιστικών εφαρμογών με το *BMIS*.
- Σαφής αναγνώριση των ισχυρών σημείων και των αδυναμιών του περιβάλλοντος ασφάλειας.
- Συνεχής αξιολόγηση του περιβάλλοντος ασφάλειας με γνώμονα την ανάδειξη κινδύνων και την ανάδειξη ευκαιριών.

Επιπλέον το μοντέλο μπορεί να αξιοποιηθεί ως ένα εργαλείο ανίχνευσης επιπτώσεων μεγάλων αλλαγών. Όπως αναφέρθηκε νωρίτερα, η σχηματική απεικόνιση του μοντέλου παρομοιάζεται μία τετράεδρη πυραμίδα η οποία ιδανικά θα πρέπει να παρουσιάζει ισορροπία μεταξύ των ακμών της. Όταν σε μία ακμή της, δηλαδή σε ένα *DI*, εμφανίζεται η λεγόμενη «τάση» όπως ορίστηκε στην ενότητα 7, τότε έχουμε μία προβληματική επίδραση μίας αλλαγής στο σύστημα. Είναι προφανές ότι η «τάση» έχει μεταφορικό χαρακτήρα μιας και δεν αποτελεί μετρήσιμο μέγεθος και όπως και η ίδια η τετράεδρη πυραμίδα έχει απλώς ως σκοπό την σχηματική απεικόνιση του μοντέλου.

Όταν συμβαίνει λοιπόν μία μεγάλη αλλαγή σε κάποια περιοχή του *BMIS*, τότε το πιθανότερο είναι να υπάρχουν επιδράσεις σε όλα τα υπόλοιπα. Το σημείο στο οποίο βοηθάει η σχηματική απεικόνιση της τετράεδρης πυραμίδας είναι ότι όταν η αλλαγή αυτή συμβαίνει σε ένα στοιχείο ή ένα σύνδεσμο, τότε οι περισσότερες πιθανότητες να εμφανιστεί «τάση» είναι στις γειτονικές του περιοχές.

Συνεπώς, η αξιοποίηση του μοντέλου έχει τρεις εκδοχές.

- Τη διερεύνηση μίας προβληματικής κατάστασης της οποίας η επίλυση δεν είναι προφανής.
- Την συνεχιζόμενη βελτιστοποίηση του *security programme*
- Την πρόβλεψη ύπαρξης «τάσης» έπειτα από την επίδραση μίας μεγάλης αλλαγής.

9. Μελέτες Περίπτωσης

Σε αυτή την ενότητα παρουσιάζονται τρία πραγματικά σενάρια τα οποία αναλύονται υπό το πρίσμα του *BMIS* ως μελέτες περιπτώσεως. Και τα τρία σενάρια έχουν παρθεί από όμιλο εταιρειών ο οποίος δραστηριοποιείται κυρίως στον τραπεζικό κλάδο και έχει ισχυρή παρουσία σε ολόκληρη την Ανατολική Ευρώπη. Ολόκληρος ο όμιλος απαρτίζεται συνολικά από 27 εταιρείες ενώ η μητρική εταιρεία αποτελεί μία από τις μεγαλύτερες τράπεζας της Ελλάδας. Οι υπηρεσίες Πληροφορικής που δίνονται στις εταιρείες του Ομίλου παρέχονται στην πλειοψηφία τους κεντρικά από μία ομιλική μονάδα μηχανογράφησης η οποία λειτουργεί στην Αθήνα και στελεχώνεται από περισσότερα από 500 άτομα τα οποία είναι είτε προσωπικό της μητρικής εταιρείας είτε ειδικοί συνεργάτες, είτε ενοικιαζόμενο προσωπικό.

Η ασφάλεια εν γένει δεν έχει υπάρξει κατά το παρελθόν άμεση προτεραιότητα για την επίτευξη των στόχων του οργανισμού χωρίς αυτό βέβαια να σημαίνει ότι οι διεργασίες Πληροφορικής δε λειτουργούσαν στα επίπεδα της εύλογης διασφάλισης *(reasonable assurance)*. Τόσο όμως η οικονομική κρίση όσο και η ραγδαία αύξηση των νέων τεχνολογιών έφεραν τον οργανισμό σε δύσκολα διλλήματα σχετικά με την επένδυση στην Ασφάλεια της Πληροφορίας.

Τα σενάρια που παρουσιάζονται συνέβησαν με χρονολογική σειρά και έχουν επιλεχθεί με σκοπό να αναδείξουν τις τρεις εκδοχές αξιοποίησης του μοντέλου όπως αναφέρθηκαν στην προηγούμενη ενότητα, δηλαδή διερεύνηση, βελτιστοποίηση και πρόβλεψη.

9.1 Περίπτωση Α': Διαχείριση Περιστατικών Ασφάλειας και SIEM

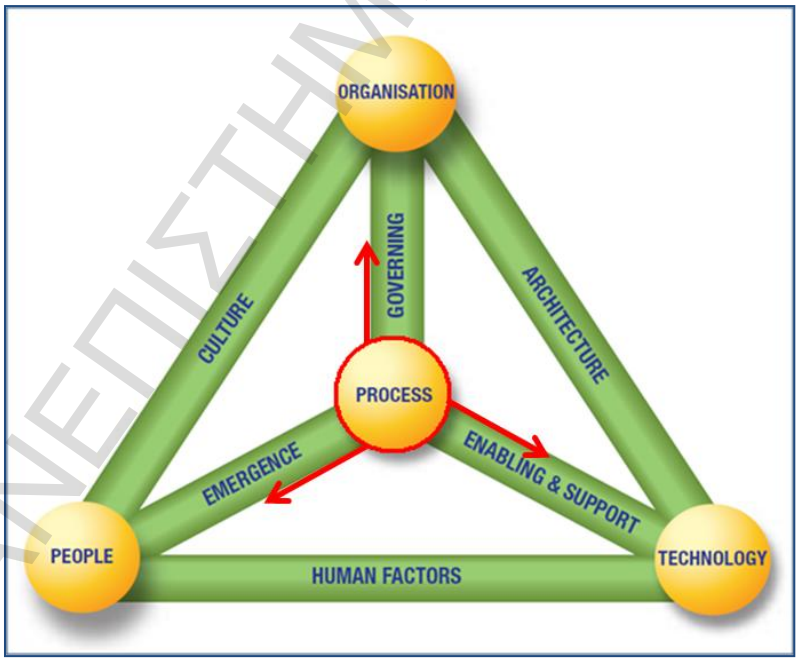
Κάποια στιγμή, κατόπιν παρατηρήσεων από τον Εσωτερικό Έλεγχο, διαπιστώθηκε ότι η διεργασία Διαχείρισης Περιστατικών Ασφάλειας *(Security Incident Management - SIM)* είχε ουσιαστικές αδυναμίες. Συγκεκριμένα:

- Δεν εντοπίστηκαν μέθοδοι απόδοσης *ownership* των περιστατικών με συνέπεια τη μη τακτική τους παρακολούθηση.
- Τα περιστατικά δεν κατηγοριοποιούνταν σωστά με συνέπεια την αναποτελεσματική απόδοση προτεραιότητας.
- Δεν υπήρχαν σαφείς μέθοδοι κλιμάκωσης *(incident escalation)* για την διαχείρισή τους.
- Τα περιστατικά δεν τεκμηριώνονταν επαρκώς και δεν χρησιμοποιούνταν επαρκή εργαλεία αναζήτησης και διαχείρισης.

- Η υφιστάμενη Διαδικασία δεν προέβλεπε στάδιο *"lessons learned"* ώστε να αποφεύγεται η επανεμφάνισή παρόμοιων περιστατικών στο μέλλον.
- Διορθωτικές ενέργειες που προέκυπταν από τα περιστατικά και επιλύονταν ως *emergency changes* δεν τεκμηριώνονταν επαρκώς, δημιουργώντας πρόβλημα και στη διεργασία διαχείρισης αλλαγών.

Η μέχρι τότε υπάρχουσα κατάσταση της Διαχείρισης Περιστατικών Ασφάλειας πλαισιωνόταν από την ύπαρξη μίας Πολιτικής με τις σχετικές επιμέρους Διαδικασίες, την εγκατάσταση μίας πλατφόρμας *IDS* αφιερωμένη στην περιμετρική ασφάλεια και την ύπαρξη ενός *Service Desk* εργαλείου για τη χειροκίνητη καταχώρηση και παρακολούθηση όλων των περιστατικών πληροφορικής, συμπεριλαμβανομένων και αυτών που αφορούσαν Ασφάλεια Πληροφοριών.

Το πρώτο που μπορεί να κάνει κάποιος ο οποίος έχει να μελετήσει μία προβληματική κατάσταση ασφάλειας όπως τη συγκεκριμένη, είναι να εντάξει τις αδυναμίες που προκύπτουν από αυτή στα στοιχεία και τους συνδέσμους του *BMIS*. Δεδομένου ότι, η Διαχείριση Περιστατικών Ασφάλειας αποτελεί μία διεργασία Ασφάλειας Πληροφοριών, θέτουμε το πρόβλημα στο στοιχείο *Process* του μοντέλου και στη συνέχεια ξεκινούμε να το «προβάλλουμε» σε όλες τις υπόλοιπες περιοχές (εικόνα 20).



Εικόνα 20: Η Διαχείριση Περιστατικών Ασφάλειας τοποθετείται στο Process

Στον πίνακα Α', αφού αποτυπώσουμε τις αναγνωρισμένες αδυναμίες που προκύπτουν από την προβολή του προβλήματος στα υπόλοιπα στοιχεία και τους συνδέσμους, μπορούμε να τις κατατάξουμε βάσει σπουδαιότητας ώστε να εντοπίσουμε τις κρισιμότερες περιοχές του

BMIS στις οποίες πρέπει να εστιάσουμε για τη βελτίωση της διεργασίας Διαχείρισης Περιστατικών Ασφάλειας.

Πίνακας Α: Προβολή των αδυναμιών της διεργασίας SIM στις περιοχές του BMIS

BMIS Περιοχή		Αδυναμία
Process "SIM"	Governing	Ελλιπής Πολιτική και πολλαπλές Διαδικασίες Διαχείρισης Περιστατικών Ασφάλειας.
	Emergence	Έλλειψη Ownership.
		Ανεπαρκές Incident Escalation.
		Ανεπαρκές Prioritization.
		Απουσία μεθόδου "Lessons learned".
	Enabling & Support	Ανεπαρκείς μέθοδοι διαχείρισης και αναζήτησης των περιστατικών μέσω ενός Service Desk tool.
	Organization	Αναποτελεσματική εποπτεία των διεργασιών ασφάλειας.
	Culture	Αυξημένες τάσεις αποποίησης ευθύνης.
	People	Πιθανή αυξημένη άγνοια θεμάτων ασφάλειας.
	Human Factor	Πολλές χειροκίνητες μέθοδοι αυξάνουν τα ενδεχόμενα λαθών.
	Technology	Πιθανότητα περιορισμένων εργαλείων (Intrusion Detection System, Service Desk tool).
	Architecture	Επικέντρωση στην περιφερειακή ασφάλεια.

Από την αντιστοίχηση των αδυναμιών που προκύπτουν στις υπόλοιπες περιοχές του *BMIS*, τα σημεία που εντοπίζονται στα οποία πρέπει να δοθεί μεγαλύτερη προσοχή για τη διερεύνηση της προβληματικής κατάστασης της Διαχείρισης Περιστατικών Ασφάλειας, είναι οι περιοχές *Governing*, *Emergence* και *Organization*.

Θεωρώντας ότι ο στρατηγικός στόχος στο θέμα της Διαχείρισης Περιστατικών Ασφάλειας είναι η συνεχή παρακολούθηση των περιστατικών και η προάσπιση του οργανισμού απέναντι σε απρόβλεπτες απειλές, εξωτερικές και εσωτερικές, προκύπτει ότι υπάρχει ουσιαστικό έλλειμμα Διακυβέρνησης δεδομένης της απώλειας της εποπτικής εικόνας μίας από τις σπουδαιότερες εκ των διεργασιών ασφάλειας.

Όπως διατυπώθηκε και στη σχετική ενότητα, η Διακυβέρνηση περιλαμβάνει το σύνολο των τακτικών ενεργειών που χρειάζονται για την επίτευξη των στρατηγικών στόχων στα πλαίσια ενός οργανισμού. Εν προκειμένω, η απουσία των εποπτικών μεθόδων των διεργασιών ασφάλειας δημιουργεί πλήθος προβλημάτων και ανεξήγητων ενδεχόμενων περιστατικών ασφάλειας, τα οποία στο BMIS μεταφράζονται ως αρνητικό *Emergence* (βλ ενότητα 7.5). Η έλλειψη *ownership*, οι ελλείψεις στην προτεραιοποίηση και στην ανάθεση των

περιστατικών καθώς και η απουσία μεθόδου *"lessons learned"*, πηγάζουν από ατεκμηρίωτες ή ανενημέρωτες Διαδικασίες. Από την άλλη, ο ίδιος ο οργανισμός δεν φαίνεται να έχει πετύχει στο να εποπτεύσει το σύνολο των διεργασιών ασφάλειας σαν οντότητα κάτι το οποίο διαφαίνεται και από το γεγονός ότι μία προβληματική διεργασία ασφάλειας όπως η Διαχείριση Περιστατικών Ασφάλειας οδηγεί στην εμφάνιση προβλημάτων και σε άλλες διεργασίες όπως η Διαχείριση Αλλαγών *(Change Management).*

Η διερεύνηση των αδυναμιών μέσω του *BMIS* έχει σκοπό στο βοηθήσει έναν αναλυτή ασφάλειας στο να σχεδιάσει τον «οδικό χάρτη» για τη βελτίωση της προβληματικής κατάστασης. Βάσει των παραπάνω, θα μπορούσε κάποιος να ακολουθήσει τα εξής βήματα:

I. Δημιουργία μίας σαφούς Πολιτικής Ασφάλειας η οποία θα μπορεί να περιγράφει τα στάδια των απαιτήσεων ασφάλειας τόσο σε επίπεδο παρακολούθησης όσο και σε επίπεδο επίλυσης και η οποία θα διευρύνεται τόσο σε περιπτώσεις εξωτερικών περιστατικών όσο και σε περιπτώσεις εσωτερικών. Η υιοθέτηση ενός διευρυμένου προτύπου ασφάλειας πληροφοριών θα μπορούσε να αποδειχθεί πολύτιμη.

II. Σύνταξη σαφών Διαδικασιών ανά τεχνολογική πλατφόρμα (*core banking* συστήματα, περιβάλλοντα εργασίας, δίκτυα, συστήματα πληρωμών) οι οποίες θα πλαισιώνονται σε μία κοινή μέθοδο, όπως για παράδειγμα με την αξιοποίηση ενός ενιαίου *service desk* εργαλείου και μίας κοινής βάσης δεδομένων για την εντοπισμό ίδιων ή παρόμοιων περιστατικών.

III. Για την αποτελεσματικότερη απόδοση της διεργασίας, θα πρέπει να γίνει μία αξιολόγηση της υπάρχουσας αρχιτεκτονικής ώστε να μπορέσουν να αξιοποιηθούν εργαλεία παρακολούθησης περιστατικών ασφάλειας με δυνατότητες συσχετισμού γεγονότων *(event correlation)* για κάθε πλατφόρμα. Εάν από την αξιολόγηση της αρχιτεκτονικής προκύψει ότι υφίσταται η ανάγκη για αναβάθμιση της τεχνολογίας, θα πρέπει να γίνει με τρόπο που να εξυπηρετεί τις Διαδικασίες και τις Πολιτικές Ασφάλειας αλλά και να συνοδευτεί με τις αντίστοιχες εκπαιδεύσεις.

Στον πίνακα Β' έχουν επιλεχθεί *controls* (στην αγγλική) από το πλαίσιο Διακυβέρνησης *COBIT 4.1 – IT Assurance Guide* [35] τα οποία έχουν αντιστοιχηθεί με τις περιοχές του *BMIS*. Στη δεξιά στήλη έχουν αποτυπωθεί οι παράγοντες επικινδυνότητας *(risk drivers)* που καλύπτουν τα εν λόγω *controls*. Ο πίνακας αυτός μπορεί να αξιοποιηθεί στη δημιουργία ενός προγράμματος που θα διευθετεί τις αδυναμίες της διεργασίας Διαχείρισης Περιστατικών Ασφάλειας και στη συνέχεια να ενταχθεί στο ευρύτερο *security programme*.

Πίνακας Β': BMIS to COBIT 4.1

BMIS Area	COBIT 4.1 Controls	Risk Drivers
Governing	**PO 6.1:** IT Policy and Control Environment	Actions not aligned with the organization's business objectives
		No transparent IT control environment
		Compliance and security issues
Organization	**PO 4.1:** IT Process Framework	Incomplete framework of IT processes
		Conflicts and unclear interdependencies amongst processes
		Inflexible IT organization
		Gaps between processes
Emergence	**DS 5.6:** Security Incident Definition	Undetected security breaches
		Lack of information for performing counterattacks
		Missing classification of security breaches
Emergence	**DS 8.1:** Service Desk	Increased downtime
		Decreased customer satisfaction
		Users unaware of the follow-up procedures on reported incidents
		Recurring problems not addressed
Emergence	**DS 8.3:** Incident Escalation	Inefficient use of resources
		Unavailability of service desk resources
		Inability to follow up incident resolution
Enabling & Support	**ME 1.2:** Definition and Collection of Monitoring Data	Metrics based on incorrect or incomplete data
		Ineffective reporting
		Monitored data failing to support the analysis of the overall process performance
People	**DS 7.1:** Identification of Education and Training Needs	Staff members inadequately trained to fulfill their job function
		Installed application capabilities underutilized
Technology	**AI 1.1:** Definition and Maintenance of Business Functional and Technical Requirements	Incorrect solution selected on the basis of an inadequate understanding of requirements
		Significant requirements discovered later, causing costly reworking and implementation delays

Σε αυτό το σημείο κρίνεται απαραίτητο να διευκρινιστεί ότι ο οργανισμός δεν ακολούθησε καμία συστεμική ανάλυση του προβλήματος της ανεπιτυχούς Διαχείρισης Περιστατικών Ασφάλειας. Μπροστά στις αδυναμίες ασφάλειας που αναδείχθηκαν, επιλέχθηκε να δοθεί προτεραιότητα στην απευθείας επιλογή τεχνολογικών υλοποιήσεων, φαινόμενο το οποίο όπως έχει ειπωθεί, εμφανίζεται πολύ συχνά στους κόλπους των οργανισμών με σύνθετα πληροφοριακά συστήματα, δεδομένης της λαθεμένης αντιμετώπισης της ασφάλειας ως ένα αυστηρά τεχνικό θέμα.

Αυτό το οποίο ακολούθησε ήταν η διερεύνηση για την αγορά μίας πλατφόρμας *SIEM (Security Information and Event Management)* η οποία θα μπορεί να διασυνδεθεί με όλα τα συστήματα παρακολούθησης με σκοπό να συσχετίζει τα παραγόμενα γεγονότα για την ανίχνευση περιστατικών ασφάλειας. Δεδομένου ότι ο οργανισμός διαθέτει μεγάλο πλήθος διαφορετικών τεχνολογικών πλατφορμών για το σύνολο των λειτουργιών του, χρειάστηκε να γίνει μία πολύ μεγάλη ανάλυση της υπάρχουσας αρχιτεκτονικής. Ακολουθήθηκε δηλαδή μία «γραμμική προσέγγιση αξιοποίησης της τεχνολογίας» (βλέπε ενότητα 7.4). Τόσο η ανάλυση όσο και η προμήθεια και η εγκατάσταση αποδείχθηκαν εξαιρετικά κοστοβόρες με αποτέλεσμα την έντονη αντίδραση της Διοίκησης για την έκβαση του έργου εγκατάστασης της *SIEM* πλατφόρμας.

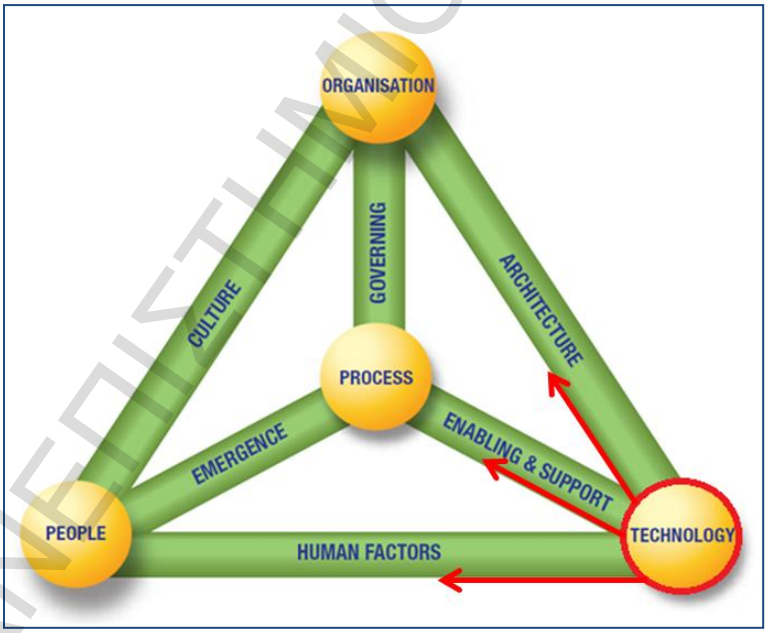
Ως αποτέλεσμα, για λόγους περιορισμού κόστους, λήφθηκε η απόφαση αφού γίνει η επιλογή του προϊόντος βάσει των δυνατοτήτων διασύνδεσης με την υπάρχουσα υποδομή, η διαμόρφωση και η ανάπτυξη των σεναρίων να γίνει αποκλειστικά από το προσωπικό το οποίο θα το διαχειρίζεται. Έτσι στην ουσία, ο οργανισμός βρέθηκε να έχει εντάξει στην αρχιτεκτονική του ένα περίπλοκο εργαλείο από το οποίο η διεργασία Διαχείρισης Περιστατικών Ασφάλειας είχε αποκλειστική εξάρτηση. Αξίζει να σημειωθεί ότι οι τελευταίες αναλύσεις επικινδυνότητας που είχαν πραγματοποιηθεί, είχαν γίνει σε πολύ υψηλό επίπεδο *(high-level risk assessments)* με αποτέλεσμα τα παραγόμενα στοιχεία τους να μην μπορούν να αξιοποιηθούν για τη διαμόρφωση της *SIEM* πλατοφόρμας.

Το προσωπικό Ασφάλειας Πληροφοριακών Συστημάτων το οποίο ανέλαβε τη διαμόρφωση της νέας πλατφόρμας, ασχολήθηκε πολλές ανθρωποημέρες για την ολοκλήρωση του έργου, βασιζόμενο αποκλειστικά στην εμπειρία του, με αποτέλεσμα την εμφάνιση διαφορετικών εργασιακών αναγκών οι οποίες απαιτούσαν άμεση προσοχή. Με την έκβαση του χρόνου, διαπιστώθηκε ότι η πλατφόρμα θα πρέπει να μπει σε παραγωγική λειτουργία, ώστε αφενός μεν να καλυφθούν οι αδυναμίες ασφάλειας για τις οποίες δεσμεύτηκε η Διοίκηση στους κανονιστικούς φορείς και αφετέρου δε η πλατφόρμα να αρχίσει να αποσβένει το ομολογουμένως υψηλό κόστος προμήθειας.

Η συνέπεια ήταν, όταν η πλατφόρμα τέθηκε σε παραγωγική λειτουργία, να παράγει ένα εξαιρετικά μεγάλο πλήθος ψευδώς αληθών αντλώντας γεγονότα από *firewalls, application*

firewalls, IDS και *performance monitoring tools*. Παρόλο που η παρακολούθηση και η διαχείριση των γεγονότων ήταν ουσιαστικά ανέφικτη, η πλατφόρμα παρέμεινε σε παραγωγική λειτουργία για αρκετό καιρό ώστε να υφίσταται τεκμηρίωση για τη διαχείριση των περιστατικών ασφάλειας απέναντι στις κανονιστικές αρχές. Για όλο αυτό το χρονικό διάστημα δεν υπήρξε διαβεβαίωση ότι δεν συνέβησαν πραγματικά περιστατικά ασφάλειας με αποτέλεσμα ο Εσωτερικός Έλεγχος, όταν επανήλθε, να διαπιστώσει τη δυσλειτουργία της εγκατεστημένης πλατφόρμας και να αναδείξει την διεργασία Διαχείρισης Περιστατικών Ασφάλειας και πάλι ως ανεπαρκής. Τελικά, για λόγους εξοικονόμησης πόρων, η πλατφόρμα απεγκαταστάθηκε οριστικά αφήνοντας την αναγνώριση των «δυνητικών γεγονότων» ασφάλειας στα χέρια των υπαλλήλων μέσω του προϋπάρχοντος *Service Desk* εργαλείου.

Προκειμένου να συγκρίνουμε την προβληματική κατάσταση που αναδείχθηκε αρχικά με την προβληματική κατάσταση που προέκυψε μετά την εγκατάσταση της τεχνολογίας που επιλέχθηκε, είναι σκόπιμο να γίνει μία *BMIS* ανάλυση ειδικά στο κομμάτι της ανεπαρκούς υλοποίησης της *SIEM* πλατφόρμας. Η ανάλυση μέσω του *BMIS* θα έθετε αρχικά το πρόβλημα στο στοιχείο *Technology* του μοντέλου ώστε να μπορέσει κάποιος να αρχίσει να προβάλλει τις επιπτώσεις της στις υπόλοιπες περιοχές (εικόνα 21).



Εικόνα 21: Η λύση SIEM τοποθετείται στο Technology element

Όπως και πριν, θέτοντας στον Πίνακα Γ' τις αναγνωρισμένες αδυναμίες που προκύπτουν από την προβολή του προβλήματος στα υπόλοιπα στοιχεία και συνδέσμους, μπορούμε να εντοπίσουμε τις περιοχές με τη μεγαλύτερη σπουδαιότητα.

Πίνακας Γ': Προβολή των αδυναμιών της υλοποίησης SIEM στις περιοχές του BMIS

BMIS Περιοχή		Αδυναμία
Technology "SIEM"	Enabling & Support	Αδυναμία παρακολούθησης περιστατικών ασφάλειας.
		Ανεπαρκή εργαλεία διαχείρισης και αναζήτησης.
	Architecture	Πολυσύνθετες υποδομές οι οποίες δεν αναλύθηκαν επαρκώς ως προς τα επίπεδα επικινδυνότητας.
	Human Factor	Η διαμόρφωση έγινε από μη εξειδικευμένους ανθρώπους βασιζόμενους αποκλειστικά στην εμπειρία τους αυξάνοντας το περιθώριο λαθών.
	Process	Η διεργασία βασίζεται εξ ολοκλήρου στην τεχνική υλοποίηση η οποία και αποτυγχάνει.
	Governing	Δεδομένου ότι η τεχνική υλοποίηση αποτυγχάνει, οι Πολιτικές και οι Διαδικασίες δεν ευσταθούν.
	Organization	Ο οργανισμός, παρουσία τεχνικής υλοποίησης, θεωρεί ότι τα επίπεδα ασφάλειας είναι ικανοποιητικά.
	Emergence	Η ύπαρξη μεγάλου πλήθους ψευδώς αληθών διατηρεί το *Emergence* σε αρνητικό επίπεδο.
	People	Οι άνθρωποι θεωρούν ότι δεν είναι δική τους αρμοδιότητα η επιτυχία της υλοποίησης, όπως αυτή επιλέχθηκε να γίνει.
		Πιθανή αυξημένη άγνοια θεμάτων ασφάλειας.
	Culture	Αυξημένες τάσεις αποποίησης ευθύνης.

Από την αντιστοίχηση των αδυναμιών που προκύπτουν στις υπόλοιπες περιοχές του *BMIS*, τα σημεία που εντοπίζονται στα οποία πρέπει να δοθεί μεγαλύτερη προσοχή είναι τα *Human Factor, Architecture* και *Enabling and Support*. Η εικόνα αυτή είναι σε πολύ μεγάλο βαθμό διαφοροποιημένη με το αποτέλεσμα της προηγούμενης ανάλυσης που έθεσε την προβληματική κατάσταση στο στοιχείο *Process*. Αν ωστόσο θεωρούσαμε ως εύστοχη την στρατηγική που επέλεξε ο οργανισμός προκειμένου να βελτιώσει την διεργασία Διαχείρισης Περιστατικών Ασφάλειας, αυτό το οποίο θα έπρεπε οπωσδήποτε να έχει προηγηθεί για να μειωθούν οι αδυναμίες τουλάχιστον στις περιοχές *Architecture* και *Human Factor* είναι μία εκτεταμένη και εις βάθος ανάλυση επικινδυνότητας.

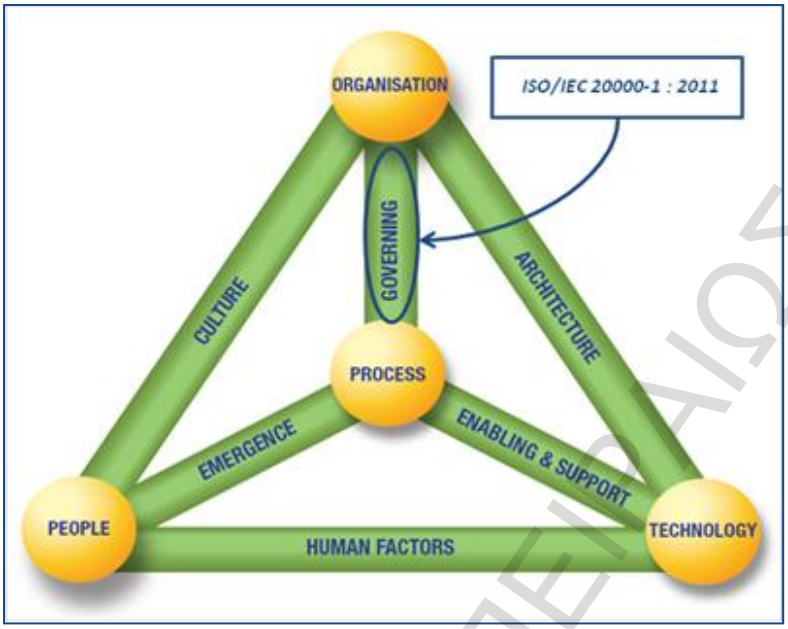
Δεδομένης της πολύπλοκης αρχιτεκτονικής, με το εξαιρετικά μεγάλο πλήθος συστημάτων και τις δαιδαλώδεις διασυνδέσεις, ο οργανισμός είχε επιλέξει μεθοδολογίες ανάλυσης επικινδυνότητας οι οποίες, όπως ειπώθηκε νωρίτερα, έφταναν σε επίπεδο διεργασιών. Από την άλλη, η εγκατάσταση μίας πλατφόρμας *SIEM* η οποία θα μπορεί να συσχετίζει γεγονότα από πολλαπλές συσκευές ασφάλειας, απαιτεί ένα λεπτομερές σχέδιο διαμόρφωσης το

οποίο θα πρέπει να προκύπτει από ένα *Risk Assessment* που θα λαμβάνει υπόψη του τη διαβάθμιση της πληροφορίας που διακινείται/αποθηκεύεται στα συστήματα του οργανισμού και θα φτάνει μέχρι και το χαμηλότερου επιπέδου *Configuration Item*. Η ανάλυση που έπρεπε να γίνει από τον πάροχο της πλατφόρμας και η οποία παρακάμφθηκε για λόγους υψηλού κόστους, πιθανόν να κάλυπτε το στάδιο της ανάπτυξης σεναρίων που θα προέκυπταν από ένα *low-level Risk Assessment* περιορίζοντας την πιθανότητα λανθασμένης διαμόρφωσης από το προσωπικό του οργανισμού.

Συγκρίνοντας τις αναλύσεις των δύο προβληματικών καταστάσεων σχετικά με τη Διαχείριση Περιστατικών Ασφάλειας, γίνεται εύκολα αντιληπτή η σημασία του έγκαιρου εντοπισμού των αδυναμιών που προκύπτουν. Στην πρώτη περίπτωση, όπου η ανάλυση έγινε τη στιγμή που εντοπίστηκαν οι πρώτες αδυναμίες, προέκυψε ότι θα πρέπει να δοθεί έμφαση στον τρόπο με τον οποίο λειτουργεί η Διακυβέρνηση Πληροφοριακών Συστημάτων και στην επάρκεια των Πολιτικών και των Διαδικασιών Ασφάλειας. Στη δεύτερη περίπτωση όπου έγινε η παραδοχή να θεωρηθεί ως *de-facto* λύση η επιλογή μίας *SIEM* πλατφόρμας (όπως και έγινε στην πραγματικότητα) αναδείχθηκε ότι πριν την εγκατάσταση και τη διαμόρφωση θα έπρεπε να έχει προηγηθεί το πολύ μεγάλο και κρίσιμο στάδιο του *Risk Assessment* σε ολόκληρη την αρχιτεκτονική υποδομή. Τόσο η βελτίωση της λειτουργίας της Διακυβέρνησης μέσω των Πολιτικών και των Διαδικασιών όσο και η διενέργεια μίας λεπτομερούς ανάλυσης επικινδυνότητας αποτελούν στόχους οι οποίοι, εκτός από την διεργασία Διαχείρισης Περιστατικών Ασφάλειας, μπορούν να διαμορφώσουν καθοριστικά προς το καλύτερο το *security programme* του οργανισμού.

9.2 Περίπτωση Β': "ISO/IEC 20000:2011" & "ISO/IEC 27001:2005"

Όπως ειπώθηκε και στην περιγραφή του υπό μελέτη οργανισμού, ο οργανισμός συνθέτει έναν όμιλο εταιρειών, με τη διαχείριση των υπηρεσιών πληροφορικής να γίνεται κεντρικά από την Πληροφορική της μητρικής εταιρείας – τράπεζας και να προσφέρεται προς όλες τις θυγατρικές εσωτερικού και εξωτερικού. Λόγω των συνεχώς αυξανόμενων απαιτήσεων των θυγατρικών εταιρειών αλλά κυρίως λόγω κανονιστικών υποχρεώσεων στις χώρες κάποιων εξ αυτών, κρίθηκε αναγκαία η εφαρμογή του προτύπου Διαχείρισης Συστημάτων Υπηρεσιών Πληροφορικής *(IT Service Management System) "ISO/IEC 20000-1 : 2011"*. Το *ITSMS* αποτελεί ένα διευρυμένο κανονιστικό πρότυπο διαχείρισης υπηρεσιών πληροφορικής, η εφαρμογή του οποίου είναι μία επένδυση στη Διακυβέρνηση. Συνεπώς για τους σκοπούς της μελέτης περίπτωσης, τοποθετείται στον αντίστοιχο σύνδεσμο του μοντέλου.



Εικόνα 22: Τα κανονιστικά πρότυπα αποτελούν επένδυση στη Διακυβέρνηση

Το πρώτο πράγμα που χρειάστηκε να γίνει ήταν η καταγραφή του συνόλου της αρχιτεκτονικής που συνθέτει την Πληροφορική του ομίλου σε επίπεδο *CI* και η αντιστοίχηση της υποδομής της σε συστατικά τελικών υπηρεσιών Πληροφορικής *(service components)*. Ο σκοπός αυτού το μεγάλου έργου ήταν η σύνθεση μίας ολοκληρωμένης και λεπτομερούς *CMDB (Configuration Management Data Base)* [36], η οποία αφού ολοκληρώθηκε και καταγράφηκε, διατηρήθηκε σε ελεγχόμενα *(version controlled)* αρχεία [37].

Η εφαρμογή ενός *ITSMS* προτύπου όπως το *"ISO/IEC 20000-1 : 2011"* απαιτεί την ύπαρξη ενός εργαλείου *"IT Management Suite" (ITMS)* μέσω του οποίου θα γίνεται η διαχείριση και παρακολούθηση του επιπέδου των προσφερόμενων υπηρεσιών. Για το σκοπό αυτό, αξιοποιήθηκε το *service desk* εργαλείο που προϋπήρχε στην υποδομή του οργανισμού όπως αναφέρθηκε και στην πρώτη μελέτη περίπτωσης. Ωστόσο για την πλήρη αξιοποίηση του προεγκατεστημένου εργαλείου χρειάστηκε να γίνουν τροποποιήσεις ώστε αφενός μεν να εισαχθούν επιπλέον λειτουργικές δυνατότητες και αφετέρου δε το εργαλείο να επεκταθεί σε ολόκληρό τον όμιλο εταιρειών.

Η εφαρμογή του προτύπου οδήγησε στον μετασχηματισμό του τρόπου εργασίας των στελεχών της Πληροφορικής αφού οι διαχειριστές συστημάτων έγιναν διαχειριστές υπηρεσιών καθώς το ίδιο το *ITSMS* υποχρέωνε την εποπτεία και την παρακολούθηση των επιπέδων των υπηρεσιών πληροφορικής μέσω των Διαδικασιών του παρακάτω πίνακα:

Πίνακας Δ': ITSMS Διαδικασίες

Κωδικός	Διαδικασία
Δ 1.1	Σχεδιασμός – Αλλαγή Υπηρεσιών
Δ 1.2	Διαχείριση Εκδόσεων
Δ 1.3	Διαχείριση Επιπέδου Υπηρεσιών
Δ 1.4	Διαχείριση Διαθεσιμότητας
Δ 2.1	Διαχείριση Επικοινωνίας
Δ 2.2	Διαχείριση Περιστατικών
Δ 2.3	Διαχείριση Προβλημάτων
Δ 2.4	Διαχείριση Αιτημάτων Αλλαγών
Δ 3.1	Ανασκόπηση Υπηρεσιών
Δ 3.2	Διαχείριση Παραπόνων
Δ 3.3	Μέτρηση Ικανοποίησης Πελατών
Δ 4.1	Διαχείριση Προμηθευτών
Δ 5.1	Διαχείριση Διαμόρφωσης
Δ 5.2	Διαχείριση Επάρκειας
Δ 6.1	Κατάρτιση Προϋπολογισμού
Δ 6.2	Κοστολόγηση Υπηρεσιών
Δ 7.1	Εκπαίδευση Προσωπικού
Δ 7.2	Έλεγχος Εγγράφων Αρχείων
Δ 8.1	Εσωτερικές Επιθεωρήσεις
Δ 8.2	Μέτρηση Απόδοσης – Στοχοθεσία
Δ 8.3	Διορθωτικές - Προληπτικές Ενέργειες
Δ 8.4	Management Review

Ποιες όμως ήταν οι απαιτήσεις του προτύπου σχετικά με τα επίπεδα ασφάλειας και πως αυτά μπορεί να επηρεάστηκαν από την εφαρμογή του *ITSMS* σε ολόκληρο το εύρος της Πληροφορικής του Ομίλου; Αν και ο κύριος σκοπός του *"ISO/IEC 20000-1 : 2011"* είναι η μεθοδολογική διαχείριση για την απρόσκοπτη διάθεση Υπηρεσιών Πληροφορικής βάσει συμφωνηθέντων *SLAs (Service Level Agreements)* το ίδιο το πρότυπο, όταν θίγονται θέματα χειρισμού Ασφάλειας Πληροφοριών, επικαλείται τις αντίστοιχες προτάσεις του *Information Security Management System (ISMS)* προτύπου *"ISO/IEC 27001 : 2005"* αφήνοντας στην ευχέρεια του εκάστοτε υλοποιητή τη μέθοδο που θα ακολουθηθεί.

Ο οργανισμός προχώρησε στην άμεση υλοποίηση των παραπάνω Διαδικασιών ώστε να ληφθεί και η αντίστοιχη πιστοποίηση Διαχείρισης Υπηρεσιών Πληροφορικής *"ISO/IEC 20000-1 : 2011"* και να είναι σύμφωνος με τις κανονιστικές αρχές οι οποίες παρουσιάσανε την εν λόγω υποχρέωση. Πράγματι, η εφαρμογή των Διαδικασιών, η παραγωγή ανάλογων στατιστικών εκθέσεων με τα υψηλά επίπεδα των υπηρεσιών καθώς και το ικανοποιητικό

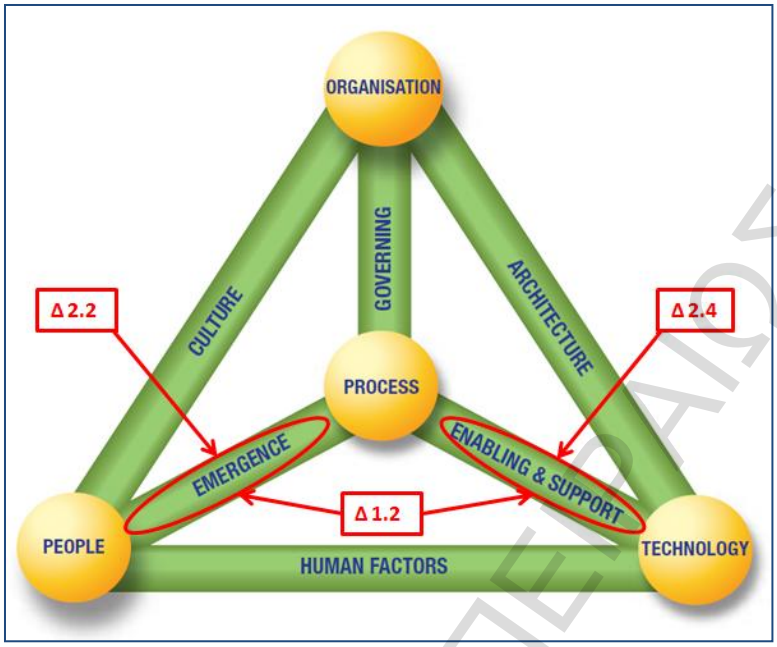
feedback των εταιρειών του ομίλου που λάμβαναν Υπηρεσίες Πληροφορικής οδήγησαν στην επιτυχή υλοποίηση του συστήματος Διαχείρισης Υπηρεσιών Πληροφορικής και στη λήψη της *"ISO/IEC 20000-1 : 2011"* πιστοποίησης. Μελετώντας όμως υπό το πρίσμα της Ασφάλειας της Πληροφορίας τις παραπάνω Διαδικασίες, μπορεί εύκολα κάποιος να διακρίνει μεγάλη εξάρτηση μερικών από αυτές σε θέματα χειρισμού ασφάλειας. Συγκεκριμένα οι Διαδικασίες *«Δ1.2 - Διαχείριση Εκδόσεων», «Δ2.2 - Διαχείριση Περιστατικών»* και *«Δ2.4 Διαχείριση Αιτημάτων Αλλαγών»* αποδείχθηκαν ότι άφηναν διαχειριστικά κενά ασφάλειας τα οποία αναλυτικότερα έχουν ως εξής:

- *Δ1.2 - Διαχείριση Εκδόσεων:* Ως έκδοση *(release)* ορίζεται η συλλογή νέων ή τροποποιημένων συστατικών μερών *(CIs)* μιας υπηρεσίας τα οποία εισάγονται σε παραγωγικό περιβάλλον μετά την ολοκλήρωση επαρκών ελέγχων. Η Διαδικασία δεν προέβλεπε στάδιο αναγνώρισης και εκτίμησης κινδύνων ενώ οι επαρκείς έλεγχοι στους οποίους αναφέρεται δεν περιλαμβάνουν στάδιο *security acceptance* από το *Security Office*.

- *Δ2.2 - Διαχείριση Περιστατικών:* Η εν λόγω Διαδικασία κληρονομεί την διεργασία της Διαχείρισης Περιστατικών Ασφάλειας όπως αποτυπώθηκε στην μελέτη περίπτωσης Α'. Η καταγραφή και η διαχείριση των περιστατικών, γίνεται αποκλειστικά από το *service desk* εργαλείο το οποίο πλέον είναι η επίσημη *ITMS* πλατφόρμα του οργανισμού για τη διαχείριση των υπηρεσιών.

- *Δ2.4 - Διαχείριση Αιτημάτων Αλλαγών*: Ως αλλαγή *(change)* ορίζεται η προσθήκη, μεταβολή ή αφαίρεση οποιουδήποτε *CI* επηρεάζει την υποδομή μίας υπηρεσίας. Αντιθέτως της περίπτωσης της *Δ1.2*, υπάρχει στάδιο αναγνώρισης και εκτίμησης κινδύνων από τον υποβάλλοντα το αίτημα αλλαγής, ωστόσο η διατήρηση της *CMDB* σε *version controlled* αρχεία και όχι σε μία μηχανογραφημένη βάση δεδομένων διασυνδεδεμένη με την *ITMS* πλατφόρμα δυσχεραίνει την αλληλεπίδραση των αλλαγών σε άλλα *CIs* και την παρακολούθηση τυχόν κινδύνων που απορρέουν από αυτά.

Η Διαδικασία *«Δ1.2 - Διαχείριση Εκδόσεων»* επιδρά τόσο στο σύνδεσμο *"Emergence"* λόγω της απουσίας σταδίου *security acceptance* όσο και στο σύνδεσμο *"Enabling & Support"* λόγω της περιορισμένης δυνατότητας αξιολόγησης κινδύνων με την υπάρχουσα υποδομή. Η Διαδικασία *«Δ2.2 - Διαχείριση Περιστατικών»*, όπως παρουσιάστηκε και στην προηγούμενη μελέτη περίπτωσης επιδρά στο σύνδεσμο *"Emergence"* ενώ η Διαδικασία *«Δ2.4 - Διαχείριση Αιτημάτων Αλλαγών»* επιδρά στο σύνδεσμο *"Enabling & Support"* λόγω του ότι η *ITMS* πλατφόρμα δεν παρέχει τη δυνατότητα υποστήριξης εκτίμησης κινδύνων για αλλαγές σε επίπεδο *CI*.



Εικόνα 23: Διαδικασίες Δ1.2, Δ2.2, Δ2.4

Δεδομένου ότι τα Συστήματα Διαχείρισης όπως αυτά που προκύπτουν από τα *ISO/IEC* πρότυπα διαθέτουν μηχανισμούς αναγνώρισης αδυναμιών και βελτίωσης *(«Δ8.1 - Εσωτερικές Επιθεωρήσεις», «Δ8.3 - Διορθωτικές Προληπτικές Ενέργειες»)* τα θέματα αυτά, αν και δεν ήταν άγνωστα στο χώρο της Πληροφορικής, αναγνωρίστηκαν ως προς τα ενδεχόμενα προβλήματα που θα προξενούσαν στην επιτυχή λειτουργία του Συστήματος Διαχείρισης Υπηρεσιών Πληροφορικής και στη διατήρηση της πιστοποίησης *"ISO/IEC 20000-1 : 2011"*. Αυτή άλλωστε είναι και η προστιθέμενη αξία της υιοθέτησης προτύπων που ελέγχονται και πιστοποιούνται από εξωτερικούς φορείς.

Αμέσως συστάθηκε μία ομάδα έργου η οποία με τη βοήθεια του παρόχου της *ITMS* πλατφόρμας ξεκίνησε την υλοποίηση μίας μηχανογραφημένης *CMDB* η οποία θα είναι διασυνδεδεμένη με την *ITMS* πλατφόρμα. Σκοπός είναι για κάθε προσθήκη, μεταβολή ή αφαίρεση ενός *CI* που αποτελεί μέρος υποδομής μίας υπηρεσίας η επιλογή να γίνεται μέσα από το ίδιο το *ITMS*. Το σύστημα θα προωθεί το αίτημα αλλαγής στην ομάδα του *Security Office* για την αξιολόγηση κινδύνων μαζί με την προβολή όλων των *CIs* που επηρεάζονται από αυτό και από τη στιγμή που θα υλοποιείται θα ενημερώνεται αυτομάτως η *CMDB.* Για παράδειγμα αν το αίτημα αλλαγής αφορά μία δικτυακή πρόσβαση κάποιου χρήστη η οποία θα υλοποιείται μέσα από τροποποιήσεις στους κανόνες του *firewall*, τότε το *ITMS* θα πρέπει να εμφανίζει το σύστημα στο οποίο ζητείται η πρόσβαση, τη διαβάθμιση της πληροφορίας που το σύστημα διαθέτει καθώς και τα στοιχεία ρόλου/αρμοδιοτήτων του χρήστη. Όλα αυτά θα πρέπει να αξιολογούνται από το *Security Office* και αν υπάρχουν σημαντικές αλλαγές οι οποίες οδηγούν σε νέες εκδόσεις *(releases)* τα νέα επίπεδα επικινδυνότητας θα πρέπει να καταγράφονται και να ενημερώνονται.

Σχετικά με τη Διαδικασία *«Δ2.2 - Διαχείριση Περιστατικών»* και την αναφορά σε περιστατικά ασφάλειας, κρίθηκε αναγκαίο να συμπεριληφθεί στάδιο ειδικού χειρισμού στο οποίο θα γίνεται αξιολόγηση από το *Security Office*. Ωστόσο, επειδή η αναγνώριση των περιστατικών ασφάλειας, απουσία ειδικού εργαλείου, εξακολούθησε να αποτελεί χειροκίνητη διαδικασία, κρίθηκε αναγκαία η λήψη ενεργειών για την υιοθέτηση Πολιτικών και Διαδικασιών Ασφάλειας υπό το πρότυπο *"ISO/IEC 27001 : 2005".* Δεδομένου ότι για τα στελέχη της Πληροφορικής ήταν ήδη γνωστή η ροή εργασιών μέσα από τις Διαδικασίες ενός συστήματος διαχείρισης αλλά και για να αποφευχθεί η συσσώρευση όγκου εργασίας στο *Security Office* από τη συνεχή αξιολόγηση όλων των περιστατικών για το κατά πόσο αφορούν ασφάλεια, αποφασίστηκε η καθολική λειτουργία των διεργασιών ασφάλειας μέσα από ένα *Information Security Management System (ISMS)* πιστοποιημένου κατά *"ISO/IEC 27001 : 2005"*. Με αυτόν τον τρόπο έγινε μία επιπλέον επένδυση στη Διακυβέρνηση, με σκοπό την ευαισθητοποίηση και το χειρισμό των θεμάτων ασφάλειας από όλα τα στελέχη της Πληροφορικής.

Ως αποτέλεσμα δημιουργήθηκε ένα πλαίσιο Επιμέρους Πολιτικών Ασφάλειας (πίνακας Ε') και για όσα θέματα ασφάλειας δεν υπήρχε σαφής κάλυψη από τις υπάρχουσες Διαδικασίες του *ITSMS* όπως για τις *Δ1.2, Δ2.2* και *Δ2.4*, δημιουργήθηκαν οι *ISMS* Διαδικασίες του πίνακα ΣΤ'.

Πίνακας Ε': Πολιτικές Ασφάλειας

Κωδικός	Πολιτική Ασφάλειας
A4	Διαχείριση Κινδύνων Πληροφοριακών Αγαθών
A6	Οργάνωση Ασφάλειας Πληροφοριακών Αγαθών
A7	Διαχείριση Πληροφοριακών Αγαθών
A8	Ασφάλεια Ανθρωπίνων Πόρων
A9	Φυσική και Περιβαλλοντική Ασφάλεια
A10	Διαχείριση Επικοινωνιών και Λειτουργιών
A11	Έλεγχος Προσβάσεων
A12	Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων
A13	Διαχείριση Περιστατικών Ασφάλειας Πληροφοριών
A14	Διαχείριση Επιχειρησιακής Συνέχειας
A15	Συμμόρφωση

Πίνακας ΣΤ': ISMS Διαδικασίες

Κωδικός	Διαδικασία Ασφάλειας
A4.2	Διαδικασία Διαχείρισης Κινδύνων Ασφάλειας Πληροφοριακών Συστημάτων
A8.2	Διαδικασία Ανάπτυξης Προγράμματος Ενημέρωσης και Εκπαίδευσης Χρηστών σε Θέματα Ασφάλειας Πληροφοριακών Αγαθών
A10.5	Διαδικασία Τήρησης Αντιγράφων Ασφαλείας
A10.6	Διαδικασία Διαχείρισης Διασυνδέσεων Συστημάτων Πληροφορικής με Τρίτους
A11.2	Διαδικασία Διαχείρισης Πρόσβασης Χρηστών
A11.4	Διαδικασία Απομακρυσμένης Πρόσβασης στα Πληροφοριακά Συστήματα
A13.2	Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας Πληροφοριακών Συστημάτων

Έτσι λοιπόν με μία τεχνική υλοποίηση (διασύνδεση μηχανογραφημένης *CMDB* στο *ITMS*) και με την εφαρμογή του προτύπου *"ISO/IEC 27001 : 2005"* και συγκεκριμένα με την υιοθέτηση των Διαδικασιών Ασφάλειας «*A4.2 - Διαχείριση Κινδύνων Ασφάλειας Πληροφοριακών Συστημάτων»* και *«A13.2 - Διαχείριση Περιστατικών Ασφάλειας Πληροφοριακών Συστημάτων»* κρίθηκε ότι σε επίπεδο σχεδιασμού, υπάρχει επαρκής κάλυψη των αδυναμιών ασφάλειας που είχαν ανακύψει από την εφαρμογή του *ITSMS*. Ωστόσο αξίζει να μελετηθούν στο σύνολο, υπό το πρίσμα του *BMIS,* τα - έως σήμερα - αποτελέσματα της εφαρμογής των δύο προτύπων. Όπως αποτυπώνεται στον παρακάτω πίνακα, οι συνέπειες της προτυποποίησης της παροχής Υπηρεσιών Πληροφορικής και της Ασφάλειας της Πληροφορίας, έφεραν περαιτέρω μεταβολές οι οποίες επί της ουσία έδρασαν σε όλες τις περιοχές του *BMIS* δημιουργώντας ένα εξαιρετικά διαφοροποιημένο περιβάλλον.

Πίνακας Ζ': Προβολή των επιπτώσεων των δύο προτύπων στις περιοχές του BMIS

BMIS Περιοχή		Επίπτωση Προτύπων	
		ITSMS	*ISMS*
Governing "ISO/IEC 20000 : 2011" & "ISO/IEC 27001 : 2005"	**Organization**	Ως επιχειρηματική ανάγκη αναδείχτηκε η ικανότητα μέτρησης και παρακολούθησης των επιπέδων εξυπηρέτησης Υπηρεσιών από την Πληροφορική	Ως επιχειρηματική ανάγκη αναδείχτηκε η αύξηση των επιπέδων ασφάλειας των Υπηρεσιών Πληροφορικής.
	Culture	Η έμφαση στην απόδοση των Υπηρεσιών και όχι στη μεμονωμένη απόδοση των συστημάτων δημιούργησε «τάσεις» στο DI Culture.	Οι Πολιτικές Ασφάλειας (Α6, Α7) έθεσαν υπεύθυνους ασφάλειας σε διαφορετικά επίπεδα (υπηρεσία, σύστημα, αγαθό), ξεκαθαρίζοντας τα προβλήματα ευθύνης και λογοδοσίας.
	Process	Η προτυποποίηση δημιούργησε νέες διεργασίες παροχής Υπηρεσιών Πληροφορικής όπως π.χ. η Μέτρηση Ικανοποίησης Πελατών μέσω της Διαδικασίας Δ3.3.	Οι διεργασίες ασφάλειας, παρόλο που προϋπήρχαν, ενισχύθηκαν ως προς την απόδοσή τους από τον καθορισμό ρόλων και αρμοδιοτήτων και από την επιβολή εσωτερικών ελέγχων.
	Emergence	Η προτυποποίηση των Διαδικασιών βελτίωσε την προσαρμογή των στελεχών και την καλύτερη διαχείριση προβλημάτων (θετικό *Emergence*).	Η προτυποποίηση των Διαδικασιών Ασφάλειας και ο σαφής καθορισμός υπευθύνων ασφάλειας έδωσε περισσότερες ευκαιρίες για ανάδειξη και διαχείριση προβλημάτων ασφάλειας (θετικό *Emergence*).
	Enabling & Support	Οι αδυναμίες που προέκυψαν από την έλλειψη μηχανογραφημένης CMDB μέσω των Διαδικασιών Δ1.2, Δ2..4 οδήγησαν σε τεχνολογικές επενδύσεις.	Τα Security Controls που επέβαλε το πρότυπο ξεκαθάρισαν τις τεχνολογικές ανάγκες για την αποτελεσματικότερη λειτουργία του προτύπου.
	Technology	- ITMS (Service Desk) - CMDB (Configuration Management DB) - ITQMS (IT Quality Management System) - ADDM (Automatic Database Diagnostic Monitor) - NMS (Network Management System)	- ISMS Tool (Risk Assessment & Audit) - DLP (Data Leakage Prevention) - SIEM-as-a-service (Outsourced)
	Human Factor	Η προτυποποίηση των Διαδικασιών και η παρακολούθηση της ποιότητας παροχής υπηρεσιών, εισήγαγε περαιτέρω έλεγχο στις λειτουργίες Πληροφορικής με αποτέλεσμα να αναγνωρίζονται περισσότερες ανθρώπινες αστοχίες.	Η προτυποποίηση των Διαδικασιών Ασφάλειας εισήγαγε περαιτέρω έλεγχο στις διεργασίες ασφάλειας με αποτέλεσμα να αναγνωρίζονται περισσότερες ανθρώπινες αστοχίες.
	People	Χρειάστηκε να γίνουν πολλαπλές εκπαιδεύσεις ενώ κρίθηκε αναγκαία και η πρόσληψη νέου προσωπικού με ITIL εμπειρία.	Με απόφαση της Διοίκησης κρίθηκε αναγκαία η διενέργεια εκπαιδευτικών προγραμμάτων για αύξηση της επίγνωσης των πληροφοριακών κινδύνων στις μονάδες Πληροφορικής ολόκληρου το ομίλου.
	Architecture	Η ανάγκη για CMDB υποχρέωσε τον οργανισμό στο να καταγράψει και να παρακολουθεί το σύνολο του πληροφοριακού του εξοπλισμού σε συνεχή βάση. Επιπλέον βοήθησε στο να εντοπιστούν παρωχημένες υποδομές.	Το πρότυπο επέβαλε την διαβάθμιση των υποδομών ως προς την κρισιμότητά τους τόσο σε επίπεδο συστήματος όσο και σε επίπεδο πληροφορίας ενώ υποχρέωσε τον οργανισμό να συνθέσει μία δομημένη αρχιτεκτονική ασφάλειας.

9.3 Περίπτωση Γ': Συγχώνευση Εταιρειών

Όπως είναι γνωστό, το έτος 2013 υπήρξε για το ελληνικό τραπεζικό σύστημα περίοδος συγχωνεύσεων πιστωτικών ιδρυμάτων. Σκοπός ήταν να απομείνουν τέσσερις συστεμικές τράπεζες οι οποίες με τις επιδράσεις των συνεπαγόμενων συνεργειών αλλά και με τη βοήθεια του Ταμείου Χρηματοπιστωτικής Σταθερότητας, θα μπορούν, σύμφωνα με τις προβλέψεις, να αυξήσουν τη ρευστότητά τους και να τροφοδοτήσουν την ελληνική αγορά με ελκυστικά τραπεζικά προϊόντα. Η μαζική τραπεζική ένωση υπήρξε μία εκ των δεσμεύσεων της Ελλάδας απέναντι στους δανειστές της, με ένα πιεστικό σχέδιο το οποίο χαρακτηρίστηκε από μικρά χρονοδιαγράμματα και εξαιρετικά περίπλοκα έργα.

Όπως αναφέρθηκε στην αρχή του κεφαλαίου, ο όμιλος εταιρειών που έχει επιλεχθεί για τις μελέτες περίπτωσης δραστηριοποιείται πρωτίστως στον τραπεζικό κλάδο, με την ίδια τη μητρική εταιρεία να αποτελεί μία από τις μεγαλύτερες τράπεζες στην Ελλάδα και την Ανατολική Μεσόγειο. Συνεπώς δε θα μπορούσε να εξαιρεθεί από το σχέδιο της τραπεζικής ένωσης η οποία είχε ως αποτέλεσμα την απορρόφηση του «υγιούς τμήματος» δύο μικρότερων Ελληνικών τραπεζών, οι οποίες εφεξής θα καλούνται για ευνόητους λόγους ως «Τ1» και «Τ2».

Η Τ1 υπήρξε μία σχετικά μικρή τράπεζα με τραπεζικά προϊόντα κυρίως επενδυτικού χαρακτήρα. Απασχολούσε περίπου 300 υπαλλήλους ενώ το δίκτυό της αποτελούταν από 19 καταστήματα. Οι περισσότερες μονάδες βρίσκονταν συγκεντρωμένες σε ένα κτήριο με την Πληροφορική να αποτελείται από 15 μόνο στελέχη. Αν και υπήρξε τράπεζα με περιορισμένη πελατεία, τα αρκετά ελκυστικά επενδυτικά προγράμματα που προωθούσε κατά το παρελθόν οδήγησαν το σύνολο της αξίας του τμήματος που αποκτήθηκε από τον υπό μελέτη οργανισμό στα περίπου 2,5 δισεκατομμύρια ευρώ, ενεργητικό και παθητικό.

Στην Πληροφορική της Τ1, δεδομένου ότι το πλήθος των υπαλλήλων ήταν σχετικά μικρό, υπήρχε μεγάλη αλληλοεπικάλυψη εργασιών και περιορισμένος διαχωρισμός καθηκόντων. Οι εργασίες των λειτουργιών ασφάλειας είχαν αποδοθεί σε 2 άτομα τα οποία είχαν παράλληλα πολλές διαφορετικές ασχολίες. Τα καθήκοντα του *Security Office* είχαν αποδοθεί σε ένα μόνο άτομο το οποίο αναφερόταν στο Γενικό Διευθυντή Λειτουργιών.

Οι όροι απορρόφησης της Τ1 δεν είχαν καμία πρόβλεψη για την απόκτηση του προσωπικού. Συνεπώς η απορρόφηση έγινε με την παύση της Τ1 και την οριστική απόλυση όλων των υπαλλήλων της. Ωστόσο, η μητρική εταιρεία του υπό μελέτη οργανισμού, προκειμένου να διατηρήσει το κοινωνικό της προφίλ εν μέσω μίας περιόδου που το τραπεζικό σύστημα στοχοποιούνταν από μεγάλη μερίδα πολιτών για την οικονομική κατάσταση της χώρας, επέλεξε να επαναπροσλάβει άμεσα το σύνολο του προσωπικού της πρώην Τ1 και να το εντάξει στον κανονισμό εργασίας της. Ο κανονισμός εργασίας της υπό μελέτη εταιρείας είναι ένας κανονισμός σύμφωνα με τον οποίο η μισθολογική και η βαθμολογική εξέλιξη των

υπαλλήλων της βασίζεται πρωτίστως στα χρόνια υπηρεσίας εντός της τράπεζας. Ως συνέπεια, οι υπάλληλοι της πρώην Τ1, ανεξαρτήτως της εμπειρίας τους και των ετών προϋπηρεσίας τους, εντάχθηκαν στο προσωπικό της υπό μελέτη εταιρείας αφού υπέστησαν μισθολογικές μειώσεις οι οποίες σε κάποιες περιπτώσεις ξεπέρασαν και το 70%. Επιπλέον, αξίζει να σημειωθεί ότι δεν αξιοποιήθηκε καμία τεχνική υποδομή της Τ1 εκτός από εξοπλισμό καταστημάτων και *ATMs*.

Η Τ2 ήταν μία σχετικά μεγάλη για τα ελληνικά δεδομένα εμπορική τράπεζα με δίκτυο 540 καταστημάτων και πάνω 2500 υπαλλήλους. Οι μονάδες της τράπεζας υπήρχαν διασκορπισμένες σε διάφορα σημεία της Αθήνας με την Πληροφορική να αποτελεί μία από τις μεγαλύτερες, στελεχώνοντας περίπου 150 υπαλλήλους. Υπήρξε τράπεζα με σημαντική παρουσία, με το σύνολο του αποκτηθέντος τμήματος να φτάνει περίπου σε ενεργητικό και παθητικό τα 6 δισεκατομμύρια ευρώ.

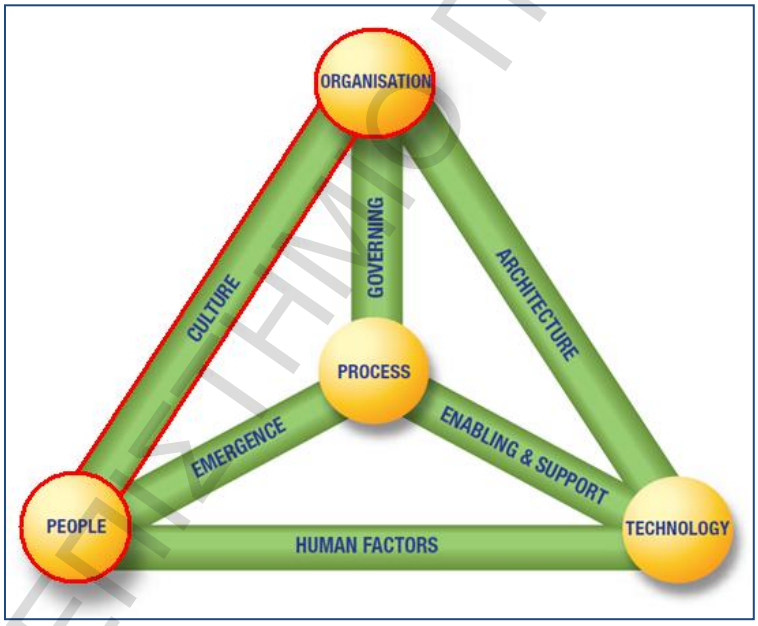
Στην Πληροφορική υπήρχε ένα δομημένο οργανόγραμμα το οποίο διαχώριζε σαφώς ανά τμήμα τις εργασίες και τα καθήκοντα των στελεχών. Η ασφάλεια ήταν μία εκ των βασικών λειτουργιών πληροφορικής, ωστόσο το *Security Office* δεν ήταν ανεξάρτητο από την Πληροφορική ενώ υπήρχε και περιορισμένη στελέχωση του Τμήματος *IT Audit*.

Οι όροι απορρόφησης της Τ2 προέβλεπαν και την απόκτηση του συνόλου του προσωπικού της, υποχρεώνοντας την υπό μελέτη εταιρεία να εντάξει το προσωπικό της Τ2 στο κανονισμό εργασίας της χωρίς να προηγηθεί απόλυση. Με αυτόν τον τρόπο, αν και πάλι οι υπάλληλοι της Τ2 υπέστησαν οικονομικές απώλειες λόγω του διαφορετικού κανονισμού εργασίας, αναγνωρίστηκαν τα χρόνια υπηρεσίας περιορίζοντας τις μισθολογικές μειώσεις σε σχέση με την περίπτωση της απορρόφησης της Τ1. Όσον αφορά τις τεχνικές υποδομές της Τ2, εκτός από εξοπλισμό καταστημάτων και *ATMs*, υπήρξε και αξιοποίηση μηχανογραφικού και τηλεπικοινωνιακού εξοπλισμού ώστε να υπάρχει επάρκεια πληροφοριακών πόρων ενόψει των καινούργιων αναγκών.

Όπως είναι αντιληπτό από τις περιγραφές της απορρόφησης των δύο τραπεζών, μία από τις σημαντικότερες επιπτώσεις είναι οι μισθολογικές αποκλίσεις του προσωπικού. Οι διαδικασίες συγχώνευσης είχαν ως αποτέλεσμα την δημιουργία δύο νέων κατηγοριών προσωπικού με διαφορετικές συνθήκες αποδοχών. Την κατηγορία προσωπικού της πρώην Τ1 και την κατηγορία προσωπικού της πρώην Τ2. Όπως ειπώθηκε και στην αρχή του κεφαλαίου, στην υπό μελέτη εταιρεία υπήρχαν εκ των προτέρων τρεις κατηγορίες υπαλλήλων. Η κατηγορία των ενταγμένων στον κανονισμό εργασίας υπαλλήλων, η κατηγορία ειδικών συνεργατών με τις εν γένει υψηλότερες αποδοχές και η κατηγορία του ενοικιαζόμενου προσωπικού με τις χαμηλότερες αποδοχές όλων.

Έτσι, στο σύνολό της η εταιρεία βρέθηκε να απασχολεί πέντε διαφορετικές κατηγορίες υπαλλήλων, καλυπτόμενων από διαφορετικές συμβάσεις, με διαφορετικές παροχές, μεγάλες μισθολογικές αποκλίσεις αλλά όμως με τα ίδια εργασιακά καθήκοντα. Η προϋπάρχουσα κατάσταση, με τις τρεις κατηγορίες υπαλλήλων είχε δημιουργήσει κατά το παρελθόν πολλές τριβές μεταξύ των συλλόγων των υπαλλήλων και της Διοίκησης ενώ σε άλλες περιπτώσεις συγχωνεύσεων που είχαν συμβεί παλιότερα οι όροι ήταν ως επί το πλείστων ευνοϊκοί για το συγχωνευθέν προσωπικό.

Η κατάσταση έτσι όπως διαμορφώθηκε μετά τις απορροφήσεις των Τ1 και Τ2, αναζωπύρωσε το κλίμα έντασης μεταξύ των κατηγοριών που προϋπήρχαν ενώ και οι νεοαποκτηθέντες υπάλληλοι της πρώην Τ1 συσπειρώθηκαν υπό την εκπροσώπηση ενός επιπλέον συλλόγου εργαζομένων. Υπό το πρίσμα του *BMIS*, η ύπαρξη πολλών κατηγοριών προσωπικού δημιουργεί «τάση» μεταξύ των περιοχών *Organization* και *People* η οποία ενισχύθηκε ακόμα περισσότερο μετά από τις απορροφήσεις των Τ1 και Τ2.



Εικόνα 24: Η «τάση» εντοπίζεται μεταξύ των περιοχών People και Organization (Culture)

Η εμφάνιση «τάσης» στο *DI Culture*, απλοϊκά εξηγείται με την εισαγωγή νέου προσωπικού με διαφορετικές εργασιακές εμπειρίες. Ωστόσο, εκτός από τις όποιες διαφοροποιήσεις υπάρχουν στις συμβάσεις εργασίας των υπαλλήλων, υπάρχουν και άλλα σημεία τα οποία πρέπει να ληφθούν υπόψη. Από άποψη Πληροφορικής, οι εργασιακές απαιτήσεις μίας μεγάλης τράπεζας η οποία εξυπηρετεί και τις πληροφοριακές ανάγκες άλλων εταιρειών, είναι πολύ περισσότερες από ότι σε μία σχετικά μικρή τράπεζα με καθιερωμένο τραπεζικό ωράριο. Οι διεργασίες ασφάλειας εντός της Πληροφορικής της πρώην Τ1, με τον τρόπο που λειτουργούσαν είχαν διεκπεραιωτικό χαρακτήρα με τις όποιες υλοποιήσεις να καλύπτουν κυρίως κανονιστικές αρχές ασφάλειας πληροφορικής. Από την άλλη, η Πληροφορική της Τ2

ενώ υπήρξε στελεχωμένη με αρκετό προσωπικό το οποίο είχε σαφώς διαχωρισμένα καθήκοντα και σε επίπεδο διεργασιών ασφάλειας, λειτουργούσε με το *Security Office* να μην έχει την απόλυτη ελευθερία της εποπτείας των μηχανισμών ασφάλειας και χωρίς να έχει τη δυνατότητα να παρέμβει άμεσα σε περιπτώσεις παράκαμψής τους από την υπόλοιπη Πληροφορική. Επιπλέον στην Τ2, οι εσωτερικοί έλεγχοι Πληροφοριακών Συστημάτων υπήρξαν πολύ περιορισμένοι σε σχέση με το μέγεθος της τράπεζας και το πλήθος των Πληροφοριακών της Συστημάτων. Τέλος, τόσο στην Τ1 όσο και στην Τ2, δεν υπήρξε σαφής μηχανισμός Διακυβέρνησης ενώ παράλληλα δεν είχε εμφανιστεί ποτέ από το *business* η ανάγκη υιοθέτησης κάποιου προτύπου διαχείρισης, είτε αυτό είχε να κάνει με λειτουργίες ασφάλειας είτε είχε να κάνει με τη διαχείριση επιπέδου υπηρεσιών πληροφορικής.

Οι υπάλληλοι πληροφορικής των πρώην Τ1 και Τ2, έπρεπε σε πολύ σύντομο χρονικό διάστημα, εκτός από τα νέα για αυτούς οικονομικά δεδομένα, να προσαρμοστούν και στους τρόπους λειτουργίας της Πληροφορικής του ομίλου εταιρειών η οποία πλέον λειτουργούσε υπό την αυστηρότητα των προτύπων *“ISO/IEC 20000 : 2011”* και *“ISO/IEC 27001 : 2005”*. Συνεπώς βρέθηκαν σε ένα περιβάλλον το οποίο ελεγχότανε τακτικά είτε από το *Internal IT Audit*, είτε από το *SOX Audit*, είτε από τους φορείς πιστοποίησης και με ένα αυστηρά δομημένο πλαίσιο ασφάλειας το οποίο εποπτευότανε από ανεξάρτητο *Security Office*.

Η Διοίκηση της Πληροφορικής, αν και τα χρονοδιαγράμματα για την τραπεζική ένωση ήταν ιδιαίτερα πιεστικά, μπόρεσε και προνόησε για το μεταβατικό στάδιο προσαρμογής των στελεχών με σειρά εκπαιδεύσεων, τόσο για τις λειτουργίες πληροφορικής όσο και για την αύξηση των επιπέδων επίγνωσης κινδύνου. Ωστόσο, για την προσαρμογή των νέων στελεχών πληροφορικής σε ένα σχετικά αυστηρότερο πλαίσιο ασφάλειας, ειδικά όταν αυτό συνοδεύεται από δυσμενέστερες αποδοχές και μισθολογικές αποκλίσεις μεταξύ του προσωπικού, μπορεί να μην επαρκούν οι εκπαιδεύσεις. Η παραμονή πολλαπλών κατηγοριών υπαλλήλων με διαφορετικούς όρους εργασίας είναι ένα πρόβλημα το οποίο πλέον έχει άμεσο αντίκτυπο το στοιχείο του Οργανισμού. Η δημιουργία πολλαπλών συλλόγων με διαφορετικούς εκπροσώπους, σε ένα μεγάλο οργανισμό δημιουργεί καινούργιο ρεύμα στον *Informal Organization* (βλέπε ενότητα 7.4).

Η Διοίκηση της Πληροφορικής του υπό μελέτη οργανισμού, αν και είχε κατανοήσει το πρόβλημα των πολλαπλών κατηγοριών υπαλλήλων από πριν πραγματοποιηθούν οι νέες συγχωνεύσεις των Τ1 και Τ2, είναι στην πραγματικότητα αναρμόδια για τη θέσπιση καινούργιων και ομογενοποιημένων όρων εργασίας για το σύνολο των στελεχών της. Για αυτό το λόγο, θα πρέπει να γίνει μία εκτεταμένη και λεπτομερής παρουσίαση στο Διοικητικό Συμβούλιο αναφορικά με τις πιθανές επιπτώσεις από την ύπαρξη εργαζόμενων πολλαπλών κατηγοριών σε έναν οργανισμό ο οποίος εξαρτάται ζωτικά από τα

Πληροφοριακά του Συστήματα, να αξιολογηθεί αν πρέπει να ληφθούν μέτρα ομογενοποίησης των καθεστώτων εργασίας ή αν πρέπει να ενισχυθούν συγκεκριμένες δικλείδες ασφάλειας και να εφαρμοστούν προς την κατεύθυνση μετρίασης κινδύνων από πιθανές επιθέσεις εκ των έσω.

10. Συμπεράσματα

Στην σημερινή εποχή, ο κόσμος των επιχειρήσεων είναι ολοκληρωτικά εξαρτημένος από τις τεχνολογίες πληροφορικής και συνεπώς από την ανάγκη για Ασφάλεια της Πληροφορίας. Ωστόσο, ακόμα και σήμερα που το έργο στην έρευνα καινοτόμων τεχνολογιών ασφάλειας είναι τεράστιο και αποδίδει καθημερινά μεγάλο πλήθος αξιοποιήσιμων εφαρμογών, παραμένει ένα μεγάλο θεμελιώδες πρόβλημα: Ποια είναι η βέλτιστη δαπάνη για την Ασφάλεια της Πληροφορίας και ποιος είναι αυτός ο οποίος αποφασίζει για αυτή; Τον πρώτο λόγο πάντα, σε οτιδήποτε έχει να κάνει με την επένδυση σε τεχνολογικές λύσεις, τον έχει η υψηλή Διοίκηση. Η ασφάλεια είναι ένας τομέας ο οποίος δεν αποφέρει κέρδος ενώ τις περισσότερες φορές τα στελέχη της Διοίκησης στερούνται των ειδικών γνώσεων προκειμένου να αποφανθούν για την προμήθεια ή μη τεχνολογικών υλοποιήσεων που κοστίζουν χρήματα. Ωστόσο και για έναν αναλυτή ασφάλειας, η εκτίμηση των πιθανών οικονομικών απωλειών από περιστατικά ασφάλειας δεν είναι εύκολη υπόθεση. Για αυτό το λόγο έχουν αναπτυχθεί οι μέθοδοι ανάλυσης επικινδυνότητας τις οποίες οι αναλυτές ασφάλειας οφείλουν να αξιοποιούν, ωστόσο τον τελευταίο λόγο διατηρεί πάντα η Διοίκηση.

Η ανάγκη για όλο και αποτελεσματικότερη Ασφάλεια της Πληροφορίας έχει οδηγήσει σε αναζητήσεις λύσεων οι οποίες δεν επικεντρώνονται αποκλειστικά στις τεχνολογικές υλοποιήσεις. Στα πλαίσια αυτά, δημοσιεύονται μελέτες οι οποίες θέτουν την ασφάλεια στα χέρια της Διοίκησης και που, αν χρειάζεται, ορίζουν εκ των προτέρων την Ασφάλεια της Πληροφορίας ως προϋπόθεση για την επίτευξη των επιχειρηματικών στόχων. Όπως συμβαίνει συνήθως, η Πληροφορική εκτελεί για λογαριασμό του *business* ενώ η Ασφάλεια Πληροφοριακών Συστημάτων επεμβαίνει στην Πληροφορική. Δημοσιεύσεις μοντέλων όπως αυτή του *Business Model for Information Security* έχουν ως σκοπό τη γεφύρωση του χάσματος αρχικά μεταξύ των τριών οντοτήτων, ξεκινώντας από τα όργανα ασφάλειας και φτάνοντας μέχρι την κορυφή της Διοίκησης.

Το *BMIS* παρουσιάζει μία σχηματοποιημένη μοντελοποίηση των περιοχών του οργανισμού που επηρεάζονται από τις αλλαγές στα επίπεδα ασφάλειας. Η απεικόνιση της τετράεδρης πυραμίδας προσφέρει αρχικά έναν απλό και κατανοητό χάρτη ο οποίος μπορεί να γίνει αντιληπτός από οποιονδήποτε. Βάσει αυτού του χάρτη μπορούν να γίνουν οι απαραίτητες διερευνήσεις σε μεταβολές και γεγονότα ασφάλειας καθώς και στην εξεύρεση λύσης όταν αυτή χρειάζεται. Ο σκοπός του μοντέλου είναι να γίνονται αντιληπτές από το *business* οι ανάγκες ενός *security programme* ούτως ώστε όταν η Διοίκηση κληθεί να επενδύσει σε υλοποιήσεις ασφάλειας, να γνωρίζει ακριβώς για ποιους λειτουργικούς κινδύνους το πράττει.

Στην ελληνική πραγματικότητα αλλά και στον υπό μελέτη οργανισμό της ενότητας 9, τα προβλήματα επικοινωνίας είναι παραπάνω από αισθητά. Το *business* απαιτεί την εκπλήρωση των επιχειρησιακών του αναγκών με χαμηλό κόστος από την Πληροφορική και η Ασφάλεια Πληροφοριακών Συστημάτων προσπαθεί να διατηρήσει με ότι μέσο διαθέτει την ασφάλεια σε ικανοποιητικά επίπεδα. Ταυτόχρονα, κάθε στέλεχος προσπαθεί να κάνει την εργασία του χωρίς να παρουσιάζει ενδιαφέρον για τις υπόλοιπες λειτουργίες του οργανισμού, ειδικά όταν αυτές αποτελούν διεργασίες ασφάλειας. Η υιοθέτηση προτύπων βελτιώνει πολύ σημαντικά την εικόνα, όπως φαίνεται και από τη 2η μελέτη περίπτωσης, όχι όμως και στο επίπεδο κουλτούρας και επικοινωνίας, όπου εκεί απαιτούνται περαιτέρω χειρισμοί.

Μελετώντας το *BMIS*, μπορεί κάποιος να συμπεράνει ότι το ίδιο το μοντέλο δεν καταφέρνει να απαλλαχθεί από ένα σχετικά μικρό βαθμό αυθαιρεσίας. Για παράδειγμα ενώ ο σύνδεσμος *Human Factor* τοποθετείται ανάμεσα στα στοιχεία *People* και *Technology* δεν σημαίνει απαραίτητα ότι δεν μπορούν να υπάρξουν και καταστροφικοί ανθρώπινοι χειρισμοί σε περιοχές του οργανισμού που δεν σχετίζονται με την αξιοποιούμενη τεχνολογία. Επιπλέον ο σύνδεσμος *Emergence* θα μπορούσε να βρίσκεται μεταξύ του στοιχείου *Process* και οποιουδήποτε στοιχείου *(Organization, Technology, People)* αφού ανάδειξη αναγκών ή ευκαιριών για βελτίωση μιας διεργασίας ασφάλειας μπορεί να προκύψει από οποιοδήποτε σημείο.

Από την άλλη όμως, οι πιο ντετερμινιστικές μελέτες που έχουν γίνει μέχρι τώρα για την επίλυση αυτού του προβλήματος, όπως είναι το μοντέλο *Gordon & Loeb* το οποίο προσπαθεί να αποδείξει τη βέλτιστη μέθοδο απόδοσης των επενδύσεων ασφάλειας, αντιμετωπίζουν ακόμα περισσότερους επικρίσεις ως προς την αξιοπιστία τους. Μέχρι να μπορέσει να αναπτυχθεί ένα μοντέλο το οποίο και θα είναι απτό ως προς τα αποτελέσματά του και θα είναι αποδεκτό από το σύνολο της επιστημονικής κοινότητας, θα συνεχίσουν να αναζητούνται λύσεις σε επίπεδο διοικητικής οργάνωσης για τη διαχείριση της Ασφάλειας της Πληροφορίας.

Το σημαντικό παραμένει η πλήρης κατανόηση των αναγκών ασφάλειας από τη Διοίκηση και αυτό είναι κάτι που το *BMIS* μπορεί να καταφέρει σε μεγάλο βαθμό. Αυτό που έχει τη μεγαλύτερη αξία, δεν είναι τόσο η σχηματική μοντελοποίηση που προσφέρει όσο η καλλιέργεια της ικανότητας για συστεμική προσέγγιση των ζητημάτων ασφάλειας. Το να μπορεί δηλαδή κάποιος να προβλέπει το βαθμό στον οποίο επηρεάζονται τα επίπεδα ασφάλειας σε όλες τις περιοχές του οργανισμού έπειτα από μία δραματική αλλαγή. Για αυτό το λόγο άλλωστε το υλικό του *BMIS* έχει αξιοποιηθεί για την δημιουργία του *COBIT 5* το οποίο σήμερα θεωρείται το πλέον ολοκληρωμένο πλαίσιο Διακυβέρνησης Πληροφορικής.

Αναφορές

1. **ISACA,** *"The Business Model for Information Security"*, 2010

2. **ISACA,** *"COBIT 5 (A Business Framework for the Governance and Management of Enterprise IT)",* 2012

3. **Ross Anderson,** *"Why Information Security is Hard - An Economic Perspective",* 2000

4. **Bruce Schneier,** *Schneier on Security - "Security ROI",* 2008 https://www.schneier.com/blog/archives/2008/09/security_roi_1.html (11/12/2013)

5. **Jason Albanese & Bruce Stout,** *"Return On Security Investment (ROSI) – A Practical Quantitative Model",* 2006

6. **Wikipedia The Free Encyclopedia, "***Return of investment (ROI)"* http://en.wikipedia.org/wiki/Return_on_investment (14/12/2013)

7. **Salvatore Alessandro Sarcia, Giovanni Cantore & Victor R. Basili,** *"A Statistical Neural Network Framework for Risk Management Process – From the Proposal to its Preliminary Validation for Efficiency",* 2006

8. **Sigve Oltedal, Bjørg-Elin Moen, Hroar Klempe, Torbjørn Rundmo,** *"Explaining risk perception. An evaluation of cultural theory",* 2004

9. **ENISA,** *"Introduction to Return on Security Investment Helping CERTs assessing the cost of (lack of) security",* 2012.

10. **Lawrence A. Gordon and Martin P. Loeb**, *"The Economics of Information Security Investment"*, 2002

11. **Tanaka et al,** *"Vulnerability and information security investment: An empirical analysis of e-local government in Japan",* 2005.

12. **Jan Willemson,** *"On the Gordon & Loeb model for Information Security Investment*", 2006.

13. **Ponemon Institute,** *"2013 Annual Study: Cost of Data Breach Study: Global Analysis"*, 2013

14. **Anders Sundelin,** *The Business Model Database, "Business model example: Xerox – Business Model Innovation in 1959"* http://tbmdb.blogspot.gr/2009/12/business-model-example-xerox-business.html (25/01/2014)

15. **ISACA,** *"COBIT 5 for Information Security",* 2012

16. **Software Engineering Institute,** *"OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)",* 1999

17. **Office of Government Commerce (OGC),** UK, *"Information Technology and Infrastructure Library",* 2011

18. **British Standards Institute,** *"What Is a Standard?",* 2010

19. **International Organization for Standardization, International Electrochemical Commission,** *"Information Security Management System (ISMS) Family of Standards",* 2005

20. **National Institute of Standards and Technology, U.S. Department of Commerce,** *"Recommended Security Controls for Federal Information Systems and Organizations, Revision 3"*, 2010.

21. **Payment Card Industry Security Standards Council,** *"Payment Card Industry Data Security Standard (PCI DSS)",* 2006.

22. **IT Policy Compliance Group,** *"Best Practices for Managing Information Security",* 2010

23. **Carnegie Mellon University,** *"Capability Maturity Model Integration version 1.3",* 2010

24. **Michael Thompson, Aaron Wildavsky,** *"A Cultural Theory of Information Bias in Organizations",* 1986

25. **Aggeliki Tsohou, Maria Karyda, Spyros Kokolakis,** *"Formulating Information Systems Risk Management Strategies through Cultural Theory",* 2006

26. **IT Governance Institute,** *"Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition",* 2006

27. **International Organization for Standardization, International Electrochemical Commission,** *"Information Technology Service Management System (ITSMS) Family of Standards",* 2011

28. **Kiely, Benzel,** *"Systemic Security Management", Security & Privacy, IEEE, vol. 4, no. 6*, 2006

29. **ISACA,** *"CISM Review Manual, USA, 2010, section 3.13.2, Objectives of Information Security Architectures",* 2011.

30. **Wikipedia The Free Encyclopedia, "***The Open Group Architecture Framework (TOGAF)"* http://en.wikipedia.org/wiki/The_Open_Group_Architecture_Framework (13/02/2014)

31. **Wikipedia The Free Encyclopedia, "***Sherwood Applied Business Security Architecture"* http://en.wikipedia.org/wiki/Sherwood_Applied_Business_Security_Architecture (13/02/2014)

32. **Wikipedia The Free Encyclopedia,** "*Zachman Framework"* http://en.wikipedia.org/wiki/Zachman_Framework (13/02/2014)

33. **SANS Institute InfoSec Reading Room,** *"The Weakest Link: The Human Factor Lessons Learned from the German WWII Enigma Cryptosystem",* 2001

34. **TechDirt,** *"Humans: Still the weakest link in the security chain"* https://www.techdirt.com/articles/20120810/18401819991/humans-still-weakest-link-security-chain.shtml (02/03/2014)

35. **ISACA,** *"COBIT 4.1 - IT Assurance Guide",* 2009

36. **Wikipedia The Free Encyclopedia,** "*Configuration Management database (CMDB)"* http://en.wikipedia.org/wiki/Configuration_management_database (03/03/2014)

37. **Wikipedia The Free Encyclpedia,** "*Revision control",* http://en.wikipedia.org/wiki/Revision_control (13/04/2014)