ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Πλαίσιο Κουλτούρας Κυβερνοασφάλειας Με Πρακτική Εφαρμογή Σε Κρίσιμες Υποδομές

Διδακτορική Διατριβή

Άννα Γεωργιάδου
Υποψήφια Διδάκτορας Ε.Μ.Π.

Επιβλέπων: **Ι. Ψαρράς**
Καθηγητής Ε.Μ.Π.

Αθήνα, Μάρτιος 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Πλαίσιο Κουλτούρας Κυβερνοασφάλειας Με Πρακτική Εφαρμογή Σε Κρίσιμες Υποδομές

Διδακτορική Διατριβή

Άννα Γεωργιάδου

Υποψήφια Διδάκτορας Ε.Μ.Π.

Επιβλέπων: **Ι. Ψαρράς**
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την **23/03/2023**

.....	.....	.....
Ιωάννης Ψαρράς Καθηγητής Ε.Μ.Π.	Δημήτριος Ασκούνης Καθηγητής Ε.Μ.Π.	Χρυσόστομος Δούκας Αναπληρωτής Καθηγητής Ε.Μ.Π.
.....	.....	
Γρηγόριος Μέντζας Καθηγητής Ε.Μ.Π.	Ιωάννης Γκόνος Καθηγητής Ε.Μ.Π.	
.....	.....	
Ευάγγελος Μαρινάκης Επίκουρος Καθηγητής Ε.Μ.Π.	Γεώργιος Τσιχριτζής Καθηγητής ΠΑΠΕΙ	

Αθήνα, Μάρτιος 2023

.....

Άννα Γεωργιάδου

Υποψήφια Διδάκτορας Ε.Μ.Π.

Περίληψη

Η παρούσα διατριβή παρουσιάζει ένα πλαίσιο κουλτούρας κυβερνοασφάλειας για την αξιολόγηση της τρέχουσας ετοιμότητας κυβερνοασφάλειας του εργατικού δυναμικού ενός οργανισμού. Έχοντας πραγματοποιήσει μια ενδελεχή ανασκόπηση των πιο συχνά χρησιμοποιούμενων πλαισίων ασφαλείας, προσδιορίζουμε τα βασικά στοιχεία ασφάλειας που σχετίζονται με τον ανθρώπινο παράγοντα και τα ταξινομούμε κατασκευάζοντας ένα γενικευμένο μοντέλο κουλτούρας ασφάλειας. Ακολούθως, προσδιορίζουμε το κάθε στοιχείο του μοντέλου και αναδεικνύουμε ποσοτικούς δείκτες με στόχο τον προσδιορισμό μιας διεξοδικής μεθοδολογίας αξιολόγησης.

Ακολούθως, προχωράμε στη συσχέτιση του προτεινόμενου μοντέλου κουλτούρας κυβερνοασφάλειας με δυο ευρέως διαδεδομένα και αναγνωρισμένα μοντέλα ασφαλείας:

- Εσωτερικής Απειλής (Insider Threat): Η εσωτερική απειλή έχει αναγνωριστεί τόσο από την επιστημονική κοινότητα όσο και από τους επαγγελματίες ασφαλείας ως ένας από τους σοβαρότερους κινδύνους για την ασφάλεια ιδιωτικών οργανισμών, ιδρυμάτων και κυβερνητικών οργανισμών. Εκτεταμένη έρευνα σχετικά με τους τύπους, τους σχετικούς εσωτερικούς και εξωτερικούς παράγοντες, τις προσεγγίσεις ανίχνευσης και τις στρατηγικές μετριασμού της έχει διεξαχθεί τις τελευταίες δεκαετίες. Διάφορα πλαίσια έχουν προταθεί σε μια προσπάθεια κατανόησης του κινδύνου που ενέχει αυτή η απειλή, ενώ πολλαπλές περιπτώσεις που εντοπίστηκαν έχουν ταξινομηθεί σε ιδιωτικές ή δημόσιες βάσεις δεδομένων. Το προτεινόμενο πλαίσιο κουλτούρας κυβερνοασφάλειας, εστιάζοντας στον ανθρώπινο παράγοντα, μπορεί να συνδράμει στον εντοπισμό πιθανών απειλών τόσο από κακόβουλες όσο και από ακουσίως επικίνδυνες οντότητες. Εξετάζοντας τεχνικούς, συμπεριφορικούς, πολιτιστικούς και προσωπικούς δείκτες, βοηθά στον εντοπισμό πιθανών κινδύνων ασφαλείας που προέρχονται από τον άνθρωπο.
- MITRE ATT&CK: Το πλαίσιο MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) παρέχει ένα πλούσιο και λειτουργικό αποθετήριο κακόβουλων τακτικών, τεχνικών και διαδικασιών. Η χρήση του εκτείνεται από την εξομοίωση αντιπάλου και την ανάπτυξη αναλυτικών στοιχείων συμπεριφοράς έως την αξιολόγηση ωριμότητας της άμυνας και του SOC (Security Operations Center) ενός οργανισμού. Ενώ έχει γίνει εκτεταμένη έρευνα για την ανάλυση συγκεκριμένων επιθέσεων ή συγκεκριμένων παραγόντων οργανωτικής κουλτούρας και ανθρώπινης συμπεριφοράς που οδηγούν σε τέτοιες επιθέσεις, απουσίαζε μια ολιστική άποψη για τη συσχέτιση των δύο. Σε αυτή τη διατριβή αξιοποιούνται οι δυνατότητες του MITRE ATT&CK προς μια επιστημονική κατεύθυνση που δεν έχει ακόμη διερευνηθεί: αξιολόγηση ασφάλειας και αμυντικών υποδομών, ένα βήμα πριν από τον τρέχοντα τομέα εφαρμογής του. Το προτεινόμενο πλαίσιο κουλτούρας κυβερνοασφάλειας σχεδιάστηκε αρχικά με στόχο κρίσιμες υποδομές και, πιο συγκεκριμένα, τον ενεργειακό τομέα. Οι οργανισμοί αυτών των τομέων εμφανίζουν συνύπαρξη και ισχυρή αλληλεπίδραση των δικτύων IT (Τεχνολογία Πληροφορικής) και OT (Επιχειρησιακή Τεχνολογία). Ως αποτέλεσμα, κάνουμε χρήση του υβριδικού μοντέλου MITRE ATT&CK for Enterprise και ICS (Industrial Control Systems) ως μια ευρύτερη και πιο ολιστική προσέγγιση.

Απώτερος στόχος των προαναφερθέντων συσχετίσεων είναι η ανάδειξη ενός πλαισίου κουλτούρας κυβερνοασφάλειας ικανού να αξιολογήσει την τρέχουσα κατάσταση

ασφαλείας μιας κρίσιμης υποδομής εντοπίζοντας τα κενά και τις αδυναμίες της και υποδεικνύοντας αντίμετρα, συστάσεις και εναλλακτικές προσεγγίσεις συμπεριλαμβανομένων προγραμμάτων κατάρτισης εργατικού δυναμικού.

Το πλαίσιο κουλτούρας κυβερνοασφάλειας έχει σχεδιαστεί για να προσαρμόζεται εύκολα σε διάφορους επιχειρησιακούς τομείς με ιδιαίτερη έμφαση τις κρίσιμες υποδομές δεδομένων των αυστηρότερων κανονισμών στους οποίους αυτές υπόκεινται. Στην παρούσα διατριβή παρουσιάζονται εκτεταμένες εφαρμογές του πλαισίου κουλτούρας κυβερνοασφάλειας σε κρίσιμες υποδομές παρέχοντας πληροφορίες αναφορικά με το σχεδιασμό, τη στόχευση και την προσαρμογή των εκστρατειών αξιολόγησης σε κάθε περίπτωση ανάλογα με τη στοχοθεσία και τους απώτερους σκοπούς που καλούνται να εκπληρώσουν. Τα αποτελέσματα και τα ευρήματά τους αναλύονται εις βάθος αναδεικνύοντας και υπογραμμίζοντας τη σπουδαιότητα υιοθέτησης ενός πολύπλευρου και πολυκριτηριακού μοντέλου κουλτούρας κυβερνοασφάλειας προσανατολισμένου στον ανθρώπινο παράγοντα με συνεξέταση εσωτερικών και εξωτερικών παραγόντων.

Λέξεις Κλειδιά: κουλτούρα κυβερνοασφάλειας, συμπεριφορά ασφαλείας, αξιολόγηση κυβερνοάμυνας, εσωτερική απειλή, MITRE ATT&CK for Enterprise & ICS, κρίσιμες υποδομές

ABSTRACT

The PhD dissertation at hand presents a cybersecurity culture framework for assessing the current security readiness of an organization's workforce. Having carried out a thorough review of the most commonly used security frameworks, we identify the key human-related security elements and classify them by constructing a generalized security culture model. Next, we define each element of the model and highlight quantitative factors in order to determine a comprehensive evaluation methodology.

Next, we proceed by relating the proposed cybersecurity culture model with two commonly acceptable and recognizable security models:

- Insider Threat: Insider threat has been recognized by both scientific community and security professionals as one of the gravest security hazards for private companies, institutions, and governmental organizations. Extended research on the types, associated internal and external factors, detection approaches and mitigation strategies has been conducted over the last decades. Various frameworks have been introduced in an attempt to understand and reflect the danger posed by this threat, whereas multiple identified cases have been classified in private or public databases. The proposed cybersecurity culture framework with a clear focus on the human factor can assist in detecting possible threats of both malicious and unintentional insiders. Examining technical, behavioural, cultural, and personal indicators helps identify potential security risks posed by humans.
- MITRE ATT&CK: The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework provides a rich and actionable repository of adversarial tactics, techniques, and procedures. Its usage extends from adversary emulation, red teaming, behavioural analytics development to a defensive gap and SOC (Security Operations Centre) maturity assessment. While extensive research has been done on analysing specific attacks or specific organizational culture and human behaviour factors leading to such attacks, a holistic view on the association of both is currently missing. This dissertation exploits MITRE ATT&CK's possibilities towards a scientific direction that has not yet been explored: security assessment and defensive design, a step prior to its current application domain. The proposed cybersecurity culture framework was initially designed to target critical infrastructures and, more specifically, the energy sector. Organizations of these domains exhibit a co-existence and strong interaction of the IT (Information Technology) and OT (Operational Technology) networks. As a result, we emphasize our scientific effort on the hybrid MITRE ATT&CK for Enterprise and ICS (Industrial Control Systems) model as a broader and more holistic approach.

The ultimate goal of the above relations is to develop a cybersecurity culture framework capable of assessing the current state of a critical infrastructure by identifying gaps and weaknesses and suggesting countermeasures, recommendations and alternative approaches including workforce training programs.

The cybersecurity culture framework is designed to be easily adapted to a variety of business areas with a particular emphasis on the critical infrastructures which need to obey to a number of strict regulations. This dissertation contains extensive applications of the cybersecurity culture framework to critical infrastructures, providing information

on the planning, targeting and adaptation of assessment campaigns in each case according to the goals and objectives they are called to fulfil. Their results and findings are analysed in depth, highlighting and emphasizing the importance of adopting a multidimensional and multi-disciplinary human-oriented cybersecurity culture model by co-examining internal and external factors.

Keywords: cybersecurity culture, security behaviour, cyberdefence assessment, insider threat, MITRE ATT&CK for Enterprise & ICS, critical infrastructures

Πρόλογος

Η παρούσα διδακτορική διατριβή έλαβε χώρα στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου, στο πλαίσιο των ερευνητικών δραστηριοτήτων του Εργαστηρίου Συστημάτων Αποφάσεων και Διοίκησης, το διάστημα 10/2019 – 03/2023.

Αντικείμενο της διατριβής είναι η διαμόρφωση ενός πλαισίου κουλτούρας κυβερνοασφάλειας με επίκεντρο τον ανθρώπινο παράγοντα στοχευμένο στις κρίσιμες υποδομές που σκοπό έχει να αναγνωρίσει και να αναδείξει τις αδυναμίες και τα κενά ασφαλείας προτείνοντας κατάλληλα αντίμετρα, πολιτικές, πρακτικές και προγράμματα ευαισθητοποίησης, καλλιέργειας και ενίσχυσης κυβερνοασφάλειας.

Η διατριβή σχεδιάστηκε, υλοποιήθηκε και ολοκληρώθηκε υπό την επίβλεψη και την καθοδήγηση των Καθηγητών της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ε.Μ.Π. Ιωάννη Ψαρρά και Δημητρίου Ασκούνη. Στους κυρίους Ψαρρά και Ασκούνη οφείλω ιδιαίτερες ευχαριστίες για την εμπιστοσύνη και τη στήριξη που μου προσέφεραν καθ' όλη τη διάρκεια της εκπόνησης της διατριβής. Επιπλέον, θερμές ευχαριστίες οφείλω στο συνάδελφο και στενό συνεργάτη κ. Μουζακίτη Σπύρο για τις πολύτιμες συμβουλές και συνδρομή του στην έρευνά μου. Επιπρόσθετα, θα ήθελα να ευχαριστήσω τον Αναπληρωτή Καθηγητή Χρυσόστομο Δούκα, τον Καθηγητή Γρηγόριο Μέντζα, τον Καθηγητή Ιωάννη Γκόνο, τον Επίκουρο Καθηγητή Ευάγγελο Μαρινάκη και τον Καθηγητή Γεώργιο Τσιχριτζή για την τιμή που μου έκαναν να παρευρεθούν στην εξέταση υποστήριξης της διατριβής.

Ιδιαίτερες ευχαριστίες οφείλω σε όλους τους φίλους και συναδέλφους με τους οποίους συνεργαστήκαμε αυτά τα χρόνια παρουσίας μου στο Εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης.

Κλείνοντας, θα ήθελα να ευχαριστήσω μέσα από την καρδιά μου τον πατέρα μου Χριστόφορο, τη μητέρα μου Χρυσάνθη και την αδελφή μου Δέσποινα για την παρότρυνση, την υποστήριξη, το κουράγιο και την απεριόριστη στήριξη που ανιδιοτελώς μου παρέχουν όλα αυτά τα χρόνια.

Τέλος, το πιο μεγάλο ευχαριστώ για τη συγκεκριμένη διατριβή οφείλω στο σύζυγό μου Παναγιώτη και στις κόρες μου Φωτεινή και Χριστίνα για την απεριόριστη αγάπη, κατανόηση και υπομονή που επέδειξαν καθόλη την προσπάθειά ολοκλήρωσης της διδακτορικής μου διατριβής. Αποτέλεσαν την κινητήριο δύναμη και το ουσιαστικότερο κίνητρο και σε αυτό το εγχείρημά μου.

Άννα Γεωργιάδου

Αθήνα, Μάρτιος 2023

Περιεχόμενα

Εικόνες

Πίνακες

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Ορισμός προβλήματος

Το σύγχρονο επιχειρησιακό και κοινωνικο-πολιτικό περιβάλλον κλήθηκε να αναδιοργανωθεί εκ βάθρων και να στραφεί άμεσα προς την ψηφιοποίησή του τόσο λόγω των εμφανών ωφελειών που οι ψηφιακές τεχνολογίες και η ψηφιακή πραγματικότητα υπόσχονται και υλοποιούν, όσο και εξαιτίας μη αναμενόμενων ανατρεπτικών συμβάντων, όπως αυτό της πανδημίας του κορονοϊού.

Σε αυτό το περιβάλλον, απολύτως αναμενόμενα, η σημασία της Ασφάλειας Πληροφοριών αναβαθμίστηκε ως απόλυτη προτεραιότητα στη συντριπτική πλειονότητα των οργανισμών, ανεξαρτήτως του πεδίου δραστηριοποίησής τους. Για να καταστεί όμως δυνατή η σωστή πλαισίωση ενός οργανισμού αναφορικά με την Ασφάλεια Πληροφοριών, είναι σημαντικό να μελετηθεί σωστά από τι αυτή εξαρτάται.

Μια σημαντική παράμετρος που η εξελικτική πορεία της Ασφάλειας Πληροφοριών υπογράμμισε και ανέδειξε είναι η σημασία του ανθρώπινου παράγοντα ως καταλυτικού συντελεστή στο πολυδιάστατο και πολυκριτηριακό αυτό θέμα. Έχει διατυπωθεί πως η μεγαλύτερη απειλή για το απόρρητο και την ασφάλεια ενός οργανισμού, ακόμη κι αν δεν αναγνωρίζεται, είναι το ίδιο του το προσωπικό. Η ευαισθητοποίηση των εργαζομένων ως προς την ασφάλεια πληροφοριών είναι βασικός κρίκος στην αλυσίδα ασφαλείας ενός οργανισμού, καθώς ακόμη και η πιο άρτια διασφαλισμένη εταιρεία θεωρείται ανυπεράσπιστη χωρίς κουλτούρα ασφάλειας.

Αρχικά, η αντιμετώπιση της ασφάλειας πληροφοριών χαρακτηρίστηκε από μια ιδιαίτερα τεχνοκρατική προσέγγιση που απευθυνόταν κυρίως σε ειδικούς. Ο επιχειρηματικός κόσμος επικεντρώθηκε στο σχεδιασμό πλαισίων αξιολόγησης ασφάλειας ως μέσο διαμόρφωσης των επιχειρηματικών, περιβαλλοντικών και κοινωνικών συνθηκών που θα μπορούσαν να θεμελιώσουν μια σωστή και πολλά υποσχόμενη κουλτούρα ασφάλειας.

Από μια διαφορετική σκοπιά, η ακαδημαϊκή κοινότητα προσέγγισε την κυβερνοασφάλεια μέσω ανθρωπολογικών και κοινωνικών επιστημών που στόχο είχαν να κατανοήσουν τους περιβαλλοντικούς παράγοντες, τα μεμονωμένα χαρακτηριστικά και γνωρίσματα που επηρεάζουν, προκαλούν και τελικά υπαγορεύουν τη συνολική Ασφάλεια Πληροφοριών ενός οργανισμού.

Αυτό που όμως είχε μείνει ανεξερεύνητο, είναι ο συνδυασμός των δύο αυτών φαινομενικά ασυμβίβαστων, αλλά στην πραγματικότητα αλληλοσυμπληρούμενων προσεγγίσεων στο χώρο της Κυβερνοασφάλειας. Πώς δηλαδή η διαμόρφωση κανόνων και πολιτικών ασφαλείας, η εφαρμογή ελέγχων και η εγκατάσταση, λειτουργία και ισχυροποίηση υποδομών, εργαλείων και αντίμετρων ασφαλείας μπορούν να δομήσουν, να διαμορφώσουν και να πλαισιώσουν τα μέλη ενός οργανισμού που καλούνται να εργαστούν και να δραστηριοποιηθούν εντός και εκτός της φυσικής και νοητής περιμέτρου των ψηφιακών εγκαταστάσεών του λαμβάνοντας ως παραμέτρους και το χαρακτήρα, τη νοοτροπία, τη συμπεριφορά και την ευρύτερη ατομική, ομαδική, εθνική και γενικότερα πολυδιάστατη και πολυεπίπεδη κουλτούρα της κάθε μεμονωμένης οντότητας αυτού του ευρύτερου συνόλου.

1.2 Αντικείμενο και Συμβολή Διατριβής

Καθοδηγούμενη από τη σημασία αυτού του αναμφισβήτητα σημαντικού παράγοντα κυβερνοασφάλειας, η υποκείμενη διατριβή επικεντρώνει τις προσπάθειές της στο σχεδιασμό ενός γενικευμένου πλαισίου κουλτούρας κυβερνοασφάλειας ικανού να εφαρμόζεται σε διαφορετικούς τομείς και να προσαρμόζει ανάλογα τη μεθοδολογία αξιολόγησής του.

Αντικείμενό της είναι η δημιουργία ενός μοντέλου που απεικονίζει τα βασικά επίπεδα κουλτούρας κυβερνοασφάλειας, τις διαστάσεις και τους τομείς, συνδυάζοντας τους παράγοντες και ελέγχους ασφαλείας που έχουν εντοπιστεί, αναδυθεί και τεκμηριωθεί από προηγούμενες επιστημονικές έρευνες και επαγγελματικές προσεγγίσεις, ενώ ταυτόχρονα καλύπτει τα κενά και τις αδυναμίες τους και γεφυρώνει τις διαφορές τους ακολουθώντας μια πολυδιάστατη και πολυκριτηριακή προσέγγιση.

Ως κύρια συμβολή, το συγκεκριμένο πλαίσιο δεν περιορίζεται σε μέτρα και πολιτικές ασφαλείας, σε ελέγχους χρήσης εργαλείων και τεχνικών λύσεων, σε ψυχολογικές, γνωσιακές και συμπεριφοριστικές αξιολογήσεις αλλά προχωρά στη συνεξέταση εσωτερικών και εξωτερικών παραμέτρων και μεταβλητών του ευρύτερου προβλήματος της Ασφάλειας Πληροφοριών εξετάζοντας και αξιολογώντας με πολλαπλούς τρόπους και μεθόδους καθέναν από αυτούς και σε συνδυασμό.

Επιπρόσθετα, το προτεινόμενο πλαίσιο δεν περιορίζεται στην αξιολόγηση και εντοπισμό των τρωτών σημείων της ασφάλειας ενός οργανισμού – προχωράει στη σύνδεση των αποτελεσμάτων της αξιολόγησης με πολύτιμες συστάσεις και πρακτικούς τρόπους ενίσχυσης της οργανωτικής και ατομικής ευαισθητοποίησης, ενσυναίσθησης και δέσμευσης έναντι στην κυβερνοασφάλεια και τις θεματικές της.

Υλοποιώντας το προτεινόμενο πλαίσιο, αναπτύχθηκε ένα εργαλείο αξιολόγησης κουλτούρας κυβερνοασφάλειας που κάνει χρήση διαφόρων μεθόδων και τεχνικών που ποικίλουν από απλά ερωτηματολόγια, δοκιμές, προσομοιώσεις και σοβαρά παιχνίδια στοχεύοντας με διαφορετικούς διαδραστικούς τρόπους στην εκτίμηση της κατάστασης κυβερνοασφάλειας ενός οργανισμού.

Για την πιλοτική εφαρμογή του προτεινόμενου πλαισίου επιλέχθηκε ένα ιδιαίτερα απαιτητικό και ευαίσθητο συνάμα πεδίο εφαρμογής, αυτό των κρίσιμων υποδομών που έχουν στοχοποιηθεί ιδιαίτερα τα τελευταία χρόνια. Οι κρατικές και παγκόσμιες νομοθεσίες σε θέματα κυβερνοασφάλειας, στις οποίες οι κρίσιμες υποδομές καλούνται να συμμορφωθούν είναι άκρως αυστηρές και απαιτητικές. Ταυτόχρονα, οι κρίσιμοι φορείς βάλλονται, σχεδόν καθημερινά, από ασήμαντους και σημαντικούς, εσωτερικούς και εξωτερικούς, επιτιθέμενους που κάνουν χρήση ποικίλων μέσων ψηφιακής τεχνολογίας. Το προτεινόμενο πλαίσιο καλείται να συμβάλει και να συνδράμει τις κρίσιμες υποδομές στην κατανόηση της τρέχουσας θέσης τους αναφορικά με το επίπεδο κυβερνοετοιμότητάς τους υποδεικνύοντας τους τομείς και τις διαστάσεις που χρήζουν της προσοχής τους και της διοικητικής μέριμνας.

1.3 Δομή έκθεσης

Η παρούσα διατριβή παρουσιάζει μια μεθοδολογία για την αξιολόγηση της κουλτούρας κυβερνοασφάλειας ενός οργανισμού με έμφαση στις πτυχές του ανθρώπινου παράγοντα. Έχει δομηθεί σε έξι (6) βασικά κεφάλαια και δύο (2) παραρτήματα.

Το *πρώτο* κεφάλαιο αποτελεί μια εισαγωγή στον τόμο, δίνοντας μια πλήρη εικόνα των στόχων της παρούσας διατριβής και της μεθοδολογίας που ακολουθήθηκε για την επίτευξή τους.

Στο *δεύτερο* κεφάλαιο γίνεται μια ιστορική ανασκόπηση της εξέλιξης της Ασφάλειας Πληροφοριών και παρουσιάζονται οι τρέχουσες ερευνητικές προσεγγίσεις, καθώς και κορυφαία πρότυπα και πλαίσια ασφάλειας στον κυβερνοχώρο, αναδεικνύοντας τις μεταξύ τους θεμελιώδεις διαφορές στον τρόπο αντιμετώπισης των παραγόντων που συμβάλουν και διαμορφώνουν την κουλτούρα κυβερνοασφάλειας.

Στο *τρίτο* κεφάλαιο παρουσιάζεται ένα ολιστικό μοντέλο κουλτούρας κυβερνοασφάλειας, σε μια προσπάθεια ανάπτυξης ενός καινοτόμου εργαλείου για την αξιολόγηση της ετοιμότητας ενός οργανισμού στον τομέα της κυβερνοασφάλειας με έμφαση στον ανθρώπινο παράγοντα. Το μοντέλο απεικονίζει λεπτομερώς τους βασικούς παράγοντες ασφαλείας σε διαφορετικά επίπεδα, διαστάσεις και τομείς. Ακολούθως, συσχετίζεται με δυο από τα επικρατέστερα γνωσιακά πλαίσια ασφαλείας, αυτό της Εσωτερικής Απειλής και το υβριδικό μοντέλο MITRE ATT&CK for Enterprise & ICS, με στόχο την αναγνώριση των αδυναμιών και κενών ασφαλείας του υπό αξιολόγηση οργανισμού. Με τον τρόπο αυτό καθίσταται δυνατή η ανάδειξη αντίμετρων ασφαλείας υποδομών αλλά και η σύσταση κατάλληλων εκπαιδευτικών προγραμμάτων στοχευμένων στις ανάγκες του εργατικού δυναμικού του εκάστοτε οργανισμού. Το κεφάλαιο ολοκληρώνεται με την παρουσίαση του εργαλείου που αναπτύχθηκε για την πρακτική εφαρμογή του προτεινόμενου πλαισίου κουλτούρας κυβερνοασφάλειας.

Το *τέταρτο* κεφάλαιο αναλύει την πιλοτική εφαρμογή του προτεινόμενου πλαισίου κουλτούρας κυβερνοασφάλειας σε κρίσιμες υποδομές κατά την περίοδο του κορονοϊού παραθέτοντας το σχεδιασμό της εκστρατείας αξιολόγησης και τις παραμέτρους ασφαλείας που στοχεύθηκαν κάνοντας χρήση του μοντέλου που παρουσιάστηκε στο προηγούμενο κεφάλαιο. Ακολουθεί η ανάλυση των αποτελεσμάτων ανά τομέα ασφαλείας αναδεικνύοντας τα επιμέρους ευρήματα και τους τομείς που χρήζουν προσοχής και ενίσχυσης στις εξεταζόμενες κρίσιμες υποδομές.

Το *πέμπτο* κεφάλαιο παραθέτει την εκτεταμένη πιλοτική εφαρμογή του πλαισίου στον τομέα της υγείας παρέχοντας πληροφορίες αναφορικά με το σχεδιασμό, τη στόχευση και την προσαρμογή των επιμέρους εκστρατειών αξιολόγησης ανάλογα με τη στοχοθεσία και τους απώτερους σκοπούς που καλούνται να εκπληρώσουν. Τα αποτελέσματα και τα ευρήματα της κάθε εκστρατείας παρουσιάζονται αναλυτικά αναδεικνύοντας τη σπουδαιότητα της πολυδιάστασης προσέγγισης του πλαισίου και υπογραμμίζοντας τις προτεινόμενες λύσεις και προσεγγίσεις στα εντοπισμένα κενά και ελλείματα κυβερνοασφάλειας.

Το *έκτο* κεφάλαιο συνοψίζει τα συμπεράσματα της διατριβής αναδεικνύοντας την προστιθέμενη αξία του πλαισίου κουλτούρας κυβερνοασφάλειας όπως αυτή προκύπτει από τις πρακτικές εφαρμογές του.

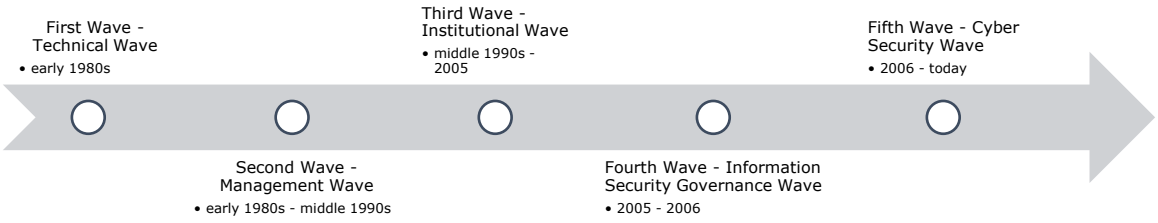
Ακολουθεί το κεφάλαιο της βιβλιογραφίας και τα παραρτήματα που φιλοξενούν:

- το εγχειρίδιο χρήσης του εργαλείου κουλτούρας κυβερνοασφάλειας που αναπτύχθηκε προς εφαρμογή του προτεινόμενου πλαισίου (Παράρτημα Ι)
- μια λίστα των δημοσιεύσεων σε επιστημονικά περιοδικά, βιβλία και πρακτικά συνεδρίων (Παράρτημα ΙΙ)

ΚΕΦΑΛΑΙΟ 2: ΑΝΑΣΚΟΠΗΣΗ ΥΦΙΣΤΑΜΕΝΗΣ ΚΑΤΑΣΤΑΣΗΣ

2.1 Εισαγωγή

Η ***Ασφάλεια Πληροφοριών (Information Security)*** είναι ένας διεπιστημονικός τομέας μελέτης και επαγγελματικής δραστηριότητας που επικεντρώνεται στη διαφύλαξη και προστασία της ***Τεχνολογίας Πληροφοριών (Information Technology)*** από ποικίλους κινδύνους και απειλές [1, 2]. Αρχικά, η Ασφάλεια Πληροφοριών χαρακτηρίστηκε από μια ιδιαίτερα τεχνοκρατική προσέγγιση που απευθυνόταν κυρίως σε ειδικούς [3]. Ακόμα και σε αυτά τα πρώιμα στάδια, οι υπεύθυνοι για την εφαρμογή της αναγνώρισαν την ανάγκη συμμετοχής των ανώτερων διοικητικών στρωμάτων του εκάστοτε οργανισμού. Αυτό οδήγησε σε μια δεύτερη εξελικτική φάση όπου η Ασφάλεια Πληροφοριών ενσωματώθηκε στις οργανωτικές δομές των οργανισμών και ορίστηκαν Διευθυντές Ασφάλειας Πληροφοριών (Information Security Managers). Συντάχθηκαν πολιτικές και διαδικασίες ασφάλειας δημιουργώντας την ανάγκη κατανόησης της αποτελεσματικότητάς τους και αξιολόγησης του αντίκτυπού τους. Με αυτό τον τρόπο αποκαλύφθηκε ότι υπήρχαν και άλλα στοιχεία ασφάλειας πληροφοριών που είχαν αγνοηθεί μέχρι τότε. Η τυποποίηση, η πιστοποίηση και η αξιολόγηση της ασφάλειας πληροφοριών εισήχθησαν μαζί με μια προσπάθεια κατανόησης και αντιμετώπισης του ανθρώπινου στοιχείου ως σημαντικό παράγοντα ασφάλειας [4].



Εικόνα 1. Εξελικτικά Κύματα της Ασφάλειας Πληροφοριών

Πιο αναλυτικά, η εξέλιξη της Ασφάλειας Πληροφοριών ήταν σταδιακή (Εικόνα 1) και έχουν αναγνωριστεί σε αυτή 5 φάσεις ή αλλιώς εξελικτικά κύματα [5]:

- **Πρώτο Κύμα – Τεχνικό**: Το κύμα αυτό ήταν αποκλειστικά αφιερωμένο στο mainframe περιβάλλον, με απλοϊκά τερματικά και πλήρως κεντρική επεξεργασία. Η ασφάλεια πληροφοριών περιοριζόταν σε απλές μορφές αναγνώρισης και ελέγχου ταυτότητας για σύνδεση στο σύστημα mainframe, και ίσως κάποια ακατέργαστη μορφή εξουσιοδότησης ή λογικού ελέγχου πρόσβασης. Οι περισσότερες από αυτές τις λειτουργίες διεκπεραιώνονταν από το λειτουργικό σύστημα mainframe, το οποίο βασικά ήταν κατανοητό μόνο από τους τεχνικούς που το χειρίζονταν. Πτυχές όπως πολιτικές και διαδικασίες ασφαλείας δεν είχαν ακόμα αναδυθεί. Η συνειδητοποίηση ότι αυτό το στάδιο δεν ήταν επαρκές για την ασφάλεια των πληροφοριών άρχισε να αναδύεται στις αρχές της δεκαετίας του 1980 με τη συνδρομή του Κρίστιαν Μπέκμαν, ο οποίος συγκάλεσε την πρώτη διεθνή διάσκεψη για την ασφάλεια των πληροφοριών (IFIP/Sec 83) και ίδρυσε μια Τεχνική Επιτροπή για θέματα ασφάλεια πληροφοριών.

- **Δεύτερο Κύμα – Διοικητικό**: Η ανάπτυξη των κατανεμημένων υπολογιστών, και πιο συγκεκριμένα του προσωπικού υπολογιστή, ανέδειξε πολλές νέες παραμέτρους στο πεδίο της Ασφάλειας Πληροφοριών. Το γεγονός ότι οι πληροφορίες δεν αποθηκεύονταν πλέον σε έναν κεντρικό υπολογιστή καλά προστατευμένο, αλλά διανέμονταν σε πολλούς επιτραπέζιους υπολογιστές που συνδέονταν μέσω δικτύων, ελλόχευε σοβαρούς κινδύνους που έπρεπε να αντιμετωπιστούν.

  Η Ασφάλεια Πληροφοριών αναδύθηκε σε θέμα που τράβηξε την προσοχή της Διοίκησης με αποτέλεσμα να οριστούν οι πρώτοι Διευθυντές Ασφάλειας Πληροφοριών (Information Security Managers). Άρχισαν να δημιουργούν πολιτικές και διαδικασίες ασφαλείας και οργανωτικές δομές για να στεγαστούν Τμήματα Ασφάλειας Πληροφοριών.

  Λόγω αυτών των εξελίξεων κατά τη διάρκεια του δεύτερου κύματος, άρχισε η διερεύνηση πτυχών που σχετίζονταν με τις βέλτιστες πρακτικές και την τυποποίηση στην Ασφάλεια Πληροφορίων. Τέθηκαν θεμελιώδη ερωτήματα μεταξύ των οποίων και:

  - Πώς συγκρίνουμε την ασφάλεια με τους ανταγωνιστές μας;
  - Τι πρέπει να περιλαμβάνει μια Πολιτική Ασφάλειας Πληροφοριών;
  - Πώς θα μπορούσαν να λάβουν κάποια μορφή επίσημης πιστοποίησης για την κατάσταση της Τεχνολογίας Πληροφοριών της εταιρείας;

  Πιο σημαντική εξέλιξη όμως ήταν ότι αναδύθηκε ο ρόλος του εργαζομένου ως τελικού χρήστη του συστήματος και έγινε αποδεκτή η σημασία της ανθρώπινης διάστασης οδηγώντας στο Τρίτο Κύμα, που ονομάζεται Κύμα Θεσμοποίησης, το οποίο έγινε εμφανές περίπου στα μέσα της δεκαετίας του 1990.

- **Τρίτο Κύμα – Θεσμοποίηση**: Το γεγονός ότι η Ασφάλεια Πληροφοριών έχει πολύ περισσότερες διαστάσεις από την τεχνική καθώς και ότι ο ρόλος της είναι ζωτικής σημασίας για την υγεία και τη στρατηγική εξέλιξη μιας εταιρείας, οδήγησαν σε νέες προσπάθειες για τη θεσμοθέτησή της.

  Δύο ήταν οι καταληκτικοί παράγοντες σε αυτό το κύμα:

  - η ιδέα των διεθνών βέλτιστων πρακτικών και η άφιξη του BS 7799 Μέρος 1 και 2 [6]. Το Μέρος 1 ήταν το πρώτο πραγματικά ευρέως αποδεκτό έγγραφο που καθόριζε τις βασικές πτυχές της ασφάλειας πληροφοριών ενώ το Μέρος 2 παρείχε την πλατφόρμα για την απόκτηση κάποιας διεθνούς πιστοποίησης σύμφωνα με το Μέρος 1.
  - η αυξανόμενη έμφαση στην ευαισθητοποίηση για την ασφάλεια πληροφοριών και ο κίνδυνος του ανθρώπινου παράγοντα.

  Σε αυτό το στάδιο, οι εταιρείες άρχισαν επίσης να αναπτύσσουν τεχνικές για την αξιολόγηση της κατάστασης και του επίπεδου συμμόρφωσής τους με την Ασφάλεια Πληροφοριών με στόχο την αναφορά αυτών στην ανώτερη διοίκηση.

  Στις αρχές της τρέχουσας δεκαετίας, εισάγεται η σημασία της καλής Εταιρικής Διακυβέρνησης (Corporate Governance) και ο ρόλος που διαδραματίζει η Ασφάλεια Πληροφοριών σε αυτήν. Θέματα που άπτονται του απόρρητου των δεδομένων και των πληροφοριών τίθενται υπόψιν του Διοικητικού Συμβουλίου και οδηγούν στο Τέταρτο Κύμα.

- **Τέταρτο Κύμα - Διακυβέρνηση Ασφάλειας Πληροφοριών**: Εμφανίστηκαν αρκετές διεθνείς βέλτιστες πρακτικές για καλή Εταιρική Διακυβέρνηση οι οποίες υπογράμμιζαν το ρόλο της Διαχείρισης Κινδύνων Πληροφορικής (Information Technology Risk Management) και της Διακυβέρνησης Πληροφορίας (Information Technology Governance) [7].

  Οι οικονομικές πληροφορίες των εταιρειών αποθηκεύτηκαν και υποβλήθηκαν σε επεξεργασία από υπολογιστές. Οι κίνδυνοι απάτης και κατάχρησης οικονομικών πόρων χειραγωγώντας τα ηλεκτρονικά δεδομένα και μέσα της εταιρείας έγιναν εμφανείς καθώς και το μερίδιο ευθύνης που βάραινε τη διοίκηση σε τέτοιες περιπτώσεις. Αυτή η αυξανόμενη έμφαση στην Ασφάλεια Πληροφοριών οδήγησε στην εμφάνιση της έννοιας της ***Διακυβέρνησης Ασφάλειας Πληροφοριών (Information Security Governance)***.

- **Πέμπτο Κύμα – Κυβερνοασφάλεια**: Το διαδίκτυο είναι αναμφισβήτητα μια από τις μεγαλύτερες εφευρέσεις που αναπτύχθηκαν ποτέ από την ανθρωπότητα, αλλά έχει μαζί της εξαιρετικά σοβαρούς κινδύνους. Η ανάπτυξη οποιουδήποτε συστήματος που βασίζεται στο διαδίκτυο συνεπάγεται την έκθεσή του σε κίνδυνο επίθεσης ή παραβίασης από τους εγκληματίες του κυβερνοχώρου. Οι κυβερνοεγκληματίες, εκμεταλλευόμενοι την αυξανόμενη χρήση του διαδικτύου από τις εταιρείες για την παροχή υπηρεσιών και αγαθών, διαπράττουν καθημερινά εγκλήματα τεράστιων διαστάσεων. Κακόβουλο λογισμικό, phishing, πλαστογράφηση και ποικίλες άλλες τεχνικές απειλούν καθημερινά τους χρήστες του διαδικτύου.

  Η εγκαθίδρυση και ευρεία χρήση του διαδικτύου διευκόλυνε την εξάπλωση του κυβερνοεγκλήματος ενώ ταυτόχρονα αύξησε το βαθμό δυσκολίας για τους ειδικούς στο χώρο της Ασφάλειας Πληροφοριών.

Η εξελικτική πορεία της Ασφάλειας Πληροφοριών, ακολουθώντας τις τεχνολογικές και κοινωνικοπολιτικές εξελίξεις των τελευταίων δεκαετιών, υπογράμμισε και ανέδειξε τη σημασία του ανθρώπινου παράγοντα ως καταλυτικού συντελεστή στο πολυδιάστατο και πολυκριτηριακό αυτό θέμα. Η μεγαλύτερη απειλή για το απόρρητο και την ασφάλεια ενός οργανισμού, ακόμη κι αν δεν αναγνωρίζεται, θεωρείται ότι είναι το προσωπικό του [8]. Η ευαισθητοποίηση για την ασφάλεια των εργαζομένων είναι βασικός κρίκος στην αλυσίδα ασφαλείας ενός οργανισμού, καθώς ακόμη και η πιο άρτια διασφαλισμένη εταιρεία είναι ανυπεράσπιστη χωρίς κουλτούρα ασφάλειας [9, 10]. Αυτός ο όρος, «***κουλτούρα ασφάλειας***», κυριάρχησε σύντομα και του αποδόθηκαν διάφοροι ορισμοί [11]. Η συντριπτική τους πλειονότητα συμφωνεί ότι «*υπάρχει όταν κάθε συμμετέχων στην κοινωνία της πληροφορίας, ανάλογα με τον ρόλο του, γνωρίζει τους σχετικούς κινδύνους ασφαλείας και προληπτικά μέτρα, αναλαμβάνει την ευθύνη και λαμβάνει μέτρα για τη βελτίωση της ασφάλειας των πληροφοριακών συστημάτων και των δικτύων τους*» [12].

Η κουλτούρα ασφαλείας καλλιεργείται μέσω μιας μακράς και χρονοβόρας διαδικασίας που επηρεάζεται από διάφορους παράγοντες με διαφορετική βαρύτητα [13, 14, 15, 16]. Έχουν διατυπωθεί πολυάριθμες προσεγγίσεις και απόψεις σχετικά με τα βασικά της στοιχεία και τη μεθοδολογία αξιολόγησής τους. Και ενώ υφίστανται συγκεκριμένες μεθοδολογίες αξιολόγησης της Ασφάλειας Πληροφοριών, το ίδιο δεν ισχύει και για τις μεθόδους αξιολόγησης της αντίστοιχης κουλτούρας κυβερνοασφάλειας [17, 18].

2.2 Ερευνητική και Επιστημονική Προσέγγιση

Η πολυπλοκότητα της ανθρώπινης φύσης όσον αφορά στην Ασφάλεια Πληροφοριών αποτελεί εδώ και καιρό αντικείμενο έρευνας για διάφορους επιστημονικούς κλάδους. Στόχος τους ήταν να προσεγγίσουν, να κατανοήσουν, και τέλος να αναλύσουν πώς τα συναισθήματα, οι πεποιθήσεις, η συμπεριφορά, η στάση και οι ενέργειες ενός εργαζόμενου μπορούν άμεσα ή έμμεσα, εκούσια ή ακούσια, να επηρεάσουν και πιθανώς να υπονομεύσουν την ασφάλεια ενός οργανισμού. Κατανόηση των θεμελίων του προβλήματος θα μπορούσε να οδηγήσει σε αποτελεσματικές λύσεις: εφαρμόσιμες και γόνιμες πολιτικές και διαδικασίες ασφάλειας καθώς και προγράμματα κατάρτισης που θα μπορούσαν να συμβάλουν στην καλλιέργεια μια ευημερούσας κουλτούρας ασφάλειας.

Η συμμόρφωση των εργαζομένων στις πολιτικές ασφάλειας πληροφοριών υπήρξε αφετηρία για πολλές επιστημονικές έρευνες αξιοποιώντας διάφορες θεωρίες, όπως η Θεωρία Προγραμματισμένων Οφελών (Theory of Planned Benefits, TPB), η Θεωρία Ορθολογικής Επιλογής (Rational Choice Theory, RCT), η Θεωρία Κινήτρων Προστασίας (Protection Motivation Theory, PMT), η Γενική Θεωρία Αποτροπής (General Deterrence Theory, GDT), η Κοινωνική Γνωσιακή Θεωρία (Social Cognitive Theory, SCT) και η Θεωρία Αιτιολογημένης Δράσης (Theory of Reasoned Action, TRA) [19, 20]. Η πρόθεση συμμόρφωσης με τις πολιτικές ασφάλειας πληροφοριών αποδείχθηκε ότι επηρεάζεται θεμελιωδώς από τη στάση των εργαζομένων, τις κανονιστικές τους πεποιθήσεις και συνήθειες ενώ, ταυτόχρονα, οι κυρώσεις και η πρόθεση είχαν σημαντικό αντίκτυπο στην πραγματική συμμόρφωση [21]. Πιο συγκεκριμένα, η απειλή συνεπειών και οι συνθήκες διευκόλυνσης αποδείχθηκε ότι επηρεάζουν θετικά ενώ, αντίθετα, η μίμηση και οι κυρώσεις αρνητικά ή και καθόλου [22].

Στοιχεία που αποδείκνυαν ότι άτομα που έχουν τόσο τις γνώσεις ασφαλείας όσο και τις δεξιότητες ενδέχεται να αποτύχουν να τις εφαρμόσουν αποτελεσματικά στην καθημερινή ρουτίνα εργασίας τους πυροδότησε μια άλλη ερευνητική ιδέα με στόχο τη διερεύνηση των σχέσεων μεταξύ της αυτο-αποτελεσματικότητας (self-efficacy) στην Ασφάλεια Πληροφοριών, της πρακτικής συμπεριφοράς ασφάλειας και του κίνητρου [23]. Η αυτο-αποτελεσματικότητα, στο πλαίσιο της Ασφάλειας Πληροφοριών, αναφέρεται στην αυτοπεποίθηση ενός εργαζομένου στις δεξιότητές του ή στην ικανότητά του να συμμορφωθεί με τις πολιτικές που έχει θέσει ο οργανισμός στον οποίο απασχολείται [24]. Έρευνα έδειξε ότι άτομα με υψηλή αυτό-αποτελεσματικότητα επιδεικνύουν υψηλότερο βαθμό πεποίθησης για την ικανότητά τους να αξιοποιήσουν τα κίνητρα και τους γνωστικούς πόρους που απαιτούνται για την επιτυχή εφαρμογή των πολιτικών ασφαλείας του οργανισμού [25]. Ταυτόχρονα, συνήθειες και υποκειμενικές νόρμες επηρεάζουν άμεσα την πραγματική συμπεριφορά και μειώνουν τον αντίκτυπο των προθέσεων συμμόρφωσης με τις οργανωτικές πολιτικές ασφαλείας [26].

Αν και τα ευρήματα αυτά αποκάλυψαν την ανάγκη χρηστο-κεντρικής (user-centered) προσέγγισης της Ασφάλειας Πληροφοριών, ταυτόχρονα υπογράμμισαν τον προφανή αντίκτυπο που έχει το κοινωνικό και εργασιακό περιβάλλον στη συμπεριφορά του ατόμου και στη συμμόρφωσή του με τις πολιτικές ασφαλείας [27]. Ως εκ τούτου, οι μελετητές επικεντρώθηκαν στη γεφύρωση του χάσματος μεταξύ της ατομικής πρόθεσης και της πραγματικής συμπεριφοράς δεδομένης μιας συγκεκριμένης εργασιακής πραγματικότητας και προσέγγισης στην Ασφάλεια Πληροφοριών [21, 22, 24, 26]. Οι Robert E. Crossler et al., Zahoor Ahmed Soomro et al., Qing Hu et al. είναι μερικοί από τους ερευνητές που εντόπισαν την ανάγκη συνεξέτασης των οργανωτικών (organizational) και ατομικών (individual) παραγόντων που επηρεάζουν και διαμορφώνουν την οργανωτική κουλτούρα και, κατ' επέκταση, επιδρούν άμεσα στα αποτελέσματα της Ασφάλειας Πληροφοριών,

ανοίγοντας το δρόμο για νέους ορίζοντες επιστημονικής έρευνας [28, 29, 30]. Η ανάγκη μελέτης, διερεύνησης και, τέλος, ποσοτικοποίησης οργανωτικών και ατομικών διαστάσεων ασφάλειας παράλληλα με τις πολλές αλληλεπιδράσεις και αλληλεξαρτήσεις τους ήταν πλέον εμφανής και αδιαμφισβήτητη.

2.3 Πλαίσια και Πρότυπα Ασφάλειας Πληροφοριών

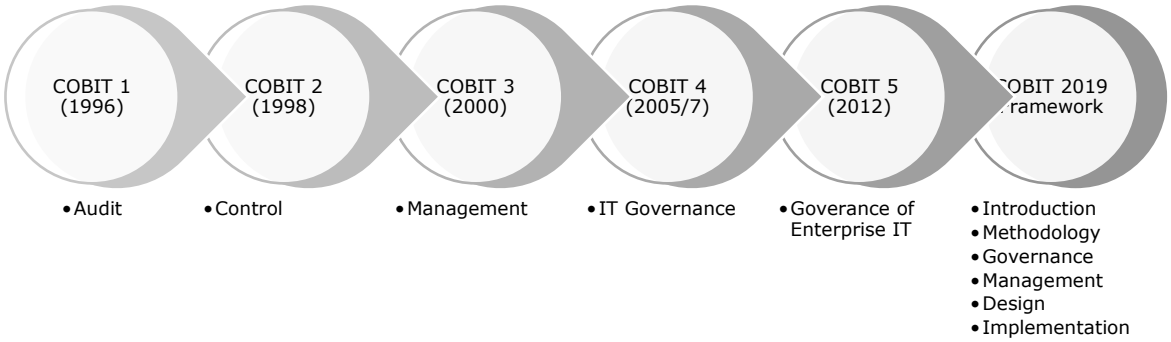
Παράλληλα, ο επιχειρηματικός κόσμος επικεντρώθηκε στο σχεδιασμό πλαισίων αξιολόγησης ασφάλειας ως μέσο διαμόρφωσης των επιχειρηματικών, περιβαλλοντικών και κοινωνικών συνθηκών που θα μπορούσαν να θεμελιώσουν μια σωστή και πολλά υποσχόμενη κουλτούρα ασφάλειας.

Εικόνα 2. ISO/IEC *27001:2005*

Οι προσπάθειες σε αυτό το πεδίο ξεκίνησαν πολύ νωρίτερα από τις αντίστοιχες ερευνητικές (όπως αυτές παρουσιάστηκαν στην προηγούμενη παράγραφο), όταν το 1995 το BSI Group δημοσίευσε το ***BS 7799*** ως πρότυπο [6]. Το πρώτο μέρος του περιείχε βέλτιστες πρακτικές για τη διαχείριση της ασφάλειας πληροφοριών ενώ το δεύτερο μέρος του, με τίτλο

«Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Προδιαγραφή με οδηγίες χρήσης» (Information Security Management Systems – Specification with guidance for use), επικεντρώθηκε στον τρόπο εφαρμογής ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (Information Security Management Systems, ISMS). Και τα δύο μέρη υιοθετήθηκαν αργότερα από τον Παγκόσμιο Οργανισμό Προτυποποίησης (International Organization for Standardization, ISO) και ενσωματώθηκαν στη σειρά προτύπων ISO 27000 ως ***ISO/IEC 27002:2007*** και ως ***ISO/IEC 27001:2005*** αντίστοιχα [31, 32]. Μαζί, διαμορφώνουν μια από τις ευρύτερα δεδομένες παγκοσμίως συστάσεις ασφάλειας[1].

Ένα χρόνο μετά, η Ένωση Ελέγχου Πληροφοριακών Συστημάτων (Information Systems Audit and Control Association, ISACA) κυκλοφόρησε το ***COBIT (Control Objectives for Information and Related Technologies)*** [33]. Το COBIT (Εικόνα 3), Στόχοι Ελέγχου για Πληροφορίες και Συναφείς Τεχνολογίες, ήταν ένα πλαίσιο που σχεδιάστηκε για να γεφυρώσει το κρίσιμο χάσμα μεταξύ τεχνικών θεμάτων, επιχειρηματικών κίνδυνων και απαιτήσεων ελέγχου. Σύντομα εξελίχθηκε σε μια ευρέως αναγνωρισμένη σύσταση με δυνατότητα εφαρμογής σε οποιονδήποτε οργανισμό σε οποιονδήποτε κλάδο. Χρησιμοποιείται για τη διασφάλιση της ποιότητας, του ελέγχου και της αξιοπιστίας των πληροφοριακών συστημάτων σε έναν οργανισμό.



Εικόνα 3. Εξελικτική πορεία COBIT

Το 2005, μια νέα ολοκληρωμένη πρόταση προσέγγισης της Ασφάλειας Πληροφοριών παρουσιάζεται με το όνομα ***PROTECT***. Το όνομά του αντιστοιχούσε σε ακρωνύμιο των επτά στοιχείων ελέγχου: Πολιτικές, Κίνδυνοι, Στόχοι, Τεχνολογία, Εκτέλεση, Συμμόρφωση και Ομάδα ***(Policies, Risks, Objectives, Technology, Execute, Compliance, and Team)*** τα οποία αναγνώριζε ως βασικά στοιχεία ενός αποτελεσματικού προγράμματος ασφάλειας με απώτερο σκοπό την αντιμετώπιση όλων των πτυχών της Ασφάλειας Πληροφοριών [34].

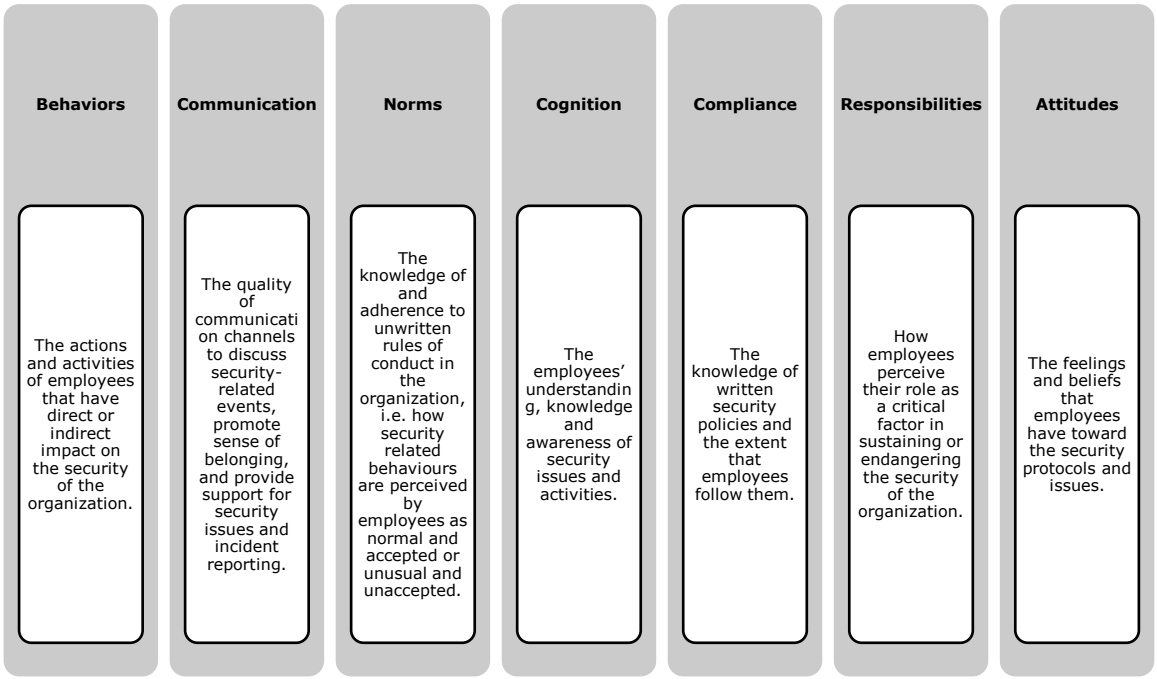
Το 2007, οι A. Da Veiga και J. H. P. Eloff παρουσίασαν το ***Πλαίσιο Διακυβέρνησης Ασφάλειας Πληροφοριών (Information Security Governance framework)***

[1] Καθώς ο κόσμος αντιμετωπίζει νέες εξελισσόμενες προκλήσεις ασφαλείας, το διεθνώς αναγνωρισμένο πρότυπο ***ISO/IEC 27001***, το οποίο στοχεύει στην προστασία του απορρήτου, της διαθεσιμότητας και της ακεραιότητας των στοιχείων των πληροφοριών των οργανισμών ενημερώθηκε στα τέλη του 2022. Ο πλήρης τίτλος της νέας έκδοσης είναι ***ISO/IEC 27001:2022 Ασφάλεια Πληροφοριών, Κυβερνοασφάλεια και Προστασία Απορρήτου*** και φέρει σημαντικές αλλαγές του Παραρτήματος Α του ISO/IEC 27001/2013.

προκειμένου να χρησιμοποιηθεί ως σημείο εκκίνησης από έναν οργανισμό για την ελαχιστοποίηση του κινδύνου και την καλλιέργεια ενός αποδεκτού επιπέδου κουλτούρας ασφάλειας πληροφοριών [4]. Απευθυνόταν σε τεχνικές, διαδικαστικές και ανθρώπινες παραμέτρους ενώ επέτρεπε περαιτέρω προσαρμογή στις ποικίλες εθνικές και διεθνείς νομοθεσίες και κανονισμούς στους οποίους υπόκειται κάθε οργανισμός.

Λίγα χρόνια αργότερα, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology, NIST) εξέδωσε την Ειδική Έκδοση (Special Publication, SP) ***SP 800–53 Αναθεώρηση 4***, Έλεγχοι Ασφάλειας και Απορρήτου για Ομοσπονδιακά Συστήματα Πληροφοριών και Οργανισμούς (Security and Privacy Controls for Federal Information Systems and Organizations) [35]. Βασικός σκοπός του ήταν η παροχή κατευθυντήριων γραμμών για την επιλογή και τον προσδιορισμό ελέγχων ασφάλειας για πληροφοριακά συστήματα που υποστηρίζουν εκτελεστικούς φορείς της ομοσπονδιακής κυβέρνησης.

Το 2017, ο Οργανισμός Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης (European Union Agency for Cybersecurity, ENISA), λαμβάνοντας υπόψη την τάση και τα ευρήματα της επιστημονικής και ερευνητικής κοινότητας που εξελισσόταν παράλληλα, διαφοροποιεί για πρώτη φορά την προσέγγιση της επαγγελματικής κοινωνίας με τη δημοσίευση του ***Πλαισίου Κουλτούρας Κυβερνοασφάλειας (Cybersecurity Culture Framework, CSC Framework)***. Σύμφωνα με το πλαίσιο αυτό (Εικόνα 4), η κουλτούρα κυβερνοασφάλειας αναφέρεται στη γνώση, τις πεποιθήσεις, τις αντιλήψεις, τις στάσεις, τις υποθέσεις, τους κανόνες και τις αξίες των ανθρώπων σχετικά με την ασφάλεια στον κυβερνοχώρο και πώς αυτά εκδηλώνονται μέσω της συμπεριφοράς των ανθρώπων σε θέματα Ασφάλειας Πληροφοριών [36]. Σύντομα, αναπτύχθηκε μια εργαλειοθήκη βασισμένη στις αρχές και τις κατευθυντήριες γραμμές του πλαισίου αυτού, το Security CLTRe Toolkit [37], που επιτρέπει σε έναν οργανισμό να αξιολογήσει και να απεικονίσει γραφικά την κατάσταση κουλτούρας κυβερνοασφάλειας μέσω επτά συγκεκριμένων διαστάσεων. Αυτή ήταν η πρώτη προσπάθεια επισημοποίησης της επιστημονικής προσέγγισης του ανθρώπινου παράγοντα ως καθοριστικού συντελεστή ασφάλειας.



Εικόνα 4. ENISA Πλαισίο Κουλτούρας Κυβερνοασφάλειας

Έως τότε, οι ειδικοί ασφαλείας (security experts) επικεντρώνονταν στο σχεδιασμό πρότυπων και πλαισίων ασφαλείας που στόχευαν στην υποδομή ασφάλειας, στις πολιτικές και διαδικασίες που προστατεύουν τους χώρους εργασίας και τους εργαζομένους αλλά χωρίς πρακτικά να ενθαρρύνεται η ατομική δέσμευση, συμμετοχή και ευαισθητοποίηση. Επιπρόσθετα, τα προτεινόμενα πλαίσια αγνόησαν την πρόθεση των εργαζομένων και την πραγματική συμπεριφορά τους κατά την προσπάθεια συμμόρφωσης στους ελέγχους και προτάσεις ασφαλείας που οριοθετούν ένα επιχειρησιακό περιβάλλον.

Από την άλλη πλευρά, όπως παρουσιάστηκε στην προηγούμενη ενότητα, η ακαδημαϊκή κοινότητα προσέγγισε την κυβερνοασφάλεια μέσω ανθρωπολογικών και κοινωνικών επιστημών που στόχο είχαν να κατανοήσουν τους περιβαλλοντικούς παράγοντες, τα μεμονωμένα χαρακτηριστικά και γνωρίσματα που επηρεάζουν, προκαλούν και τελικά υπαγορεύουν τη συνολική Ασφάλεια Πληροφοριών ενός οργανισμού. Η δυνατότητα συνδυασμού αυτών των δύο φαινομενικά ασυμβίβαστων, αλλά στην πραγματικότητα αλληλοσυμπληρούμενων, προσεγγίσεων στο χώρο της Κυβερνοασφάλειας είχε μείνει ανεξερεύνητη.

Η βιομηχανία ασφάλειας πληροφοριών και οι εμπειρογνώμονες του είδους έχουν εστιάσει σε αντίμετρα και λύσεις για τον εντοπισμό, την πρόληψη και την ελαχιστοποίηση των απωλειών από επιθέσεις ασφάλειας πληροφοριών. Ωστόσο, λαμβάνοντας υπόψιν ότι:

1. Τα τεχνικά μέτρα ασφάλειας στον κυβερνοχώρο πρέπει να λειτουργούν σε αρμονία με τις υπόλοιπες επιχειρηματικές διαδικασίες και χωρίς να επηρεάζουν δυσμενώς τον κύκλο εργασιών των οργανισμών.
2. Οι εργαζόμενοι δεν πρέπει να βιώνουν αντιφατικές καταστάσεις στις οποίες καλούνται να επιλέξουν μεταξύ της συμμόρφωσης με τις πολιτικές ασφαλείας ή της αποτελεσματικής εκτέλεσης της εργασίας τους.
3. Οι εκστρατείες ευαισθητοποίησης για τις απειλές στον κυβερνοχώρο δεν αποτελούν επαρκή προστασία από τις συνεχώς εξελισσόμενες επιθέσεις στον κυβερνοχώρο.
4. Η συμπεριφορά ενός οργανισμού εξαρτάται από τις κοινές πεποιθήσεις, αξίες και ενέργειες των εργαζομένων του για την ασφάλεια των πληροφοριών.
5. Οι εργαζόμενοι δεν πρέπει να θεωρούνται ο πιο αδύναμος κρίκος στις αλυσίδες κυβερνοασφάλεια. Αντιθέτως, θα πρέπει να αποτελέσουν τη πιο σημαντική γραμμή άμυνας (ένα ανθρώπινο τείχος προστασίας) ενάντια στις κυβερνοεπιθέσεις.

είναι πλέον εμφανής και ευρέως αποδεκτή η σημασία της ανάπτυξης μιας ισχυρής **κουλτούρας ασφάλειας** η οποία διαμορφώνεται και γαλουχείται μέσω μιας μακράς διαδικασίας ζύμωσης εντός ενός οργανισμού λαμβάνοντας υπόψιν πολλαπλούς παράγοντες που συμμετέχουν σε αυτήν.

Η κουλτούρα κυβερνοασφάλειας επηρεάζεται τόσο από εξωτερικούς (διεθνείς, εθνικούς, ρυθμιστικούς, νομικούς, κανονιστικούς, κλπ.) όσο και από εσωτερικούς (επιχειρησιακούς, ομαδικούς, κλπ.) παράγοντες, τόσο από οργανωτικούς όσο και από ατομικούς, τόσο από τεχνικούς όσο και από ανθρωπιστικούς. Ως εκ τούτου, επιβάλλεται η από κοινού εξέταση, εκτίμηση και αξιολόγηση όλων των διαστάσεων και παραμέτρων που επηρεάζουν, συναποτελούν και διαμορφώνουν την κουλτούρα κυβερνοασφάλειας.

Η παρούσα διατριβή εστιάζει στον συνδυασμό των επιστημονικών αποτελεσμάτων και των επιχειρηματικών ευρημάτων με παράλληλη γεφύρωση των διαφορών τους. Ο τελικός της στόχος δεν είναι άλλος από το σχεδιασμό, την υλοποίηση, και τελικά εφαρμογή ενός

στιβαρού ***πλαισίου κουλτούρας κυβερνοασφάλειας*** ικανού να αξιολογήσει και να συμβάλει ουσιαστικά στη βελτίωση της ασφάλειας ενός οργανισμού.

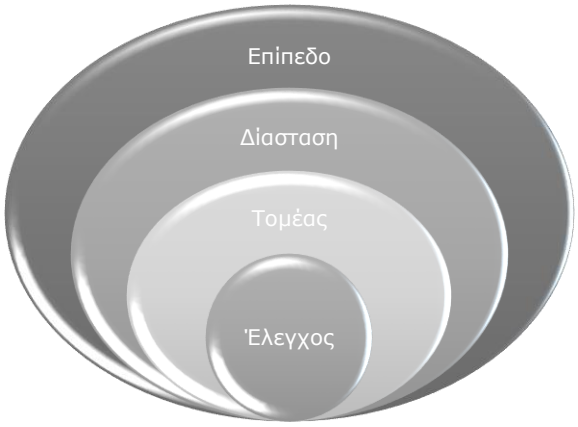
ΚΕΦΑΛΑΙΟ 3: ΠΛΑΙΣΙΟ ΚΟΥΛΤΟΥΡΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

3.1 Εισαγωγή

Έχοντας πραγματοποιήσει μια διεπιστημονική ερευνητική ανασκόπηση και μελετήσει διεξοδικά διάφορες ακαδημαϊκές αρχές και προσεγγίσεις εμπειρογνωμόνων ασφαλείας προς την Ασφάλεια Πληροφοριών, συμπεριλαμβανομένων τεχνικών αναλύσεων, αλγοριθμικών πλαισίων, μαθηματικών μοντέλων, στατιστικών υπολογισμών, συμπεριφορικών, οργανωτικών και εγκληματολογικών θεωριών, δομήθηκε ένα πλαίσιο κρίσιμων παραγόντων κουλτούρας κυβερνοασφάλειας. Συνδυάζοντας ανθρωποκεντρικά στοιχεία με οργανωτικά χαρακτηριστικά, εξωτερικές με εσωτερικές παραμέτρους, σχεδιάστηκε ένα γενικευμένο μοντέλο για την προσέγγιση της κουλτούρας κυβερνοασφάλειας.

Το προσχέδιο αυτό παρουσιάστηκε ακολούθως σε μια σειρά επιστημονικών συνεδρίων και εργαστηρίων με συμμετοχή εμπειρογνωμόνων και ειδικών σε θέματα Ασφαλείας Πληροφοριών [38, 39, 40, 41] στο πλαίσιο του ερευνητικού έργου EnergyShield [42], το οποίο χρηματοδοτήθηκε από την Ευρωπαϊκή Επιτροπή. Εκπρόσωποι εταιρειών λογισμικού που ειδικεύονται σε λύσεις ασφαλείας και βιομηχανικά προϊόντα, συμβουλευτικοί οργανισμοί κυβερνοασφάλειας και πανεπιστημιακά τμήματα που σχετίζονται με την Ασφάλεια Πληροφοριών συμμετείχαν συνέβαλαν στη διαμόρφωση και οριστικοποίηση του μοντέλου οδηγώντας στην πρώτη του ολοκληρωμένη έκδοση [43].

Οι βασικές δομές του μοντέλου παρουσιάζονται στην Εικόνα 5. Σύμφωνα με αυτήν, το μοντέλο ορίζει ***επίπεδα*** (***levels***), που χρησιμοποιούνται για το διαχωρισμό των «εξωτερικών» οργανωτικών παραγόντων με τα «εσωτερικά» ατομικά χαρακτηριστικά. Κάθε επίπεδο αναλύεται σε διαφορετικές ***διαστάσεις*** (***dimensions***) που αντιστοιχούν στις διαφορετικές θεματικές της κυβερνοασφάλειας. Κάθε διάσταση (dimension) αναλύεται με τη σειρά της σε ***τομείς*** (***domains***) με διακριτές περιοχές εφαρμογής και μετρητικούς δείκτες που αντιστοιχούν στους ***ελέγχους (controls)*** του μοντέλου.

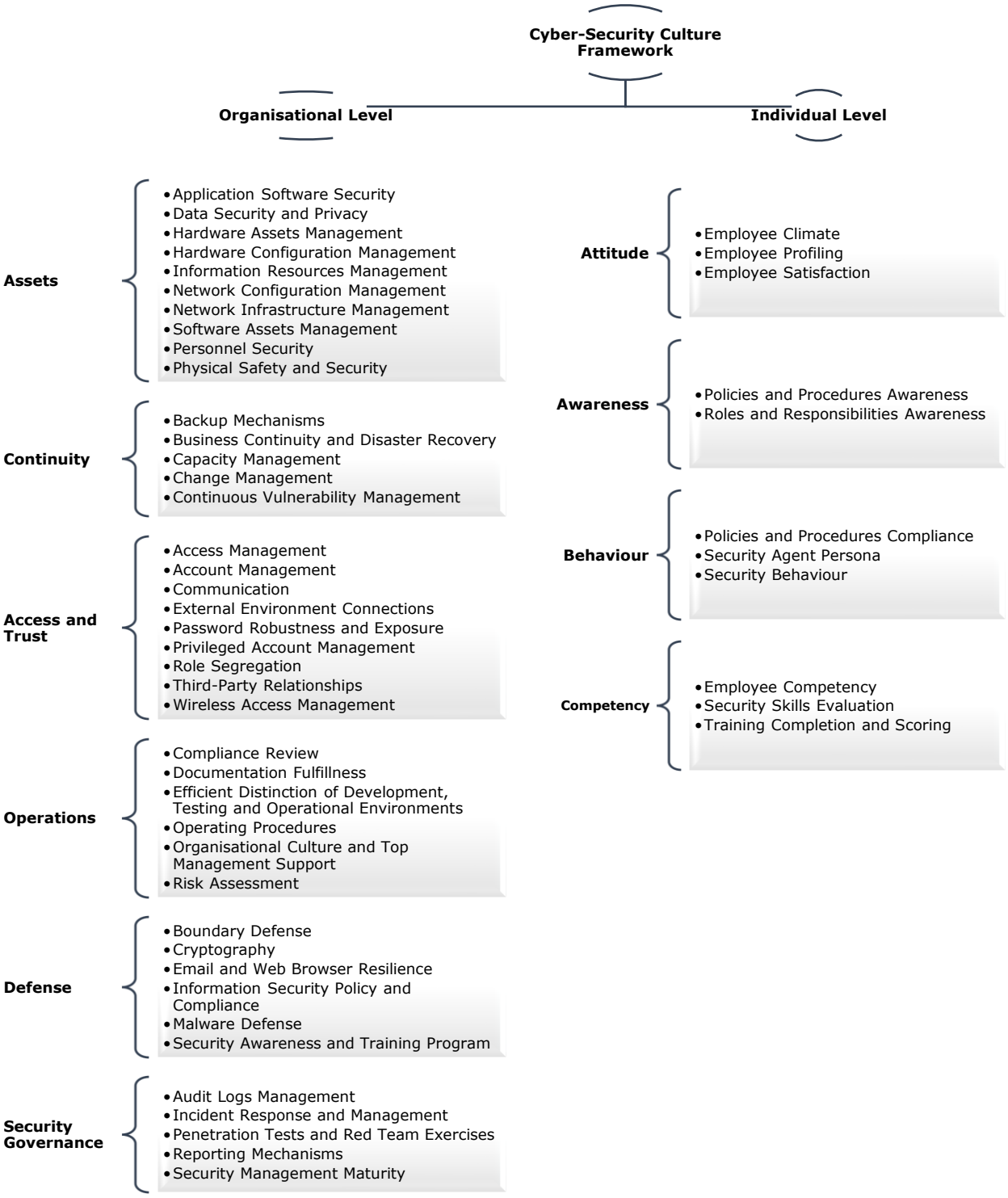


Εικόνα 5. Πλαίσιο Κουλτούρας Κυβερνοασφάλειας – Βασικές Δομές

Στην παράγραφο που ακολουθεί γίνεται μια αναλυτική παρουσίαση του μοντέλου και των δομών αυτού παρουσιάζοντας τους ακριβείς τεχνικούς ορισμούς τους καθώς και την επιστημονική τους τεκμηρίωση.

3.2 Μοντέλο

Η Εικόνα 6 παρουσιάζει το μοντέλο κουλτούρας κυβερνοασφάλειας με σαφή διαχωρισμό των επιπέδων, διαστάσεων και τομέων από τα οποία αυτό συναποτελείται.



Εικόνα 6. Μοντέλο Κουλτούρας Κυβερνοασφάλειας [43]

Το μοντέλο κουλτούρας κυβερνοασφάλειας ορίζει σαφώς δύο ***επίπεδα*** (***levels***):

- **Οργανωτικό επίπεδο (Organizational level)**: περιλαμβάνει όλους τους παράγοντες που σχετίζονται με την τεχνολογική υποδομή ασφάλειας ενός οργανισμού καθώς και τις λειτουργίες, πολιτικές και διαδικασίες ασφαλείας του.
- **Ατομικό επίπεδο (Individual level)**: στοχεύει στα ατομικά χαρακτηριστικά των εργαζομένων με άμεσο αντίκτυπο στη στάση και τη συμπεριφορά τους ως προς την Ασφάλεια Πληροφοριών.

Με αυτόν τον τρόπο, συνδυάζονται οι δύο προοπτικές που παρουσιάστηκαν στο προηγούμενο κεφάλαιο γεφυρώνοντας τους «εξωτερικούς» οργανωτικούς παράγοντες με τα «εσωτερικά» ατομικά χαρακτηριστικά.

Ακολούθως, κάθε επίπεδο αναλύεται σε διαφορετικές ***διαστάσεις*** (***dimensions***). Το οργανωτικό επίπεδο χωρίζεται σε διαστάσεις που αφορούν στο σχεδιασμό, την ανάπτυξη, την τεκμηρίωση και την υλοποίηση πολιτικών και διαδικασιών ασφαλείας που στοχεύουν σε διαφορετικούς επιχειρηματικούς τομείς (Πίνακας 1) ενώ το ατομικό επίπεδο διαιρείται σε διαστάσεις που αποδίδουν ανθρώπινα χαρακτηριστικά, προσεγγίσεις και επιδόσεις ως προς την κυβερνοασφάλεια (Πίνακας 2).

Πίνακας 1. Οργανωτικές Διαστάσεις (Organizational Dimensions)

Διάσταση	**Ορισμός**
Δυναμικό (Assets)	Αυτή η διάσταση περιλαμβάνει το σχεδιασμό, την ανάπτυξη, την τεκμηρίωση και την εφαρμογή πολιτικών και διαδικασιών ασφαλείας που στοχεύουν στην προστασία των στοιχείων ενός οργανισμού (συμπεριλαμβανομένων ατόμων, κτιρίων, μηχανών, συστημάτων και στοιχείων ενεργητικού) μέσω της επιβολής πολλών επιπέδων ελέγχων εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας.
Συνέχεια (Continuity)	Αυτή η διάσταση περιλαμβάνει τον σχεδιασμό, την ανάπτυξη, την τεκμηρίωση και την εφαρμογή πολιτικών και διαδικασιών ασφάλειας που στοχεύουν στη διασφάλιση των λειτουργιών, των υπηρεσιών και τη συνέχεια παραγωγής για έναν οργανισμό σε προκαθορισμένα επίπεδα, ενώ παράλληλα διασφαλίζουν τη φήμη και τα συμφέροντα των βασικών ενδιαφερομένων σε περιπτώσεις ανατρεπτικών συμβάντων.
Πρόσβαση και Εμπιστοσύνη (Access and Trust)	Αυτή η διάσταση περιλαμβάνει το σχεδιασμό, την ανάπτυξη, την τεκμηρίωση και την εφαρμογή επιχειρηματικών διαδικασιών, πολιτικών και διαδικασιών που στοχεύουν στη διασφάλιση της κατάλληλης πρόσβασης σε πόρους ολόκληρου του οργανισμού διευκρινίζοντας τους διαφορετικούς ρόλους και προσβάσεις. Επιπλέον, οριοθετεί τυχούσες αλληλεπιδράσεις του οργανισμού με τρίτους παράγοντες, όπως προμηθευτές, πελάτες, αρχές κ.λπ.
Λειτουργίες (Operations)	Αυτή η διάσταση αναφέρεται στη διαχείριση επιχειρηματικών πρακτικών για τη δημιουργία του υψηλότερου δυνατού επιπέδου αποτελεσματικότητας σε έναν οργανισμό,

	λαμβάνοντας παράλληλα υπόψη τις πτυχές ασφάλειας που διαφυλάσσουν τα τελικά του αποτελέσματα.
Άμυνα (Defence)	Αυτή η διάσταση εστιάζει στο σχεδιασμό, απόκτηση και διαμόρφωση όλων των τεχνικών στοιχείων που είναι απαραίτητα για τη βελτίωση και την αποτελεσματική λειτουργία της ασφάλειας πληροφοριών του.
Διακυβέρνηση Ασφάλειας (Security Governance)	Αυτή η διάσταση περιλαμβάνει το σχεδιασμό, την ανάπτυξη, την τεκμηρίωση και την εφαρμογή πολιτικών ώστε να προγραμματίζεται, να διαχειρίζεται και να βελτιώνεται αποτελεσματικά η ασφάλεια των πληροφοριών του οργανισμού.

Πίνακας 2. Ατομικές Διαστάσεις (Individual Dimensions)

Διάσταση	**Ορισμός**
Στάση (Attitude)	Αυτή η διάσταση αναφέρεται στα συναισθήματα και τις πεποιθήσεις που έχουν οι εργαζόμενοι για τα πρωτόκολλα και τα θέματα ασφαλείας.
Επίγνωση (Awareness)	Αυτή η διάσταση αναφέρεται στην κατανόηση, τη γνώση και την ευαισθητοποίηση των εργαζομένων σε θέματα και δραστηριότητες ασφάλειας.
Συμπεριφορά (Behaviour)	Αυτή η διάσταση αναφέρεται στις ενέργειες και τις δραστηριότητες των εργαζομένων που έχουν άμεσο ή έμμεσο αντίκτυπο στην ασφάλεια του οργανισμού.
Ικανότητα (Competency)	Αυτή η διάσταση αναφέρεται στις ικανότητες, τις δεξιότητες, τις γνώσεις και την τεχνογνωσία των εργαζομένων που τους επιτρέπουν να συμμορφώνονται με τις πολιτικές και τις διαδικασίες ασφαλείας του οργανισμού.

Κάθε διάσταση (dimension) αναλύεται με τη σειρά της σε ***τομείς*** (***domains***) με διακριτές περιοχές εφαρμογής και μετρητικούς δείκτες. Ο Πίνακας 3 παρουσιάζει ένα συνοπτικό ορισμό για καθέναν από αυτούς ενώ ταυτόχρονα αποδίδει τα καθιερωμένα ερευνητικά αποτελέσματα που αποτέλεσαν τη βάση τους.

Πίνακας 3. Συσχέτιση Μοντέλου Κυβερνοασφάλειας με καθιερωμένα ερευνητικά αποτελέσματα.

Επίπεδο	Διάσταση	Τομέας	Ορισμός	Πηγές
Οργανωτικό	**Δυναμικό (Assets)**	Ασφάλεια λογισμικού εφαρμογών (Application Software Security)	Διαχείριση του κύκλου ζωής ασφαλείας όλων των λογισμικών που έχουν αναπτυχθεί εσωτερικά και όσων έχουν αποκτηθεί για την πρόληψη, τον εντοπισμό και τη διόρθωση αδυναμιών ασφάλειας.	[31, 32, 44, 45]
		Ασφάλεια Δεδομένων και Απόρρητο (Data Security and Privacy)	Οι διαδικασίες και τα εργαλεία που χρησιμοποιούνται για την πρόληψη της υποκλοπής δεδομένων, το μετριασμό των επιπτώσεων των απολεσθέντων δεδομένων και τη διασφάλιση του απορρήτου και της ακεραιότητας των ευαίσθητων πληροφοριών.	[32, 44, 45, 46, 47, 48]
		Διαχείριση Εξοπλισμού (Hardware Assets Management)	Ενεργή τεκμηρίωση, απογραφή και διαχείριση όλου του εξοπλισμού ή φυσικών περιουσιακών στοιχείων, ώστε να διασφαλίζεται η αποτελεσματική προστασία τους.	[31, 32, 44, 48]
		Διαχείριση Παραμετροποίησης Εξοπλισμού (Hardware Configuration Management)	Καθιέρωση, υλοποίηση και ενεργή διαχείριση παραμετροποίησης ασφαλείας για όλες τις συσκευές ή τα φυσικά περιουσιακά στοιχεία χρησιμοποιώντας μια αυστηρή διαδικασία διαχείρισης διαμόρφωσης και ελέγχου αλλαγών για να αποτρέψει τους εισβολείς να εκμεταλλευτούν ευάλωτες υπηρεσίες και ρυθμίσεις.	[44, 45, 48]
		Διαχείριση Πληροφοριακών Πόρων (Information Resources Management)	Ταξινόμηση όλων των πληροφοριακών πόρων ανάλογα με την κρισιμότητα, την εμπιστευτικότητα και την επιχειρηματική τους αξία.	[48, 49]
		Διαχείριση Παραμετροποίησης Δικτύου (Network Configuration Management)	Καθιέρωση, υλοποίηση και ενεργή διαχείριση παραμετροποίησης ασφαλείας των δικτυακών συσκευών χρησιμοποιώντας μια αυστηρή διαδικασία διαχείρισης και ελέγχου αλλαγών για να αποτρέψει τους εισβολείς να	[31, 32, 44, 45]

			εκμεταλλευτούν ευάλωτες υπηρεσίες και ρυθμίσεις.	
		Διαχείριση Δικτυακών Πόρων (Network Infrastructure Management)	Διαχείριση της συνεχούς λειτουργικής χρήσης θυρών, πρωτοκόλλων και υπηρεσιών σε δικτυακές συσκευές για την ελαχιστοποίηση των παραθύρων ευπάθειας που είναι διαθέσιμα στους εισβολείς.	[44]
		Διαχείριση Πόρων Λογισμικού (Software Assets Management)	Ενεργή τεκμηρίωση, απογραφή και διαχείριση όλων των περιουσιακών στοιχείων εταιρικού λογισμικού, ώστε να διασφαλίζεται η αποτελεσματική προστασία τους.	[31, 32, 44, 48]
		Ασφάλεια Προσωπικού (Personnel Security)	Διαχείριση του κατάλληλου επιπέδου ταυτοποίησης και εξουσιοδότησης που ελέγχει το προσωπικό ή/και την πρόσβαση των επισκεπτών στις φυσικές εγκαταστάσεις του οργανισμού.	[31, 32, 46, 47, 50, 51, 52]
		Φυσική Ασφάλεια (Physical Safety and Security)	Ίδρυση, υλοποίηση και ενεργή διαχείριση της φυσικής ασφάλειας των εγκαταστάσεων.	[31, 32, 45, 46, 48]
	Συνέχεια (Continuity)	Μηχανισμοί Αντιγράφων Ασφαλείας (Backup Mechanisms)	Διαδικασίες δημιουργίας αντιγράφων ασφαλείας που χρησιμοποιούνται για την αποφυγή απώλειας κρίσιμων πληροφοριών παρέχοντας ένα επίπεδο αποδεκτής επιχειρηματικής συνέχειας σε περίπτωση καταστροφικών συμβάντων.	[31, 32]
		Επιχειρησιακή Συνέχεια & Ανακάμψη από Καταστροφή (Business Continuity & Disaster Recovery)	Οι διαδικασίες και τα εργαλεία που χρησιμοποιούνται για τη σωστή δημιουργία αντιγράφων ασφαλείας κρίσιμων πληροφοριών με μια δοκιμασμένη μεθοδολογία για την έγκαιρη ανάκτησή τους.	[31, 32, 44, 45, 46]
		Διαχείριση Χωρητικότητας (Capacity Management)	Διαδικασίες με τις οποίες ο οργανισμός μπορεί να διασφαλίσει ότι οι πόροι της τεχνολογίας πληροφοριών έχουν το σωστό μέγεθος ώστε να ανταποκρίνονται στις τρέχουσες και μελλοντικές επιχειρηματικές απαιτήσεις με	[31, 32]

			οικονομικά αποδοτικό τρόπο.	
		Διαχείριση Αλλαγών (Change Management)	Διαδικασίες που χρησιμοποιούνται για τη διαχείριση τυχόν αλλαγών, εσωτερικών και εξωτερικών, στον οργανισμό.	[31, 32, 53, 54, 55, 56, 57]
		Συνεχής Διαχείριση Ευπαθειών (Continuous Vulnerability Management)	Συνεχής απόκτηση, αξιολόγηση και επεξεργασία νέων πληροφοριών για τον εντοπισμό τρωτών σημείων, την αποκατάσταση και την ελαχιστοποίηση του παραθύρου ευκαιρίας για εισβολείς.	[44]
	Πρόσβαση και Εμπιστοσύνη (Access and Trust)	Διαχείριση Προσβάσεων (Access Management)	Διαδικασίες και εργαλεία που χρησιμοποιούνται για την παρακολούθηση, τον έλεγχο, την πρόληψη και τη διόρθωση της ασφαλούς πρόσβασης σε κρίσιμα περιουσιακά στοιχεία σύμφωνα με τον επίσημο προσδιορισμό των ατόμων, των υπολογιστών και των εφαρμογών που έχουν ανάγκη και δικαίωμα πρόσβασης σε αυτά τα κρίσιμα στοιχεία βάσει εγκεκριμένης ταξινόμησης.	[31, 32, 44, 45, 48]
		Διαχείριση Λογαριασμών (Account Management)	Ενεργή διαχείριση του κύκλου ζωής των λογαριασμών συστήματος και εφαρμογών για να ελαχιστοποιηθούν οι ευκαιρίες να τους εκμεταλλευτούν οι εισβολείς.	[31, 32, 44, 46]
		Επικοινωνία (Communication)	Διάφοροι έλεγχοι με στόχο την προστασία δεδομένων, πληροφοριών και συστημάτων κατά τις διαδικασίες επικοινωνίας.	[31, 32]
		Εξωτερικές Διασυνδέσεις (External Environment Connections)	Δημιουργία και ενεργή διαχείριση των συνδέσεων εξωτερικού περιβάλλοντος του οργανισμού.	[49]
		Ευρωστία και Έκθεση Συνθηματικών (Password Robustness and Exposure)	Μέτρα που λαμβάνει ο οργανισμός για τη διασφάλιση της ευρωστίας του κωδικού πρόσβασης μαζί με τις πολιτικές διαφύλαξης του απορρήτου.	[31, 32, 47]

		Διαχείριση Προνομιακών Λογαριασμών (Privileged Account Management)	Διαδικασίες και εργαλεία που χρησιμοποιούνται για την παρακολούθηση, τον έλεγχο, την πρόληψη και τη διόρθωση της χρήσης, της εκχώρησης και της διαμόρφωσης των δικαιωμάτων διαχειριστών σε υπολογιστές, δίκτυα και εφαρμογές.	[31, 32, 44]
		Διαχωρισμός Ρόλων (Role Segregation)	Σωστός ορισμός ρόλων και ευθυνών διασφαλίζοντας τον διαχωρισμό τους σε διάφορες διαδικασίες για την αποφυγή πιθανής σύγκρουσης συμφερόντων.	[31, 32]
		Σχέσεις Τρίτων (Third-Party Relationships)	Καθορισμός των απαραίτητων απαιτήσεων που πρέπει να πληρούνται από ένα τρίτο προκειμένου να θεωρηθεί αξιόπιστος, παράλληλα με την εφαρμογή των απαραίτητων διαδικασιών με τις οποίες πληρούνται αυτές οι απαιτήσεις.	[31, 32, 49, 58, 59, 60]
		Διαχείριση Ασύρματων Προσβάσεων (Wireless Access Management)	Διαδικασίες και εργαλεία που χρησιμοποιούνται για την παρακολούθηση, τον έλεγχο, την πρόληψη και τη διόρθωση της ασφαλούς χρήσης ασύρματων τοπικών δικτύων (WLAN), σημείων πρόσβασης και συστημάτων ασύρματων πελατών.	[31, 32, 44, 45]
	Λειτουργίες (Operations)	Επιθεώρηση Συμμόρφωσης (Compliance Review)	Έλεγχοι που καθορίζουν το επίπεδο ασφάλειας όπως αυτό ορίζεται από τα αποτελέσματα του ελέγχου ασφαλείας.	[31, 46]
		Πληρότητα Τεκμηρίωσης (Documentation Fulfillness)	Όλη η απαραίτητη τεκμηρίωση συνιστάται να διαθέτει ένας οργανισμός για να διατηρεί ένα κατάλληλο επίπεδο ασφάλειας πληροφοριών.	[31, 32]
		Επαρκής Διαχωρισμός Περιβάλλοντος Ανάπτυξης, Δοκιμών και Παραγωγής (Efficient Distinction of Development, Testing and Operational Environments)	Σαφής διαχωρισμός των περιβαλλόντων ανάπτυξης, δοκιμής και λειτουργίας.	[31, 32, 61]

		Παραγωγικές Διαδικασίες (Operating Procedures)	Καθορισμός λειτουργικών διαδικασιών με έμφαση στην ελαχιστοποίηση της πιθανότητας σφαλμάτων και αθέμιτων πρακτικών.	[31, 32]
		Οργανωτική Κουλτούρα και Υποστήριξη Ανώτερης Διοίκησης (Organizational Culture and Top Management Support)	Προσδιορισμός, καθιέρωση και ενεργή διαχείριση της οργανωτικής κουλτούρας και υποστήριξη της ανώτατης διοίκησης που επηρεάζει και διαμορφώνει τη συνολική κουλτούρα ασφάλειας του οργανισμού.	[32, 45, 49, 60]
		Αξιολόγηση Ρίσκου (Risk Assessment)	Εκτιμήσεις κινδύνου για τον εντοπισμό τρωτών σημείων του οργανισμού που επαναλαμβάνονται σε τακτά χρονικά διαστήματα ή όταν συμβαίνουν σημαντικές αλλαγές.	[32, 59, 61, 62, 63]
	Άμυνα (Defence)	Συνοριακή Προστασία (Boundary Defence)	Ανίχνευση, πρόληψη και διόρθωση της ροής πληροφοριών που μεταφέρεται σε δίκτυα διαφορετικών επιπέδων εμπιστοσύνης με έμφαση σε δεδομένα που βλάπτουν την ασφάλεια.	[44]
		Κρυπτογραφία (Cryptography)	Κρυπτογραφικοί έλεγχοι που χρησιμοποιούνται από τον οργανισμό.	[31, 32]
		Αντίσταση Ηλεκτρονικής Αλληλογραφίας και Διαδικτύου (Email and Web Browser Resilience)	Ελαχιστοποίηση της επιφάνειας επίθεσης και των ευκαιριών για τους εισβολείς να χειραγωγήσουν την ανθρώπινη συμπεριφορά μέσω της αλληλεπίδρασής τους με προγράμματα περιήγησης ιστού και συστήματα ηλεκτρονικής αλληλογραφίας.	[44, 48, 58]
		Πολιτική Ασφάλειας Πληροφοριών και Συμμόρφωση (Information Security Policy and Compliance)	Καθιέρωση, εφαρμογή και ενεργή διαχείριση πολιτικών ασφάλειας πληροφοριών και συμμόρφωση με αυτές.	[32, 49, 57, 62, 64, 65, 66]
		Άμυνα από Κακόβουλο	Έλεγχοι που αφορούν την εγκατάσταση, τη διάδοση και την	[31, 32, 44]

		Λογισμικό (Malware Defence)	εκτέλεση κακόβουλου κώδικα σε πολλαπλά οργανωτικά σημεία, ενώ βελτιστοποιούν τη χρήση αυτοματισμών με στόχο την ταχεία ενημέρωση της άμυνας, τη συλλογή δεδομένων και τις διορθωτικές ενέργειες.	
		Πρόγραμμα Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια (Security Awareness and Training Program)	Αναγνώριση ειδικών γνώσεων, δεξιοτήτων και ικανοτήτων που απαιτούνται για την υποστήριξη της υπεράσπισης του οργανισμού. Ανάπτυξη και εκτέλεση ενός ολοκληρωμένου σχεδίου για την αξιολόγηση, τον εντοπισμό κενών και την αποκατάσταση μέσω προγραμμάτων, οργανωτικού σχεδιασμού, κατάρτισης και ευαισθητοποίησης.	[44, 46, 47, 48, 50, 67, 68, 69, 70, 71]
	Διακυβέρνηση Ασφάλειας (Security Governance)	Διαχείριση Αρχείων Καταγραφής Ελέγχου (Audit Logs Management)	Συλλογή, διαχείριση και ανάλυση αρχείων καταγραφής συμβάντων που θα μπορούσαν να βοηθήσουν στον εντοπισμό, την κατανόηση ή την ανάκαμψη από επιθέσεις.	[31, 32, 44]
		Απόκριση και Διαχείριση Περιστατικών (Incident Response and Management)	Προστασία των πληροφοριών του οργανισμού, καθώς και της φήμης του, με την ανάπτυξη και την εφαρμογή υποδομής αντιμετώπισης συμβάντων.	[31, 32, 44, 48, 49]
		Ασκήσεις Διείσδυσης και Κόκκινης Ομάδας (Penetration Tests and Red Team Exercises)	Δοκιμή της συνολικής αντοχής της άμυνας ενός οργανισμού προσομοιώνοντας τους στόχους και τις ενέργειες ενός επιτιθέμενου.	[44, 45, 58]
		Μηχανισμοί Αναφορών (Reporting Mechanisms)	Κανάλια που χρησιμοποιεί ο οργανισμός για τους υπαλλήλους ή άλλα σχετικά μέρη για την αναφορά τρωτών σημείων ή περιστατικών που εντοπίστηκαν.	[31, 32, 48, 67]
		Ωριμότητα Διαχείρισης Ασφαλείας (Security Management Maturity)	Έλεγχοι αξιολόγησης της ωριμότητας διαχείρισης ασφάλειας ενός οργανισμού.	[32, 49, 62, 72]
Ατομικό	**Στάση (Attitude)**	Εργασιακό Κλίμα (Employee Climate)	Αξιολόγηση της ικανοποίησης που έχει κάθε εργαζόμενος από την ασφάλεια πληροφοριών, επηρεάζοντας άμεσα τη	[28, 51, 52, 73, 74, 75, 76]

			συμπεριφορά ασφαλείας του.	
		Εργασιακό Προφίλ (Employee Profiling)	Γενικό εργασιακό προφίλ που συμβάλει στον εντοπισμό πιθανών προτύπων συμπεριφοράς ασφάλειας.	[28, 77, 78, 79, 80]
		Εργασιακή Ικανοποίηση (Employee Satisfaction)	Αξιολόγηση της ικανοποίησης που έχει κάθε εργαζόμενος τόσο προς τον οργανισμό όσο και προς άλλους συναδέλφους και η οποία επηρεάζει άμεσα τη συμπεριφορά ασφαλείας του/της.	[4, 31, 32, 53, 55, 68, 79]
	Επίγνωση (Awareness)	Επίγνωση Πολιτικών και Διαδικασιών (Policies and Procedures Awareness)	Αξιολόγηση της γνώσης που έχει κάθε εργαζόμενος σχετικά με τις πολιτικές και τις διαδικασίες ασφαλείας του οργανισμού.	[73, 81]
		Επίγνωση Ρόλων και Καθηκόντων (Roles and Responsibilities Awareness)	Αξιολόγηση της γνώσης που έχει κάθε εργαζόμενος σχετικά με το ρόλο και τις ευθύνες του αναφορικά με την ασφάλεια πληροφοριών.	[9, 31, 32]
	Συμπεριφορά (Behaviour)	Συμμόρφωσης στις Πολιτικές και Διαδικασίες (Policies and Procedures Compliance)	Έλεγχος και καταγραφή τυχόν παραβιάσεων πολιτικών και διαδικασιών ασφαλείας από υπαλλήλους ή άλλα επηρεαζόμενα μέρη.	[31, 32, 62, 73, 82]
		Security Agent Persona	Προσδιορισμός του συναίσθησης της ασφάλειας που τείνουν να εκδηλώνουν τα άτομα σε καθημερινή βάση στο χώρο εργασίας τους.	[77, 83]
		Συμπεριφορά Ασφαλείας (Security Behaviour)	Συμπεριφορά ασφάλειας που επιδεικνύεται σε καθημερινή βάση στο χώρο εργασίας.	[9, 74]
	Ικανότητα (Competency)	Εργασιακή Ικανότητα (Employee Competency)	Ο προσδιορισμός της ικανότητας που απαιτείται για κάθε ρόλο και ευθύνη μαζί με την τεκμηριωμένη απόδειξη ικανότητας που φέρει κάθε εργαζόμενος.	[31, 32]
		Αξιολόγηση Δεξιοτήτων Ασφαλείας (Security Skills	Δεξιότητες ασφάλειας, εξοικείωση και αξιολόγηση	[65, 79, 84]

		Evaluation)	ευαισθητοποίησης.	
		Ολοκλήρωση Εκπαίδευσης και Βαθμολόγηση (Training Completion and Scoring)	Καταγραφή τυχόν εκπαιδευτικών προγραμμάτων που παρακολούθησαν άτομα μαζί με βαθμολόγηση, ποσοστό πληρότητας και αξιολόγηση της αποτελεσματικότητάς τους.	[31, 32]

Στη συνέχεια, κάθε τομέας αναλύεται σε έναν αριθμό ***ελέγχων*** (***controls***) που ποικίλλουν από απλές Ναι/Όχι, Likert ή πολλαπλών επιλογών ερωτήσεις που αφορούν ποσοτικούς και ποιοτικούς παράγοντες ασφαλείας. Κάθε στοιχείο ελέγχου έχει διαφορετική βαρύτητα στο αποτέλεσμα της αξιολόγησης του εκάστοτε τομέα προκειμένου να αποδοθεί η διαφορετική βαρύτητα και, ως εκ τούτου, ο ειδικός παράγοντας αντίκτυπου που έχει στη διαμόρφωση κουλτούρας κυβερνοασφάλειας.

Οι έλεγχοι αξιολογούνται χρησιμοποιώντας διαφορετικές τεχνικές ανάλογα με τη φύση και τη σημασία τους [85]:

- **Ερωτηματολόγια** (**Questionnaires**): ευρέως χρησιμοποιούμενα για τους ελέγχους που αφορούν τους τομείς οργανωτικού επίπεδου. Είναι σύντομα, κατανοητά και στοχευμένα με στόχο τη διευκόλυνση των συνεντευξιαζόμενων.
- **Προσομοιώσεις** (**Simulations**): καλύπτουν ένα ευρύ φάσμα τεχνουργημάτων όπως phishing email, τεχνικές απάτης μέσων κοινωνικής δικτύωσης (social media fraud techniques), μόλυνση από ιό σταθμού εργασίας (workstation virus contamination), κ.λπ.
- **Δοκιμές** (**Tests**): ποικίλουν από χρηστο-κεντρικές σε πραγματικό χρόνο, όπως για παράδειγμα στιβαρότητα κωδικού πρόσβασης, έκθεση ηλεκτρονικού ταχυδρομείου, ανθεκτικότητα σε ransomware, έως και εκτεταμένων οργανωτικών στοχευμένων, όπως πλαστογράφηση τομέα (domain spoofing), αντίσταση διακομιστή αλληλογραφίας κ.λπ.
- **Σοβαρά παιχνίδια** (**Serious Games**): χρησιμοποιούνται όχι μόνο ως πιο αξιόπιστες μέθοδοι αξιολόγησης, αλλά και λόγω του διδακτικού τους χαρακτήρα και των εντυπωσιακών διδακτικών αποτελεσμάτων τους.
- Απλή παρατήρηση, αναφορά από διαφορετικές πηγές και διασταυρούμενη ανάλυση των συλλεγόμενων πληροφοριών.

Το προτεινόμενο μοντέλο ισχύει για κάθε μέγεθος και είδος οργανισμού ανεξάρτητα από τον επιχειρηματικό του τομέα, την εξειδίκευση, την τεχνολογική του κατάσταση και την ετοιμότητα αναφορικά με την Ασφάλεια Πληροφοριών. Μπορεί επίσης να χρησιμοποιηθεί από οποιαδήποτε επιχειρησιακή δομή που καταδεικνύει μια σαφή διάκριση μεταξύ ενός συμβουλίου λήψης αποφάσεων και μιας μονάδας παραγωγής. Μπορεί να προσαρμοστεί σε οποιοδήποτε επιχειρηματικό πεδίο βαθμονομώντας τους ελέγχους που ορίζονται για κάθε τομέα. Επιπλέον, μπορεί να επεκταθεί και να προσαρμοστεί στο συνεχώς μεταβαλλόμενο επιχειρηματικό περιβάλλον.

3.3 Μέθοδος Αξιολόγησης

Το προτεινόμενο μοντέλο αναπαριστά τους βασικούς παράγοντες ασφαλείας με όλες τις αλληλεξαρτήσεις, τις επιρροές και τις ποικιλίες τους. Το επόμενο βήμα ήταν ο καθορισμός μιας μεθόδου αξιολόγησης η οποία όχι μόνο θα επέτρεπε σε έναν οργανισμό να αναπαραστήσει την καθημερινή του πραγματικότητα κυβερνοασφάλειας, αλλά και θα βοηθούσε ενεργά στον εντοπισμό των τρωτών σημείων και των αδυναμιών του.

Η μέθοδος αξιολόγησης (Εικόνα 7) αποτελείται από σαφώς καθορισμένα και διακριτά βήματα:

- Η απόφαση διενέργειας αξιολόγησης ασφάλειας (***Decision Making***), είτε ως πρωτοβουλία ενός οργανωτικού συμβουλίου είτε (πιο πιθανό σενάριο) ως απόρροια

της ανάγκης άμυνας ενάντια στις πολυάριθμες απειλές της τρέχουσας κυβερνο-πραγματικότητας (πιθανόν μετά από ένα απροσδόκητο περιστατικό ασφαλείας).

- Η ομάδα λήψης αποφάσεων, γνωρίζοντας τους πραγματικούς λόγους πίσω από αυτό το εγχείρημα, πρέπει να θέσει τους στόχους και να προδιαγράψει σαφώς τις επιχειρησιακές απαιτήσεις (***Targeting***). Ανάλογα με τις προσδοκίες τους, η συνολική μεθοδολογία θα προσαρμοστεί και θα στοχεύσει σε συγκεκριμένες ομάδες και τομείς ασφάλειας.
- Επαναλήψεις αξιολόγησης, αποκαλούμενες αξιολογητικές εκστρατείες (***Assessment Campaigns***), σχεδιάζονται από διευθυντές και αρχηγούς ομάδων με κατάλληλες προσαρμογές στις διαφορετικές ομάδες χρηστών ή ακόμα και οργανωτικά τμήματα. Σύμφωνα με τη μεθοδολογία 4W1H [86], οι εκστρατείες αξιολόγησης καλούνται να απαντήσουν στις ακόλουθες ερωτήσεις:
  - ***What*** - Ποιες διαστάσεις και τομείς, με άλλα λόγια, ποιοι παράγοντες ασφαλείας θα αξιολογηθούν;
  - ***Who*** - Ποιους θα στοχεύει και θα αξιολογεί η εκστρατεία; Ποιοι θα συμμετέχουν στην εκστρατεία;
  - ***When*** - Πότε θα πραγματοποιηθεί;
  - ***Where*** - Πού θα επικεντρωθεί η εκστρατεία; Ο πρωταρχικός στόχος της αξιολόγησης.
  - ***How*** - Πώς θα αξιολογηθούν οι παράγοντες ασφάλειας; Χρησιμοποιώντας ποιες μεθόδους και τεχνικές;

  Έχοντας υπόψη τα αποτελέσματα στόχευσης του προηγούμενου βήματος, βαθμονομούν και σχεδιάζουν προσεκτικά και συνεργατικά τη διαδικασία αξιολόγησης που πραγματοποιείται στο επόμενο βήμα.
- Χρησιμοποιώντας δοκιμασμένες τεχνικές, όπως δοκιμή, εξέταση, συνεντεύξεις [17, 87], προσομοίωση, gamification [85], κ.λπ. συλλέγουν όσο το δυνατόν περισσότερες πληροφορίες από τους συμμετέχοντες (***Evaluation Procedures***).

Εικόνα 7. Μέθοδος αξιολόγησης κουλτούρας κυβερνοασφάλειας

- Φτάνοντας στο πιο απαιτητικό βήμα της μεθοδολογίας, τα αποτελέσματα συγκεντρώνονται και αναλύονται καταλήγοντας σε μια σειρά γραφικών αναπαραστάσεων και αναφορών σε ατομικό, αλλά και οργανωτικό επίπεδο (***Results Elaboration***). Χρησιμοποιώντας τα αποτελέσματα της μεθοδολογίας αξιολόγησης κάθε συμμετέχοντα, η μεθοδολογία προχωρά στην κατάλληλη ομαδοποίηση τους μαζί με τα οργανωτικά δεδομένα παράγοντας κατάλληλες βαθμολογίες για τμήματα, μονάδες και τελικά για τον οργανισμό στο σύνολό του.
- Τέλος, τα αξιολογητικά αποτελέσματα επισημαίνουν τις υπάρχουσες αδυναμίες ασφάλειας και κενά υποβοηθώντας στην εξατομίκευση και προσαρμογή των εκπαιδευτικών προγραμμάτων ασφάλειας στις ανάγκες του κάθε χρήστη. Προτάσεις και συστάσεις παρέχονται τόσο στους μισθωτούς όσο και στα μέλη της διοίκησης ενώ το συμβούλιο λήψης αποφάσεων διαθέτει πλέον πολύτιμη γνώση για την κουλτούρα κυβερνοασφαλείας του οργανισμού καθώς για τα τρωτά της σημεία. Πολύτιμα εφόδια για την έναρξη ενός νέου αξιολογητικού κύκλου (***Decision Making***).

Ένα ενδεικτικό-απλουστευμένο παράδειγμα εφαρμογής της ανωτέρω μεθοδολογίας αξιολόγησης είναι το ακόλουθο: Οι υπεύθυνοι ασφαλείας (Security Officers) της εταιρείας Χ έχουν ενημερωθεί από το κέντρο επιχειρήσεων ασφαλείας (Security Operations Center, SOC) ότι ένας μεγάλος αριθμός ηλεκτρονικών μηνυμάτων απάτης φτάνουν στο τμήμα Marketing. Μετά από περαιτέρω διερεύνηση και έχοντας εντοπίσει κακή χρήση των κοινωνικών δικτύων από το συγκεκριμένο τμήμα που διαχειρίζεται την ψηφιακή παρουσία της εταιρίας στο διαδίκτυο, λαμβάνουν την απόφαση να εκτελέσουν μια στοχευμένη εκστρατεία αξιολόγησης (campaign) για το συγκεκριμένο τμήμα. Εστιάζοντας στη χρήση ηλεκτρονικού ταχυδρομείου, διαδικτύου και μέσων κοινωνικής δικτύωσης, περιλαμβάνουν στην αξιολόγηση έναν αριθμό σχετικών ερωτηματολογίων, δοκιμές προσομοίωσης phishing, παιχνίδια κοινωνικής δικτύωσης και ηλεκτρονικού ταχυδρομείου και ελέγχους έκθεσης κωδικού πρόσβασης. Μετά το πέρας της εκστρατείας, οι υπεύθυνοι ασφαλείας συγκεντρώνουν τα αποτελέσματα και μέσω μια γραφικής αναπαράστασης είναι σε θέση να κατανοήσουν τόσο τα τρωτά σημεία ασφαλείας που αντιμετωπίζουν, όσο και το βαθμό επικινδυνότητάς για καθένα από αυτά. Οι χρήστες θα δέχονταν και θα ενεργοποιούσαν έναν ιό που ελήφθη ως συνημμένο ενός μηνύματος ηλεκτρονικός αλληλογραφίας; Θα απαντούσε κάποιος σε ένα παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου παρέχοντας σημαντικές προσωπικές ή εταιρικές πληροφορίες; Κατανοούν τους κινδύνους που καλούνται να αντιμετωπίσουν ως μέλη του τμήματος Δημοσίων Σχέσεων και Marketing (διαθεσιμότητα και έκθεση των διευθύνσεων ηλεκτρονικού ταχυδρομείου στο ευρύ κοινό); Συμμορφώνονται με τις πολιτικές κωδικών πρόσβασης της εταιρίας; Γνωρίζοντας πού απέτυχαν οι περισσότεροι υπάλληλοι, μπορούν να ενισχύσουν την άμυνα του οργανισμού με προσαρμογή των υφιστάμενων τεχνολογικών πόρων για την προστασία τους και, το πιο σημαντικό, να επενδύσουν χρόνο και προσπάθεια στην εκπαίδευση τους ενάντια στις κυβερνοαπειλές που καλούνται να αντιμετωπίσουν. Το πιο σημαντικό ωστόσο είναι ότι, μέσω της διαδικασίας αξιολόγησης, έχουν ήδη κινητοποιηθεί ξεκινώντας μια πολιτισμική ζύμωση ασφαλείας.

3.4 Συσχέτιση με Υφιστάμενα Πλαίσια Ασφαλείας

3.4.1 Μελέτη Εσωτερικής Απειλής (Insider Threat Study)

Στην ***Εσωτερική Απειλή*** (***Insider Threat***) έχουν αποδοθεί πολυάριθμοι ορισμοί όλα αυτά τα χρόνια. Μια έκθεση εργαστηρίου το 2004 όρισε την εσωτερική απειλή ως «*ένα κακόβουλο άτομο που ενεργεί είτε μόνο του είτε σε συνεννόηση με κάποιον εξωτερικό αυτών των συστημάτων*» [88]. Ο Bishop καθορίζει την εσωτερική απειλή ως συμβάν που λαμβάνει χώρα όταν «*μια αξιόπιστη οντότητα καταχράται την εξουσία που της έχει παραχωρηθεί για να παραβιάσει έναν ή περισσότερους κανόνες μιας δεδομένης πολιτικής ασφάλειας*» [89]. Σύμφωνα με τον Greitzer, «*η εσωτερική απειλή σχετίζεται με κακόβουλες πράξεις έμπιστων ατόμων. Για παράδειγμα, κάτι που προκαλεί βλάβη στον οργανισμό ή μια μη εξουσιοδοτημένη πράξη που ωφελεί ένα άτομο*» [90]. Οι Hunker και Probst υποστηρίζουν ότι «*μια εσωτερική απειλή τίθεται από ένα άτομο με προνόμια που τα καταχράζεται ή του οποίου η πρόσβαση οδηγεί σε κακή χρήση*» [91].

Το CERT National Insider Threat Center [92] προχωρά στον ορισμό τόσο του κακόβουλου έμπιστου προσώπου (***malicious insider***):

> «*ενός υπαλλήλου, εργολάβου ή επιχειρηματικού συνεργάτη που έχει ή είχε εξουσιοδοτημένη πρόσβαση στο δίκτυο, το σύστημα ή τα δεδομένα ενός οργανισμού και έχει εσκεμμένα προβεί σε υπέρβαση ή χρήση αυτής της πρόσβασης με τρόπο που επηρέασε αρνητικά την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα ή τη φυσική ευημερία των πληροφοριών, των συστημάτων πληροφοριών ή του εργατικού δυναμικού του οργανισμού*»

όσο και του ακούσιου εσωτερικού (***unintentional insider***):

> «*νυν ή πρώην υπάλληλος, εργολάβος ή άλλος επιχειρηματικός εταίρος που έχει ή είχε εξουσιοδοτημένη πρόσβαση στο δίκτυο, το σύστημα ή τα δεδομένα ενός οργανισμού και ο οποίος, μέσω της δράσης/αδράνειάς του χωρίς κακόβουλη πρόθεση προκαλεί βλάβη ή αυξάνει σημαντικά την πιθανότητα μελλοντικής σοβαρής βλάβης στην εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των πληροφοριών ή των συστημάτων πληροφοριών του οργανισμού*».

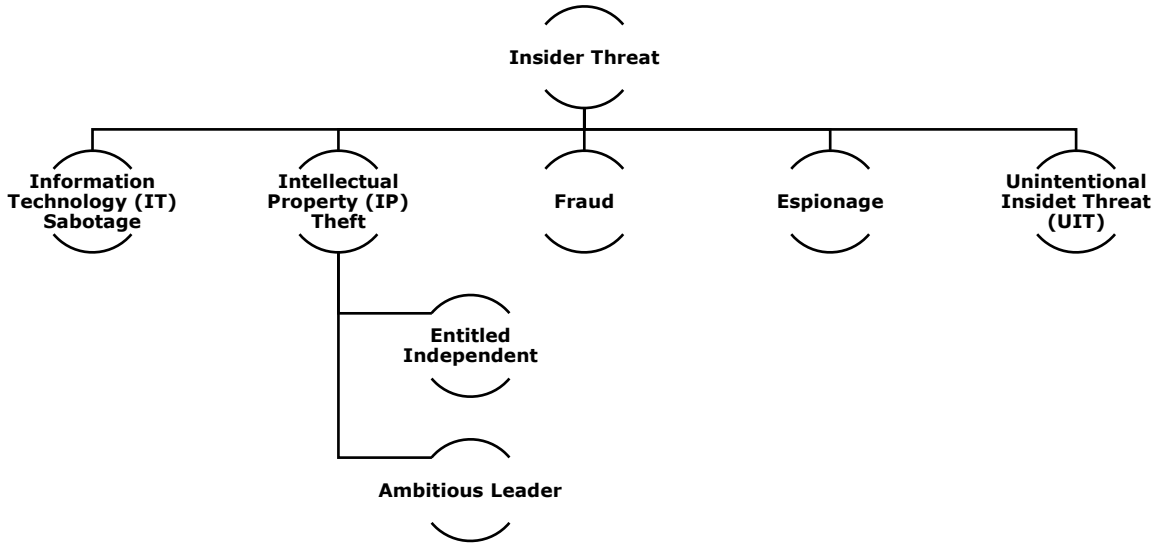
Δεν αποτελεί έκπληξη το γεγονός ότι μια αναλογική ποικιλία ταξινομήσεων εσωτερικών απειλών μπορεί να βρεθεί στη βιβλιογραφία [93]. Μία από τις παλαιότερες ταξινομήσεις προτάθηκε από τον Anderson το 1980, ο οποίος διέκρινε τρεις τύπους παράνομων εσωτερικών χρηστών [94]:

- ***Masquerader***: μπορεί να είναι είτε ένας εξωτερικός διεισδυτής που έχει καταφέρει να παρακάμψει τους ελέγχους ασφαλείας, είτε ένας υπάλληλος με πλήρη πρόσβαση σε ένα σύστημα υπολογιστή που σκοπεύει να εκμεταλλευτεί τα διαπιστευτήρια ενός άλλου νόμιμου χρήστη.
- ***Νόμιμος χρήστης***: που δεν αποκρύπτει την ταυτότητά του, αλλά καταχράται τα δικά του προνόμια για να κάνει κακή χρήση του συστήματος, και
- ***Κρυφός Χρήστης***: ο οποίος έχει ή μπορεί να καταλάβει εποπτικούς ελέγχους παραμένοντας εκτός της ανίχνευσης και εντοπισμού των υποδομών ασφαλείας.

Μια πολύ παρόμοια προσέγγιση παρουσιάστηκε από τους Salem και λοιπούς πολλά χρόνια αργότερα, το 2008, διακρίνοντας δύο κατηγορίες επιθέσεων εμπιστευτικών πληροφοριών: μεταμφιεσμένους (***masqueraders***) και προδότες (***traitors***) [95]. Οι ***masqueraders***

ορίστηκαν ως εισβολείς που καταφέρνουν να κλέψουν την ταυτότητα νόμιμων χρηστών και υποδύονται άλλους χρήστες για κακόβουλους σκοπούς, ενώ οι ***traitors*** είναι νόμιμοι χρήστες σε έναν οργανισμό που τους έχει παραχωρηθεί πρόσβαση σε συστήματα και πόρους πληροφοριών, αλλά των οποίων οι ενέργειες είναι αντίθετες με την πολιτική του οργανισμού και στόχος τους είναι να επηρεάσουν αρνητικά το απόρρητο, την ακεραιότητα ή τη διαθεσιμότητα ορισμένων περιουσιακών στοιχείων πληροφοριών.

Υπάρχουν πολλές παρόμοιες προσεγγίσεις που υπογραμμίζουν ξεκάθαρα τα κίνητρα πίσω από τη συμπεριφορά και τις ενέργειες των εσωτερικών απειλών διαφοροποιώντας τις σκόπιμες από τις ακούσιες παραβιάσεις ασφάλειας. Ταξινομήσεις εσωτερικών απειλών βάσει διαφορετικών κριτηρίων, όπως η επαγγελματική σχέση ή οι πιθανές συνέπειες και η βλάβη στον οργανισμό που παραβιάστηκε ή ακόμη και με βάση το στοχευόμενο σύστημα [96, 97, 98].



Εικόνα 8. Τύποι εσωτερικών απειλών κατά CERT

Μία από τις πιο αναγνωρίσιμες και κοινά αποδεκτές κατηγοριοποιήσεις εσωτερικών απειλών είναι αυτή που προτείνεται από το «Insider Threat Study», ένα έργο που διεξάγεται από κοινού τη Μυστική Υπηρεσία Ηνωμένων Πολιτειών (Secret Service) και το Πρόγραμμα CERT Software Engineering Institute στο Πανεπιστήμιο Carnegie Mellon [99, 100, 101, 102, 103, 104, 105, 106]. Από το 2001, το CERT National Insider Threat Center έχει πραγματοποιήσει μια ποικιλία ερευνητικών έργων σχετικά με την εσωτερική απειλή που βασίζονται σε ένα διευρυμένο σύνολο περισσότερων από 1.500 υποθέσεων σε οργανισμούς από όλους τους τομείς [92, 107, 108, 109]. Η επιστημονική τους συνεισφορά αποδεικνύεται μέσω ποικίλων δημοσιεύσεων σε όλη τη μακροχρόνια παρουσία τους στο χώρο [110, 111, 112, 113, 114]. Αν και οι μέθοδοι επίθεσης ποικίλλουν ανάλογα με τον κλάδο, έχουν εντοπίσει, αναλύσει και παρουσιάσει μέσω πολλών τεχνικών αναφορών τους κύριους τύπους εσωτερικών απειλών και τις υποκατηγορίες τους (Εικόνα 8):

- Δολιοφθορά Τεχνολογίας Πληροφοριών (***Information Technology Sabotage, ITS)***: Χρήση της τεχνολογίας πληροφοριών για άμεση στοχευμένη βλάβη σε έναν οργανισμό ή ένα άτομο ατομική [115].
- Κλοπή Πνευματικής Ιδιοκτησίας (***Intellectual Property Theft, IPT***): Σκόπιμη κατάχρηση των διαπιστευτηρίων κάποιου για κλοπή εμπιστευτικών ή αποκλειστικών πληροφοριών από τον οργανισμό [116, 117].

- Ανεξάρτητος Δικαιούχος (***Entitled Independent***): Ένας έμπιστος άνθρωπος που ενεργεί πρωτίστως μόνος για να κλέψει πληροφορίες για μια νέα δουλειά ή δική του δευτερεύουσα επιχείρηση.
- Φιλόδοξος Ηγέτης (***Ambitious Leader***): Ένας εγκληματίας-ηγέτης που στρατολογεί εσωτερικούς για να κλέψει πληροφορίες για απώτερους σκοπούς.

❖ Απάτη (***Fraud***): Μη εξουσιοδοτημένη τροποποίηση, προσθήκη ή διαγραφή δεδομένων ενός οργανισμού για προσωπικό όφελος ή κλοπή πληροφοριών που οδηγούν σε έγκλημα ταυτότητας (π.χ. κλοπή ταυτότητας, απάτη πιστωτικών καρτών) [101].

❖ Κατασκοπεία (***Espionage***): Απόκτηση, παράδοση, μετάδοση, επικοινωνία ή λήψη πληροφοριών σχετικών με την εθνική άμυνα με πρόθεση ή σκοπό να βλάψουν τη χώρα ή να ωφελήσουν ένα ξένο κράτος [99].

❖ Μη σκόπιμη εσωτερική απειλή (***Unintentional Insider Threat***, ***UIT***): Επηρεάζει αρνητικά την εμπιστευτικότητα, διαθεσιμότητα ή ακεραιότητα ενός οργανισμού, μέσω δράσης ή αδράνειας χωρίς κακόβουλη πρόθεση [118].

Η προαναφερθείσα κατηγοριοποίηση έχει χρησιμοποιηθεί για την ταξινόμηση μια συνεχώς εξελισσόμενης βάσης δεδομένων περιστατικών εσωτερικών απειλών που διατηρεί το Software Engineering Institute. Ταυτόχρονα, πολλοί ερευνητές έχουν βασιστεί σε αυτή τη διαρκή προσπάθεια περαιτέρω διερεύνησης, ανάλυσης και μελέτης του φαινομένου της εσωτερικής απειλής. Για τους λόγους αυτούς, το συγκεκριμένο πλαίσιο εσωτερικής απειλής χρησιμοποιήθηκε από το προτεινόμενο Πλαίσιο Κουλτούρας Κυβερνοασφάλειας για τον εντοπισμό και την ανάδειξη εσωτερικών απειλών σε έναν οργανισμό.

3.4.1.1 Παράγοντες Εσωτερικής Απειλής

Αρχικά, πραγματοποιήσαμε μια κριτική ανασκόπηση των ερευνητικών προσεγγίσεων της επιστημονικής κοινότητας, των διαθέσιμων ευρημάτων της εμπειρικής βιβλιογραφίας και των μαρτυριών των επαγγελματιών του χώρου της κυβερνοασφάλειας. Αυτή η αναθεώρηση είχε ως αποτέλεσμα την αναγνώριση και καταγραφή μιας σειράς συμπεριφορικών και τεχνικών, ατομικών και οργανωτικών, ποιοτικών και ποσοτικών δεικτών που πρακτικά επηρεάζουν και διαμορφώνουν γόνιμο έδαφος για εσωτερικές απειλές και παρουσιάζονται συνοπτικά στον Πίνακας 4.

Πίνακας 4. Τύποι εσωτερικών απειλών και συνεισφέροντες παράγοντες

Τύπος Εσωτερικής Απειλής	Συνεισφέρων παράγοντας	Πηγές
Information Technology Sabotage (ITS)	Dissatisfaction	[108, 119, 120, 121]
	Personality predispositions	[118, 120, 121]
	Type of position (Access, Knowledge, Privileges, Skills)	[88, 108, 119, 121, 122]

	Gender	[108, 119]
	Concerning Behaviours	[88, 108, 120, 121]
	Lack of Physical and Electronic Access Controls	[120]
Intellectual Property Theft (IPT)	Dissatisfaction (only for *Entitled Independent*)	[99, 117, 123, 124]
	Type of position	[88, 117, 122, 125]
	Gender	[117, 125]
	Sense of ownership/entitlement	[117, 123]
Fraud	Enterprise Role (Access, Knowledge, Privileges, Skills)	[109]
	Age, tenure & level of seniority	[109]
	Policy violation	[109]
	Lack of Physical and Electronic Access Controls	[109]
	Lack of Auditing	[109]
Espionage	Personality predispositions	[120, 126]
	Concerning Behaviours	[120, 126]
	Rule violation	[120]
	Stressful Events	[88, 120, 126]
	Lack of Physical and Electronic Access Controls	[120]
	Lack of Detection of Rule Violations	[120]
Unintentional Insider Threat (UIT)	Fatigue or sleepiness	[118, 127]
	High Subjective mental workload	[118, 127]
	Lack of situation awareness	[118, 127]
	Mind wandering	[118, 127]

	Framing	[118, 127]
	Cognitive limitations, biases, or faulty reasoning	[118, 127]
	Personality predispositions	[88, 118, 126, 127, 128, 129]
	Concerning Behaviours	[88, 118, 127, 129, 130]
	Age, gender, culture	[118, 127, 128]
	Mood	[118]
	Influence of physical states, drugs or hormone imbalances	[88, 118, 127]
	Business processes and environment (work planning and control, data flow, work setting)	[118, 127]

Το επόμενο λογικό βήμα ήταν η ταξινόμηση των παραγόντων εσωτερικής απειλής σε γενικότερες κατηγορίες που τους ενοποιούν και τους οριοθετούν σε μετρήσιμους δείκτες ασφαλείας που μπορούν να ποσοτικοποιηθούν και μετρηθούν από ένα πλαίσιο κουλτούρας κυβερνοασφάλειας. Με βάση τη σημασιολογική τους ερμηνεία αναλύσαμε τους ορισμούς και τις μεθόδους αξιολόγησης των διαφόρων πηγών της βιβλιογραφίας εντοπίζοντας τις επικαλύψεις, σχέσεις και μεταξύ τους αλληλεπιδράσεις καταλήγοντας στις ενοποιήσεις και ταξινομήσεις που παρουσιάζονται στον Πίνακας 5.

Πίνακας 5. Τύποι εσωτερικών απειλών και κανονικοποιημένοι συνεισφέροντες παράγοντες

	Ορισμός	ITS	IPT	Fraud	Espionage	UIT
1 – Δυσαρέσκεια (Dissatisfaction)	Αγχωτικά γεγονότα, είτε σχετιζόμενα με την εργασία είτε προσωπικά, συνήθως προηγούνται των επιθέσεων εσωτερικής απειλής [107, 108, 120, 131]. Παραδείγματα τέτοιων γεγονότων περιλαμβάνουν απόλυση εργαζομένων, διαφωνίες με εργοδότες, αντιληπτές αδικίες, μεταθέσεις ή υποβιβασμούς, μειώσεις μισθών, οικογενειακά προβλήματα [132, 133]. Η δυσαρέσκεια που προκύπτει από αυτά τα γεγονότα πυροδοτεί συμπεριφορές σε άτομα με προδιάθεση για κακόβουλες πράξεις.	●	● (only for Entitled Independent)		●	●
2 - Προδιαθέσεις προσωπικότητας (Personality predispositions)	Οι προδιαθέσεις προσωπικότητας περιλαμβάνουν σοβαρές διαταραχές ψυχικής υγείας, ζητήματα προσωπικότητας (π.χ. έλλειψη αυτοεκτίμησης, πρότυπα μεροληπτικής αντίληψης για τον εαυτό του/της και τους άλλους), εθισμούς, ελλείμματα κοινωνικών δεξιοτήτων και αδυναμία/δυσκολία λήψης αποφάσεων, ιστορικό παραβιάσεων νομικού τύπου, ασφάλειας ή διαδικαστικών κανόνων [88, 126, 128, 129]. Συγκεκριμένα χαρακτηριστικά της προσωπικότητας, όπως η εξωστρέφεια, η κοινωνικότητα, η ευχαρίστηση, η ευσυνειδησία, η αντίληψη του κινδύνου και η ανεκτικότητα, τα οποία έχουν προσδιοριστεί ως σχετιζόμενα με συγκεκριμένες συμπεριφορές ασφάλειας, έχουν επίσης συμπεριληφθεί σε αυτόν τον γενικό όρο [128, 130].	●			●	●
3 – Επιχειρησιακός ρόλος (Enterprise role)	Η θέση που κατέχει ένας εσωτερικός χρήστης σε έναν οργανισμό (π.χ. τεχνική, διευθυντική) μαζί με τις ειδικές δεξιότητες, γνώσεις, προνόμια (π.χ. διαχειριστής τομέα ή συστήματος, προχωρημένος χρήστης) και την παραχωρούμενη πρόσβαση που ενδέχεται να διαφοροποιήσουν σοβαρά τόσο τη δυνατότητα όσο και τον τύπο της απειλής κατά της επιχείρησης στην οποία εργάζεται [88, 107, 119, 121, 122].	●	●	●		

4 – Ανησυχητική συμπεριφορά (Concerning behaviour)	Ανησυχητικές συμπεριφορές, συμπεριλαμβανομένων παραβιάσεων προσωπικού και ασφάλειας, προηγούνται της συντριπτικής πλειοψηφίας περιπτώσεων εσωτερικών απειλών [120]. Παραδείγματα τέτοιων συμπεριφορών περιλαμβάνουν καθυστερήσεις, απουσίες, καυγάδες με συναδέλφους, κακή εργασιακή απόδοση, παραβιάσεις ασφάλειας [88, 108, 120, 121, 127].	●		●	●
5 – Εργασιακό προφίλ (Employee profile)	Το εργασιακό προφίλ, που αντικατοπτρίζει μια σειρά ανθρώπινων χαρακτηριστικών όπως η ηλικία, το φύλο, η εμπειρία, η παλαιότητα, έχει υπογραμμιστεί σε πολλές περιπτώσεις περιστατικών εσωτερικής απειλής και έχει αναδειχθεί σε ένα σημαντικό παράγοντα που συμβάλλει στη συνολική προδιάθεση εσωτερικής απειλής [108, 119]. Εφόσον αυτά τα χαρακτηριστικά είναι μόνο παράμετροι σε ένα πολυδιάστατο ζήτημα, είναι δίκαιο να ομαδοποιηθούν και να εξεταστούν συνδυαστικά.	●	●	●	●
6 – Έλεγχοι προσβάσεων (Access Controls)	Οι έλεγχοι φυσικής πρόσβασης (περιορισμοί στην απόκτηση πρόσβασης σε οργανωτικές εγκαταστάσεις) ή/και οι έλεγχοι απομακρυσμένης πρόσβασης (περιορισμοί στους υπολογιστικούς πόρους και τους δικτυακούς πόρους της επιχείρησης) ενισχύουν την άμυνα του οργανισμού έναντι της εσωτερικής απειλής [120]. Ωστόσο, η έλλειψη αυτών των ελέγχων ή οι πιθανές ελλείψεις στην επιβολή τους ενθαρρύνουν σημαντική τα περιστατικά εσωτερικών παραβιάσεων [109].	●		●	●
7 – Αίσθηση δικαιώματος (Sense of entitlement)	Αυτός ο παράγοντας συναντάται μόνο σε περιπτώσεις κλοπής πνευματικής ιδιοκτησίας και αναφέρεται στο βαθμό στον οποίο οι εργαζόμενοι ένιωθαν ότι δικαιούνται πληροφορίες που έκλεψαν [117, 123]. Οι πληροφορίες σε αυτές τις περιπτώσεις αναφέρονται σε αποτελέσματα εργασίας που παρήγαγαν οι εργαζόμενοι κατά τη διάρκεια της ενασχόλησής τους στην επιχείρηση, ανεξάρτητα από		●		

	το αν έχουν ή δεν έχουν υπογράψει σχετικές συμφωνίες ή συμβάσεις.			
8 – Παραβίαση πολιτικών (Policy violation)	Οι παραβιάσεις πολιτικών μπορεί να είναι συμπεριφορικής ή τεχνικής φύσης [120]. Αυτός ο δείκτης χρησιμοποιείται για την αξιολόγηση της συμμόρφωσης των εργαζομένων με τις ισχύουσες πολιτικές και διαδικασίες ασφαλείας.	●	●	
9 – Έλεγχοι (Auditing)	Το auditing χρησιμοποιείται για να περιγράψει και να αξιολογήσει την ικανότητα και τα μέσα που χρησιμοποιεί ένας οργανισμός για να ανιχνεύσει, να αξιολογήσει και να αντιδράσει σε παραβιάσεις πολιτικής, τεχνικές ή μη, προκειμένου να αποτρέψει πραγματικές περιπτώσεις επιθέσεων από εσωτερικές απειλές μέσω θετικών ή αρνητικών τεχνικών πλαισίωσης [109, 120].	●	●	
10 – Επίγνωση πολιτικών και ρόλων (Policies and roles awareness)	Η επίγνωση των πολιτικών και διαδικασιών της επιχείρησης μαζί με τη γνώση των ρόλων και των ευθυνών διαφοροποιεί τις σκόπιμες από τις ακούσιες παραβιάσεις ασφάλειας [118, 127].			●
11 – Επίγνωση καταστάσεων (Situation awareness)	Τα ακούσια περιστατικά εσωτερικών απειλών προκύπτουν συχνά από τεχνολογική αγνοία και ελλιπή γνώση κυβερνοασφάλειας. Απλά παραδείγματα αυτής της κατηγορίας περιλαμβάνουν τη μη αναγνώριση ενός phishing μηνύματος ηλεκτρονικής αλληλογραφίας, την επίσκεψη ενός αναξιόπιστου ιστότοπου, τη εκτέλεση ενός κακόβουλου αρχείου [118, 127].			●

3.4.1.2 Αξιολόγηση Εσωτερικής Απειλής

Έχοντας ως απώτερο σκοπό να προσδιορίσουμε πιθανές εσωτερικές απειλές για έναν οργανισμό με βάση την αξιολόγηση της κουλτούρας κυβερνοασφάλειας, προχωρήσαμε στον εντοπισμό των τομέων ασφάλειας του προτεινόμενου πλαισίου που σχετίζονται άμεσα με τους 11 βασικούς παράγοντες εσωτερικής απειλής [134], όπως αυτοί παρουσιάστηκαν στην προηγούμενη ενότητα. Τα αποτελέσματα αξιολόγησης από αυτούς τους τομείς ασφαλείας θα μπορούσαν να βοηθήσουν στον εντοπισμό πιθανών κινδύνων από εσωτερική απειλή όταν εξετάζονται συνδυαστικά, όπως παρουσιάζεται στον Πίνακας 6.

Πίνακας 6. Συσχέτιση Πλαισίου Κουλτούρας Κυβερνοασφάλειας με τους παράγοντες εσωτερικών απειλών

Level	Dimension	Domain	Insider Threat Factor
Individual	**Attitude**	Employee Satisfaction	1 - Dissatisfaction
		Employee Profiling	3 – Enterprise role 5 – Employee profile
	Awareness	Policies and Procedures Awareness	10 – Policies and roles awareness
		Roles and Responsibilities Awareness	10 – Policies and roles awareness
	Behavior	Policies and Procedures Compliance	8 – Policy violation
		Security Agent Persona	2 - Personality predispositions 7 – Sense of entitlement
		Security Behavior	4 – Concerning behavior
	Competency	Security Skills Evaluation	11 – Situation awareness
		Training Completion and Scoring	11 – Situation awareness
Organizational	**Assets**	Personnel Security	6 – Access Controls
	Access & Trust	Access Management	6 – Access Controls

	Defense	Information Security Policy & Compliance	9 – Auditing
	Security Governance	Audit Logs Management	9 – Auditing
		Incident Response & Management	9 – Auditing

Όπως αναμενόταν, ο κίνδυνος εσωτερικών απειλών αντιμετωπίζεται κυρίως από το ατομικό επίπεδο του προτεινόμενου πλαισίου που σχετίζεται με τη στάση, την επίγνωση, την ικανότητα και τη συμπεριφορά των εργαζομένων. Προκειμένου να αξιολογηθούν οι προδιαθέσεις προσωπικότητας που υπαγορεύονται από τους παράγοντες εσωτερικής απειλής και να συσχετιστούν με τη συμπεριφορά των εργαζομένων, εμπλουτίσαμε τους ελέγχους που χρησιμοποιήθηκαν για την αξιολόγηση αυτής της διάστασης ασφάλειας του πλαισίου μας. Πιο συγκεκριμένα, βελτιώσαμε τους τομείς «*Security Agent Persona*» και «*Security Behaviour*» συμπεριλαμβάνοντας εργαλεία μέτρησης που διερευνούν μια ποικιλία ψυχολογικών δομών που σχετίζονται με τη συμπεριφορά ασφαλείας, όπως η Κλίμακα Ανάληψης Κινδύνων Ειδικού Τομέα (***Domain-Specific Risk-Taking Scale***) [135], η Γενική Προσέγγιση Λήψης Αποφάσεων (***General Decision-Making Style***) [136], Εξέταση Μελλοντικών Συνεπειών (***Consideration for Future Consequences***) [137], Κλίμακα Παρορμητικότητας Barratt (***Barratt Impulsiveness Scale***) [138], Ανάγκη για Γνώση (***Need for Cognition***) [139], Κλίμακα Προθέσεων Συμπεριφοράς Ασφαλείας (***Security Behavior Intentions Scale***) [140].

Οι λίγες οργανωτικές διαστάσεις και τομείς που συνεισφέρουν στη συνολική εκτίμηση του κινδύνου εμπιστευτικών πληροφοριών συνδέονται άμεσα με τη διαχείριση του φυσικού και ψηφιακού ελέγχου πρόσβασης σε συνδυασμό με τον έλεγχο συμμόρφωσης με την ασφάλεια, την παρακολούθηση και τη διαχείριση απόκρισης συμβάντων. Κατά συνέπεια, το προτεινόμενο πλαίσιο κουλτούρας κυβερνοασφάλειας μπορεί πράγματι να εντοπίσει, μεταξύ άλλων πιθανών απειλών ή ελλείψεων στον κυβερνοχώρο, κινδύνους από εσωτερικές απειλές δεδομένης μιας συγκεκριμένης λειτουργικής πραγματικότητας.

3.4.2 MITRE ATT&CK

Το ***MITRE ATT&CK*** (***Adversarial Tactics, Techniques, and Common Knowledge***) ξεκίνησε το 2013 σε μια προσπάθεια τεκμηρίωσης και κατηγοριοποίησης των τακτικών, τεχνικών και διαδικασιών που χρησιμοποιούν οι επιτιθέμενοι στον κυβερνοχώρο έναντι Microsoft Windows συστημάτων με στόχο τη βελτίωση της ανίχνευσης κακόβουλης ενέργειας [141, 142]. Με την πάροδο των ετών, το ATT&CK επεκτάθηκε αρκετά, εξετάζοντας και άλλες πλατφόρμες και τεχνολογίες, εξελισσόμενη σε μια βάση δεδομένων για τη συμπεριφορά των επιτιθέμενων στον κυβερνοχώρο και μια ταξινόμηση για αντίπαλες ενέργειες σε όλο τον κύκλο ζωής τους. Τώρα αξιοποιείται τόσο ως βάση εξομοίωσης εχθρικών συμπεριφορών όσο και ως μέθοδος για την ανακάλυψη των κενών ασφαλείας και άμυνας [143].

Ως μοντέλο συμπεριφοράς, το ATT&CK βασίζεται σε μια σειρά βασικών στοιχείων:

- Τακτικές (***Tactics***): δηλώνει τον στόχο τακτικού αντιπάλου για την εκτέλεση μιας επίθεσης. Αντιμετωπίζει πρακτικά το «γιατί» [141, 144]. Οι τακτικές χρησιμεύουν ως σημασιολογικές κατηγορίες για μεμονωμένες τεχνικές και καλύπτουν τυπικές, υψηλότερου επιπέδου, ενέργειες που εκτελούν οι κυβερνοεγκληματίες κατά τη διάρκεια μιας επίθεσης, όπως η εξαγωγή δεδομένων, η κλιμάκωση των προνομίων και η διαφυγή άμυνας [142].
- Τεχνικές (***Techniques***): περιγραφή των μέσων με τα οποία οι αντίπαλοι επιτυγχάνουν τους τακτικούς στόχους τους εκτελώντας μια ενέργεια. Με άλλα λόγια, απευθύνονται στο «πώς» και, σε ορισμένες περιπτώσεις, στο «τι» κερδίζει ένας αντίπαλος εκτελώντας μια ενέργεια [142, 145]. Μπορεί να υπάρχουν πολλοί τρόποι ή τεχνικές για την επίτευξη τακτικών στόχων, επομένως υπάρχουν πολλές τεχνικές σε κάθε κατηγορία τακτικής.
- Υπο-τεχνικές (***Sub-techniques***): απεικόνιση πιο συγκεκριμένων μέσων με τα οποία οι αντίπαλοι επιτυγχάνουν τους τακτικούς στόχους σε χαμηλότερο επίπεδο από τις τεχνικές [142, 144].
- Διαδικασίες (***Procedures***): απόδοση της συγκεκριμένης υλοποίησης που χρησιμοποιεί ο αντίπαλος για τεχνικές ή υπο-τεχνικές [144]. Χρησιμοποιούνται για να περιγράψουν τη χρήση τεχνικών ή υπο-τεχνικών στη φύση, ενώ παρουσιάζουν αρκετές πρόσθετες συμπεριφορές στον τρόπο που εκτελούνται [142, 145].
- Αντίμετρα (***Mitigations***): ορισμός των αντίμετρων που θα μπορούσαν να εμποδίσουν τους αντιπάλους να επιτύχουν τους τακτικούς τους στόχους μέσω της χρήσης συγκεκριμένων τεχνικών. Τα αντίμετρα αφορούν στο «τι να κάνουμε» σχετικά με την ερώτηση των TTP (Τακτικές, Τεχνικές & Διαδικασίες) [146].

Σύμφωνα με τα ανωτέρω, το ATT&CK είναι μια γνωσιακή βάση τεχνικών αντιπάλου που αναλύονται σε μια σειρά υπο-τεχνικών, παρουσιάζοντας συγκεκριμένες διαδικασίες, οργανωμένες σε ένα σύνολο τακτικών, συστήνοντας βασικά αντίμετρα στον κυβερνοχώρο. Λόγω της δημόσιας υιοθέτησής του από πολλούς κυβερνητικούς οργανισμούς και κλάδους της βιομηχανίας, συμπεριλαμβανομένων των χρηματοοικονομικών, της υγειονομικής περίθαλψης, του λιανικού εμπορίου και της τεχνολογίας, γνώρισε τεράστια ανάπτυξη στο χώρο της κυβερνοασφάλειας. Σήμερα, προσφέρει τρία διαφορετικά μοντέλα:

- ***ATT&CK for Enterprise***: κάλυψη συμπεριφοράς έναντι εταιρικών δικτύων πληροφορικής και Cloud. Το πρώτο μοντέλο ATT&CK δημιουργήθηκε τον Σεπτέμβριο του 2013, εστιάζοντας στο επιχειρηματικό περιβάλλον των Windows. Μετά από βελτιώσεις και προσαρμογές μέσω εσωτερικής έρευνας, κυκλοφόρησε δημόσια τον Μάιο του 2015 με 96 τεχνικές που οργανώθηκαν κάτω από 9 τακτικές. Το 2017, επεκτάθηκε για να απευθύνεται επίσης σε λειτουργικά συστήματα Mac και Linux (εκτός από τα Windows). Για πρώτη φορά, αποδίδεται το όνομα «ATT&CK for Enterprise».

  Ένα συμπληρωματικό μοντέλο που ονομάζεται ***PRE-ATT&CK*** δημοσιεύθηκε την ίδια χρονιά, εστιάζοντας στις πρώτες φάσεις προετοιμασίας, επιτρέποντας στους οργανισμούς να προβλέψουν και να προετοιμαστούν για επιθέσεις πριν καν συμβούν [147]. Το 2019, το ATT&CK for Cloud δημοσιεύτηκε ως μέρος του Enterprise για να περιγράψει τη συμπεριφορά σε περιβάλλοντα και υπηρεσίες νεφοϋπολογιστικής. Η τρέχουσα έκδοση του μοντέλου, που κυκλοφόρησε στις 27 Οκτωβρίου 2020, ενσωματώνει 14 επιχειρηματικές τακτικές που αναλύονται σε 177 τεχνικές και 348 υπο-τεχνικές που παρέχουν 42 αντίμετρα.

- ***ATT&CK for Mobile***: εστιάζει στη συμπεριφορά ενάντια σε κινητές συσκευές (κυρίως λειτουργικές πλατφόρμες Android και iOS). Αυτό το μοντέλο κυκλοφόρησε το 2017 καλύπτοντας τεχνικές που στοχεύουν στη πρόσβαση σε ασύρματα δίκτυα και συσκευές χωρίς την απόκτηση φυσικής πρόσβασης. Η τρέχουσα έκδοση, που κυκλοφόρησε στις 23 Οκτωβρίου 2020, αποτελείται από 14 τακτικές που αναλύονται σε 86 τεχνικές που αντιμετωπίζονται από 13 αντίμετρα.
- ***ATT&CK for ICS***: χαρακτηρισμός και περιγραφή της συμπεριφοράς αντιπάλου κατά τη λειτουργία εντός δικτύων ICS (Industrial Control Systems) [148]. Η ανάπτυξή του ξεκίνησε ως ένα μικρό ερευνητικό MITRE έργο για την εφαρμογή της δομής και της μεθοδολογίας ATT&CK στον τομέα της τεχνολογίας ICS λόγω των ολοένα και πιο αυξανόμενων περιστατικών κυβερνοασφάλειας [149]. Το 2017, ξεκίνησε μια διαδικασία αναθεώρησης που επέτρεπε τη συμμετοχή οργανισμών και ατόμων από την κοινότητα του ICS με στόχο τη βελτίωσή του. Τελικά δημοσιοποιήθηκε στο ευρύ κοινό τον Ιανουάριο του 2020, με την τρέχουσα έκδοσή του (ενημερώθηκε στις 5 Οκτωβρίου 2020) που αριθμεί 11 τακτικές, 81 τεχνικές και 50 αντίμετρα.

3.4.2.1 Υβριδικό Μοντέλο MITRE ATT&CK for Enterprise και ICS

Λαμβάνοντας υπόψιν τις αυξανόμενης πολυπλοκότητας απειλές στον κυβερνοχώρο που καλούνται να αντιμετωπίσουν οι βιομηχανικές και κρίσιμες υποδομές, γίνεται προφανές ότι οι κυβερνοεπιτιθέμενοι δε σέβονται τα θεωρητικά όρια μεταξύ IT και ICS όταν μετακινούνται σε δίκτυα OT (Operations Technology) [150]. Συνεπώς, οι ειδικοί στον τομέα της κυβερνοασφάλειας συνειδητοποίησαν σύντομα ότι τα μοντέλα ATT&CK για ICS και Enterprise πρέπει να εξεταστούν συνδυαστικά. Στα τέλη του 2020, η Mandiant Threat Intelligence από κοινού με το MITRE δημοσίευσε ένα άρθρο παρουσιάζοντας την προσπάθειά τους να συγχωνεύσουν το MITRE ATT&CK for Enterprise και ICS με στόχο την αντιμετώπιση επιθέσεων κατά των δικτύων OT [151]. Σύμφωνα με αυτό, προτείνεται συνδυασμένη εξέταση και αξιολόγηση ασφάλειας των δικτύων IT και OT εντός κρίσιμων υποδομών. Η συνύπαρξή τους και ο ισχυρός συσχετισμός και αλληλεπίδρασή τους εντός αυτών των οργανισμών υπαγόρευσε την υβριδική προσέγγιση MITRE ATT&CK for Enterprise και ICS ως τον καταλληλότερο υποψήφιο για τον εντοπισμό πιθανών εξωτερικών απειλών.

Η πιθανότητα ένας αντίπαλος να επιτύχει έναν συγκεκριμένο τακτικό στόχο έναντι ενός εταιρικού δικτύου εξαρτάται σε μεγάλο βαθμό από το αν έχουν εφαρμοστεί ορισμένα αντίμετρα ασφαλείας. Ως εκ τούτου, διαμορφώθηκε μια ενιαία λίστα αντίμετρων MITRE ATT&CK για Enterprise και ICS η οποία παρουσιάζεται στον Πίνακας 7.

Πιο συγκεκριμένα, αυτός ο πίνακας συνοψίζει τα αντίμετρα του ATT&CK for Enterprise [152] και ATT&CK for ICS [153]. Κάθε καταχώριση μπορεί να ισχύει σε ένα από τα δύο μοντέλα ή και στα δύο, όπως επισημαίνεται στις δύο τελευταίες στήλες του πίνακα. Με άλλα λόγια, δημιουργήσαμε ένα υπερσύνολο αντιμέτρων ασφαλείας που πρέπει να εφαρμοστούν και να αντιμετωπιστούν σωστά, προκειμένου να προστατεύσουμε τόσο το δίκτυο πληροφορικής όσο και δίκτυο λειτουργίας μιας κρίσιμης υποδομής.

Πίνακας 7. Αντίμετρα του υβριδικού μοντέλου MITRE ATT&CK for Enterprise και ICS

ID	Name	ATT&CK for Enterprise	ATT&CK for ICS
M0800	Authorization Enforcement		●
M0801	Access Management		●
M0802	Communication Authenticity		●
M0803	Data Loss Prevention		●
M0804	Human User Authentication		●
M0805	Mechanical Protection Layers		●
M0806	Minimize Wireless Signal Propagation		●
M0807	Network Allowlists		●
M0808	Encrypt Network Traffic		●
M0809	Operational Information Confidentiality		●
M0810	Out-of-Band Communications Channel		●
M0811	Redundancy of Service		●
M0812	Safety Instrumented Systems		●
M0813	Software Process and Device Authentication		●
M0814	Static Network Configuration		●
M0815	Watchdog Timers		●
M0816	Mitigation Limited or Not Effective		●
M1013	Application Developer Guidance	●	●
M1015	Active Directory Configuration	●	●
M1016	Vulnerability Scanning	●	●
M1017	User Training	●	●
M1018	User Account Management	●	●
M1019	Threat Intelligence Program	●	●
M1020	SSL/TLS Inspection	●	●
M1021	Restrict Web-Based Content	●	●
M1022	Restrict File and Directory Permissions	●	●
M1024	Restrict Registry Permissions	●	●
M1025	Privileged Process Integrity	●	
M1026	Privileged Account Management	●	●
M1027	Password Policies	●	●
M1028	Operating System Configuration	●	●
M1029	Remote Data Storage	●	
M1030	Network Segmentation	●	●
M1031	Network Intrusion Prevention	●	●
M1032	Multi-factor Authentication	●	●
M1033	Limit Software Installation	●	
M1034	Limit Hardware Installation	●	●
M1035	Limit Access to Resource Over Network	●	●
M1036	Account Use Policies	●	●
M1037	Filter Network Traffic	●	●
M1038	Execution Prevention	●	●
M1039	Environment Variable Permissions	●	
M1040	Behavior Prevention on Endpoint	●	
M1041	Encrypt Sensitive Information	●	●

M1042	Disable or Remove Feature or Program	●	●
M1043	Credential Access Protection	●	
M1044	Restrict Library Loading	●	●
M1045	Code Signing	●	●
M1046	Boot Integrity	●	●
M1047	Audit	●	●
M1048	Application Isolation and Sandboxing	●	●
M1049	Antivirus/Antimalware	●	●
M1050	Exploit Protection	●	●
M1051	Update Software	●	●
M1052	User Account Control	●	
M1053	Data Backup	●	●
M1054	Software Configuration	●	●
M1055	Do Not Mitigate	●	
M1056	Pre-compromise	●	

3.4.2.2 Αξιολόγηση Απειλών MITRE ATT&CK

Έχοντας ενοποιήσει τα αντίμετρα που προτείνονται για την προστασία των περιβαλλόντων IT και OT σύμφωνα με τη γνωσιακή βάση ATT&CK, το επόμενο βήμα ήταν να τα συσχετίσουμε με τους προτεινόμενους τομείς και ελέγχους του προτεινόμενο πλαισίου κουλτούρας κυβερνοασφάλειας. Έτσι, τα αποτελέσματα της αξιολόγησης του πλαισίου θα εντόπιζαν άμεσα μη χρησιμοποιούμενα αντίμετρα ασφαλείας ή στοιχεία ασφαλείας που διευκολύνουν τους αντιπάλους να εφαρμόσουν συγκεκριμένα τεχνικές. Για αυτήν τη συσχέτιση, πραγματοποιήσαμε ανασκόπηση βιβλιογραφίας και εις βάθος ανάλυση κάθε στοιχείου ασφαλείας και πιθανών τακτικών και απειλών ασφαλείας. Ο Πίνακας 8 παρουσιάζει πώς ξεκινώντας από την αξιολόγηση συγκεκριμένων διαστάσεων και τομέων ασφαλείας μπορεί κανείς να προχωρήσει στον εντοπισμό μη εφαρμοζόμενων ή υποτιμημένων αντίμετρων. Το υβριδικό μοντέλο MITRE ATT&CK for Enterprise και ICS μας βοηθά να προχωρήσουμε περαιτέρω επισημαίνοντας τις πιθανές τεχνικές αντιπάλου στις οποίες ο οργανισμός είναι ευάλωτος [151].

Πίνακας 8. Συσχέτιση Μοντέλου Κουλτούρας Κυβερνοασφάλειας με το υβριδικό μοντέλο MITRE ATT&CK for Enterprise και ICS

Level	Dimension	Domain	MITRE ATT&CK Mitigation
Organizational	**Assets**	Application Software Security	M0813 M0815 M1013 M1040 M1042 M1045

	Data Security and Privacy	M0803
	Hardware Assets Management	M0813 M1034
	Hardware Configuration Management	M0815 M1024 M1028 M1039 M1046
	Network Configuration Management	M0814 M1037
	Network Infrastructure Management	M1037
	Software Assets Management	M0815 M1033 M1038 M1040 M1042 M1044 M1045 M1048 M1054
	Personnel Security	M0804
	Physical Safety and Security	M0805 M0812
Continuity	Backup Mechanisms	M1029 M1053
	Business Continuity & Disaster Recovery	M0810 M0811 M1053
	Continuous Vulnerability Management	M1016 M1051
	Access Management	M0800

		M0801
		M1015
		M1022
		M1030
		M1035
Access and Trust	Account Management	M1015
		M1018
		M1032
		M1036
		M1052
	Password Robustness and Exposure	M1027
		M1043
	Privileged Account Management	M1025
		M1026
	Role Segregation	M0800
	Wireless Access Management	M0806
Operations	Efficient Distinction of Development, Testing and Operational Environments	M1048
	Risk Assessment	M1019
Defense	Boundary Defense	M0802
		M0807
		M0808
		M0809
		M1020
		M1031
	Cryptography	M1041
	Email and Web Browser Resilience	M1021
	Malware Defense	M1049
	Security Awareness and Training Program	M1017
	Audit Logs Management	M1047

	Security Governance	Penetration Tests and Red Team Exercises	M1050
Individual	**Behavior**	Security Behavior	M1017
	Competency	Security Skills Evaluation	M1017 M1027
		Training Completion and Scoring	M1017

Σημείωση: Το αντίμετρο "***M1055 - Do Not Mitigate***", το οποίο χρησιμοποιείται σε περιπτώσεις όπου η εφαρμογή αντίμετρων ενδέχεται να αυξήσουν τον κίνδυνο έκθεσης ενός οργανισμού, έχει εξαιρεθεί από τον πίνακα.

Ο Πίνακας 8 παρουσιάζει μια σχέση πολλών προς πολλά μεταξύ του μοντέλου κουλτούρας κυβερνοασφάλειας και του υβριδικού MITRE ATT&CK for Enterprise και ICS [154]. Συνεπώς, τα αποτελέσματα αξιολόγησης πολλών διαφορετικών τομέων ασφαλείας πρέπει να μελετηθούν συγκριτικά για να αξιολογηθεί η άμυνα του οργανισμού έναντι συγκεκριμένων τεχνικών κυβερνοεπίθεσης.

Το πλαίσιο κουλτούρας κυβερνοασφάλειας έχει δημιουργηθεί χρησιμοποιώντας μια διεπιστημονική προσέγγιση για την ασφάλεια πληροφοριών. Επομένως, τα στοιχεία του προορίζονται να καλύψουν όλες τις διαφορετικές πτυχές ενός επιχειρηματικού περιβάλλοντος, συμπεριλαμβανομένων των εσωτερικών και εξωτερικών, οργανωτικών και ατομικών παραγόντων. Το MITRE ATT&CK, από την άλλη πλευρά, έχει αναπτυχθεί με βάση μια εκτεταμένη γνωσιακή βάση περιστατικών παραβίασης που έχουν καταγραφεί και τεκμηριωθεί, και τα οποία σχετίζονται κυρίως με τεχνικές καθοδηγούμενες από την τεχνολογία. Με άλλα λόγια, προορίζεται να περιγράψει πώς οι αντίπαλοι μπορούν να εκμεταλλευτούν συγκεκριμένες ευπάθειες και αδυναμίες IT & OT για την επίτευξη ορισμένων κακόβουλων στόχων. Κατά συνέπεια, η κουλτούρα της κυβερνοασφάλειας, λόγω των αρχικών της σκοπών, έχει ευρύτερο χαρακτήρα από τη γνωσιακή βάση ATT&CK. Ως εκ τούτου, η ανίχνευση απειλών κατά MITRE ATT&CK δεν απαιτεί την αξιολόγηση όλων των διαστάσεων και τομέων του πλαισίου κουλτούρας κυβερνοασφάλειας. Τουλάχιστον στην τρέχουσα έκδοσή του, δεδομένου ότι η γνωσιακή βάση ATT&CK εξελίσσεται συνεχώς ακολουθώντας τον ταυτόχρονο μετασχηματισμό του κυβερνοεγκλήματος.

Όπως διαφαίνεται στον Πίνακας 8, και οι έξι οργανωτικές διαστάσεις συμμετέχουν στην αξιολόγηση κινδύνου ATT&CK αλλά χωρίς να αξιοποιούνται όλοι οι υπο-τομείς. Ομοίως, σε ατομικό επίπεδο, χρησιμοποιούνται μόνο δύο από τις τέσσερις διαστάσεις. Η διαστάσεις «Attitude» και η «Awareness», που προέρχονται από τις ανθρωπιστικές επιστήμες, δεν σχετίζονται άμεσα με τις τεχνικές ATT&CK. Αυτές οι διαστάσεις, από την άλλη πλευρά, χρησιμοποιούνται για τον εντοπισμό της Εσωτερικής Απειλής (όπως παρουσιάστηκε σε προηγούμενο κεφάλαιο της παρούσας διατριβής) η οποία δεν αντιμετωπίζεται πρακτικά με τη χρήση της τεχνικής προσέγγισης ATT&CK.

3.5 Εργαλείο Ανάλυσης Συμπεριφοράς Ασφαλείας

Στο πλαίσιο του ερευνητικού έργου EnergyShield [42], χρηματοδοτούμενο από το πρόγραμμα έρευνας και καινοτομίας Horizon 2020 της Ευρωπαϊκής Ένωσης, σύμφωνα με τη συμφωνία επιχορήγησης με αριθμό 832907, αναπτύχθηκε ένα εργαλείο κουλτούρας

κυβερνοασφάλειας με τίτλο εργαλείο Ανάλυσης Συμπεριφοράς Ασφαλείας (***Security Behaviour Analysis, SBA***)[2]. Το εργαλείο αυτό, έχοντας ως βάση του το προτεινόμενο πλαίσιο κουλτούρας κυβερνοασφάλειας, εφαρμόζει ποικίλες τεχνικές και μεθοδολογίες αξιολόγησης με στόχο την προσμέτρηση τόσο των οργανωτικών όσο και των ατομικών δεικτών κυβερνοασφάλειας ενός οργανισμού.

Στην παρούσα έκδοση του εργαλείου (όπως αυτή έχει διαμορφωθεί κατά την συγγραφή της τρέχουσας διδακτορικής διατριβής) έχουν συμπεριληφθεί περισσότερα από 100 ερωτηματολόγια με πάνω από 1000 ποιοτικούς και ποσοτικούς ελέγχους, 2 διαδραστικές δοκιμές, 1 προσομοίωση και 1 σοβαρό παιχνίδι.

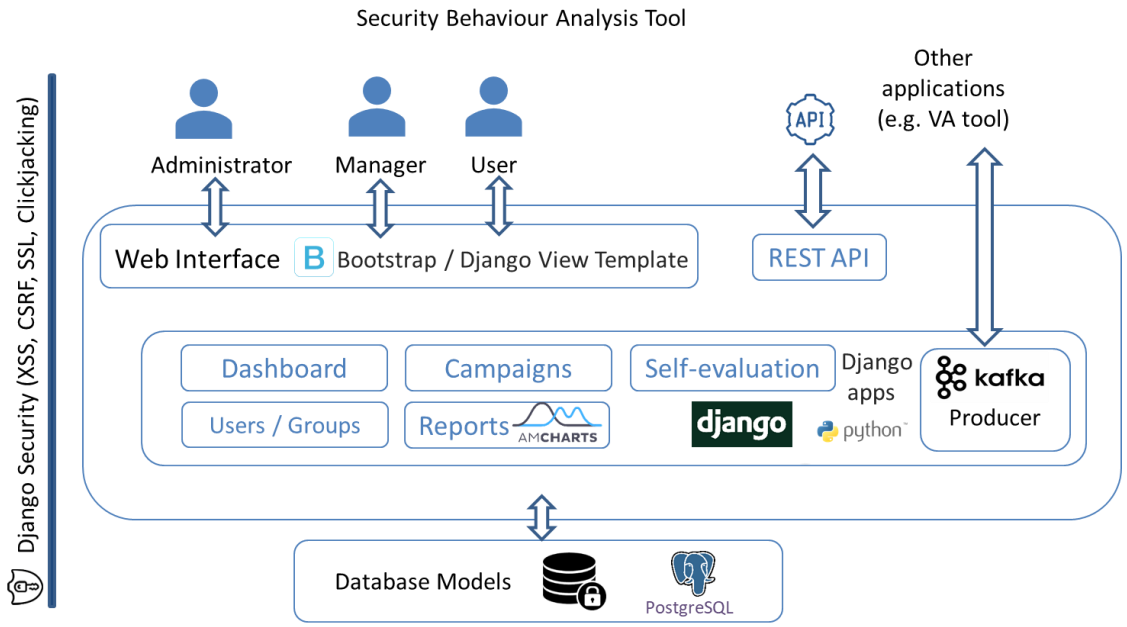
Στο εγχειρίδιο χρήσης του εργαλείου, το οποίο έχει συμπεριληφθεί στο Παράρτημα Ι για λόγους πληρότητας, παρουσιάζονται αναλυτικά οι δυνατότητες που προσφέρονται μέσω του εργαλείου.

3.5.1 Αρχιτεκτονική Εργαλείου

Το εργαλείο SBA έχει σχεδιαστεί, αναπτυχθεί και υλοποιηθεί ως μια δικτυακή εφαρμογή χρησιμοποιώντας μια σειρά από τεχνολογίες αιχμής (Εικόνα 9). Πιο συγκεκριμένα:

- **Django**: ένα πλαίσιο Web Python ανοιχτού κώδικα υψηλού επιπέδου που ενθαρρύνει την ταχεία ανάπτυξη, ενώ προσφέρει τη δυνατότητα γρήγορης και ευέλικτης κλίμακας. Τα χαρακτηριστικά ασφαλείας του επιβάλλουν την προστασία των εφαρμογών έναντι κοινών ζητημάτων ασφαλείας, όπως η έγχυση SQL (SQL injection), η δημιουργία δέσμης ενεργειών μεταξύ τοποθεσιών (cross-site scripting), η πλαστογράφηση αιτημάτων μεταξύ τοποθεσιών (cross-site request forgery) και το clickjacking.
- **PostgreSQL**: ένα ισχυρό, ανοιχτού κώδικα αντικειμενοσχεσιακό σύστημα βάσης δεδομένων με ισχυρή φήμη για αξιοπιστία, ευρωστία χαρακτηριστικών και απόδοση. Χρησιμοποιείται για να φιλοξενήσει τη λογική δομή δεδομένων πίσω από ολόκληρη την εφαρμογή, συμπεριλαμβανομένου του μοντέλου κουλτούρας ασφάλειας και της αναπαράστασης της μεθοδολογίας αξιολόγησης, μαζί με τα αποτελέσματα και τα στατιστικά της.
- **Διασύνδεση Ιστού**: υλοποιείται με χρήση συνδυασμού αρχείων HTML, Bootstrap, CSS και JavaScript για την παροχή μιας φιλικής προς το χρήστη διεπαφής για όλους τους αλληλεπιδρώντες παράγοντες του εργαλείου.
- **REST API**: μια διεπαφή ιστού που επιτρέπει την αλληλεπίδραση του εργαλείου SBA με την υπόλοιπη εργαλειοθήκη EnergyShield ή με οποιοδήποτε άλλο εταιρικό λειτουργικό σύστημα.
- **Kafka Producer**: ένας Kafka producer που δημοσιεύει μηνύματα σε συγκεκριμένα θέματα (topics) Kafka για να ενημερώσει τα μέρη που ακούν (Kafka consumers) ότι έχουν γίνει διαθέσιμα νέα δεδομένα αξιολόγησης (π.χ. στο τέλος μιας εκστρατείας αξιολόγησης).

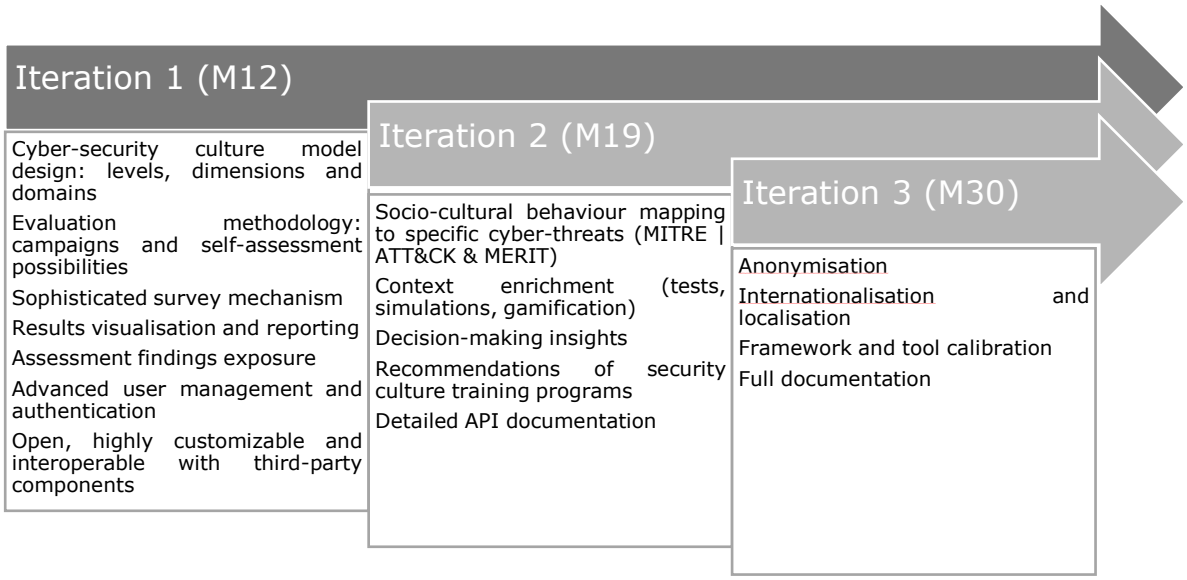
[2] Πηγαίος κώδικας: https://github.com/angeorg83/sbam



Εικόνα 9. Αρχιτεκτονική εργαλείου Ανάλυσης Συμπεριφοράς Ασφαλείας (SBA)

3.5.2 Ανάπτυξη εργαλείου

Το SBA σχεδιάστηκε, αναπτύχθηκε, δοκιμάστηκε και επικυρώθηκε σε 3 επαναλήψεις. Κάθε επανάληψη είχε ως στόχο να αντιμετωπίσει συγκεκριμένες λειτουργικές και μη λειτουργικές απαιτήσεις. Η Εικόνα 10 παρουσιάζει τα κύρια χαρακτηριστικά του εργαλείου SBA όπως αναπτύχθηκαν κατά τη διάρκεια κάθε μιας από τις επαναλήψεις του.



Εικόνα 10. Φάσεις ανάπτυξης εργαλείου Ανάλυσης Συμπεριφοράς Ασφαλείας (SBA)

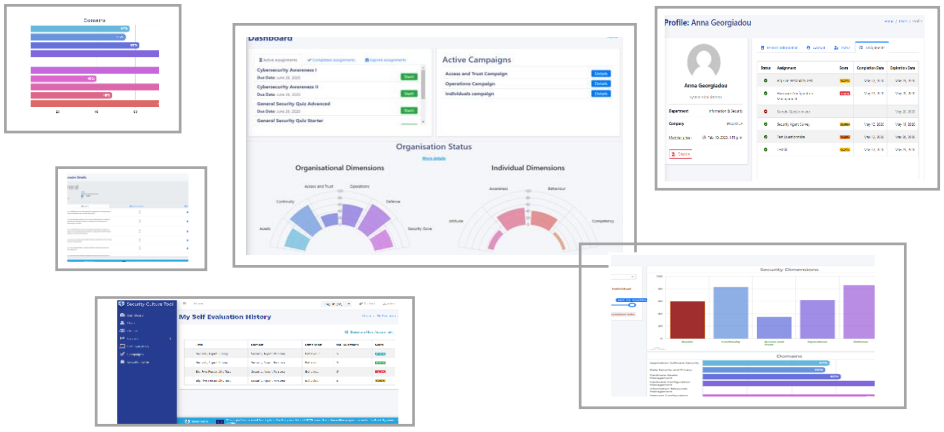
- **Α' Φάση**

  Κατά την **Α' Φάση** ανάπτυξης του SBA, διαμορφώθηκε η σχεσιακή βάση του εργαλείου σύμφωνα με το μοντέλο κουλτούρας κυβερνοασφάλειας και την προτεινόμενη μεθοδολογία. Τα επίπεδα, οι διαστάσεις, οι δομές και οι έλεγχοι του

εργαλείου αποδόθηκαν σε μορφή κατάλληλων αρχείων μεταδεδομένων επιτρέποντας τη δυναμική εισαγωγή τους στο εργαλείο και παρέχοντας μηχανισμούς ενημέρωσης, προσαρμογής και επέκτασής τους σύμφωνα με τις ανάγκες του οργανισμού που θα κάνει χρήση του εργαλείου. Παράλληλα, υλοποιήθηκαν οι έννοιες των αξιολογητικών εκστρατειών υιοθετώντας τη μεθοδολογία 4W1H μέσω διαδραστικών πλοηγών που καθοδηγούσαν το χρήστη στη διαμόρφωση και στόχευση τους σε ομάδες εργαζομένων.

Σε αυτή την Α΄Φάση ανάπτυξης εισήχθηκε ένας τρόπος διεξαγωγής ερωτηματολογίων (τόσο στα πλαίσια εκστρατειών όσο και στα πλαίσια αυτοαξιολόγησης των χρηστών) ενώ ταυτόχρονα εμπλουτίστηκε η βάση του εργαλείου με πληθώρα αξιολογητικού περιεχομένου. Επιπρόσθετα, διαμορφώθηκαν γραφικές απεικονίσεις και αναφορές για την οπτικοποίηση των αποτελεσμάτων των αξιολογήσεων με δυνατότητες προσαρμογής και φιλτραρίσματος με βάση χρονικά και λοιπά κριτήρια.

Βασικές αρχές όπως αυθεντικοποίηση (authentication), εξουσιοδότηση (authorization), διαχείριση δικαιωμάτων, κτλ. λήφθηκαν υπόψιν από τη φάση αρχιτεκτονικής του εργαλείου και θεμελιώθηκαν στην Α’ Φάση ανάπτυξης δεδομένης και της φύσης του ίδιου του εργαλείου και του αντικειμένου εφαρμογής αυτού (τομέας ασφαλείας).



Εικόνα 11. Γραφικό περιβάλλον εργαλείου Ανάλυσης Συμπεριφοράς Ασφαλείας (SBA)

- **Β’ Φάση**

Κατά την **Β’ Φάση** ανάπτυξης του SBA, επεκτάθηκε το μοντέλο της σχεσιακής βάσης και τα μεταδεδομένα αυτής προκειμένου να αποδώσουν τη συσχέτιση του μοντέλου κουλτούρας κυβερνοασφάλειας με το μοντέλο εσωτερικών απειλών και το υβριδικό μοντέλο MITRE ATT&CK for Enterprise και ICS. Η οπτικοποίηση των αποτελεσμάτων της αξιολόγησης της κουλτούρας κυβερνοασφάλειας πλέον δεν περιοριζόταν σε ποσοτικοποιημένα γραφήματα αλλά προχωρούσε στην αναγνώριση κυβερνοαπειλών και προσέφερε συστάσεις για την ενίσχυση της ασφάλειας πληροφοριών του οργανισμού.

Παράλληλα, διαμορφώθηκε μια πλούσια βάση διαδραστικών εκπαιδευτικών προγραμμάτων διαδικτυακά διαθέσιμων που προσφέρονταν ως επιλογές στους χρήστες του εργαλείου ανάλογα με τα αποτελέσματα της αξιολόγησής τους και σύμφωνα με τις ανάγκες και το προφίλ τους.

Ένα αναλυτικό μα συνάμα απλό REST API αναπτύχθηκε και τεκμηριώθηκε επιτρέποντας τη διασύνδεση του SBA με λοιπά επιχειρησιακά εργαλεία του οργανισμού στοχεύοντας στην περαιτέρω αξιοποίηση των αποτελεσμάτων του συνδυαστικά με τα ευρήματα των υποδομών ασφαλείας.

- **Γ' Φάση**

  Κατά την **Γ' Φάση** ανάπτυξης του SBA, εισήχθηκε η δυνατότητα χρήσης του εργαλείου με ανωνυμοποιημένα δεδομένα προσφέροντας περαιτέρω ευελιξία στους οργανισμούς αναλόγως των κανονιστικών τους και λοιπών υποχρεώσεων και πολιτικών διαχείρισης ανθρωπίνων πόρων.

  Παράλληλα το εργαλείο, το μοντέλο και το διαδραστικό υλικό αυτού μεταφράστηκε σε 2 γλώσσες, τα Βουλγαρικά και τα Ιταλικά, αναιρώντας τους περιοριστικούς γλωσσικούς παράγοντες και διευκολύνοντας την εφαρμογή και χρήση του από τους εταίρους του ερευνητικού έργου EnergyShield [42].

  Κατά την διευρυμένη χρήση του στο χώρο της ενέργειας προέκυψαν συστάσεις από τους χρήστες που συνέβαλαν στη βελτίωση του εργαλείου και των χαρακτηριστικών αυτού.

Το προτεινόμενο πλαίσιο εφαρμόστηκε σε διάφορους επιχειρηματικούς τομείς και κλάδους εστιάζοντας στις κρίσιμες υποδομές. Αναλόγως της ανάπτυξης, πληρότητας και διαθεσιμότητας του εργαλείου SBA, κάποιες από τις εφαρμογές του πλαισίου έλαβαν χώρα με χρήση του ενώ άλλες προσεγγίστηκαν με εναλλακτικούς τρόπους, όπως παρουσιάζεται αναλυτικά στις επόμενες ενότητες.

ΚΕΦΑΛΑΙΟ 4: ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ ΣΕ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ ΚΑΤΑ ΤΗΝ ΠΕΡΙΟΔΟ ΤΟΥ ΚΟΡΟΝΟΪΟΥ (COVID-19)

4.1 Εισαγωγή

Η νόσος του κορονοϊού 2019, ευρέως γνωστή ως COVID-19, είναι μια μολυσματική ασθένεια που προκαλείται από το σοβαρό οξύ αναπνευστικό σύνδρομο κορονοϊού 2 (SARS-CoV-2) [155]. Η ασθένεια εντοπίστηκε για πρώτη φορά τον Δεκέμβριο του 2019 στο Wuhan, στην πρωτεύουσα της επαρχίας Hubei της Κίνας [156], και έκτοτε εξαπλώθηκε παγκοσμίως. Τον Μάρτιο του 2020, ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ) κήρυξε το ξέσπασμα του COVID-19 πανδημία [157]. Τα ανθρώπινα θύματα αυξάνονται καθημερινά και δεν έχει βρεθεί ακόμη θεραπεία. Ωστόσο, ο COVID-19 είναι πολύ περισσότερο από μια κρίση υγείας.

Κατά το πρώτο εξάμηνο της εξάπλωσής του, οι πληγείσες χώρες συνειδητοποίησαν τις βαθιές πολιτικές, κοινωνικές και οικονομικές επεκτάσεις του. Οι άνθρωποι έλαβαν συμβουλές να μείνουν στο σπίτι και, στις περισσότερες περιπτώσεις, αναγκάστηκαν να το κάνουν μέσω κυβερνητικών παρεμβάσεων. Σχολεία, καταστήματα, εγκαταστάσεις ψυχαγωγίας και πολλές άλλες επιχειρήσεις έκλεισαν προσωρινά ως αντίμετρο για τον έλεγχο της εξάπλωσης του ιού, ενώ η εξ αποστάσεως εργασία ενθαρρύνθηκε σε περιπτώσεις όπου η φύση της εργασίας το επέτρεπε. Αυτή η διαταραχή της κανονικότητας προκάλεσε μια αλυσιδωτή αντίδραση στη γεωργία, τη μεταποίηση, το λιανικό εμπόριο, τις υπηρεσίες διαμονής και τροφίμων, τις επιχειρηματικές και διοικητικές δραστηριότητες και πολλούς άλλους τομείς. Οι πληγείσες επιχειρήσεις ήρθαν αντιμέτωπες με καταστροφικές συνέπειες, οι οποίες απειλούν τη λειτουργία και τη φερεγγυότητά τους, ενώ οι εργαζόμενοί τους είναι ευάλωτοι σε απώλεια εισοδήματος και απολύσεις.

Σύμφωνα με την έκθεση του Διεθνούς Οργανισμού Εργασίας (International Labour Organization, ILO), που δημοσιεύτηκε στις 7 Απριλίου 2020, τα πλήρη ή μερικά περιοριστικά μέτρα (lockdown) επηρέασαν σχεδόν 2,7 δισεκατομμύρια εργαζόμενους, που αντιπροσωπεύουν περίπου το 81% του παγκόσμιου εργατικού δυναμικού [158]. Η κρίση COVID-19 αναμενόταν να εξαλείψει το 6,7% των ωρών εργασίας παγκοσμίως το δεύτερο τρίμηνο του 2020 – που ισοδυναμεί με 195 εκατομμύρια εργαζόμενους πλήρους απασχόλησης. Ως αποτέλεσμα, οι απώλειες σε διαφορετικές εισοδηματικές ομάδες υπερέβησαν τις επιπτώσεις της οικονομικής κρίσης του 2008-9.

Οι λιγότερο επηρεασμένες επιχειρήσεις, και σε ορισμένες περιπτώσεις ακόμη και επωφελημένες από αυτήν την πρωτοφανή κρίση, είναι αυτές που είχαν επενδύσει κόπο, χρόνο και προϋπολογισμό για την ψηφιοποίησή τους. Με άλλα λόγια, αυτοί που είχαν ενσωματώσει σημαντικά την τεχνολογία της πληροφορίας στις καθημερινές τους δραστηριότητες επιτρέποντάς τους να συνεχίσουν απρόσκοπτα τη λειτουργία τους. Αυτοί οι οργανισμοί, αν και με καλύτερους όρους σε σύγκριση με τους τεχνολογικά πρωτόγονους αντιπάλους τους, αντιμετώπισαν μια άλλη παρενέργεια του κορονοϊού όχι και τόσο εμφανή: την αύξηση του εγκλήματος στον κυβερνοχώρο.

Οι κυβερνοαπειλές εξελίσσονται διαρκώς προκειμένου να επωφεληθούν από τη συμπεριφορά και τις τάσεις στο διαδίκτυο. Το ξέσπασμα του κορονοϊού δεν αποτέλεσε εξαίρεση. Από την αρχή της κρίσης COVID-19, οι εγκληματίες χρησιμοποίησαν τον κορονοϊό για να πραγματοποιήσουν επιθέσεις κοινωνικής δικτύωσης με θέμα την πανδημία για να διανείμουν διάφορα πακέτα κακόβουλου λογισμικού. Στις 9 Μαρτίου 2020, ένας ερευνητής ασφάλειας στο Reason Labs, ο Shai Alfasi, αποκάλυψε ότι οι εγκληματίες του

κυβερνοχώρου χρησιμοποιούσαν ψεύτικες εκδόσεις χαρτών θανάτων για να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα που ήταν αποθηκευμένα στα προγράμματα περιήγησης ιστού των χρηστών (διαπιστευτήρια, δεδομένα πιστωτικών καρτών κ.λπ.) [159]. Σύμφωνα με το Εθνικό Κέντρο Απάτης και Κυβερνοασφάλειας του Ηνωμένου Βασιλείου (UK National Fraud & Cyber Security Centre), οι αναφορές απάτης που σχετίζονται με τον κορονοϊό αυξήθηκαν κατά 400% τον Μάρτιο του 2020 [160] ενώ κόστισαν στα θύματά τους πάνω από 800 χιλιάδες λίρες σε ένα μήνα [161].

Με βάση την έκθεση της Europol [162], οι εγκληματίες του κυβερνοχώρου επιδιώκουν επίσης να εκμεταλλευτούν έναν αυξανόμενο αριθμό φορέων επίθεσης καθώς περισσότεροι εργοδότες εγκαθιδρύουν την τηλεργασία και επιτρέπουν εξωτερικές συνδέσεις με τα συστήματα των οργανισμών τους. Έχουν ήδη αναφερθεί επιθέσεις σε κρίσιμες υποδομές, με το ανησυχητικό παράδειγμα του Πανεπιστημιακού Νοσοκομείου του Μπρνο στην Τσεχία, στις 12 Μαρτίου 2020, το οποίο αναγκάστηκε να διακόψει ολόκληρο το δίκτυο πληροφορικής του, επηρεάζοντας και δύο από τα παραρτήματα του νοσοκομείου, το Νοσοκομείο Παίδων και το Μαιευτήριο.

Νοσοκομεία, ιατρικά κέντρα και δημόσια ιδρύματα γίνονται στόχος κυβερνοεγκληματιών για επιθέσεις ransomware - καθώς έχουν κατακλυστεί από την υγειονομική κρίση και δεν μπορούν να αντέξουν οικονομικά να αποκλειστούν από τα συστήματά τους, οι εγκληματίες πιστεύουν ότι είναι πιθανό να πληρώσουν τα λύτρα. Ταυτόχρονα, χιλιάδες νέοι ιστότοποι που σχετίζονται με την πανδημία δημιουργούνται καθημερινά για τη διεξαγωγή καμπανιών ανεπιθύμητης αλληλογραφίας, ηλεκτρονικό ψάρεμα, διάδοση κακόβουλου λογισμικού ή με στόχο την παραβίαση διακομιστών [163, 164, 165].

Κέντρα κυβερνοασφάλειας και ειδικοί σε όλο τον κόσμο έχουν εκδώσει συστάσεις και συμβουλές πρόληψης για να βοηθήσουν τα άτομα να αντισταθούν κατά του εγκλήματος στον κυβερνοχώρο και της απάτης. Με έναν αυξανόμενο αριθμό χωρών να ενθαρρύνουν τους πολίτες να μένουν, να μαθαίνουν ή να εργάζονται από το σπίτι, η ανάγκη της κυβερνοασφάλειας καθίσταται επιτακτική. Το ερώτημα που προέκυψε δεδομένων των συνθηκών είναι: ***πώς η κρίση του κορονοϊού έχει επηρεάσει την κουλτούρα της κυβερνοασφάλειας τόσο ατόμων όσο και οργανισμών;*** Η αρχική μας υπόθεση ήταν ότι η πανδημία κατέφερε ένα μεγάλο πλήγμα στον επιχειρηματικό κόσμο και, δεδομένου ότι η κουλτούρα κυβερνοασφάλειας μόλις τώρα είχε αρχίσει να εγκαθιδρύεται ως όρος, δεν θα μπορούσε να μην επηρεαστεί από αυτήν την κρίση.

Στην προσπάθεια να διερευνηθούν και να απαντηθούν όλα αυτά τα ερωτήματα, αναγνωρίσαμε την ερευνητική ευκαιρία ευρύτερης εφαρμογής του προτεινόμενου πλαισίου σε μια προσπάθεια αξιολόγησης των παρενεργειών της πανδημίας COVID-19 στην κουλτούρα κυβερνοασφάλειας κατά την εργασία από το σπίτι.

4.2 Μεθοδολογία

4.3 Σχεδιασμός Εκστρατείας Αξιολόγησης

Λαμβάνοντας υπόψη ότι η συγκεκριμένη εφαρμογή του προτεινόμενου πλαισίου είχε ως στόχο να αξιολογήσει τις παρενέργειες στην κουλτούρας κυβερνοασφάλειας κατά τη διάρκεια της κρίσης COVID-19, έπρεπε να πληρούνται ορισμένα κριτήρια:

- **Κύκλος ζωής** (**Life-cycle**): Με βάση διάφορες κοινωνικές, ψυχολογικές και ανθρωπιστικές θεωρίες, η έρευνα θα έπρεπε να διεξαχθεί ενώ η εξ αποστάσεως

εργασία εξακολουθούσε να εφαρμόζεται. Με άλλα λόγια, ενώ υπήρχαν ακόμη ειδικά νομοθετικά μέτρα και πριν επανέλθει η κανονικότητα στη ζωή μας. Με αυτόν τον τρόπο θα απέδιδε πραγματικές συνθήκες ζωής και θα απέφευγε να συναντήσει τη δυσαρέσκεια των ανθρώπων που θα καλούνταν να θυμηθούν ένα πρόσφατο οδυνηρό παρελθόν.

- **Διάρκεια** (**Duration**): Ο περιορισμός στο σπίτι, για τους περισσότερους ανθρώπους, αποδείχτηκε πιο απαιτητικός από τη συνηθισμένη ρουτίνα, καθώς έπρεπε να ανταπεξέλθουν στις επαγγελματικές, κοινωνικές και οικογενειακές τους υποχρεώσεις ταυτόχρονα. Ως αποτέλεσμα, ο χρόνος ήταν πιο πολύτιμος από ποτέ και, για να συμμετάσχει κάποιος σε μια έρευνα χωρίς κανένα προφανές κέρδος, έπρεπε να είναι σύντομη και περιεκτική και να μην απαιτεί περισσότερο από 5 έως 10 λεπτά.
- **Προσβασιμότητα** (**Accessibility**): Δεδομένου ότι η παραμονή στο σπίτι ήταν η μόνη αξιόπιστη άμυνα κατά του ιού, η έρευνα έπρεπε να ψηφιοποιηθεί και να κυκλοφορήσει στο διαδίκτυο επιτρέποντας τη συμμετοχή σε άτομα από όλο τον κόσμο.
- **Σαφήνεια** (**Plainness**): Η έρευνα στόχευε εργαζόμενους από πολλούς διαφορετικούς επιχειρηματικούς τομείς που δεν είναι απαραίτητα εξοικειωμένοι με τεχνολογικούς όρους και όρους ασφάλειας πληροφοριών. Κατά συνέπεια, οι ερωτήσεις έπρεπε να είναι απλές εξάγοντας έμμεσα τις απαιτούμενες πληροφορίες. Σε ορισμένες περιπτώσεις, παρασχέθηκε υποβοηθητικό κείμενο για τη διευκόλυνση της κατανόησης της υπό εξέταση ερώτησης.

Λαμβάνοντας υπόψη όλα τα παραπάνω, διαμορφώθηκε ένα διαδικτυακό ερωτηματολόγιο που δεν περιείχε περισσότερες από 23 ερωτήσεις (Πίνακας 9). Κάθε ερώτηση βασίστηκε στο μοντέλο κουλτούρας κυβερνοασφάλειας που παρουσιάστηκε στις προηγούμενες ενότητες (Πίνακας 10) και είχε στόχο να λάβει μια γενικευμένη ανατροφοδότηση [166, 167]. Έχει φιλοξενηθεί σε μια εταιρική λύση cloud και έχει κοινοποιηθεί μέσω δημόσιου συνδέσμου[3]. Τα συλλεγμένα δεδομένα είναι διαθέσιμα δικτυακά [168] και μέσω ενός αποθετηρίου ερευνητικών δεδομένων [169].

[3] https://forms.office.com/r/Y6KpVHdnVb

Πίνακας 9. Ερωτηματολόγιο

Q1	Prior to the COVID-19 crisis, were you able to work from home?	**Q9.2**	How were you informed how to use them?	**Q12.6**	I am proud to work for my organisation.
Q2.1	Did you receive any security guidelines from your employer regarding working from home?	**Q10.1**	Has your company adopted a specific collaboration solution?	**Q12.7**	I have access to the things I need to do my job well.
Q2.2*	Please describe the main (2-3) security guidelines provided.	**Q10.2***	What abilities does it offer?	**Q13**	What is your age?
Q3	What kind of devices are you using to connect to your corporate working environment?	**Q11.1**	Did you face any of the below cyber-security related threats during the COVID-19 crisis?	**Q14**	What is the highest degree or level of school you have completed?
Q4	Are these devices accessed by users other than yourself?	**Q11.2***	Please name any other cyber-security threats you encountered during this period, not listed above.	**Q15**	Please select the business domain of the organisation you work for.
Q5	These devices are personal or corporate assets?	**Q12.1**	To what extent do you agree with the following statements: I prefer working from home than going to the office.	**Q16**	Which of the following best describes your work position?
Q6	Are these devices managed by your organisation?	**Q12.2**	I work more productively from home.	**Q17**	Comments
Q7	Which of the following apply for the devices you currently use for your working from home employment? (providing security measures alternatives, e.g. antivirus, password protections)	**Q12.3**	I collaborate with my colleagues as effectively as when we are in office.		
Q8	How do you obtain access to your corporate working environment?	**Q12.4**	I am satisfied by my employer’s approach to the crisis.		

Q9.1	Were you asked to use applications or services that you were unfamiliar with, because of the need for remote working?	**Q12.5**	I have all the support I need to face any technical problems I have (e.g. corporate access issues, infrastructure failures, etc.).		

Πίνακας 10. Συσχέτιση ερωτηματολογίου με το Μοντέλο Κουλτούρας Κυβερνοασφάλειας

	Organisational Level						**Individual Level**			
	Assets	**Continuity**	**Access and Trust**	**Operations**	**Defense**	**Security Governance**	**Attitude**	**Awareness**	**Behaviour**	**Competency**
Q1	- Network Infrastructure Management - Network Configuration Management		- Access Management - External Environment Connections							
Q2.1		Change Management		Organisational Culture and Top Management Support	Security Awareness and Training Program	Security Management Maturity				
Q2.2*										
Q3	Hardware Assets Management		Access Management							
Q4			Access Management						- Policies and Procedures Compliance - Security Behaviour	
Q5	- Hardware Assets Management - Information Resources Management		- Access Management - External Environment Connections							

	- Data Security and Privacy									
Q6	- Hardware Assets Management - Software Assets Management - Information Resources Management - Data Security and Privacy		- Access Management - External Environment Connections							
Q7	- Hardware Configuration Management - Information Resources Management - Data Security and Privacy				Malware Defense			Policies and Procedures Awareness	- Policies and Procedures Compliance - Security Behaviour - Security Agent Persona	
Q8	- Network Infrastructure Management - Network Configuration Management		- Access Management - External Environment Connections		Boundary Defense					
Q9.1		- Business Continuity & Disaster Recovery - Change Management								
Q9.2			Communication	Organisational Culture and Top Management Support						

Q10.1				Operating Procedures						
Q10.2*										
Q11.1									- Security Behaviour - Security Agent Persona	Security Skills Evaluation
Q11.2*										
Q12.1							Employee Climate			
Q12.2										
Q12.3										
Q12.4							Employee Satisfaction			
Q12.5										
Q12.6										
Q12.7										
Q13							Employee Profiling			
Q14										
Q15										
Q16										

4.3.1 Έλεγχος Εγκυρότητας

Έχοντας διαμορφώσει μια πρώτη έκδοση του ερωτηματολογίου, το επόμενο βήμα ήταν μια δοκιμή εγκυρότητας στην οποία ζητήθηκε από 20 περίπου άτομα να εξετάσουν και να συμπληρώσουν την έρευνα. Αυτή η φάση διεξήχθη με μια εξειδικευμένη ομάδα αποτελούμενη από εμπειρογνώμονες έρευνας, έμπειρους ερευνητές και αναλυτές, πιστοποιημένους αξιωματικούς ασφαλείας και τεχνολογίας και απλούς εργαζόμενους με μέτριες τεχνολογικές γνώσεις. Στόχος του ήταν να εντοπίσει διφορούμενες ερωτήσεις ή διατυπώσεις, ασαφείς οδηγίες ή άλλα προβλήματα πριν από την ευρεία εφαρμογή του [170]. Η απολογιστική και η γνωστική συνέντευξη βοήθησαν στην αξιολόγηση της σαφήνειας των ερωτήσεων και στην κατανόηση των όρων [171]. Οι τεχνικές think-aloud και λεκτικής ανίχνευσης [172] αξιοποιήθηκαν για τον εντοπισμό περιοχών πιθανής παρανόησης. Λαμβάνοντας υπόψη τα δεδομένα από αυτήν τη φάση, φτάσαμε σε μια τελική έκδοση της έρευνας.

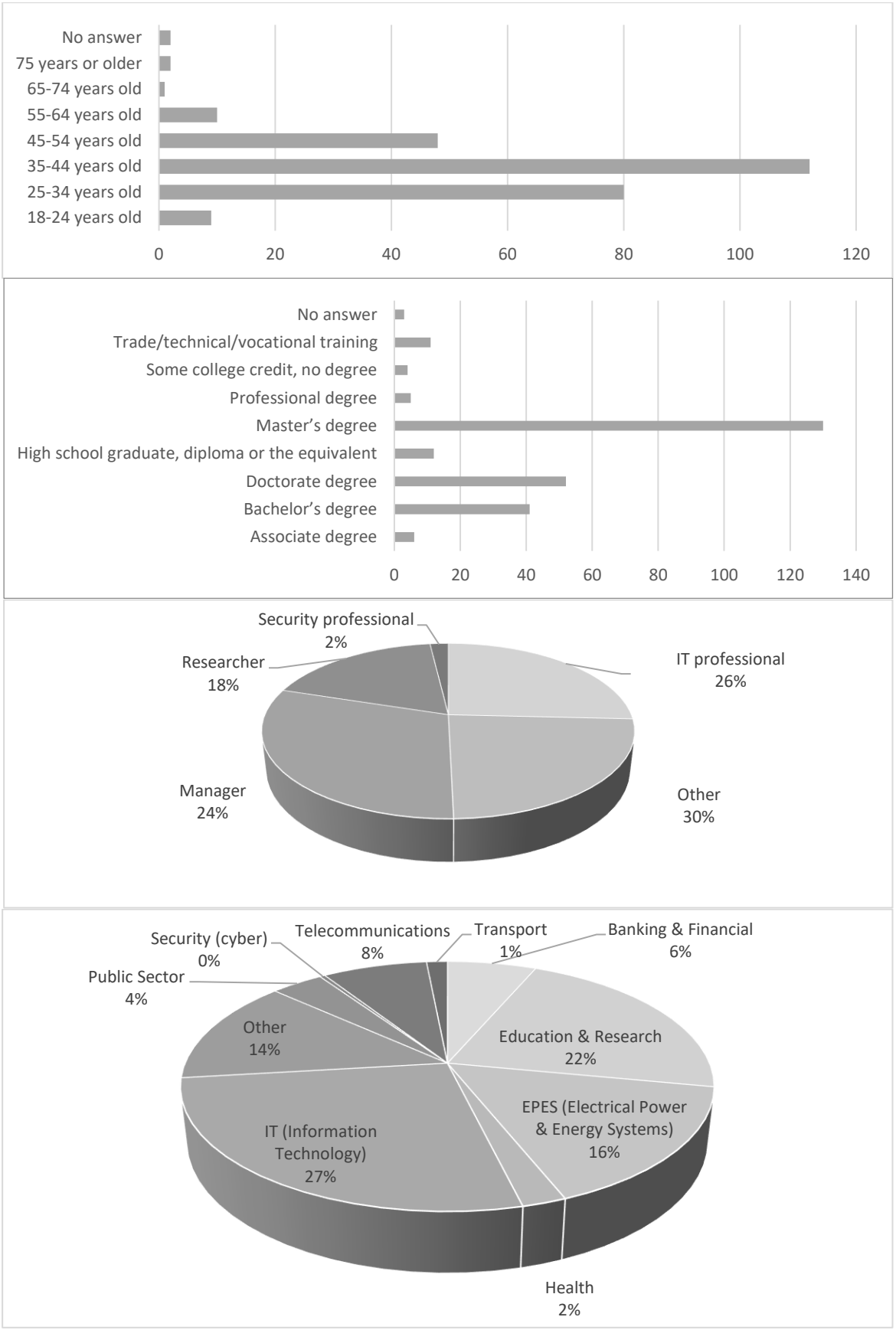
4.3.2 Επιλογή Δείγματος

Η συγκεκριμένη εφαρμογή στόχευε στο εργατικό δυναμικό χωρών που επλήγησαν από την πανδημία του κορονοϊού. Στόχος του ήταν να εντοπίσει τις παρενέργειες στην κουλτούρα κυβερνοασφάλειας με ιδιαίτερη έμφαση στις ευρωπαϊκές κρίσιμες υποδομές. Ως εκ τούτου, επιλέχθηκαν εκπρόσωποι από την ενέργεια, τις μεταφορές, την ύδρευση, τις τράπεζες, την χρηματοπιστωτική αγορά, την υγειονομική περίθαλψη και τις ψηφιακές υποδομές από διάφορες ευρωπαϊκές χώρες (π.χ. Κύπρος, Γαλλία, Γερμανία, Ελλάδα, Ιταλία, Ρουμανία, Ισπανία) που επλήγησαν από την πανδημία. Τέτοιοι οργανισμοί, οι οποίοι έπρεπε να παραμείνουν πλήρως λειτουργικοί και να περιορίσουν στο ελάχιστο τις απειλές κατά των λειτουργιών τους κατά τη διάρκεια αυτής της αρκετά απαιτητικής χρονικής περιόδου, απαιτούν μια βαθύτερη κουλτούρα κυβερνοασφάλειας. Κατά συνέπεια, η παρακολούθηση και η αξιολόγηση της κατάστασής τους και ο εντοπισμός πιθανών θεμάτων κουλτούρας έχει ιδιαίτερο επιστημονικό ενδιαφέρον.

4.3.3 Εκπόνηση Εκστρατείας Αξιολόγησης

Μια ψηφιακή πρόσκληση απεστάλη στο επιλεγμένο δείγμα, ώστε να διασφαλιστεί ότι η συλλογή δεδομένων θα περιοριζόταν στη στοχοθετημένη ομάδα. Η διάθεσή της μέσω ποικίλων καναλιών επικοινωνίας, αν και εφικτή, απορρίφθηκε με στόχο την ενίσχυση της εγκυρότητας των αποτελεσμάτων.

Η παρουσιαζόμενη έρευνα ήταν διαθέσιμη για συμμετοχή για 27 ημέρες, ξεκινώντας από τις 7 Απριλίου 2020 έως τις 3 Μαΐου 2020. Κατά τη διάρκεια αυτής της περιόδου, 264 συμμετέχοντες επισκέφτηκαν τη δικτυακή φόρμα της έρευνας και συμπλήρωσαν το ερωτηματολόγιο σε περίπου 8 λεπτά (μέσος χρόνος ολοκλήρωσης). Περίπου το 90% των συμμετεχόντων ήταν ηλικίας μεταξύ 25 και 54 ετών ενώ το 84,46% είχε πτυχίο ανώτερης εκπαίδευσης (πτυχίο, μεταπτυχιακό ή διδακτορικό). Εκπρόσωποι από διαφορετικούς επιχειρηματικούς τομείς παρείχαν σχόλια στην έρευνά μας με τρεις κυρίαρχους τομείς: IT (Τεχνολογία Πληροφορικής) (27%), Εκπαίδευση και Έρευνα (22%) και EPES (Electrical Power and Energy Systems) (16%) [173]. Η Εικόνα 12 παρουσιάζει αναλυτικά τα γενικά δημογραφικά στοιχεία της μελέτης μας.

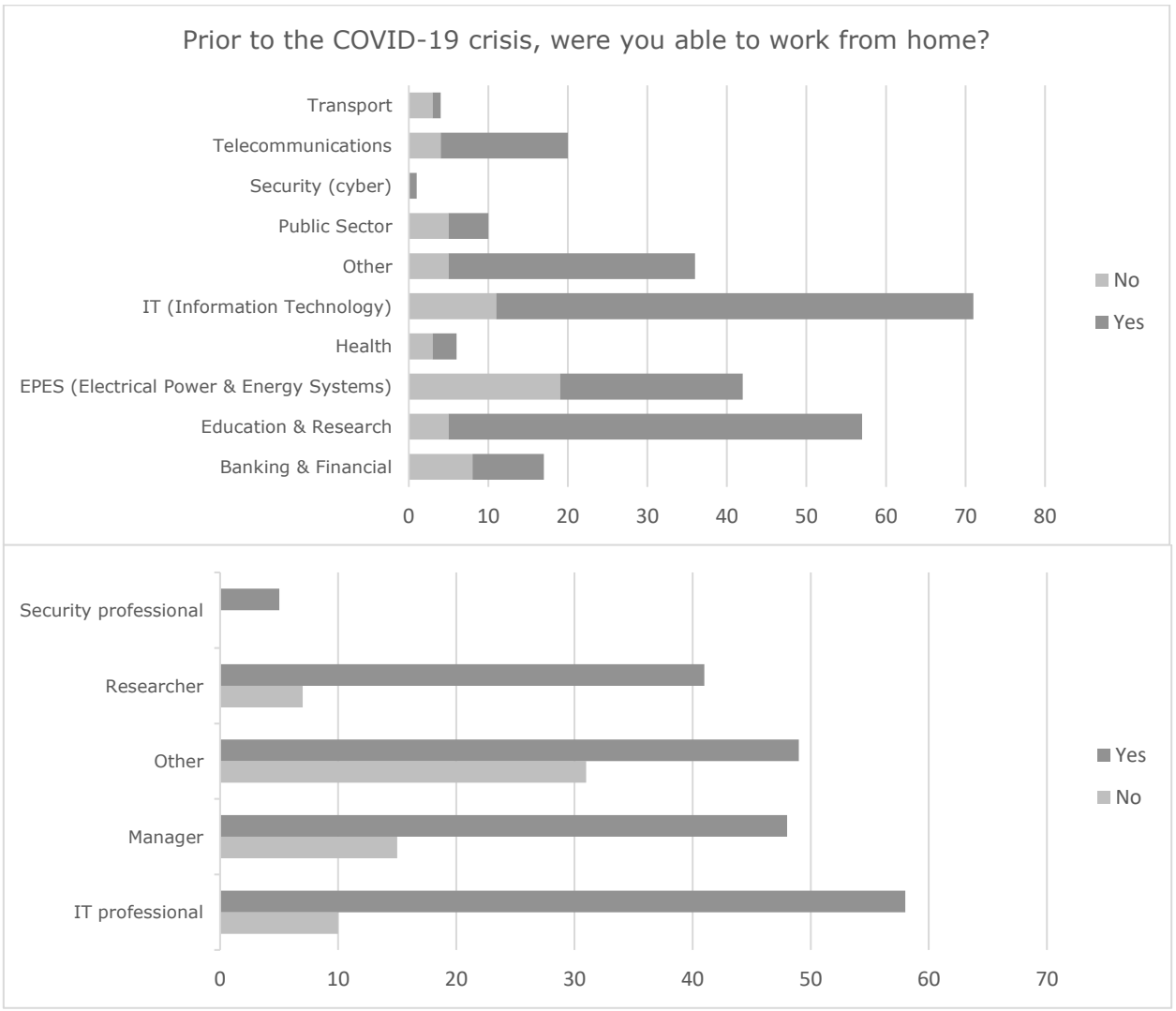


Εικόνα 12. Δημογραφικές πληροφορίες συμμετεχόντων: (α) Ηλικία, (β) Μορφωτικό Επίπεδο, (γ) Τομέας Απασχόλησης, (δ) Επιχειρηματικό Πεδίο

4.4 Ανάλυση Αποτελεσμάτων

4.4.1 Δυνατότητα απομακρυσμένης εργασίας

Με βάση τις απαντήσεις που δόθηκαν στην έρευνά μας, 1 στους 4 συμμετέχοντες δεν μπορούσε να εργαστεί από το σπίτι πριν από την κρίση COVID-19. Αυτό το ποσοστό παρέμεινε για τους διευθυντές, ενώ για τους ερευνητές και τους επαγγελματίες πληροφορικής περιορίστηκε σε 1 στους 7. Σχεδόν οι μισοί (47,06%) των εργαζομένων στον τραπεζικό και χρηματοοικονομικό τομέα ανέφεραν ότι δεν είχαν δυνατότητα τηλεργασίας πριν από την πανδημία. Περίπου το ίδιο ποσοστό (45,24%) παρατηρήθηκε στον τομέα EPES, ενώ οι τομείς της πληροφορικής και των τηλεπικοινωνιών αποδείχθηκαν καλύτερα εδραιωμένοι όσον αφορά την εξ αποστάσεως εργασία, όπως φαίνεται στην Εικόνα 13(α).

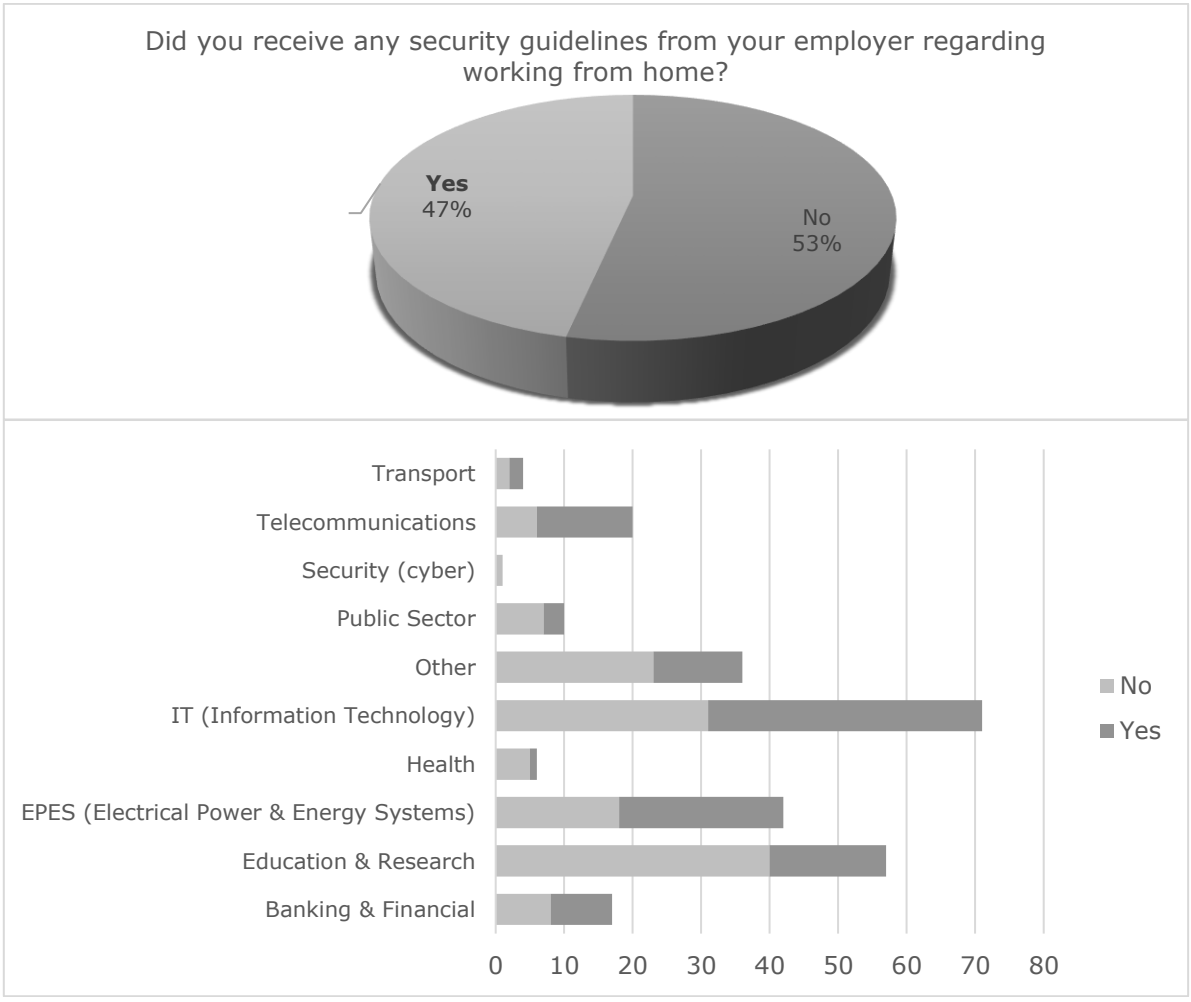


Εικόνα 13. Δυνατότητα απομακρυσμένης εργασίας ανά (α) επιχειρηματικό πεδίο και (β) θέση εργασίας

Αυτά τα ποσοστά, σε συνδυασμό με τη φύση της εργασίας και το επίπεδο ψηφιοποίησης των συμμετεχουσών επιχειρήσεων, δεν ήταν τα αναμενόμενα. Επιπλέον, υπογραμμίζουν μια σειρά πρόσθετων δυσκολιών που έπρεπε να αντιμετωπίσουν συγκεκριμένοι επιχειρηματικοί κλάδοι κατά τη διάρκεια της πανδημίας, καθώς δεν είχαν τα μέσα και πιθανώς τη νοοτροπία της εξ αποστάσεως εργασίας.

4.4.2 Επίγνωση και ετοιμότητα ασφάλειας

Κατά τη διάρκεια μιας περιόδου όπου άκμαζε το κυβερνοέγκλημα, οι απειλές για την ασφάλεια, οι απάτες και οι παραβιάσεις είχαν υπογραμμιστεί και είχαν δοθεί συστάσεις από οργανισμούς και ειδικούς στον κυβερνοχώρο σε όλο τον κόσμο [174, 175, 176], αποτελεί έκπληξη το γεγονός ότι το 53% των συμμετεχόντων αναφέρει ότι δεν έχει λάβει οδηγίες ασφαλείας από τους εργοδότες τους σχετικά με την εργασία από το σπίτι. Ακόμη πιο ανησυχητικό είναι το γεγονός ότι το 44,44% των εργαζομένων που δεν είχαν δυνατότητα εξ αποστάσεως εργασίας και, ενδεχομένως, εμπειρία, πριν την κρίση, δηλώνουν ότι δεν είχαν συμβουλές ασφαλείας για τη νέα εργασιακή τους πραγματικότητα.



Εικόνα 14. Επίγνωση και ετοιμότητα ασφάλειας (α) συνολικά και (β) ανά επιχειρηματικό πεδίο

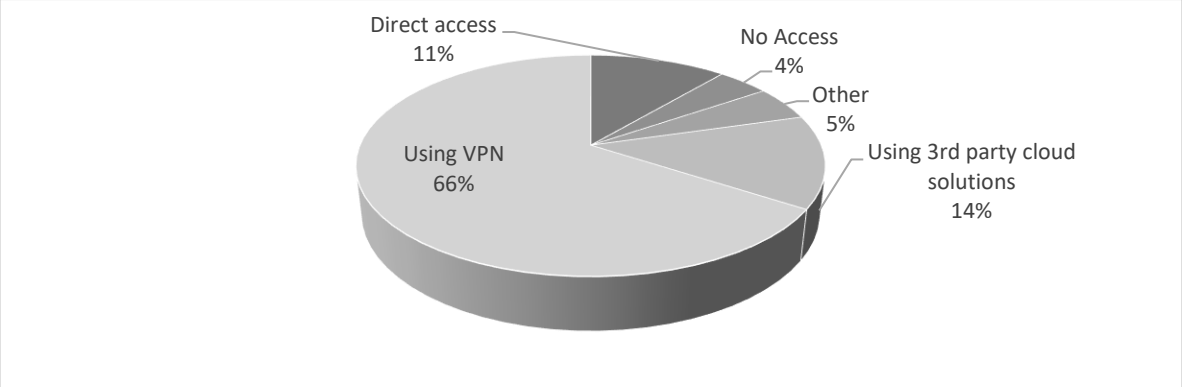
Η αποτυχία παροχής συμβουλών, επιβολής και εκπαίδευσης του εργατικού δυναμικού, ειδικά σε απαιτητικές περιόδους και κάτω από αγχωτικές συνθήκες, είναι μια ανησυχητική ένδειξη τόσο για τις διαδικασίες διαχείρισης οργανωτικών αλλαγών όσο και για το πρόγραμμα ευαισθητοποίησης και εκπαίδευσης για την ασφάλεια. Κατά συνέπεια, προκύπτουν αμφιβολίες σχετικά με το εάν οι ειδικοί της εταιρικής ασφάλειας (security officers) γνώριζαν την αξιοσημείωτη αύξηση του εγκλήματος στον κυβερνοχώρο και αντιλήφθηκαν τους κινδύνους που διατρέχουν σε συνδυασμό με το νέο καθεστώς απασχόλησης. Ανεξάρτητα από το ποια είναι η αλήθεια, δεν απέδωσαν καθόλου στο να ενημερώσουν και να υποστηρίξουν τη συνολική οργανωτική κουλτούρα κυβερνοασφάλειας.

Από την άλλη πλευρά, οι επιχειρήσεις που επέδειξαν καλύτερο επίπεδο οργανωτικής κουλτούρας και υποστήριξης από την ανώτερη διοίκηση, παρέχοντας μια σειρά από κατευθυντήριες γραμμές για την κυβερνοασφάλεια κατά την περίοδο του κορονοϊού, επικεντρώθηκαν κυρίως στη διαχείριση πρόσβασης στο εταιρικό δίκτυο (Virtual Private Network, VPN, χρήση και αποφυγή ασύρματων συνδέσεων) και λιγότερο στην ασφάλεια χρηστών (προστασία με κωδικό πρόσβασης, ενημέρωση λογισμικού, email phishing) όπως απεικονίζεται στον Πίνακας 11.

Πίνακας 11. Κορυφαίες συστάσεις ασφαλείας κατά την εξ αποστάσεων εργασίας την περίοδο του κορονοϊού.

Top Security Guidelines	
Use VPN (Virtual Private Network) to access corporate network	32,52%
Ensure password security and usage	12,19%
Be careful of phishing emails	10,56%
Avoid usage of unsecure wireless connections	10,56%
Lock working station (PC, laptop, etc.) when unattended	10,56%
Ensure daily software updates	7,31%

Αυτή η οργανωτική τάση επαληθεύεται ακόμα από τις πολιτικές διαχείρισης πρόσβασης στο δίκτυο που εφαρμόστηκαν αυτήν την περίοδο. Η Εικόνα 15. παρουσιάζει τον τρόπο διαχείρισης της δικτυακής πρόσβασης των χρηστών στις οργανωτικές υποδομές και πόρους, με μόλις το 11% να αναφέρει ελεύθερη πρόσβαση ενώ στις υπόλοιπες περιπτώσεις οι συμμετέχοντες αναφέρουν πιο ισχυρές και ασφαλείς λύσεις.

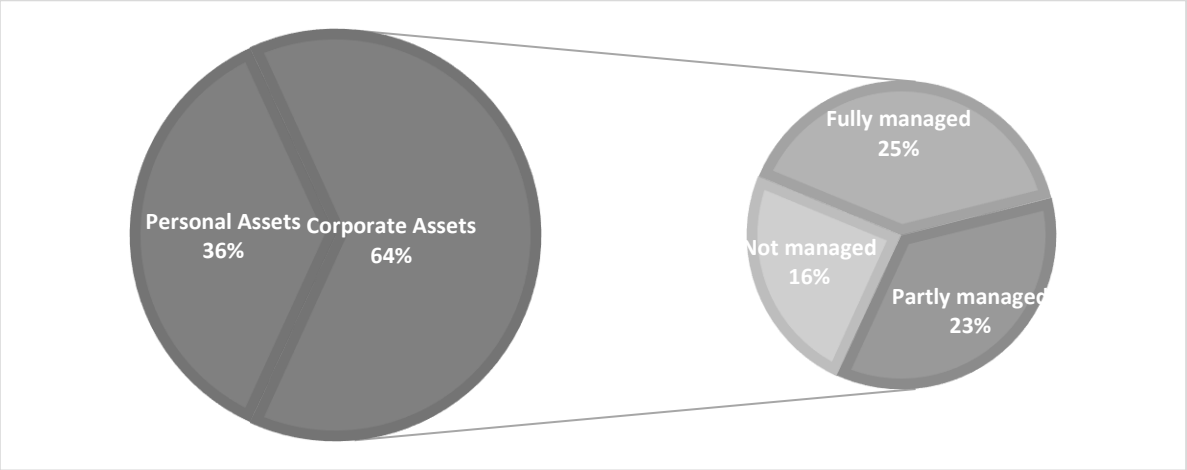


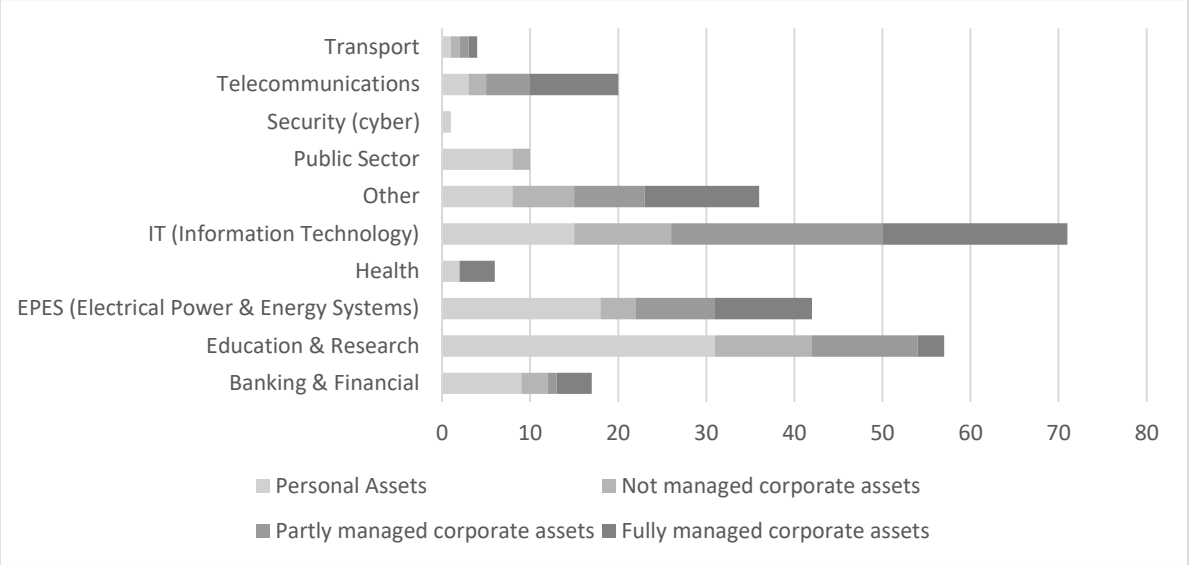
Εικόνα 15. Διαχείριση δικτυακής πρόσβασης και ασφάλειας

4.4.3 Διαχείριση Και Ασφάλεια Υλικού

Προς ενίσχυση του ευρήματος της προηγούμενης ενότητας, σημειώνεται ότι περίπου το 36% των περιουσιακών στοιχείων που χρησιμοποιήθηκαν κατά την τηλεργασία ήταν προσωπικά και μόλις το 16% ήταν εταιρικά χωρίς σύστημα MDM (Mobile Device Management) για την επιβολή πολιτικών ασφαλείας. Συνεπώς, αθροιστικά, το 52% των πόρων που χρησιμοποιήθηκαν για απομακρυσμένη εργασία, αποκτώντας πρόσβαση σε εταιρικά δίκτυα, δεν εντάχθηκαν στους προβλεπόμενους κανόνες ασφαλείας και στην αναγκαία επιτήρηση. Προς περαιτέρω επιδείνωση των ευρημάτων, το 23% των εταιρικών περιουσιακών στοιχείων ήταν εν μέρει διαχειρίσιμα από τους οργανισμούς.

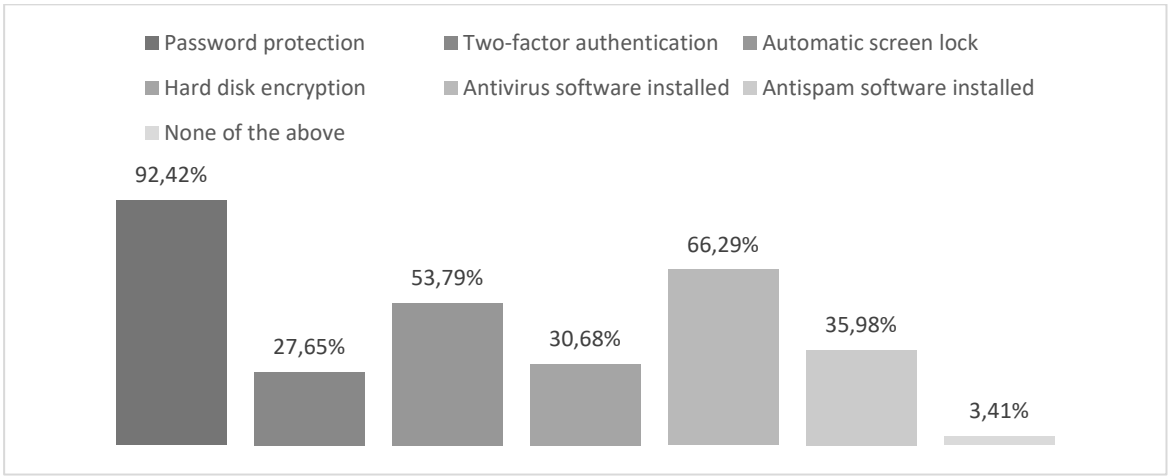
Όπως παρουσιάζεται στην Εικόνα 16, αυτά τα ποσοστά διαφοροποιούνται σημαντικά στους διάφορους επιχειρηματικούς τομείς. Εστιάζοντας στους τρεις κυρίαρχους κλάδους της έρευνάς μας (αυτοί που παρουσίασαν επαρκές δείγμα απαντήσεων), IT, Education & Research και EPES, το αντίστοιχο ποσοστό (προσωπικά περιουσιακά στοιχεία και εταιρικά περιουσιακά στοιχεία χωρίς σύστημα διαχείρισης) ανέρχεται σε 36,62%, 73,68% και 52,38% αντίστοιχα.

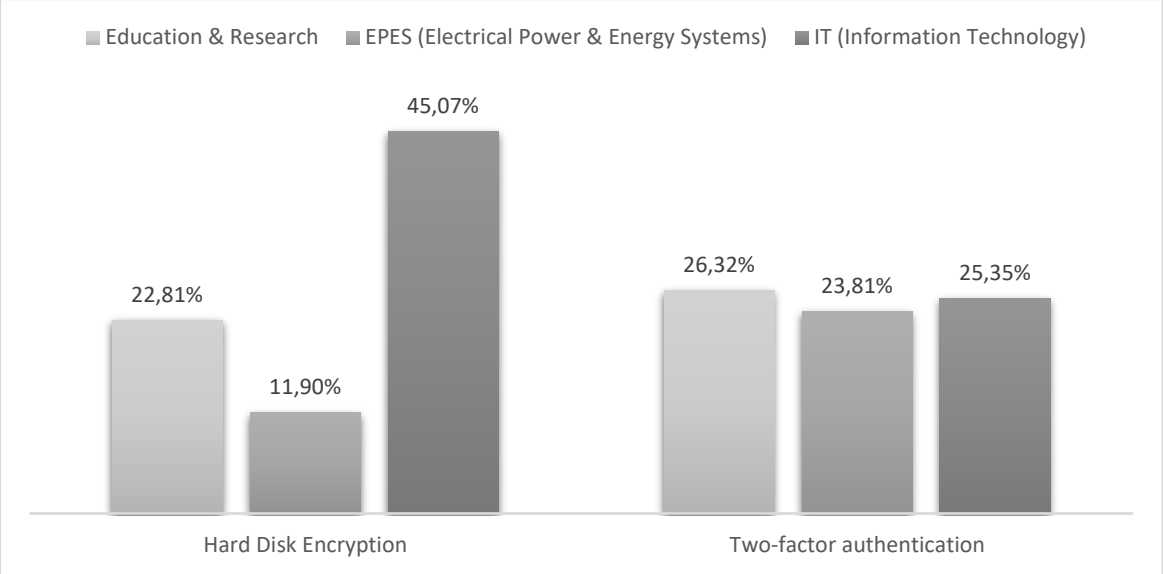




Εικόνα 16. Διαχείριση και ασφάλεια υλικού

Τα χαρακτηριστικά ασφαλείας των πόρων που χρησιμοποιήθηκαν από τους συμμετέχοντες στην έρευνα παρουσιάζονται συνοπτικά στην Εικόνα 17. Η πρώτη αποκαλυπτική παρατήρηση είναι ότι ένα μικρό ποσοστό 3,41% δεν πληρούσε κανέναν από τους βασικούς κανόνες ασφαλείας. Περίπου το 1,89% των χρησιμοποιούμενων πόρων δεν παρουσίαζε κανέναν έλεγχο πρόσβασης ή μηχανισμό ελέγχου ταυτότητας (προστασία με κωδικό πρόσβασης ή έλεγχος ταυτότητας δύο παραγόντων, Multi-Factor Authentication). Αν και φαίνεται να είναι ένα ενθαρρυντικό στατιστικό αποτέλεσμα, οι ειδικοί σε θέματα ασφάλειας θα υποστήριζαν ότι η επίδραση αυτών των μέτρων ασφαλείας σχεδόν εκμηδενίζεται όταν δεν είναι ενεργοποιημένος κανένας μηχανισμός αυτόματου κλειδώματος, όπως φαίνεται να συμβαίνει για 1 στα 2 στοιχεία (assets) που χρησιμοποιούνται, ή όταν η χρήση τους επιτρέπεται σε άλλα άτομα εκτός από τα εξουσιοδοτημένα, περίπου το 15% του δείγματός μας.





Εικόνα 17. Χαρακτηριστικά ασφαλείας υλικού

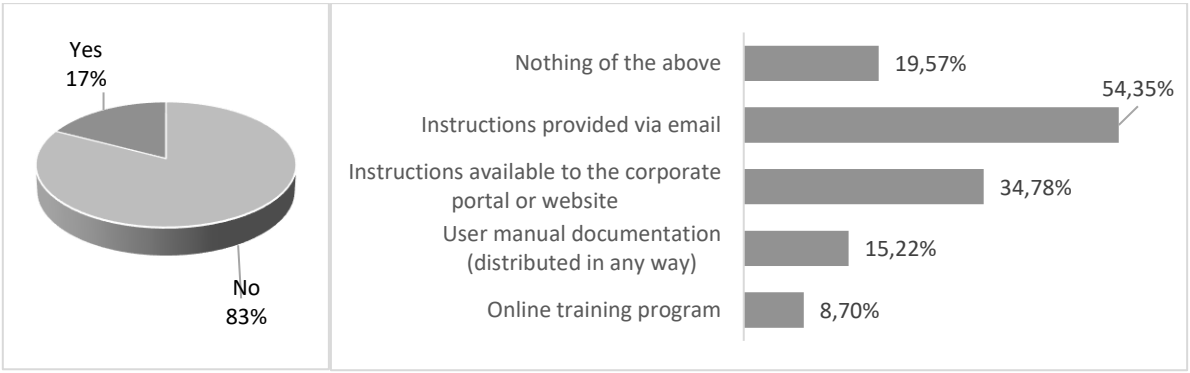
4.4.4 Διαχείριση αλλαγών

Μια άλλη αξιοσημείωτη παρατήρηση είναι ότι πιο προηγμένες τεχνικές ασφάλειας, όπως ο έλεγχος ταυτότητας δύο παραγόντων (27,65%) και η κρυπτογράφηση σκληρού δίσκου (30,68%), δεν έχουν ακόμη υιοθετηθεί από τις περισσότερες εταιρείες, ενώ καθιερωμένες λύσεις λογισμικού, όπως τα antivirus (66,29%), είναι πιο διαδεδομένα.

Όσον αφορά στις λύσεις λογισμικού antispam, δεν θα ήταν ασφαλές να καταλήξουμε σε συμπεράσματα με βάση τις απαντήσεις της έρευνάς μας, καθώς πολλοί οργανισμοί χρησιμοποιούν μια κεντρική προσέγγιση, συνήθως συνδεδεμένη με τη διαθέσιμη λύση αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου, η οποία είναι απολύτως διαφανής στον τελικό χρήστη.

Οι περισσότεροι οργανισμοί, στην προσπάθειά τους να προσαρμοστούν στις ειδικές συνθήκες αυτής της, πρωτοφανούς για τον αιώνα μας, υγειονομικής κρίσης, έπρεπε να προμηθευτούν νέες τεχνολογικές λύσεις για τη διευκόλυνση των λειτουργιών τους και της νέας εργασιακής πραγματικότητας. Κατά συνέπεια, ζητήθηκε από ορισμένους υπαλλήλους να χρησιμοποιήσουν εφαρμογές ή υπηρεσίες με τις οποίες δεν ήταν εξοικειωμένοι κατά την απομακρυσμένη εργασία τους. Με βάση τα αποτελέσματα της έρευνάς μας, αυτό συνέβη για 1 στους 6 από τους συμμετέχοντες.

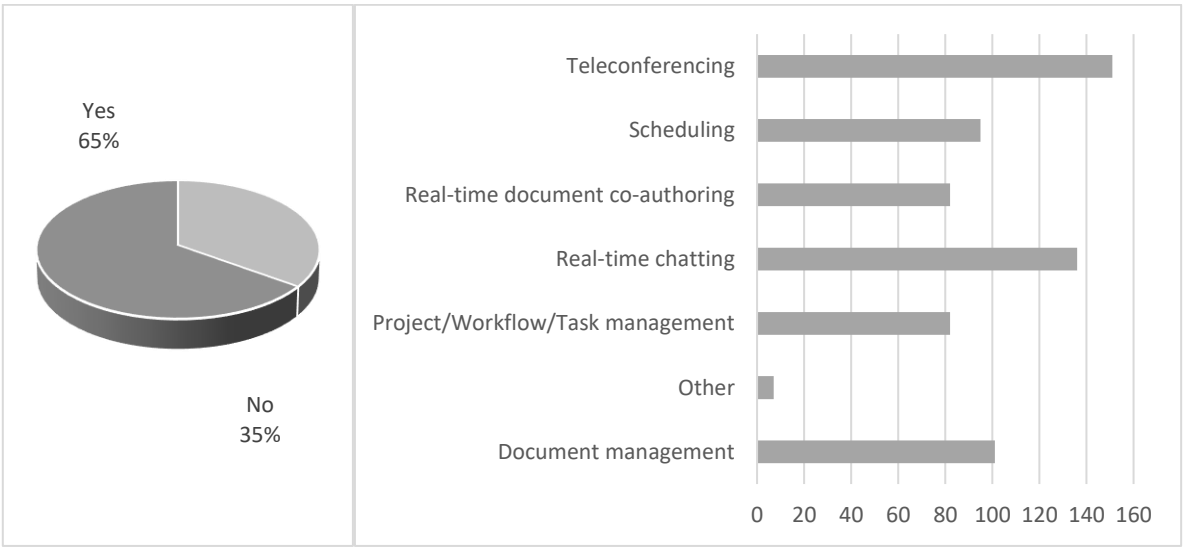
Αν και αυτός είναι σίγουρα ένας καλός δείκτης ευελιξίας για τις επιχειρήσεις, ο τρόπος που επικοινωνούνται αυτές οι αλλαγές και ενημερώνουν το εργατικό δυναμικό τους προκειμένου να προσαρμοστεί σε αυτές επηρεάζει έντονα την αποτελεσματικότητα των στρατηγικών διαχείρισης αλλαγών. Σχεδόν στις μισές περιπτώσεις, οι οδηγίες δόθηκαν μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Δεύτερη επιλογή επικοινωνίας ήταν η χρήση εταιρικών πυλών και ιστοσελίδων (34,78%), ενώ η πιο διαδραστική και συνήθως γόνιμη μέθοδος εκπαίδευσης χρησιμοποιήθηκε μόλις με ποσοστό 8,70%.

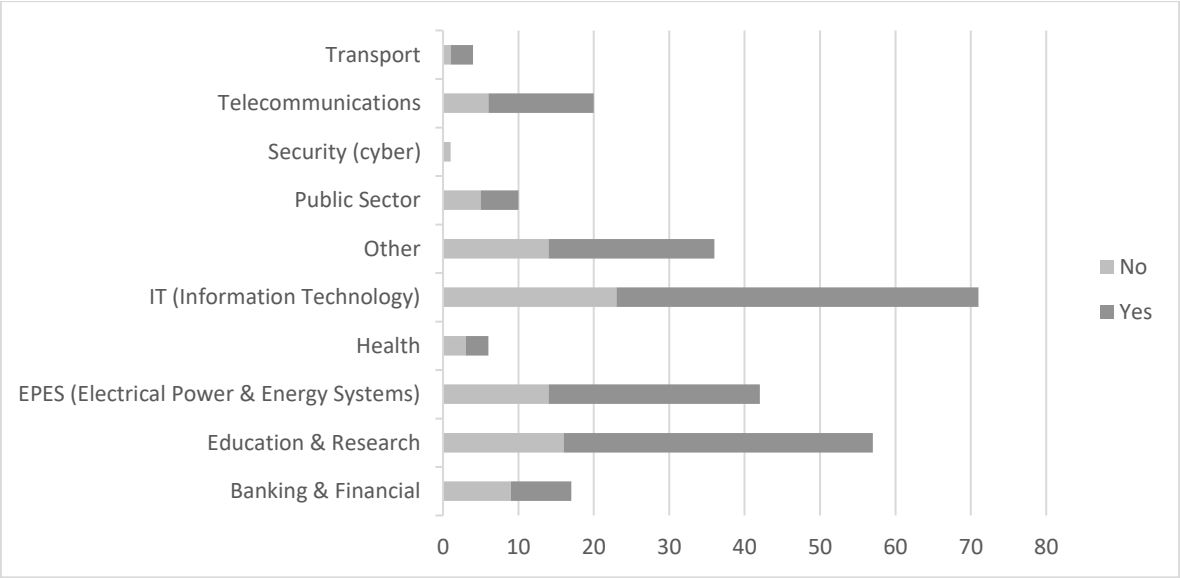


Εικόνα 18. Χρήση νέων τεχνολογιών κατά την απομακρυσμένη εργασία και τρόπος ενημέρωσης χρηστών για αυτές

4.4.5 Απομακρυσμένη Συνεργασία

Η εργασία από το σπίτι δεν πρέπει σε καμία περίπτωση να μεταφραστεί σε απομονωμένη εργασία. Η συνεργασία και η ομαδική προσπάθεια πρέπει να διευκολυνθούν και να προωθηθούν, ειδικά κατά τη διάρκεια αυτής της χρονικής περιόδου που επιβάλλεται η γενική απομόνωση ως η μόνη άμυνα κατά της εξάπλωσης του ιού. Οι εταιρείες αναμένεται να παρέχουν όλα τα απαραίτητα μέσα για να βοηθήσουν τους υπαλλήλους τους να είναι παραγωγικοί, αποτελεσματικοί και συνεργάσιμοι. Οι τρέχουσες λύσεις συνεργασίας προσφέρουν πολυάριθμες δυνατότητες από τηλεδιάσκεψη και συνομιλία σε πραγματικό χρόνο έως διαχείριση εγγράφων και από κοινού συγγραφή σε πραγματικό χρόνο, διαχείριση έργων και προγραμματισμό εργασιών. Με βάση την έρευνά μας, 2 στους 3 συμμετέχοντες αναφέρουν ότι ο οργανισμός στον οποίο εργάζονται έχει υιοθετήσει ένα εργαλείο εταιρικής συνεργασίας. Αυτή η αναλογία, επαληθεύεται ως ένα βαθμό για τους περισσότερους από τους εξεταζόμενους επιχειρηματικούς τομείς, όπως φαίνεται στην Εικόνα 19, αποδεικνύοντας μια τάση που ευνοεί τέτοιες λύσεις αιχμής.



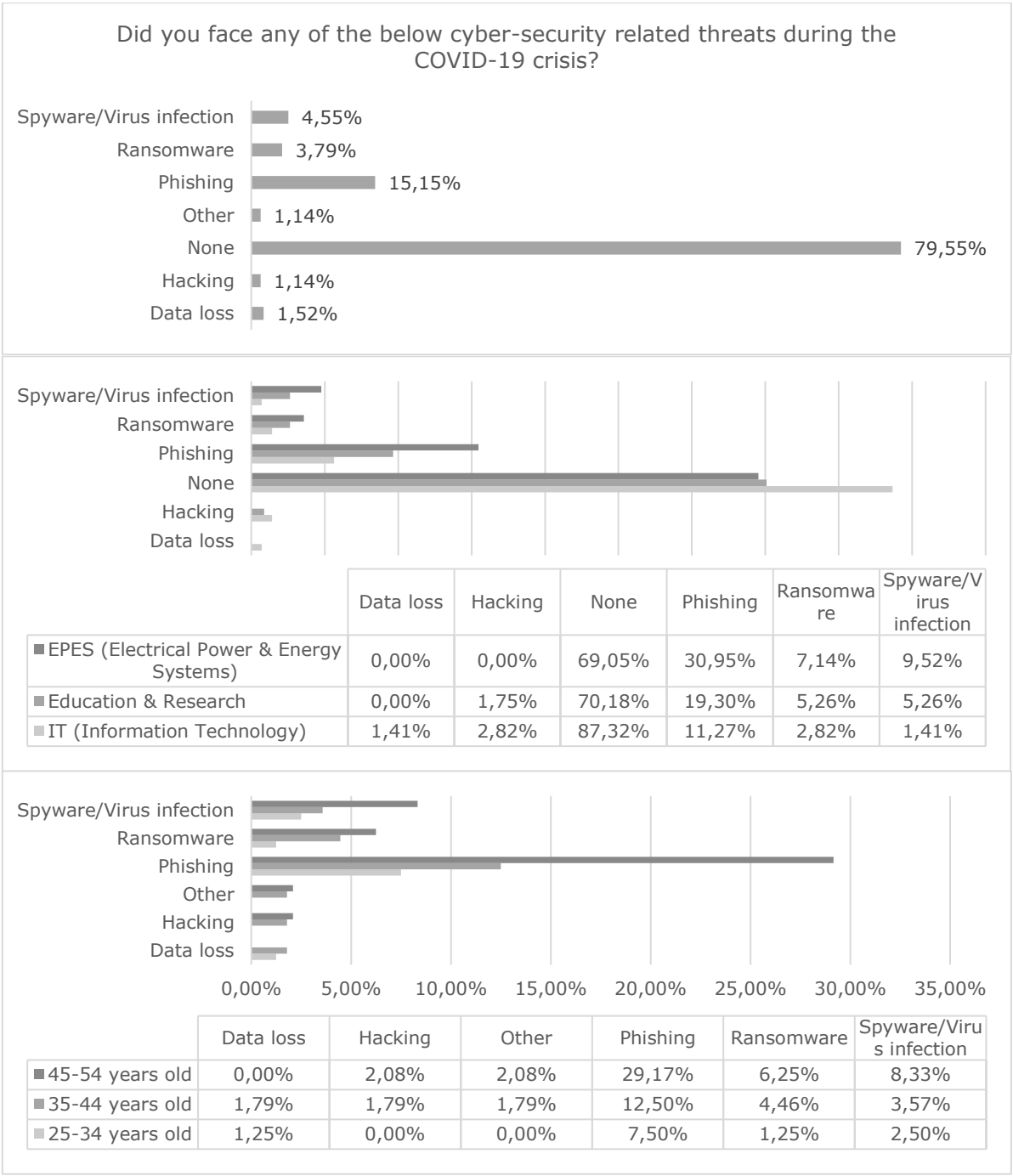


Εικόνα 19. Απομακρυσμένη συνεργασία

4.4.6 Διαχείριση Περιστατικών Ασφαλείας

Ζητήθηκε από τους συμμετέχοντες να αναφέρουν εάν αντιμετώπισαν κυβερνοαπειλές κατά τη διάρκεια της κρίσης COVID-19 χωρίς να αποκαλύψουν ευαίσθητες πληροφορίες σχετικά με αυτά τα περιστατικά. Περίπου 1 στους 5 ανέφεραν ότι αντιμετώπισαν κάποιου είδους απειλή με κυρίαρχες τις επιθέσεις phishing (15,15%).

Εξετάζοντας προσεκτικότερα αυτά τα αποτελέσματα και εστιάζοντας στους τρεις επιχειρηματικούς τομείς με το μεγαλύτερο ποσοστό συμμετοχής (Εικόνα 20), παρατηρούμε ότι τα ποσοστά απειλής αυξάνονται δραστικά μεταβαίνοντας από το IT στην Εκπαίδευση & Έρευνα και τέλος στον τομέα EPES. Είναι αξιοσημείωτο ότι οι διαφορές σε αυτή την περίπτωση είναι σημαντικές. Για παράδειγμα, περιπτώσεις μόλυνσης από λογισμικό υποκλοπής spyware/ιού εμφανίζονται 6 φορές πιο συχνά στον τομέα EPES σε σύγκριση με τον τομέα IT, ενώ οι απόπειρες ηλεκτρονικού ψαρέματος 3 φορές πιο συχνά. Μια άλλη ενδιαφέρουσα παρατήρηση είναι ότι η απώλεια δεδομένων και η παραβίαση απορρήτου αναφέρονται κυρίως από υπαλλήλους IT, εγείροντας προβληματισμούς εάν αυτό ισχύει πραγματικά. Ήταν οι μόνοι που βίωσαν τέτοιου είδους απόπειρες εγκλήματος στον κυβερνοχώρο ή ήταν οι μόνοι έμπειροι που παρατήρησαν, υπερασπίστηκαν τον εαυτό τους και κατήγγειλαν τέτοια περιστατικά; Αυτές οι παρατηρήσεις σε συνδυασμό με τα αποτελέσματα διαχείρισης και ασφάλειας υλικού που παρουσιάστηκαν στις προηγούμενες παραγράφους αποδεικνύουν την αποτελεσματικότητα των πολιτικών και των μέτρων ασφαλείας των εταιρειών πληροφορικής έναντι των υπολοίπων συμμετεχόντων τομέων.



	Data loss	Hacking	None	Phishing	Ransomware	Spyware/Virus infection
EPES (Electrical Power & Energy Systems)	0,00%	0,00%	69,05%	30,95%	7,14%	9,52%
Education & Research	0,00%	1,75%	70,18%	19,30%	5,26%	5,26%
IT (Information Technology)	1,41%	2,82%	87,32%	11,27%	2,82%	1,41%

	Data loss	Hacking	Other	Phishing	Ransomware	Spyware/Virus infection
45-54 years old	0,00%	2,08%	2,08%	29,17%	6,25%	8,33%
35-44 years old	1,79%	1,79%	1,79%	12,50%	4,46%	3,57%
25-34 years old	1,25%	0,00%	0,00%	7,50%	1,25%	2,50%

Εικόνα 20. Περιστατικά ασφαλείας κατά την περίοδο της πανδημίας

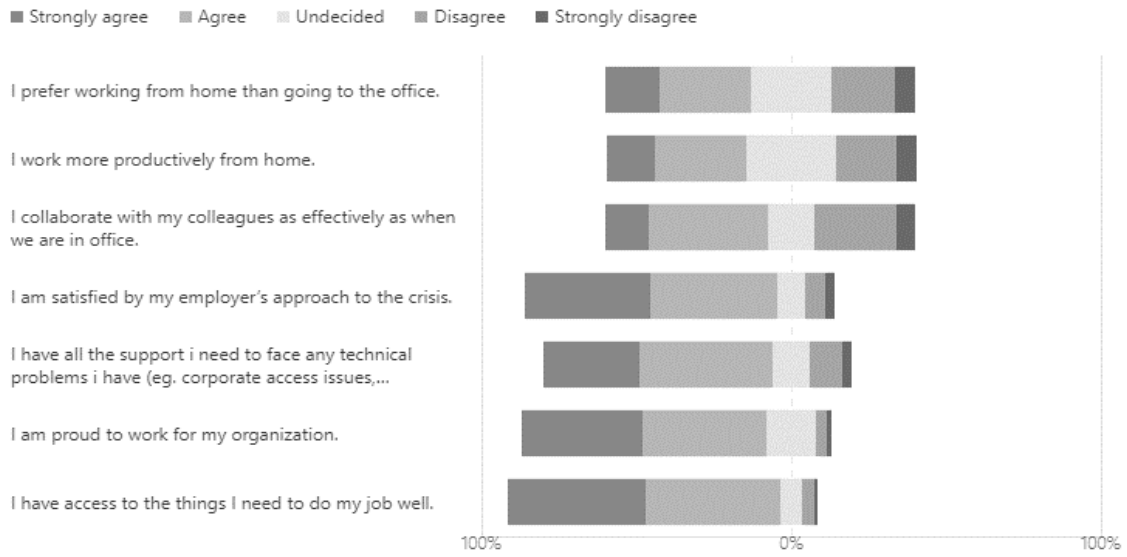
Από την άλλη, στην ίδια εικόνα αποκαλύπτεται μια αύξηση στην αναφορά απειλών στον κυβερνοχώρο κατά τη μετάβαση από νεότερους σε μεγαλύτερους ηλικιακά συμμετέχοντες. Οι αναφερόμενες μολύνσεις από ransomware και spyware/ιούς φτάνουν έως και το 6,25% και το 8,33% για ερωτηθέντες ηλικίας 45-54 ετών, ενώ τα αντίστοιχα ποσοστά για 25-34 ετών περιορίζονται στο 1,25% και 2,50%. Αυτό σημαίνει ότι οι νεότεροι χρήστες τεχνολογίας είναι πιο εξοικειωμένοι με τους κυβερνοκινδύνους και, ως εκ τούτου, επιδεικνύουν μεγαλύτερη ανθεκτικότητα και συνείδηση σε θέματα ασφάλειας ή υποδηλώνει το ακριβώς αντίθετο; Η αφέλεια και η άγνοια των νέων αντανακλούν τη συμπεριφορά τους στην ασφάλεια και επηρεάζουν την ικανότητά τους να παρατηρούν και να αντιδρούν κατά του εγκλήματος στον κυβερνοχώρο; Στοχοποιούνται περισσότεροι οι

μεγαλύτεροι σε ηλικία εργαζόμενοι, λόγω της μεγαλύτερης διαδικτυακής ύπαρξής τους και της έκθεσής τους; Είναι πιο απαιτητικό για αυτούς να ακολουθήσουν την τεχνολογική εξέλιξη και να αμυνθούν έναντι των κυβερνοκινδύνων;

4.4.7 Εργασιακό Κλίμα

Η ικανοποίηση που έχει κάθε εργαζόμενος με τον εργοδότη του, άλλους συναδέλφους, την ίδια την ασφάλεια πληροφοριών, επηρεάζει άμεσα τη συμπεριφορά του. Στην έρευνά μας περιλήφθηκαν ορισμένες σχετικές ερωτήσεις σε μια προσπάθεια να διερευνηθούν οι σκέψεις και τα συναισθήματα των συμμετεχόντων, καθώς αυτές οι παράμετροι είναι βασικοί παράγοντες στη συνολική συμπεριφορά και στάση ασφάλειας των ατόμων. Με βάση τις απαντήσεις που συλλέχθηκαν, οι εργαζόμενοι δεν δείχνουν ξεκάθαρη προτίμηση μεταξύ εργασίας από το σπίτι και μετάβασης στο γραφείο. Φαίνεται να μη συμπαθούν αυτές τις ξεχωριστές συνθήκες εργασίας και δεν αναφέρουν ριζικές διαφορές στην παραγωγικότητα και τη συνεργασία τους.

Από την άλλη πλευρά, υπάρχει μια σαφώς θετική στάση προς τον εργοδότη τους για την αντίδραση και την υποστήριξή του κατά τη διάρκεια αυτής της αρκετά ιδιαίτερης χρονικής περιόδου. Οι περισσότεροι από τους ερωτηθέντες εξέφρασαν την ικανοποίησή τους σχετικά με την εργασιακή τους εμπειρία κατά τη διάρκεια αυτής της πανδημίας, επαληθεύοντας την τεχνολογική ετοιμότητα και ευελιξία των περισσότερων εταιρειών, όπως σημειώθηκε σε προηγούμενες παραγράφους της παρούσας εφαρμογής.



Εικόνα 21. Ευρήματα εργασιακού κλίματος

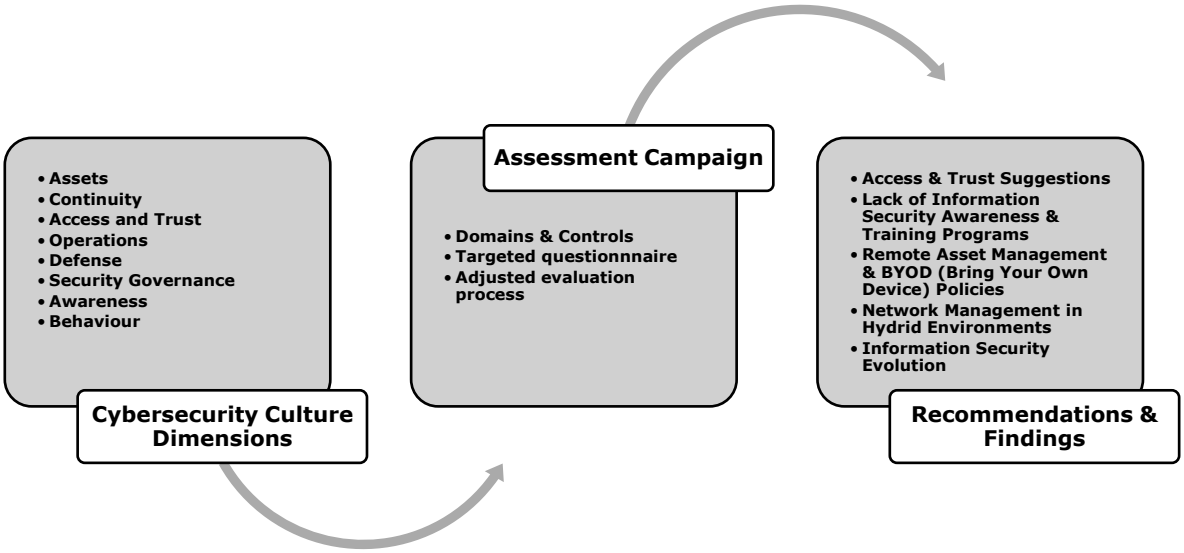
4.5 Συμπεράσματα

Οι έρευνες γενικά συναντούν την απροθυμία των ανθρώπων, ειδικά όταν δεν υπάρχει εμφανές κέρδος για αυτούς. Λαμβάνοντας υπόψη τις ειδικές συνθήκες διαβίωσης και εργασίας κάτω από τις οποίες διεξήχθη η υποκείμενη έρευνα, δικαιολογείται το χαμηλό ποσοστό συμμετοχής, το οποίο ήταν μικρότερο από το αναμενόμενο. Ωστόσο, όταν ο χρόνος γίνεται πιο πολύτιμος από ό,τι συνήθως και η πίεση είναι πιο εμφανής σε όλες τις πτυχές της καθημερινής ζωής, οι προσδοκίες πρέπει να προσαρμόζονται ανάλογα. Ένα μεγαλύτερο δείγμα θα ενίσχυε την εγκυρότητα των ευρημάτων μας καθώς και την

αξιοπιστία τους. Ωστόσο, αυτό δεν κατέστη εφικτό δεδομένων των ιδιαίτερων συνθηκών κατά την περίοδο της πανδημίας.

Οι προαναφερθείσες συνθήκες εγείρουν ορισμένους προβληματισμούς αναφορικά με τη συναισθηματική κατάσταση των συμμετεχόντων που επηρεάζουν άμεσα τη στάση ασφαλείας και την παρατηρούμενη συμπεριφορά τους. Οι απαντήσεις που σχετίζονται με τα συναισθήματα, τις σκέψεις και τις πεποιθήσεις των εργαζομένων επηρεάστηκαν από τις καταστάσεις κατ' οίκον εγκλεισμού λόγω COVID-19. Επιπλέον, τα περιστατικά κυβερνοπαραβιάσεων που αναφέρθηκαν ήταν πολύ πιθανό να σχετίζονταν με την τρέχουσα πραγματικότητα ασφάλειας στον κυβερνοχώρο που δημιουργήθηκε λόγω της κρίσης COVID-19.

Ο σεβασμός τόσο της ανωνυμίας όσο και της ιδιωτικής ζωής των συμμετεχόντων και των συνεργαζόμενων οργανισμών, απαγορεύει μια σειρά ερωτήσεων που θα μπορούσαν να αναδείξουν αρκετά ενδιαφέροντα αποτελέσματα σχετικά με την εθνικότητα, το φύλο κ.λπ. και τη σχέση τους με την κυβερνοασφάλεια. Επιπλέον, σε μια προσπάθεια να διατηρηθεί το ερωτηματολόγιο σύντομο και επίκαιρο, οι απαντήσεις σε ελεύθερο κείμενο αποφεύχθηκαν ενώ οι λίγες που χρησιμοποιήθηκαν παρουσίασαν μάλλον αποκαλυπτικά αποτελέσματα.



Εικόνα 22. Ευρήματα πλαισίου κουλτούρας κυβερνοασφάλειας

Τέλος, έγιναν κάποιες απλουστεύσεις με στόχο τη διατήρηση σύντομης χρονικής διάρκειας ολοκλήρωσης και, ταυτόχρονα, την απλοποίηση της προσέγγισής μας ως προς τις μάλλον περίπλοκες τεχνολογικές λύσεις και την αντίστοιχη ορολογία που χρησιμοποιεί η ασφάλεια πληροφοριών. Για παράδειγμα, στην ερώτηση σχετικά με την απομακρυσμένη πρόσβαση σε εταιρικά δίκτυα, ζητήσαμε από τους συμμετέχοντες να επιλέξουν μία από τις παρεχόμενες επιλογές και όχι έναν συνδυασμό αυτών. Σε ορισμένες περιπτώσεις, παρέχονται διαφορετικές επιλογές πρόσβασης από τους ίδιους οργανισμούς στους υπαλλήλους τους. Το ίδιο ισχύει και για τα στοιχεία υλικού που χρησιμοποιούνται για απομακρυσμένη εργασία.

Κάθε ερώτηση της εν λόγω έρευνας στόχευε συγκεκριμένους παράγοντες κουλτούρας κυβερνοασφάλειας σε μια προσπάθεια να αξιολογηθεί το επίπεδο ετοιμότητας και να εντοπιστούν σκοτεινά σημεία ή ακόμα και αστοχίες της υπάρχουσας υποδομής και αρχών ασφαλείας των συμμετεχόντων οργανισμών. Συνοψίζοντας και αναλύοντας συγκριτικά τα αποτελέσματα που παρουσιάστηκαν λεπτομερώς στις προηγούμενες παραγράφους, καταλήγουμε στα ακόλουθα βασικά συμπεράσματα (Εικόνα 22):

- Η εξ αποστάσεως εργασία, όποτε είναι δυνατή αναλόγως της φύσης της εργασίας, δεν προσφέρεται πάντα ως δυνατότητα στους εργαζόμενους. Συγκεκριμένοι επιχειρηματικοί τομείς εμφανίζονται πιο απρόθυμοι να υιοθετήσουν αυτή τη νέα εργασιακή πραγματικότητα, ενώ άλλοι είναι πρωτοπόροι σε αυτόν τον τομέα προσπαθώντας να επιβάλουν την καθιέρωσή του κάνοντας χρήση τεχνολογικών λύσεων που διευκολύνουν την εξ αποστάσεως συνεργασία.
- Η ασφάλεια πληροφοριών είναι αναπόσπαστο μέρος των σύγχρονων οργανισμών και διασφαλίζεται με ποικιλία τεχνολογικών λύσεων κυβερνοασφάλειας, όπως τείχη προστασίας, λογισμικό προστασίας από ιούς, συστήματα ανίχνευσης εισβολών, κέντρα λειτουργίας ασφαλείας κ.λπ. Ωστόσο, ο ανθρώπινος παράγοντας εξακολουθεί να μην αναγνωρίζεται ως βασικό στοιχείο της αλυσίδας της κυβερνοασφάλειας, όπως υποδεικνύεται τόσο από τις αναφορές περιστατικών απειλών στον κυβερνοχώρο όσο και από την έλλειψη κατευθυντήριων γραμμών και συνεχούς πληροφόρησης σχετικά με τους κινδύνους στον κυβερνοχώρο.
- Οι σύγχρονοι εργαζόμενοι έχουν μεγαλύτερη επίγνωση των θεμάτων ασφαλείας και των αντίμετρων συγκριτικά με το παρελθόν, αποδεικνύοντας μια βαθιά κουλτούρα ασφάλειας και εξοικείωση με την τεχνολογία των πληροφοριών. Ως αποτέλεσμα, τα προσωπικά περιουσιακά στοιχεία είναι καλύτερα εξοπλισμένα και προστατευμένα, αλλά ορισμένες βασικές αρχές ασφαλείας εξακολουθούν να παραβιάζονται, γεγονός που υπογραμμίζει την αναγκαιότητα εκπαίδευσης και υποστήριξης για τη διασφάλιση υψηλού επιπέδου ασφάλειας και ευαισθητοποίησης.
- Δίνεται μεγαλύτερη έμφαση στην περίμετρο του εταιρικού δικτύου, ενώ παραμελείται η διαχείριση και ασφάλεια περιουσιακών στοιχείων, ιδιαίτερα των απομακρυσμένων. Η προαναφερθείσα προσέγγιση ασφάλειας είναι αποτέλεσμα του μονολιθικού παρελθόντος, όπου ένα εταιρικό δίκτυο θα μπορούσε να προσομοιώσει ένα «κλειστό» σύστημα, το ασφαλέστερο από όλα. Ωστόσο, έρχεται σε αντίθεση με τη γνωστή αλήθεια ασφαλείας ότι «μια αλυσίδα είναι τόσο ισχυρή όσο ο πιο αδύναμος κρίκος της» και, στις μέρες μας, με την ευρεία χρήση της τηλεργασίας, αυτός ο κίνδυνος γίνεται πιο εμφανής. Κάθε επιχειρησιακό στοιχείο που αποκτά πρόσβαση σε ένα εταιρικό δίκτυο αποτελεί ένα αναπόσπαστο τμήμα του ικανό να δώσει πρόσβαση σε εισβολείς και να αποτελέσει το μέσο διείσδυσης και παραβίασης της οχύρωσης ασφαλείας του.
- Οι εταιρείες είναι πολύ πιο ευέλικτες στις μέρες μας χάρη στις υπάρχουσες τεχνολογικές λύσεις που συνδράμουν στο να ανταπεξέλθουν σε απαιτητικές και, σε ορισμένες περιπτώσεις, βίαιες αλλαγές του επιχειρηματικού περιβάλλοντος. Αυτή η καινοτόμος συμπεριφορά πρέπει να επεκταθεί και στην ασφάλεια πληροφοριών, όπου ριζικές αλλαγές συμβαίνουν σχεδόν καθημερινά, προκειμένου να συμβαδίζει με την ανάπτυξη και να παραμένει ασφαλής ανά πάσα στιγμή.

ΚΕΦΑΛΑΙΟ 5: ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ ΣΤΟΝ ΥΓΕΙΟΝΟΜΙΚΟ ΤΟΜΕΑ

5.1 Εισαγωγή

Σύμφωνα με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (European Union Agency for Cybersecurity, ENISA), ο τομέας της υγειονομικής περίθαλψης στοχοποιήθηκε από το 27% των συνολικών κυβερνοεπιθέσεων στην Ευρώπη το 2018 [177]. Το ξέσπασμα του κορονοϊού, μεταξύ των πολλών παρενεργειών του, οδήγησε σε σημαντική αύξηση του εγκλήματος στον κυβερνοχώρο. Οι κρίσιμες υποδομές, όπως αυτές κατηγοριοποιούνται σύμφωνα με την Οδηγία NIS 2016/1148 [178], έχουν βρεθεί στο επίκεντρο των κυβερνοεπιθέσεων. Μεταξύ αυτών, τα νοσοκομεία της Ευρωπαϊκής Ένωσης αντιμετωπίζουν απώλεια δεδομένων ασθενών [179, 180], επιθέσεις ransomware και διαθεσιμότητας. Δύο από τα πιο ανησυχητικά παραδείγματα είναι τα ακόλουθα:

- Το Πανεπιστημιακό Νοσοκομείο του Μπρνο στην Τσεχία, το οποίο, στις 12 Μαρτίου 2020, αναγκάστηκε να διακόψει ολόκληρο το δίκτυο πληροφορικής του, επηρεάζοντας δύο από τα παραρτήματα του νοσοκομείου, το Παίδων και το Μαιευτήριο [181].
- Θανατηφόρο περιστατικό σε γερμανικό νοσοκομείο που συνδέεται με κυβερνοεπίθεση [182].

Η ίδια έκθεση της ENISA, το 2018, αποκάλυψε ότι το 50,6% των νοσοκομείων που δέχθηκαν επίθεση αναγνώρισαν τις εσωτερικές απειλές ως τον πιο σοβαρό εχθρό τους. Όπως αναμενόταν, έχει γίνει σημαντική επιστημονική προσπάθεια για την αξιολόγηση της ετοιμότητας του προσωπικού υγειονομικής περίθαλψης τα τελευταία χρόνια [183, 184, 185] αναδεικνύοντας σημαντικά ευρήματα. Ενδεικτικά, οι έρευνες στην Πολωνία [186] και στη Φινλανδία [187] αναφέρουν ότι οι ιατροί δεν διαθέτουν επαρκή εκπαίδευση στον τομέα της κυβερνοασφάλειας. Ο Evans και λοιποί [188] επιβεβαιώνουν το ανθρώπινο λάθος ως έναν από τους πιο συνηθισμένους λόγους για συμβάντα ασφαλείας στα νοσοκομεία. Επιπρόσθετα, τονίζεται ότι η έλλειψη κουλτούρας κυβερνοασφάλειας και ευαισθητοποίησης καθώς και η αμέλεια ή η κακή στάση των εργαζομένων αποτελούν σημαντικούς παράγοντες ασφάλειας [189, 190].

Για τους λόγους αυτούς, ο υγειονομικός τομέας επιλέχθηκε για μια δεύτερη εφαρμογή του προτεινόμενου πλαισίου κυβερνοασφάλειας σε συνεργασία των ευρωπαϊκών προγραμμάτων:

- **EnergyShield** [42], χρηματοδοτούμενο από το πρόγραμμα έρευνας και καινοτομίας Horizon 2020 της Ευρωπαϊκής Ένωσης, σύμφωνα με τη συμφωνία επιχορήγησης με αριθμό 832907
- **SPHINX** [191]**,** χρηματοδοτούμενο από το πρόγραμμα έρευνας και καινοτομίας Horizon 2020 της Ευρωπαϊκής Ένωσης, σύμφωνα με τη συμφωνία επιχορήγησης με αριθμό 826183

5.2 Μεθοδολογία

5.3 Σχεδιασμός Εκστρατείας Αξιολόγησης

Το πλάνο εφαρμογής του προτεινόμενου πλαισίου κουλτούρας κυβερνοασφάλειας στον υγειονομικό χώρο περιλάμβανε πολλαπλά στάδια. Πιο συγκεκριμένα, αναλύεται στα ακόλουθα στάδια:

- **ΦΑΣΗ Α:** Αρχική εκστρατεία αξιολόγησης της κουλτούρας κυβερνοασφάλειας με χρήση ερωτηματολογίων διαφοροποιημένων για τις διαφορετικές ομάδες συμμετεχόντων, κατάλληλα προσαρμοσμένων στις επιχειρησιακές απαιτήσεις και γνώσεις τους.
- **ΦΑΣΗ Β:** Παρεμβάσεις με στόχο την ενίσχυση της ενημέρωσης, της εξοικείωσης και της εγρήγορσης του προσωπικού των οργανισμών υγειονομικού ενδιαφέροντος.
- **ΦΑΣΗ Γ:** Απολογιστική αξιολόγηση σε συνέχεια των εκπαιδεύσεων και δράσεων ενίσχυσης της κουλτούρας κυβερνοασφάλειας του προσωπικού.

Στις επόμενες παραγράφους παρουσιάζεται ο σχεδιασμός κάθε φάσης εστιάζοντας πρωτίστως στις Φάσεις Α και Γ που αντιστοιχούν σε εφαρμογές εκστρατειών αξιολόγησης του προτεινόμενου πλαισίου κουλτούρας κυβερνοασφάλειας.

Φάση Α

Για τη φάση αυτή σχεδιάστηκαν δύο ξεχωριστά δικτυακά ερωτηματολόγια στοχευμένα σε δύο διαφορετικές κατηγορίες προσωπικού:

- υπάλληλοι που απασχολούνται στα τμήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) (Ερωτηματολόγιο Α), και
- υπάλληλοι υγειονομικής περίθαλψης που δεν υπάγονται στα τμήματα ΤΠΕ, δηλαδή γιατροί, νοσηλευτές, βοηθητικό, εργαστηριακό και διοικητικό προσωπικό (Ερωτηματολόγιο Β).

Το ερωτηματολόγιο Α περιλάμβανε πέντε μέρη:

- Το πρώτο μέρος περιείχε ερωτήσεις σχετικά με δημογραφικά στοιχεία, χρόνια εμπειρίας, εξυπηρετούμενο πληθυσμό, κ.λπ. που προέρχονταν από τον τομέα ***Employee Profile*** της διάστασης ***Attitude*** (Individual Level) του πλαισίου κουλτούρας κυβερνοασφάλειας.
- Το δεύτερο μέρος επικεντρώθηκε σε πτυχές ΤΠΕ που περιλαμβάνουν τον αριθμό των εκπαιδεύσεων κυβερνοασφάλειας που πραγματοποιήθηκαν, τα ποσοστά της συνολικής κατανομής προϋπολογισμού για τις ΤΠΕ και την ασφάλεια στον κυβερνοχώρο που προέρχονται από τους τομείς ***Security Awareness and Training Program*** της διάστασης ***Defence*** και ***Security Management Maturity*** της διάστασης ***Security Governance*** (Organizational Level).
- Η τρίτη ενότητα στόχευσε τις πολιτικές δικτύου υπολογιστών και την πρόσβαση εξωτερικών μερών συνδυάζοντας δείκτες από διαφορετικούς τομείς των διαστάσεων ***Access and Trust*** και ***Assets*** (Organizational Level).
- Το τέταρτο μέρος ζήτησε από τα άτομα να απαντήσουν σε ερωτήσεις σχετικά με τις τρέχουσες μεθόδους και πρακτικές ασφάλειας στον κυβερνοχώρο που

χρησιμοποιούνται και προέρχονται από τον τομέα ***Policies and Procedures Awareness*** της διάστασης ***Awareness*** (Individual Level).

- Το τελευταίο μέρος επικεντρώθηκε στους δείκτες απόδοσης της ασφάλειας στον κυβερνοχώρο (π.χ. αριθμός περιστατικών ασφάλειας στον κυβερνοχώρο με την πάροδο του χρόνου και μέσος χρόνος για την εκ νέου επίλυση ενός περιστατικού) που προέρχονται από τη διάσταση ***Security Governance*** (Organizational Level).

Κατά αντιστοιχία, το ερωτηματολόγιο Β περιλάμβανε ερωτήσεις για δημογραφικά στοιχεία, κατάσταση απασχόλησης, κυβερνοασφάλεια ή σχετικές εκπαιδεύσεις σε θέματα ασφαλείας και απορρήτου πληροφοριών, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), η ικανότητα κατανόησης των κυβερνοαπειλών, η διαθεσιμότητα των διαδικασιών κυβερνοασφάλειας και οι προφυλάξεις που λαμβάνονται. Οι μετρήσεις ασφαλείας ήταν για άλλη μια φορά ένας συνδυασμός διαφορετικών δεικτών που περιγράφονται σε πολλαπλά επίπεδα του πλαισίου κουλτούρας κυβερνοασφάλειας, με στόχο την πολύπλευρη προσέγγιση της αξιολόγησης της κουλτούρας προσωπικού εκτός ΤΠΕ. Για να καταλάβουμε εάν το προσωπικό που δεν ανήκει στις ΤΠΕ είχε συμμετάσχει προηγουμένως σε εκστρατείες κυβερνοασφάλειας, χρησιμοποιήθηκε τεχνική ορολογία σε ορισμένες περιπτώσεις για να εξετασθεί η εξοικείωση των συμμετεχόντων με αυτούς τους όρους.

Φάση Β

Η φάση αυτή θα λάμβανε χώρα χωρίς τη δική μας παρέμβαση ή συμμετοχή καθοδηγούμενη από την ομάδα υλοποίησης του έργου SPHINX και θα αφορούσε την εκπαίδευση και ευαισθητοποίηση του προσωπικού των υπό εξέταση οργανισμών. Για λόγους πληρότητας και κατανόησης της ευρύτερης μεθοδολογίας παρατίθενται ακολούθως συνοπτικά μερικές πληροφορίες που αφορούν τη φάση.

Η εκστρατεία ευαισθητοποίησης θα είχε ως κύρια θεματολογία τις ενέργειες και τις προφυλάξεις που πρέπει να λάβει κάθε εργαζόμενος στον τομέα της υγείας για την προστασία των δεδομένων που χειρίζεται. Για τους λόγους αυτούς θα γινόταν χρήση διάφορων μέσων εκπαίδευσης, μεταξύ των οποίων:

- Πιστοποιημένο εκπαιδευτικό πρόγραμμα GDPR που αφορά υγειονομικούς υπαλλήλους.
- Έντυπο υλικό με οδηγίες κυβερνοασφάλειας, σύμφωνα με την Οδηγία 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016, με στόχο το υψηλό επίπεδο ασφάλειας δικτύων και συστημάτων πληροφοριών σε υγειονομικούς φορείς σε ολόκληρη την Ευρωπαϊκή Ένωση.
- Σεμινάριο ευαισθητοποίησης για την κυβερνοασφάλεια ειδικά προσαρμοσμένο στις ανάγκες των τμημάτων ΤΠΕ σε υγειονομικούς φορείς με τη συμμετοχή εκπαιδευτών από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), ακαδημαϊκών ιδρυμάτων και εκπρόσωπων του κλάδου της κυβερνοασφάλειας. Κύριες θεματικές του σεμιναρίου θα ήταν οι ακόλουθες:
    - ISO 27001 με στόχο τη συμμόρφωση με την οδηγία για την ασφάλεια των συστημάτων δικτύων και πληροφοριών (οδηγία NIS)
    - Παράμετροι αξιολόγησης κινδύνων στον κυβερνοχώρο για τα νοσοκομεία.
    - Πρακτικές μέθοδοι και τεχνικές κυβερνοασφάλειας προς διευκόλυνση και καθοδήγηση των υπαλλήλων ΤΠΕ στις καθημερινές τους δραστηριότητες.

Φάση Γ

Το πέρας της Φάσης Β θα ακολουθούσε νέα εκστρατεία αξιολόγησης με εφαρμογή εναλλακτικών πρακτικών στοχεύοντας στις θεματικές της εκπαίδευσης και εξετάζοντας τη βελτίωση της κουλτούρας κυβερνοασφάλειας ως απόρροια την προσπάθειας ευαισθητοποίησης.

Προκειμένου να καταστεί δυνατή η συγκριτική αξιολόγηση των αποτελεσμάτων των Φάσεων Α και Γ, διαμορφώθηκε ένα ερωτηματολόγιο που περιλάμβανε ερωτήσεις σχετικά με:

- δημογραφικά στοιχεία από τον τομέα ***Employee Profile*** της διάστασης ***Attitude*** (Individual Level) του πλαισίου κουλτούρας κυβερνοασφάλειας
- ασφάλεια και πολιτικές πληροφοριών από τον τομέα ***Policies and Procedures Awareness*** της διάστασης ***Awareness*** (Individual Level)
- ασφάλεια δικτύου και διαχείρισης δεδομένων από τον τομέα ***Information Security Policy and Compliance*** της διάστασης ***Defence*** (Organizational Level)

Η εκστρατεία αξιολόγησης, συμπληρωματικά του ερωτηματολογίου, θα έκανε χρήση και δοκιμασιών σχετικών με τεχνικές phishing. Η επιλογή αυτή έγινε εξαιτίας της τρέχουσας πραγματικότητας κυβερνοασφάλειας που παρουσιάζεται συνοπτικά στις ακόλουθες παραγράφους.

Σύμφωνα με την Έρευνα Κυβερνοασφάλειας HIMSS Healthcare 2020, τα περιστατικά ασφαλείας μαστίζουν ανησυχητικά τους οργανισμούς υγειονομικής περίθαλψης όλων των τύπων και μεγεθών, με το phishing να είναι το πιο κοινό από όλα [192]. Το phishing είναι μια τακτική κοινωνικής μηχανικής που χρησιμοποιείται για να πείσει τα άτομα να παρέχουν ευαίσθητες πληροφορίες. Οι κακόβουλοι φορείς χρησιμοποιούν τεχνικές phishing για διάφορους λόγους, όπως κλοπή ταυτότητας, πρόσβαση σε ιδιόκτητες πληροφορίες, μετάδοση κακόβουλου λογισμικού που περιλαμβάνει ransomware, μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση και έναρξη μη εξουσιοδοτημένων οικονομικών συναλλαγών [193]. Η πιο κοινή μορφή ηλεκτρονικού "ψαρέματος" είναι με χρήση μηνύματος ηλεκτρονικού ταχυδρομείου που συνήθως καταστρατηγεί τον φόβο, το καθήκον, την υποχρέωση, την περιέργεια ή την απληστία του παραλήπτη [194].

Στα τέλη Ιανουαρίου 2020, αναφέρθηκαν καμπάνιες ανεπιθύμητης αλληλογραφίας Emotet με θέμα τον κορονοϊό, που στόχευαν κυρίως ιαπωνικούς φορείς [195, 196]. Από τον Ιανουάριο έως τον Απρίλιο του 2020, η Interpol εντόπισε περίπου 907.000 ανεπιθύμητα μηνύματα που συνδέονται με τον COVID-19 [197]. Κατά τον Απρίλιο του 2020, η Google αναφέρθηκε ότι απέκλεισε περισσότερα από 18 εκατομμύρια κακόβουλα προγράμματα και μηνύματα ηλεκτρονικού ψαρέματος που σχετίζονται με τον COVID-19 και επιπλέον περισσότερα από 240 εκατομμύρια καθημερινά ανεπιθύμητα μηνύματα που σχετίζονται με τον COVID-19 [198].

Λαμβάνοντας υπόψιν τις ανωτέρω πληροφορίες, και ως τελικό μεθοδολογικό βήμα, αποφασίστηκε να συμπεριληφθεί στην εκστρατεία αξιολόγησης της κουλτούρας κυβερνοασφάλειας κάποιο παίγνιο με στόχο την εκτίμηση της εξοικείωσης του εργατικού δυναμικού του τομέα υγείας με ειδικές τεχνικές ηλεκτρονικού "ψαρέματος" (phishing). Πρόσφατη έρευνα δείχνει μια στατιστικά σημαντική θετική συσχέτιση μεταξύ του φόρτου εργασίας και της πιθανότητας του προσωπικού υγειονομικής περίθαλψης να ανοίξει ένα email ηλεκτρονικού ψαρέματος [199]. Ως εκ τούτου, αποφασίσαμε να δημιουργήσουμε ένα phishing κουίζ το οποίο θα περιλαμβάνει πολλά διαφορετικά μηνύματα ηλεκτρονικού ψαρέματος. Η διάρκειά του έπρεπε να είναι σύντομη για να εξασφαλιστεί η δέσμευση και

η συγκέντρωση των συμμετεχόντων λόγω του εξαιρετικά μεγάλου φόρτου εργασίας τους και της κούρασης που αυτός συνεπάγεται.

Μια άσκηση προσομοίωσης phishing – όπου οι συμμετέχοντες θα λάμβαναν ένα μήνυμα ηλεκτρονικού ψαρέματος χωρίς προηγούμενη γνώση, το οποίο θα περιείχε έναν σύνδεσμο στον οποίο δεν θα έπρεπε να κάνουν κλικ - θα μπορούσε να ήταν μια πιο ρεαλιστική προσέγγιση για την αξιολόγηση της πραγματικής συμπεριφοράς του εργατικού δυναμικού δεδομένων των συνθηκών. Ωστόσο, μια τέτοια προσέγγιση απορρίφθηκε από τους συνεργαζόμενους ειδικούς πληροφορικής μετά από εκτενείς συζητήσεις. Ένας από τους κύριους λόγους ήταν ότι μια τέτοια άσκηση αξιολόγησης θα υποδείκνυε μια σημαντική προσπάθεια για την αλλαγή της διαμόρφωσης των υφιστάμενων λύσεων ασφάλειας που θα επιτρέψουν σε αυτά τα μηνύματα ηλεκτρονικού "ψαρέματος" να φτάσουν στους στοχευμένους συμμετέχοντες. Επιπλέον, οι συμμετέχοντες έπρεπε να ενημερωθούν και να συναινέσουν για να γίνουν μέρος αυτής της εκστρατείας αξιολόγησης ασφάλειας. Λόγω της ψυχολογικά και συναισθηματικά απαιτητικής περιόδου της πανδημίας COVID-19, συμφωνήθηκε ότι οι περισσότεροι άνθρωποι θα έκαναν πρόθυμα ένα σύντομο κουίζ που θα ξεκινήσει κατ' απαίτηση και στον χρόνο της επιλογής τους αντί να δεχτούν να αξιολογηθούν μέσω ενός τεστ προσομοίωσης σε μια συγκεκριμένη χρονική περίοδο. Το τελευταίο θα αύξανε σημαντικά το άγχος της αξιολόγησης και, ως εκ τούτου, θα μείωνε το ποσοστό συμμετοχής.

Μηνύματα ηλεκτρονικού "ψαρέματος" που είτε αποκλείστηκαν από τις προηγμένες λύσεις antispam είτε κοινοποιήθηκαν στα τμήματα πληροφορικής από τους παραλήπτες τους για περαιτέρω διερεύνηση σύμφωνα με τα πρωτόκολλα ασφαλείας, συγκεντρώθηκαν από ειδικούς ασφαλείας των υγειονομικών φορέων και εξετάστηκαν από κοινού για ομοιότητες και διαφορές. Μετά από μια σειρά συνεδριών αξιολόγησης, καταλήξαμε σε πέντε μηνύματα ηλεκτρονικού ταχυδρομείου που παρουσιάζονται στον Πίνακας 12.

Πίνακας 12. Μηνύματα ηλεκτρονικού ψαρέματος

ID	Description	Phishing	Legit
Email I	X Bank asking recipients to protect their accounts by following a specific hyperlink.	✓	
Email II	Unknown sender blackmailing recipients asking for ransom in Bitcoin in order not to reveal personal videos recorded via their hacked workstation cameras.	✓	
Email III	Y Bank asking recipients to protect their accounts by following a specific hyperlink.	✓	
Email IV	An email supposedly sent by the IT department asking for account verification to avoid inactivation.	✓	
Email V	An email related to the Ministry of Internal Affairs deriving from the repository of public expenditures.		✓

5.3.1 Έλεγχος Εγκυρότητας

Η σχεδίαση των τριών φάσεων, όπως αυτές περιεγράφηκαν αναλυτικά στην προηγούμενη ενότητα, των ερωτηματολογίων και της δοκιμής phishing αποτέλεσε προϊόν ζύμωσης και κοινής προσπάθειας από συμμετέχοντες από τα δύο ευρωπαϊκά προγράμματα, EnergyShield και SPHINX. Στην ομάδα σχεδιασμού συμμετείχαν εμπειρογνώμονες έρευνας, έμπειροι ερευνητές και αναλυτές, πιστοποιημένοι αξιωματικοί ασφαλείας και τεχνολογίας, εκπρόσωποι από τα τμήματα ΤΠΣ των υπό εξέταση οργανισμών καθώς και υγειονομικοί υπάλληλοι σε διοικητικές θέσεις. Η στοχοθεσία, προσέγγιση, μεθοδολογία καθώς και το περιεχόμενο της εκστρατείας αξιολόγησης εξετάστηκαν από κοινού καταλήγοντας στην τελική μορφή τους [171, 172].

5.3.2 Επιλογή Δείγματος

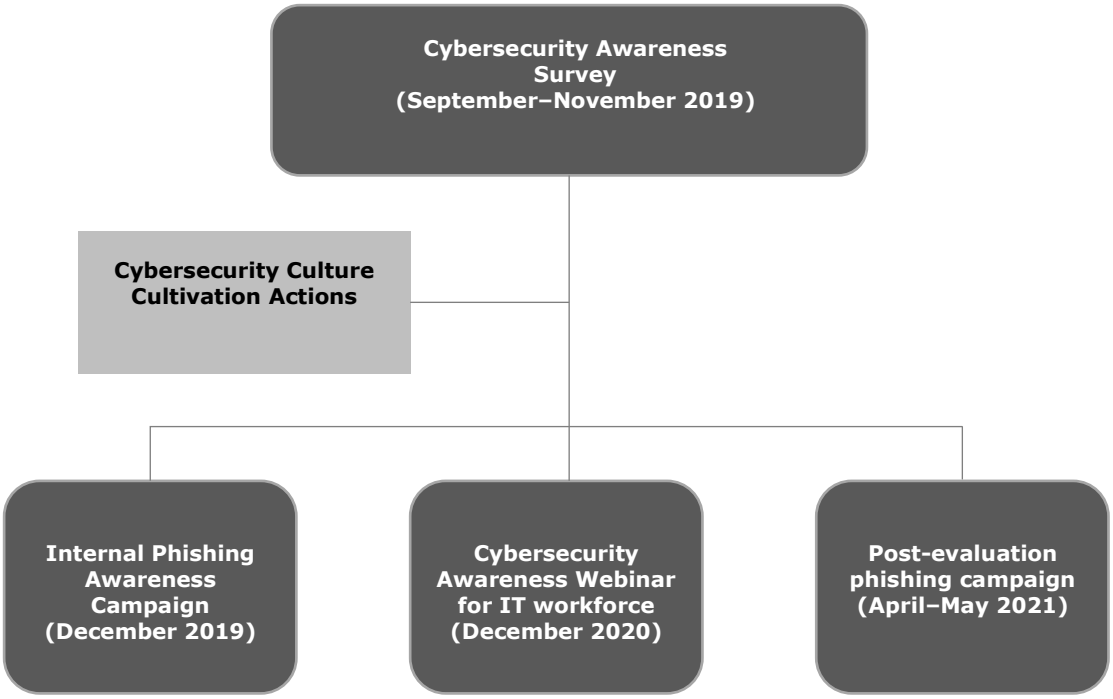
Για την εφαρμογή του ανωτέρου πλάνου αξιολόγησης κουλτούρας κυβερνοασφάλειας επιλέχθησαν τρεις διαφορετικοί φορείς υγειονομικής περίθαλψης από τρεις Ευρωπαϊκές χώρες, την Ελλάδα, την Πορτογαλία και τη Ρουμανία, που συμμετέχουν στην πιλοτική εφαρμογή του έργου SPHINX. Πιο συγκεκριμένα, οι υπό αξιολόγηση οργανισμοί περιλάμβαναν:

- μια υγειονομική περιφέρεια στην Ελλάδα που περιλαμβάνει σημαντικό αριθμό νοσοκομείων και κέντρων υγείας αναφοράς (εφεξής Ίδρυμα Α).
- ένα νοσοκομείο αναφοράς σε μεγάλη πορτογαλική περιοχή (εφεξής Ίδρυμα Β).
- μία ρουμανική ιατρική κλινική άμεσης αποκατάστασης (εφεξής Ίδρυμα Γ).

Αξίζει να σημειωθεί ότι την ίδια χρονική περίοδο, σύμφωνα με τη Eurostat [200], το ποσοστό του προσωπικού ΤΠΕ ως προς το σύνολο του εταιρικού προσωπικού για την Ελλάδα ήταν 1,8%, για την Πορτογαλία ήταν 2,4% και για τη Ρουμανία ήταν 2,2%. Η αναλογία αυτή είναι ιδιαίτερα σημαντική δεδομένου ότι στη Φάση Α έγινε διαφοροποίηση δυο ομάδων χρηστών (προσωπικό ΤΠΕ και μη).

5.3.3 Εκπόνηση Εκστρατείας Αξιολόγησης

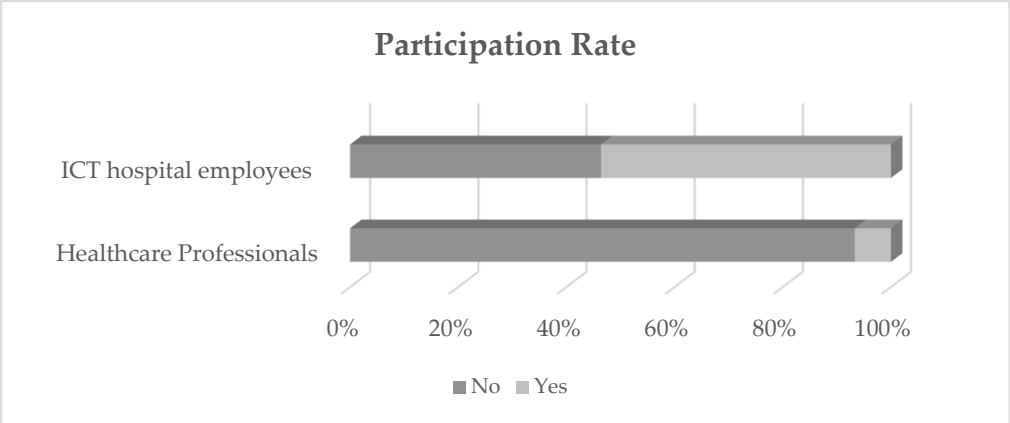
Η εφαρμογή του πλάνου αξιολόγησης κουλτούρας κυβερνοασφάλειας, με τις 3 διακριτές φάσεις του, έλαβε χώρα από το Σεπτέμβριο του 2019 έως και τον Μάιο του 2021, όπως αποδίδεται σχηματικά στην Εικόνα 23.

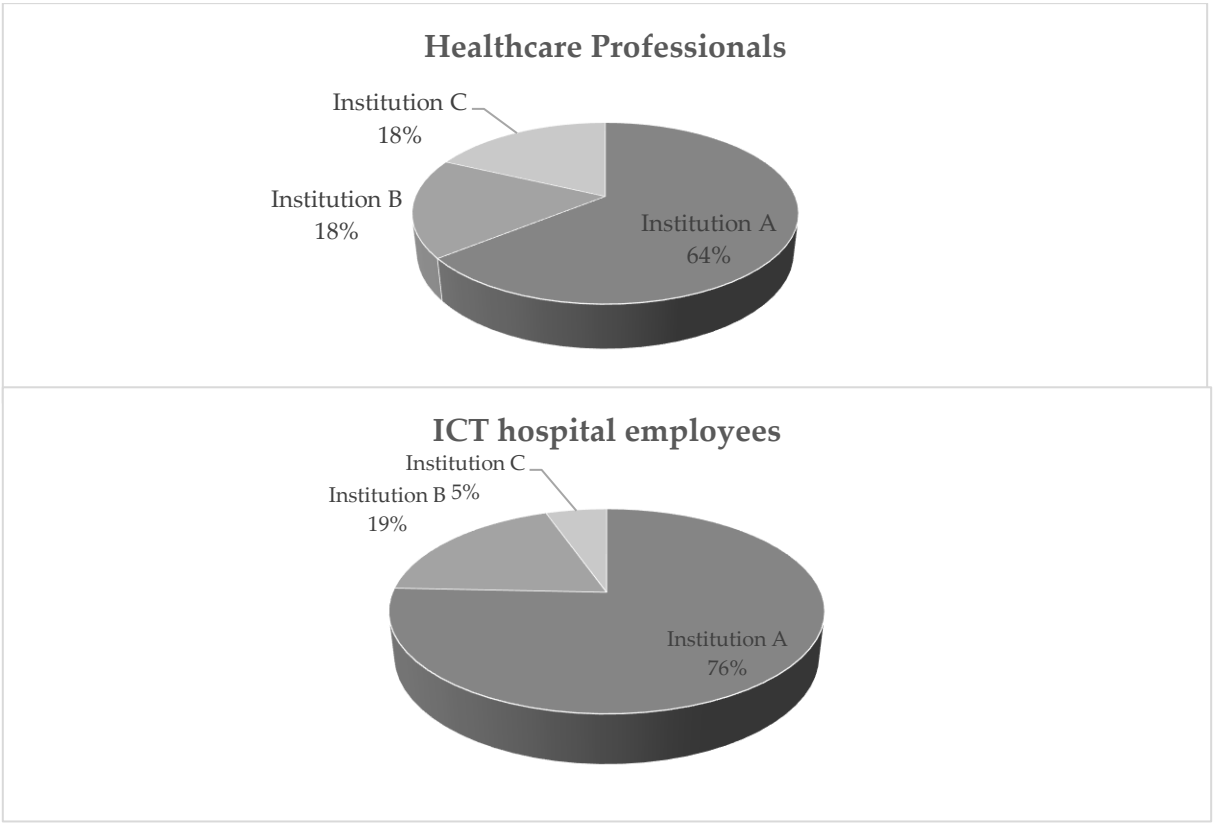


Εικόνα 23. Πλάνο αξιολόγησης κουλτούρας κυβερνοασφάλειας στον υγειονομικό τομέα

Φάση Α

Ο αριθμός των υπολογιστών που έχουν διατεθεί στο προσωπικό είναι περίπου 2800, 850, 90 για τα ιδρύματα Α, Β και Γ, αντίστοιχα. Γνωρίζοντας ότι είναι γενικά δύσκολο να συλλέξουμε οικειοθελώς απαντήσεις από το προσωπικό που δεν ανήκει στις ΤΠΕ, λόγω της φύσης της εργασίας τους, έγινε χρήση έντυπων και ηλεκτρονικών προσκλήσεων σε όλους τους υπαλλήλους με στόχο την αύξηση του ποσοστού ανταπόκρισης από το προσωπικό που δεν ανήκει στις ΤΠΕ, και ιδιαίτερα εκείνων που έχουν πρόσβαση σε υπολογιστές. Επιπρόσθετα, ερωτηματολόγια πολλαπλών επιλογών μεταφράστηκαν από τα αγγλικά στις μητρικές γλώσσες των συμμετεχόντων για καλύτερη κατανόηση του περιεχομένου τους και για την άρση του γλωσσικού φραγμού και την άμβλυνση αυτού του παράγοντα στην εξίσωση. Τα δεδομένα που συλλέχθηκαν μεταφράστηκαν στα αγγλικά, εναρμονίστηκαν και ελέγχθηκαν για συνέπεια.





Εικόνα 24. Ποσοστό συμμετοχής (α) ανά επάγγελμα, (β) ανά υγειονομικό οργανισμό και (γ) εργαζομένων πληροφορικής ανά οργανισμό

Η εκστρατεία αξιολόγησης διεξήχθη από τον Σεπτέμβριο του 2019 έως τον Νοέμβριο του 2019 [201]. Κατά το χρονικό αυτό διάστημα προσκλήθηκαν να συμμετάσχουν στην ηλεκτρονική έρευνα **10418** επαγγελματίες υγείας (8500 από την Ελλάδα, 1700 από την Πορτογαλία και 218 από τη Ρουμανία) και **69** εργαζόμενοι πληροφορικής (60 από την Ελλάδα, 7 από την Πορτογαλία και 2 από τη Ρουμανία). Το ποσοστό συμμετοχής παρουσιάζεται γραφικά στην Εικόνα 24, σύμφωνα με την οποία η ανταπόκριση των υγειονομικών εργαζομένων περιορίστηκε στο **6,71%** (**699 συμμετοχές**) ενώ η αντίστοιχη για το προσωπικό ΤΠΕ ήταν **53,62%** (**37 συμμετοχές**).

Αξίζει να σημειωθεί ότι δεν υπήρχε χρονικός περιορισμός για τη συμπλήρωση των ερωτηματολογίων και οι συμμετέχοντες δεν αποζημιώθηκαν ούτε προσφέρθηκε κανένα άλλο κίνητρο.

Φάση Γ

Μετά το πέρας της Φάσης Β, και πιο συγκεκριμένα στο τέλος του δικτυακού σεμιναρίου, ζητήθηκε από τους συμμετέχοντες να απαντήσουν σε ένα ερωτηματολόγιο, εθελοντικά και ανώνυμα, προκειμένου να μετρηθεί το επίπεδο κατανόησης των εννοιών που παρουσιάστηκαν και των κατευθυντήριων γραμμών κυβερνοασφάλειας που τέθηκαν κατά τη διάρκειά του. Από τους συνολικά 113 συμμετέχοντες, 62 εργάζονταν σε ΤΠΕ ελληνικών νοσοκομείων (περίπου το 30% του συνολικού μόνιμου εργατικού δυναμικού πληροφορικής των ελληνικών οργανισμών υγείας στο δημόσιο τομέα [202]) και 30 από αυτούς απάντησαν το προαιρετικό ερωτηματολόγιο [203].

Με βάση τα αποτελέσματά του (Πίνακας 13), το 56,7% των συμμετεχόντων ήταν ηλικίας μεταξύ 40-49 ετών, ενώ το 43,3% ήταν γυναίκες. Επιπλέον, το 56,7% κατείχε μεταπτυχιακό τίτλο σπουδών, ενώ το 80,0% είχε πάνω από δέκα χρόνια εργασιακής εμπειρίας στον τομέα της πληροφορικής της υγείας. Περίπου το 70,0% απασχολούνταν σε νοσοκομεία και το 33,3% κατείχε διευθυντικές θέσεις, ενώ το 36,7% εργαζόταν σε ιδρύματα υγειονομικής περίθαλψης που απασχολούν περισσότερους από 1.201 επαγγελματίες υγείας.

Πίνακας 13. Δημογραφικά στοιχεία αποκριθέντων στο ερωτηματολόγιο της Φάσης Γ

Category	Participants
Total	*n* = 30 (100%)
Gender	
Male	17 (56.7%)
Female	13 (43.3%)
Age	
20-29	2 (6.7%)
30-39	6 (20.0%)
40-49	17 (56.7%)
50-59	5 (16.7%)
Education	
Secondary Education	2 (6.7%)
Bachelor's degree	7(23.3%)
MSc	17 (56.7%)
PhD	4 (13.3%)
Years of Experience	
0-5	5 (16.7%)
6-Οκτ	1 (3.3%)
> 10	24 (80.0 %)
Position	
ICT staff	12 (40.0%)
ICT manager	10 (33.3%)
ICT director	3 (10.0%)
Other	5 (16.7%)
Organization	
Hospital	21 (70.0%)
Health Authority	3 (10.0%)
Other	6 (20.0%)
Number of Employees in your Organization	
<100	4 (13.3%)
100-300	2 (6.7%)
301-600	7 (23.3%)
601-1000	3 (10.0%)
1001-1200	3 (10.0%)
>1201	11 (36.7%)

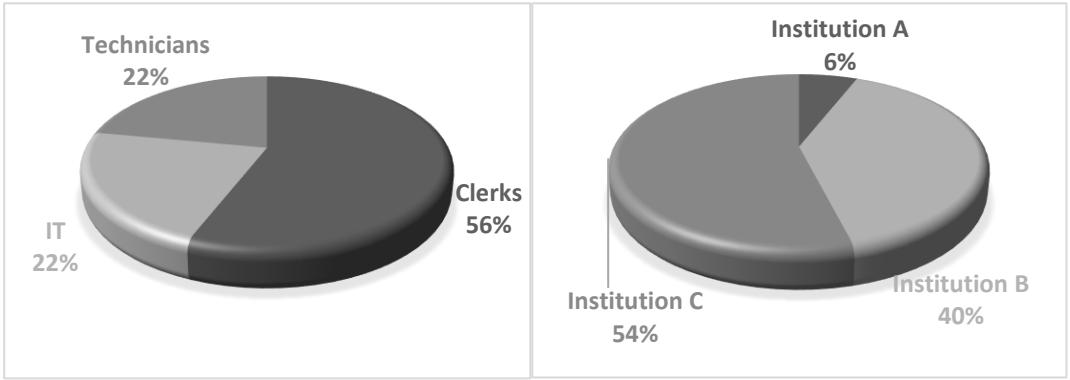
Το χαμηλό ποσοστό συμμετοχής στο ερωτηματολόγιο αυτής της φάσης, συγκριτικά με το αντίστοιχο της Φάσης Α, οφείλεται σε σημαντικό βαθμό στην πανδημία η οποία παρουσιάστηκε και κορυφώθηκε μετά το πέρας της Φάσης Α. Ο φόρτος εργασίας, η πίεση και οι αγχωτικές συνθήκες διαβίωσης αιτιολογούν τη μειωμένη προθυμία και συμμετοχή. Οι εξελίξεις μας ώθησαν στην αναπροσαρμογή της προσέγγισης μας αναφορικά με τον τρόπο διάθεσης της δοκιμής phishing.

Πιο συγκεκριμένα, στάλθηκε ένα ειδικό email πρόσκλησης σε επιλεγμένους συμμετέχοντες (Πίνακας 14) παρέχοντας έναν σύνδεσμο σύνδεσης και τα κατάλληλα διαπιστευτήρια ελέγχου ταυτότητας. Κάθε συμμετέχων μπορούσε να ολοκληρώσει μόνο μία φορά το κουίζ phishing, χωρίς χρονικούς περιορισμούς, και έπρεπε να απαντήσει σε κάθε ένα από τα μηνύματα ηλεκτρονικού ταχυδρομείου που περιλαμβάνονται στην καμπάνια. Τόσο το μήνυμα ηλεκτρονικού ταχυδρομείου της πρόσκλησης όσο και το κουίζ ηλεκτρονικού "ψαρέματος" μεταφράστηκαν, διασφαλίζοντας την εγγύτητα και αίροντας τα γλωσσικά εμπόδια που συνήθως εισάγονται σε τέτοιες αξιολογήσεις.

Πίνακας 14. Ομάδες χρηστών της δοκιμής phishing

	IT	**Technicians**	**Clerks**
Institution A	group01 (user01 – user03)		
Institution B	group02 (user04 – user06)	group03 (user07 – user09)	group04 (user10 – user23)
Institution C	group05 (user24 – user28)	group06 (user29 – user36)	group07 (user37 – user50)

Η καμπάνια ήταν διαθέσιμη για συμμετοχή για σχεδόν ένα μήνα, ξεκινώντας από τις 26 Απριλίου 2021 και ολοκληρώθηκε στις 28 Μαΐου 2021. Κατά τη διάρκεια αυτής της περιόδου, και οι 50 προσκεκλημένοι συμμετέχοντες ολοκλήρωσαν τη δοκιμή phishing ανώνυμα, επιτυγχάνοντας έτσι ποσοστό συμμετοχής 100%. Το ποσοστό συμμετοχής κυμαινόταν ανάλογα με το μέγεθος του οργανισμού, φτάνοντας σε **54%** από το ίδρυμα Α, **40%** από το ίδρυμα Β και **6%** από το ίδρυμα Γ. Πιο συγκεκριμένα, το 56% των συμμετεχόντων ήταν υπάλληλοι, το 22% ήταν επαγγελματίες πληροφορικής, και το 22% ήταν τεχνικοί (Εικόνα 25).



Εικόνα 25. Στατιστικά συμμετοχής στη δοκιμή phishing ανά (α) επάγγελμα και (β) ίδρυμα

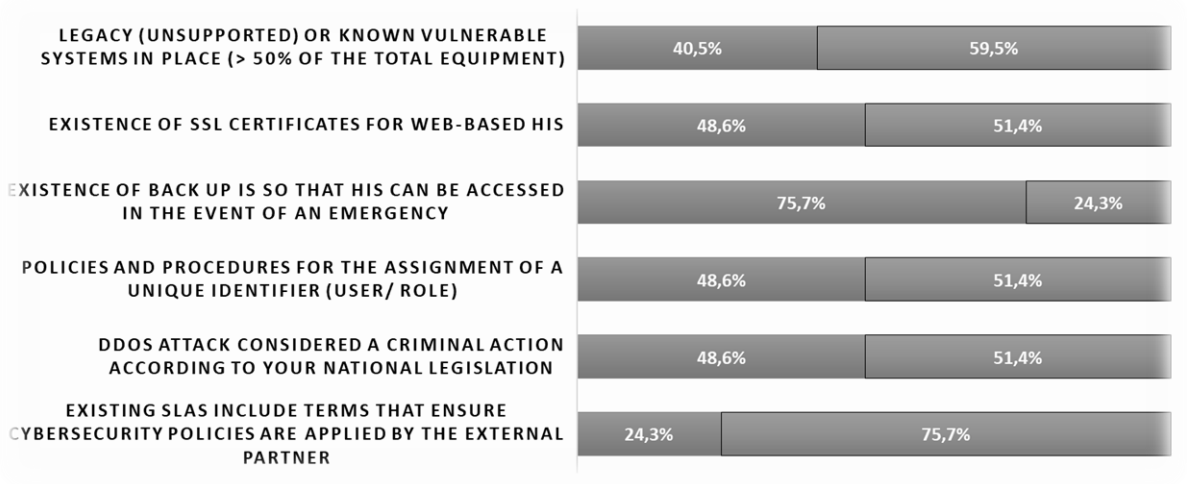
5.4 Ανάλυση Αποτελεσμάτων

Φάση Α

Τα αποτελέσματα αποκάλυψαν ότι το 89%, το 100% και το 50% του προσωπικού ΤΠΕ στα ιδρύματα Α, Β και Γ, αντίστοιχα, αναγνώρισαν την πλήρη απουσία ειδικών τμημάτων κυβερνοασφάλειας στα ιδρύματά τους. Παρόμοιες απαντήσεις δόθηκαν από το προσωπικό που δεν ανήκει στις ΤΠΕ (86%, 63% και 68% για τα ιδρύματα Α, Β και Γ, αντίστοιχα). Αυτή η απόκλιση οφείλεται στην αδυναμία των συμμετεχόντων να διακρίνουν μεταξύ των τμημάτων ΤΠΕ και ασφάλειας στον κυβερνοχώρο. Το 100% του προσωπικού ΤΠΕ στα Ιδρύματα Α και Β και το 50% στο Ίδρυμα Γ, απάντησαν ότι δεν ακολούθησαν ένα έντυπο σχεδίου αντιμετώπισης περιστατικών που ανταποκρίνεται σε παραβίαση δεδομένων έγκαιρα και οικονομικά αποδοτικά.

Οι απαντήσεις στο ερωτηματολόγιο ΤΠΕ σχετικά με τις κυβερνοευπάθειες (Εικόνα 26) αποκάλυψαν ότι δεν υιοθετήθηκαν κοινές πολιτικές, ανεξάρτητα από την εκπαιδευτική τους κατάρτιση, το φύλο ή την ηλικία τους. Αν και οι απαρχαιωμένες τεχνολογίες που εντοπίζονται στα νοσοκομεία, διαδραματίζουν σημαντικό ρόλο στις παραβιάσεις δεδομένων, το 40,5% του προσωπικού ΤΠΕ ανέφερε τη χρήση παλαιών συστημάτων με γνωστές ευπάθειες στις καθημερινές τους λειτουργίες (που αντιπροσωπεύουν περισσότερο από το 50% των συνολικού εξοπλισμού).

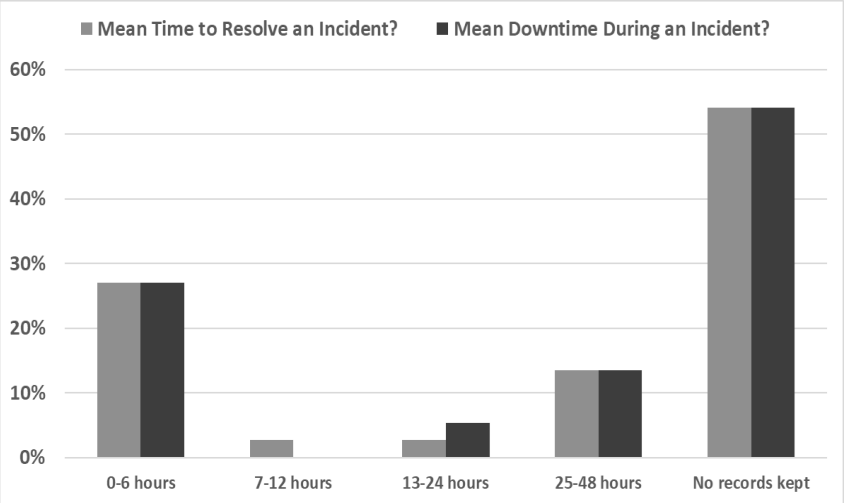
Επιπρόσθετα, μόνο το 24,3% γνώριζε την ύπαρξη όρων κυβερνοασφάλειας στο πλαίσιο των Συμφωνιών Επιπέδου Υπηρεσιών (Service Level Agreements, SLA) με προμηθευτές. Η σημασία της δημιουργίας μιας ενιαίας πολιτικής ασφαλείας για τους χρήστες και τους ρόλους με στόχο το μετριασμό των επιπτώσεων από εσωτερικές απειλές αναγνωρίστηκε μόνο από το 48,6% του προσωπικού ΤΠΕ. Η ανάγκη χρήσης πιστοποιητικών SSL (Secure Sockets Layer) από το Web-based Health Information System (HIS) επισημάνθηκε μόνο από το 48,6%. Αντίστοιχο ποσοστό του προσωπικού ΤΠΕ γνώριζε ότι ορισμένες επιθέσεις, όπως η κατανεμημένη άρνηση υπηρεσίας (Distributed Denial of Service, DDoS), θεωρούνται εγκληματικές ενέργειες. Από την άλλη πλευρά, το 75,7% αναγνώρισε τη χρήση προληπτικών εφεδρικών μετρήσεων.



Εικόνα 26. Απαντήσεις προσωπικού ΤΠΕ σε ερωτήσεις κυβερνοευπαθειών

Ωστόσο, το 54% του προσωπικού ΤΠΕ ανέφερε ότι δεν τηρούνται αρχεία καταγραφής (logs), καθιστώντας αδύνατη την ιατροδικαστική ανάλυση (forensics) περιστατικών ασφαλείας, με αποτέλεσμα επίσης να μην αντληθούν διδάγματα σχετικά με την

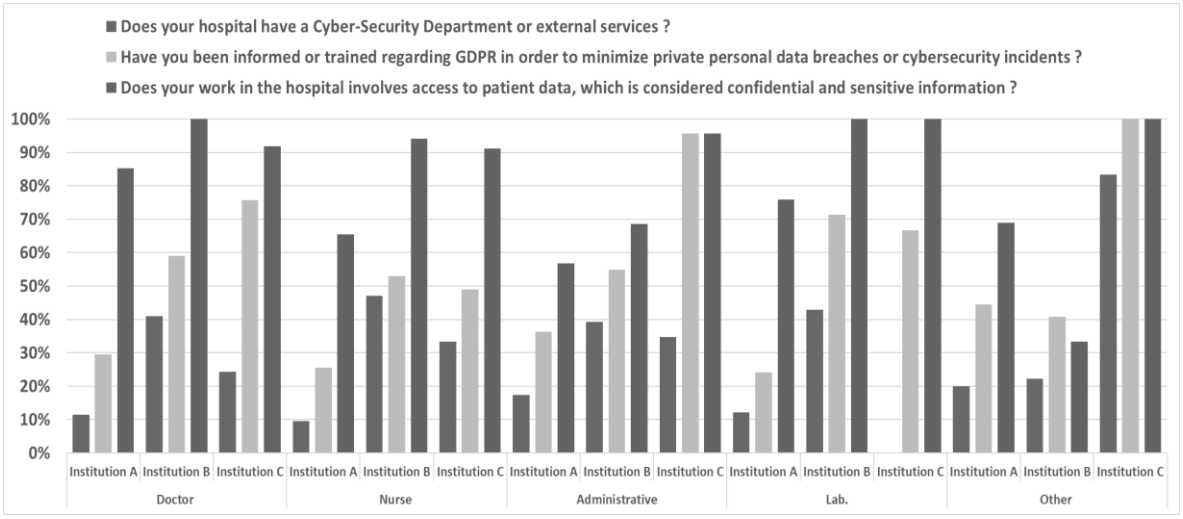
ανταπόκριση των οργανισμών. Επιπλέον, όπως φαίνεται στην Εικόνα 27, το προσωπικό ΤΠΕ απάντησε ότι τα περισσότερα περιστατικά κυβερνοασφάλειας που εντοπίστηκαν χρειάστηκαν έως και 6 ώρες για να επιλυθούν. Η ανάλυση αποκάλυψε ότι ο «μέσος χρόνος διακοπής λειτουργίας» ήταν ίσος με τον «μέσο χρόνο για την επίλυση του συμβάντος», πράγμα που σημαίνει ότι μέρος των εγκαταστάσεων και των σχετικών υπηρεσιών ΤΠΕ μπορεί να είχαν χάσει τη διαθεσιμότητα και τη λειτουργικότητά τους κατά τη διάρκεια του συμβάντος, γεγονός που μεταφράζεται πιθανώς ότι δεν υπήρχε σχέδιο επιχειρησιακής συνέχειας. Σε αυτό έρχεται να προστεθεί ο μικρός αριθμός δοκιμών διείσδυσης που αναφέρεται από τους συμμετέχοντες ότι έχει πραγματοποιηθεί τα τελευταία δύο χρόνια (καταφατικές απαντήσεις: μόνο 18% από το Α, 57% από το Β και 50% από το Γ). Όλα τα παραπάνω υποδεικνύουν την αναγκαιότητα διενέργειας τακτικών δοκιμών διείσδυσης στα συστήματα ΤΠΕ και επαναληπτικών εκπαιδεύσεων.



Εικόνα 27. Περιστατικά ασφαλείας

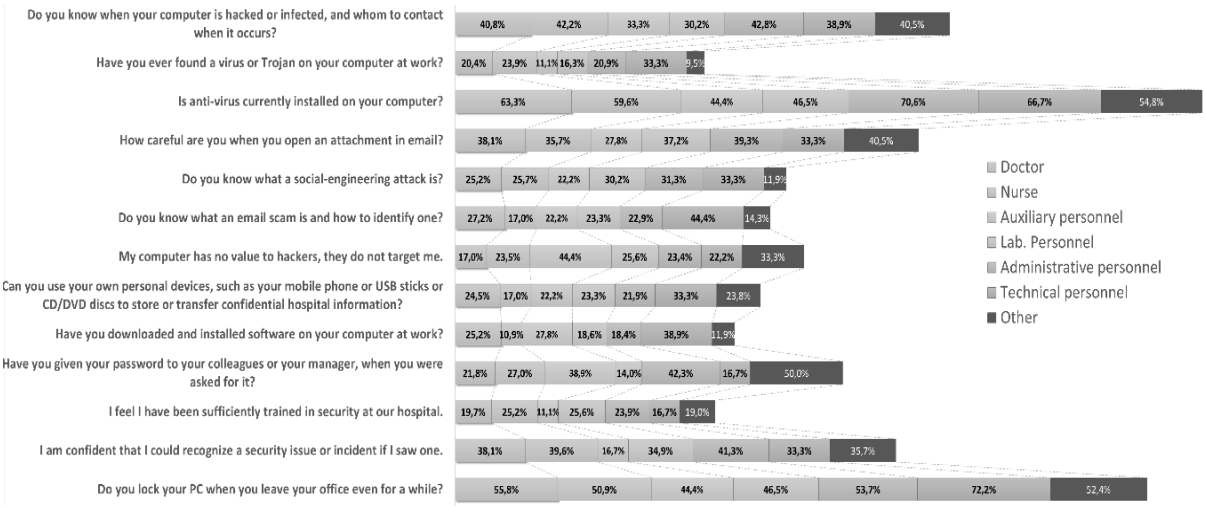
Ταυτόχρονα, η έρευνα αποκάλυψε την έλλειψη εκπαίδευσης που σχετίζεται με την κυβερνοασφάλεια και στα τρία ιδρύματα. Το 70% του προσωπικού ΤΠΕ παραδέχτηκε ότι δεν έχει λάβει επίσημη εκπαίδευση για θέματα του κυβερνοχώρου τα τελευταία 3 χρόνια, με το υπόλοιπο 30% να αποκαλύπτει συχνότητα λιγότερη από μία εκπαίδευση ετησίως ακόμη και για θέματα ευρωπαϊκής νομοθεσίας και καθοδήγησης, όπως οι οδηγίες NIS και GDPR. Ωστόσο, το προσωπικό ΤΠΕ απάντησε ότι γνώριζε αυτές τις πράξεις σε ποσοστό 80% στο ίδρυμα Α, 86% στο Β και 50% στο Γ. Από την άλλη, το 73% του προσωπικού που δεν ανήκει στις ΤΠΕ απάντησε ότι είχε πρόσβαση σε ευαίσθητες πληροφορίες και ήταν ενήμερο για τη νομοθεσία GDPR (Εικόνα 28).

Το 39% του προσωπικού ΤΠΕ στο ίδρυμα Α, το 57% στο ίδρυμα Β και το 100% στο ίδρυμα Γ απάντησε ότι συμμετείχε στην εσωτερική εκπαίδευση ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο.



Εικόνα 28. Επίγνωση υγειονομικού προσωπικού σε θέματα κυβερνοασφάλειας και απορρήτου

Η Εικόνα 29 παρουσιάζει τις απαντήσεις της υγειονομικής ομάδας συμμετεχόντων σε θέματα επίγνωσης κυβερνοασφάλειας. Μόνο το 22,7% αυτής της κατηγορίας προσωπικού αισθανόταν επαρκώς εκπαιδευμένο σε θέματα ασφάλειας, ενώ μόνο το 38,5% ήταν σίγουρο ότι θα μπορούσαν να αναγνωρίσει ένα ζήτημα ή περιστατικό ασφαλείας. Κατά την προσπάθεια ανίχνευσης της επίγνωσης του προσωπικού σε θέματα κυβερνοαπειλών, όπως phishing, και τις αντιδράσεις του σε αυτά, διαπιστώθηκε ότι μόνο το 26,8% των συμμετεχόντων γνώριζε τι είναι μια επίθεση κοινωνικής μηχανικής, και μόλις το 21,9% ήξερε πώς να αναγνωρίσει μια επίθεση ηλεκτρονικού ψαρέματος. Αν και οι συμμετέχοντες κατανοούσαν ότι χειρίζονταν ευαίσθητα δεδομένα σε καθημερινή βάση, μόνο το 23,3% αντιλαμβανόταν τη σημασία του περιεχομένου των τερματικών τους για τους επιτιθέμενους. Το 40,9% απάντησε ότι γνώριζε πότε τα τερματικά του είχαν παραβιαστεί και με ποιον να επικοινωνήσει σε μια τέτοια περίπτωση. Το 30,9% κατανοούσε τις συνέπειες της κοινής χρήσης του τερματικού ή των διαπιστευτηρίων του, ενώ το 37,3% γνώριζε πώς να χειρίζεται τα συνημμένα email. Περισσότερο από το 50% του προσωπικού που δεν ανήκει στα τμήματα ΤΠΕ αναγνώρισε την ύπαρξη λογισμικού προστασίας από ιούς και την πολιτική για το αυτόματο κλείδωμα των τερματικών σταθμών εργασίας. Η πλειοψηφία τους απάντησε επίσης (76%) ότι η τήρηση των πολιτικών ασφαλείας θα τους βοηθούσε να κάνουν καλύτερα τη δουλειά τους.



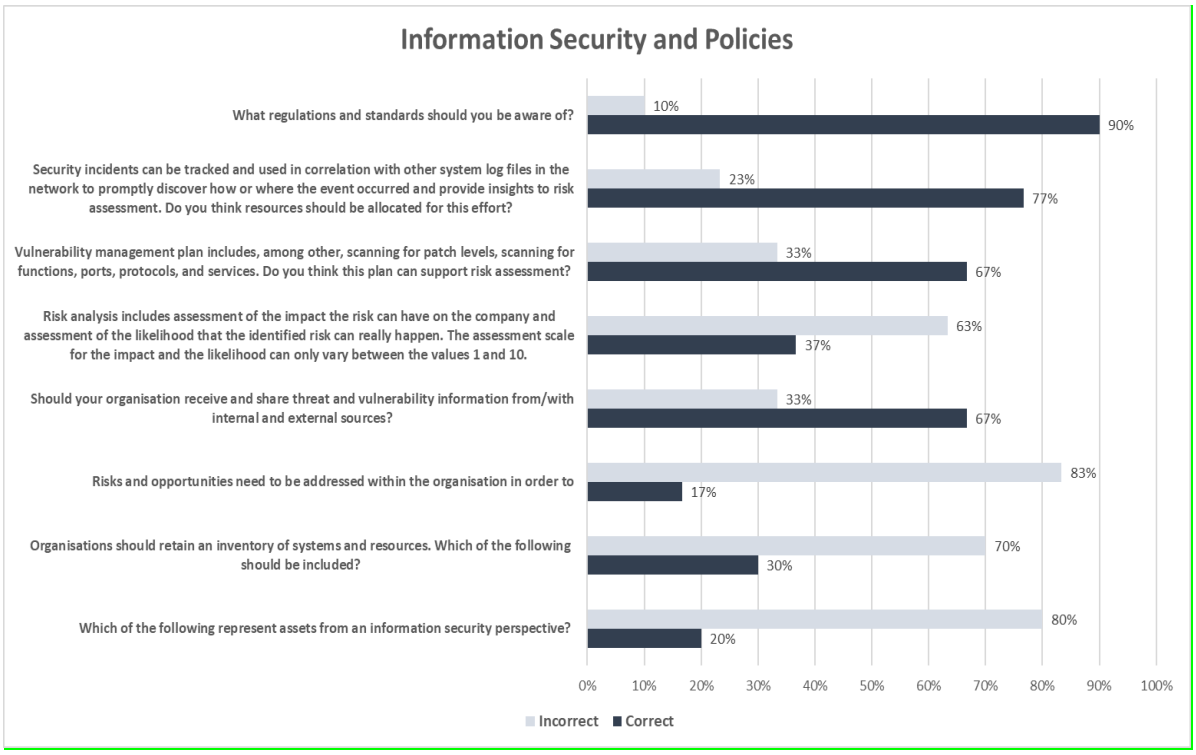
Εικόνα 29. Συμπεριφορά ασφαλείας και Επίγνωση υγειονομικού προσωπικού

Φάση Γ

Η Εικόνα 30 παρουσιάζει τα αποτελέσματα του ερωτηματολογίου που σχετίζονται με την ασφάλεια των πληροφοριών και τις πολιτικές. Πιο συγκεκριμένα, το 90% ήταν ενήμερο ότι τα πρότυπα του νόμου περί φορητότητας και λογοδοσίας ασφάλισης υγείας (Health Insurance Portability and Accountability Act, HIPAA) [204] και ISO/IEC 27799 (Πληροφορική υγείας — Διαχείριση ασφάλειας πληροφοριών στην υγεία με χρήση ISO/IEC 27002) [205] είναι αυτά στα οποία καλούνται να συμμορφώνονται. Επιπλέον, στην ερώτηση σχετικά με την κατανομή των πόρων κυβερνοασφάλειας, το 77% απάντησε ότι οι πόροι πρέπει να διατίθενται αποκλειστικά για αυτό το σκοπό. Το 67% των ερωτηθέντων δήλωσε ότι ένα σχέδιο διαχείρισης ευπαθειών που περιλαμβάνει, μεταξύ άλλων, σάρωση για επίπεδα ενημέρωσης κώδικα, λειτουργίες, θύρες, πρωτόκολλα και υπηρεσίες θα μπορούσε να υποστηρίξει την αξιολόγηση κινδύνου.

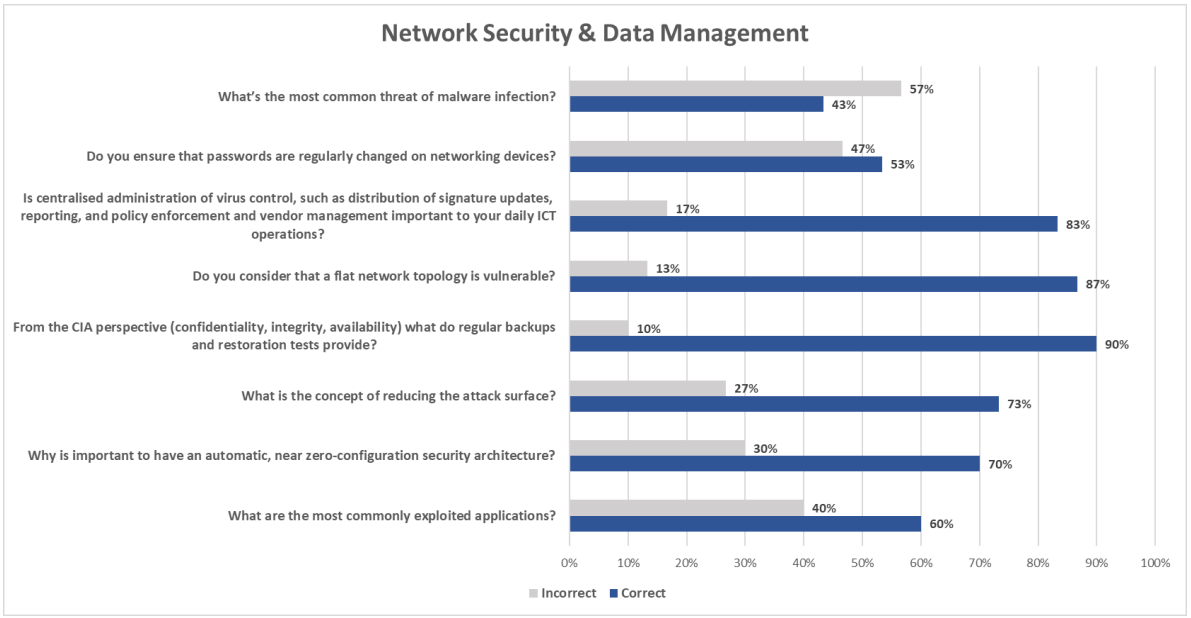
Περίπου το 67% των συμμετεχόντων είχε επίγνωση της υποχρέωσης του οργανισμού τους να διαμοιράζεται πληροφορίες απειλών και ευπαθειών με εσωτερικές και εξωτερικές πηγές. Όσον αφορά την αναγκαιότητα αντιμετώπισης κινδύνων και απειλών εντός του οργανισμού τους, μόλις το 17% αναγνώρισε την ανάγκη πρόληψης και συνεχούς βελτίωσης για τη μείωση των ανεπιθύμητων επιπτώσεων.

Το 30% είχε επίγνωση ότι κάθε περιουσιακό στοιχείο του οργανισμού πρέπει να περιλαμβάνεται στην απογραφή συστημάτων και πόρων ενώ ένα ακόμα μικρότερο ποσοστό, το 20%, κατανοεί ότι οι άνθρωποι, το λογισμικό και οι πληροφορίες υπάγονται στα περιουσιακά στοιχεία από θέμα ασφάλειας πληροφοριών.



Εικόνα 30. Ερωτηματολόγιο Φάσης Γ - Επίγνωση και κατανόηση πολιτικών ασφαλείας

Η Εικόνα 31 συνοψίζει τις απαντήσεις σε θέματα ασφάλειας δικτύου και διαχείρισης δεδομένων. Πιο συγκεκριμένα, αυτό το μέρος του ερωτηματολογίου αποκάλυψε ότι το 53% των συμμετεχόντων προτιμά μια τυπική πολιτική λήξης κωδικού πρόσβασης σε τακτά χρονικά διαστήματα, ενώ το 47% δήλωσε ότι προτιμά να αλλάζει τους προεπιλεγμένους κωδικούς πρόσβασης και, στη συνέχεια, να μην ζητείτε από τους τελικούς χρήστες να αλλάξουν τους κωδικούς εκ νέου.



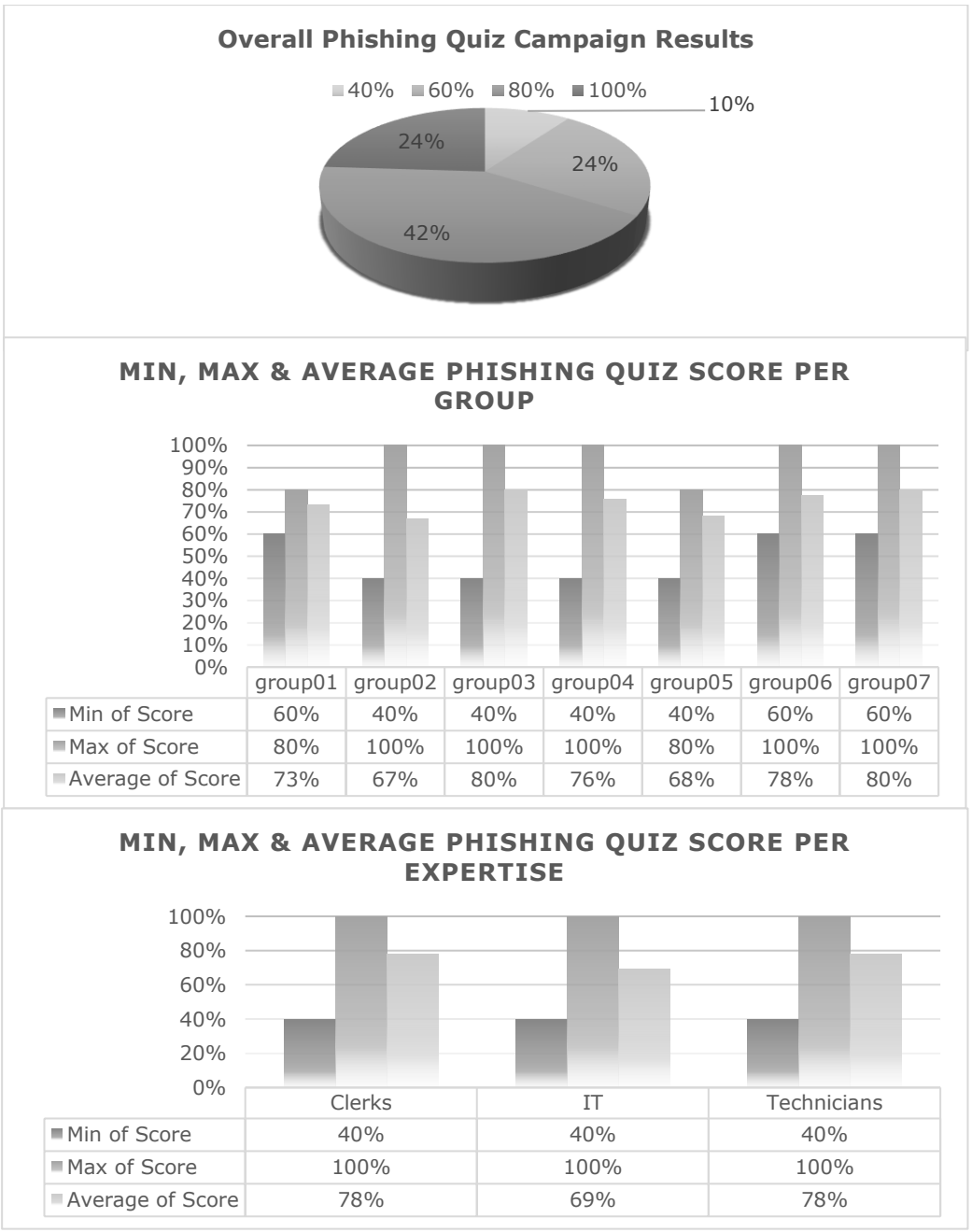
Εικόνα 31. Ερωτηματολόγιο Φάσης Γ - Επίγνωση και κατανόηση πολιτικών ασφαλείας δικτύων και διαχείρισης πληροφοριών

Το 83% των ερωτηθέντων θεωρεί ότι η κεντρική διαχείριση αντιϊκών λύσεων, όπως η διανομή ενημερωμένων υπογραφών, η αναβάθμιση, η επιβολή πολιτικών, κ.λπ. διευκολύνει τις καθημερινές εργασίες. Η συντριπτική πλειονότητα (87%) αναγνώρισε μια επίπεδη τοπολογία δικτύου ως ευάλωτη αρχιτεκτονική ενώ αντίστοιχο ποσοστό συμμετεχόντων (90%) κατανοεί ότι τα τακτικά αντίγραφα ασφαλείας και οι δοκιμές αποκατάστασης εξασφαλίζουν τη διαθεσιμότητα και τη μείωση του χρόνου ανάκτησης κατά την επαναφορά ενός συστήματος σε λειτουργία.

Το 73% αποκρίθηκε ότι η μείωση της επιφάνειας επιθέσεων συμπεριλαμβάνει την τμηματοποίηση του δικτύου, τον αποκλεισμό δραστηριοτήτων σε τρωτά σημεία και την καταπολέμηση κακόβουλου κώδικα. Επιπρόσθετα, το 70% αναγνωρίζει την ανάγκη αυτοματοποίησης στις υποδομές ασφαλείας με σχεδόν μηδενική ανάγκη διαμόρφωσης, ως μέτρα περιορισμού της χειρωνακτικής εργασίας και του ανθρώπινου σφάλματος.

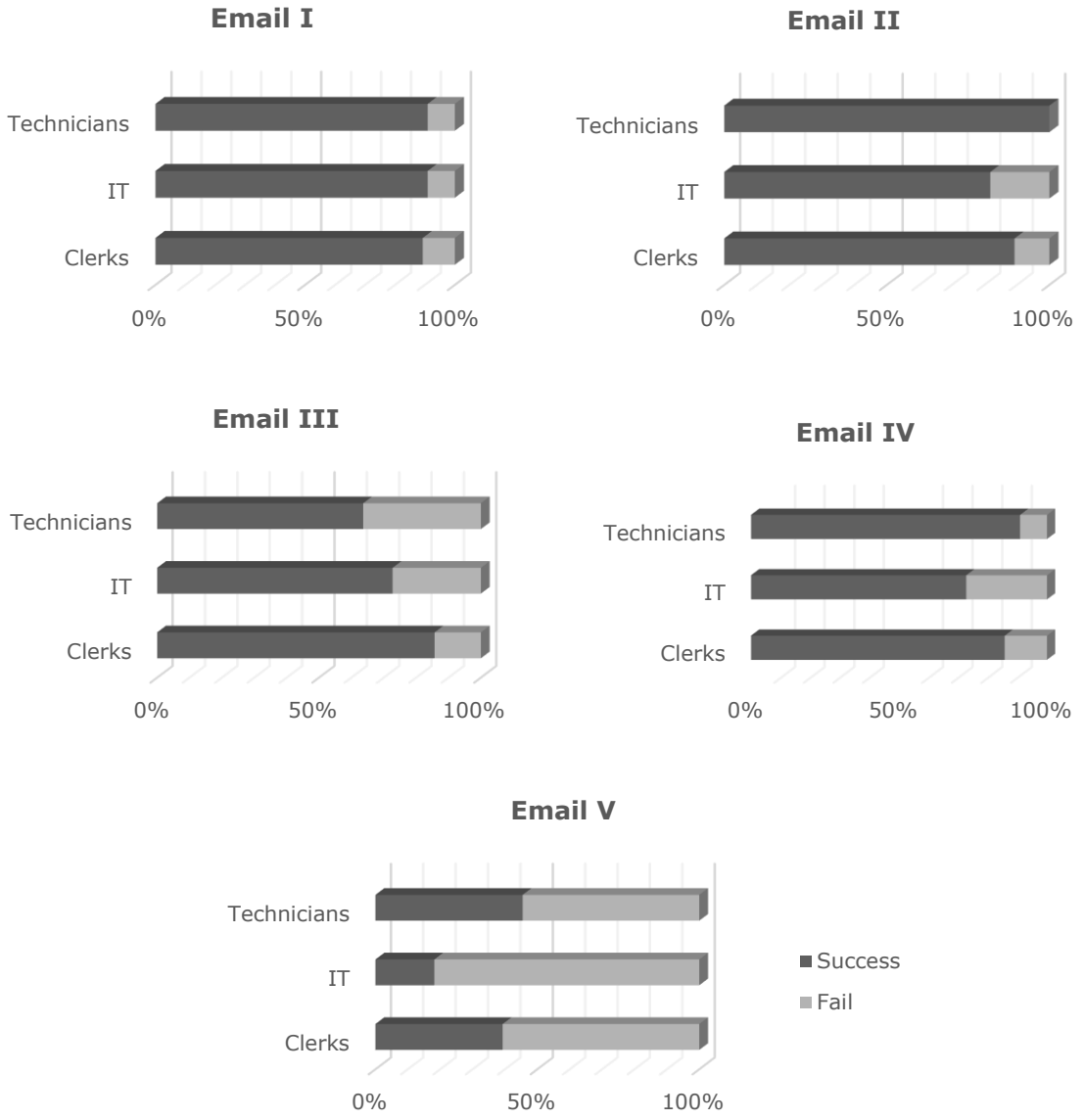
Αναφορικά με τα αποτελέσματα της δοκιμής phishing, όπως παρουσιάζονται στην Εικόνα 32, 1 στους 4 συμμετέχοντες μπόρεσε να διακρίνει ένα νόμιμο από ένα ηλεκτρονικό μήνυμα ηλεκτρονικού ψαρέματος με βαθμολογία επιτυχίας 100%. Το 10% από αυτούς κατάφερε να εντοπίσει μόνο 2 στα 5 email λαμβάνοντας το χαμηλότερο ποσοστό της εκστρατείας (40%). Αν και μια τέτοια βαθμολογία θα μπορούσε να θεωρηθεί αρκετά ικανοποιητική σε πολλές περιπτώσεις, δεν ισχύει το ίδιο για την πραγματικότητα της κυβερνοασφάλειας όπου ένας οργανισμός είναι τόσο ισχυρός όσο ο πιο αδύναμος κρίκος του.

Κατά την εξέταση των αποτελεσμάτων της συνολικής καμπάνιας από την προοπτική των ομάδων χρηστών, όπως απεικονίζεται στην Εικόνα 32(β), παρατηρούμε ότι 5 από τις 7 ομάδες κατάφεραν να επιτύχουν βαθμολογία μεγαλύτερη από 70%. Με μια προσεκτικότερη παρατήρηση των γραφημάτων εντοπίζεται ότι το προσωπικό πληροφορικής φαίνεται να έχει τον χαμηλότερο μέσο όρο σε σύγκριση με τις υπόλοιπες ομάδες, δηλαδή τους υπαλλήλους και τους τεχνικούς. Λόγω της στενής συσχέτισης των τομέων Τεχνολογίας Πληροφορικής και Ασφάλειας Πληροφοριών, αναμενόταν καλύτερη ενημέρωση για την ασφάλεια στον κυβερνοχώρο και τις τεχνικές phishing από τους ειδικούς της πληροφορικής.



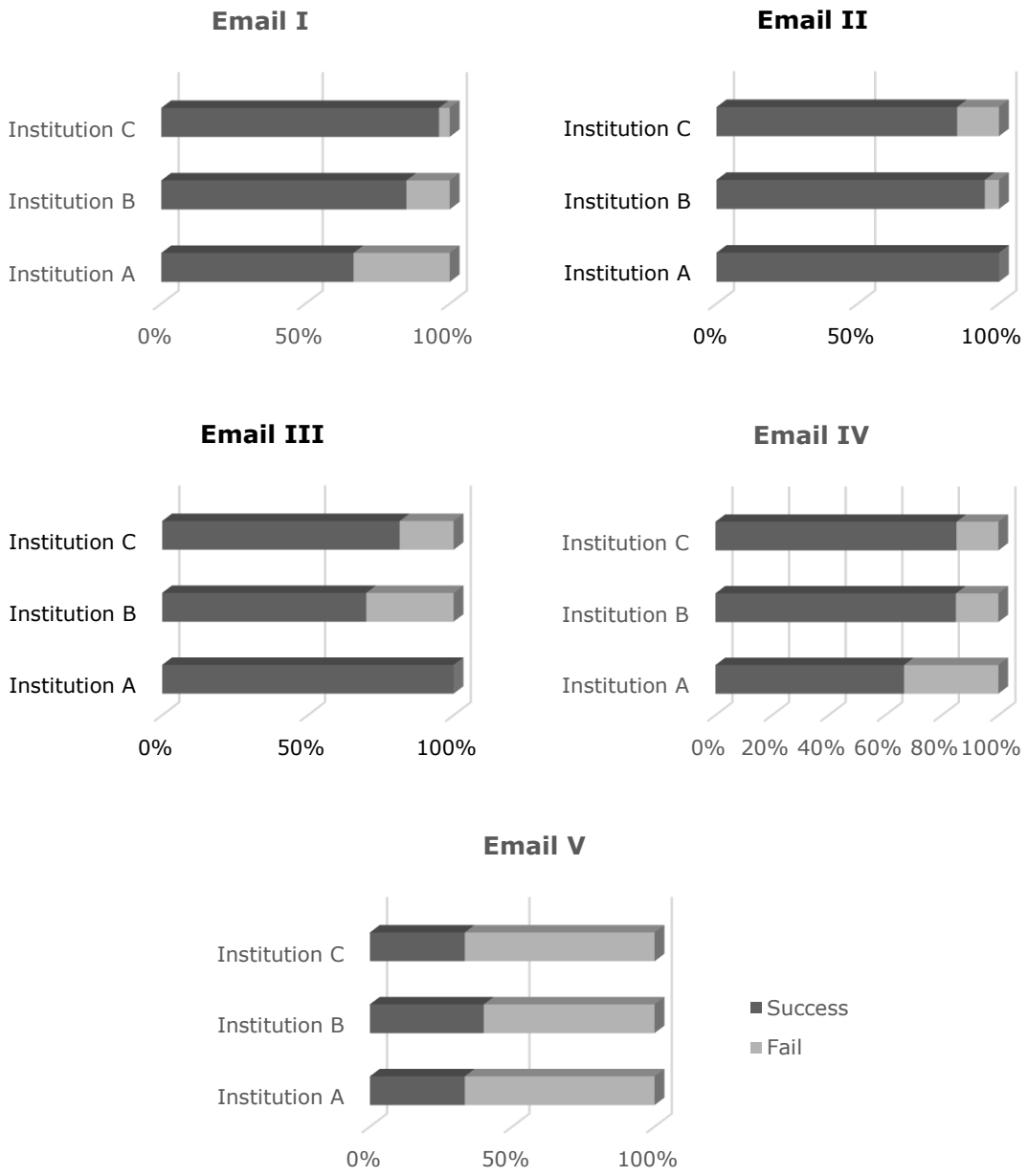
Εικόνα 32. Αποτελέσματα δοκιμής phishing: (α) συγκεντρωτικά, (β) ανά ομάδα χρηστών, (γ) ανά εξειδίκευση και (δ) ανά phishing email.

Μελετώντας τις αξιολογήσεις ανά email, τα email I & II φαίνεται να έχουν καλύτερες βαθμολογίες αναγνώρισης phishing (υψηλότερο από 80% από όλες τις συμμετέχουσες ομάδες), όπως παρουσιάζεται στις Εικόνα 33 και Εικόνα 34. Είναι ενδιαφέρον ότι αυτά τα δύο μηνύματα ηλεκτρονικού ταχυδρομείου δεν έχουν καμία ομοιότητα. Το πρώτο, όπως παρουσιάζεται στον Πίνακας 12, σχετίζεται με ένα τραπεζικό ίδρυμα, που περιέχει ένα εύκολα αναγνωρίσιμο λογότυπο και αναζητά επαλήθευση λογαριασμού κάνοντας κλικ σε ένα κείμενο με υπερσύνδεση όπου κρύβεται μια ύποπτη ανακατεύθυνση. Το δεύτερο είναι αρκετά μεγάλο, περιέχει μόνο κείμενο και προσπαθεί να πείσει, χρησιμοποιώντας αργκό, τους παραλήπτες του να πληρώσουν ένα ποσό σε Bitcoin για να μην αποκαλυφθούν προσωπικά βίντεο που έχουν καταγραφεί μέσω των παραβιασμένων καμερών του σταθμού εργασίας τους. Οι τεχνικές phishing που χρησιμοποιούνται σε αυτές τις δύο περιπτώσεις είναι αρκετά διαφορετικές και συνήθως στοχεύουν σε διαφορετικούς στόχους. Το email I κάνει επίκληση στην αίσθηση του καθήκοντος και της συνέπειας του παραλήπτη, ενώ το Email II στο φόβο και την αβεβαιότητα. Ωστόσο, οι υπάλληλοι των ιδρυμάτων που συμμετείχαν σε αυτήν την εκστρατεία αξιολόγησης κατάφεραν στην πλειονότητά τους να αναγνωρίσουν και τους δύο ως μη νόμιμους.



Εικόνα 33. Αποτελέσματα δοκιμής phishing ανά email και εξειδίκευση

Θα περίμενε κανείς ότι το Email III θα παρουσίαζε παρόμοια αποτελέσματα με το Email I αφού, όπως παρουσιάζεται στον Πίνακας 12. Το Email III σχετίζεται επίσης με ένα τραπεζικό ίδρυμα, το οποίο περιέχει το λογότυπό του, αναζητά επαλήθευση λογαριασμού παρέχοντας έναν υπερσύνδεσμο που δεν είναι κρυφός, αλλά είναι πλήρως ορατός στους αναγνώστες του. Επομένως, αναμένονταν καλύτερα αποτελέσματα καθώς χρειαζόταν λιγότερη προσπάθεια για τον εντοπισμό της παραπλανητικής ανακατεύθυνσης. Δεδομένου ότι ήταν η 3η εγγραφή στη δοκιμή phishing, η πλήξη και η απροσεξία θα μπορούσαν να ακολουθήσουν της αρχικής προσοχής και της επιφυλακτικότητας, εξηγώντας τις χαμηλότερες βαθμολογίες. Ωστόσο, ένα τέτοιο συμπέρασμα δεν θα συμφωνούσε με τα αποτελέσματα που παρατηρήθηκαν για το Email IV όπου οι βαθμολογίες είναι βελτιωμένες.



Εικόνα 34. Αποτελέσματα δοκιμής phishing ανά email και ίδρυμα

Τελευταίο αλλά εξίσου σημαντικό εύρημα είναι η παρατήρηση ότι η πλειονότητα των συμμετεχόντων (64%) απέτυχε να προσδιορίσει το μόνο νόμιμο email που περιλήφθηκε

στη δοκιμή ηλεκτρονικού ψαρέματος. Το συγκεκριμένο email ήταν σύντομο (όχι περισσότερες από 38 λέξεις), δεν περιείχε εικόνες ή λογότυπα, καμία ειδική μορφοποίηση γραμματοσειράς ή δομές email (π.χ. πίνακες). Η λέξη "εδώ" χρησιμοποιήθηκε για την παροχή ενός κρυφού υπερσυνδέσμου (θα μπορούσε να γίνει προεπισκόπηση όταν ο χρήστης τοποθετούσε το δείκτη του ποντικιού πάνω από τη λέξη με το ποντίκι) η οποία θα μπορούσε εύκολα να αναγνωριστεί ότι ανακατευθύνει στον επίσημο ιστότοπο του Υπουργείου Εσωτερικών. Παρόλο που το συγκεκριμένο αποτέλεσμα θα μπορούσε να αποδοθεί στην αυξημένη επιφυλακτικότητα των χρηστών λόγω των ειδικών συνθηκών της κρίσης και της φύσης της αξιολόγησης, παραμένει αρκετά ανησυχητικό. Τα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου ενδέχεται να προωθηθούν για ανάλυση ασφαλείας, να απορριφθούν ή ακόμη και να διαγραφούν χωρίς να κοινοποιηθεί το περιεχόμενό τους στους παραλήπτες τους, επειδή έχουν αναγνωριστεί εσφαλμένα ως απόπειρες ηλεκτρονικού ψαρέματος.

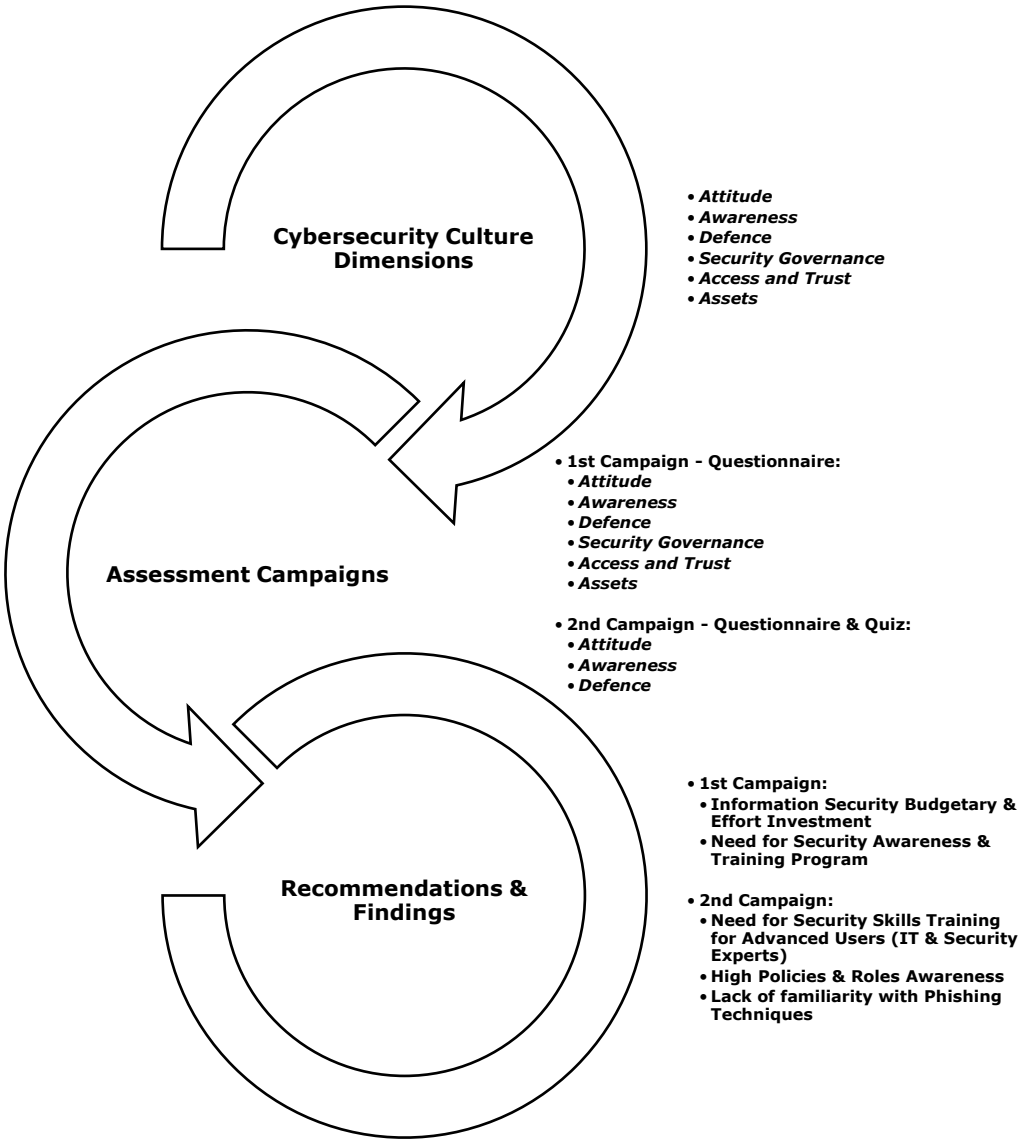
5.5 Συμπεράσματα

Φάση Α

Σύμφωνα με τα αποτελέσματα της εκστρατείας αξιολόγησης της φάσης αυτής (Εικόνα 35), το προσωπικό ΤΠΕ αντιπροσωπεύει ένα πολύ μικρό ποσοστό του συνολικού εργατικού δυναμικού, γενικά κάτω από το 1%. Οι υπό αξιολόγηση οργανισμοί έχουν αφιερώσει μόνο ένα μικρό ποσό του συνολικού προϋπολογισμού τους για ΤΠΕ (κάτω από 5%) για σκοπούς κυβερνοασφάλειας. Η σημασία της διάθεσης προϋπολογισμού για θέματα κυβερνοασφάλειας υπογραμμίζεται σε έκθεση του 2019 [206] της Εταιρείας Συστημάτων Πληροφοριών και Διαχείρισης Υγείας (Healthcare Information and Management Systems Society, HIMSS) στις ΗΠΑ. Οι συμμετέχοντες οργανισμοί ανέφεραν λιγότερο από 5% διάθεση προϋπολογισμού για θέματα κυβερνοασφάλειας στις ΤΠΕ. Οι διαφορές που εντοπίζονται στις επενδύσεις ΤΠΕ αποκαλύπτουν (όπως άλλωστε αναμενόταν) ότι τα έξυπνα νοσοκομεία έχουν επενδύσει περισσότερο στην κυβερνοασφάλεια και στην προστασία των πληροφοριών συγκριτικά με τα παραδοσιακά νοσοκομεία [207] που βρίσκονται σε διαδικασία ψηφιακού μετασχηματισμού. Η συνεχιζόμενη εφαρμογή των πολιτικών ψηφιακής σύγκλισης της ΕΕ (π.χ. διασυνοριακή ανταλλαγή δεδομένων υγείας) αναμένεται να γεφυρώσει το προαναφερθέν χάσμα).

Σχεδόν όλοι οι ερωτηθέντες (96%) στην έρευνα HIMSS 2019 [206] ανέφεραν ότι οι αντίστοιχοι οργανισμοί διεξήγαγαν αξιολογήσεις κινδύνου (37% εκ των οποίων ήταν ολοκληρωμένες, με αποτέλεσμα την υιοθέτηση νέων ή βελτιωμένων μέτρων ασφαλείας από το 72% αυτών). Στη δική μας εφαρμογή του πλαισίου κουλτούρας κυβερνοασφάλειας, η έλλειψη τμημάτων ασφάλειας και το ότι το 70% των υπαλλήλων ΤΠΕ δεν έχουν λάβει επίσημη εκπαίδευση στον κυβερνοχώρο τα τελευταία 3 χρόνια, αποκαλύπτει τη χαμηλή υιοθέτηση ή και έλλειψη τυπικών πολιτικών κυβερνοασφάλειας (100% για το Α και το Β και 50% για το C).

Σύμφωνα με τη μελέτη μας, το 21,9% παραδέχτηκε ότι δεν ξέρει πώς να ανιχνεύσει μια επίθεση ηλεκτρονικού ψαρέματος, κάτι που υποδηλώνει ότι το πραγματικό ποσοστό σε μια πραγματική επίθεση phishing μπορεί να είναι ακόμη υψηλότερο. Αυτό το εύρημα έμελλε να διασταυρωθεί (κατά το δυνατό) μετά το πέρας της φάσης εκπαίδευσης (Β) και με την εφαρμογή της δοκιμής phishing κατά τη Φάση Γ της προτεινόμενης μεθοδολογίας αξιολόγησης.



Εικόνα 35. Ευρήματα πλαισίου κουλτούρας κυβερνοασφάλειας

Όσον αφορά το προσωπικό που δεν ανήκει στις ΤΠΕ, συγκρίνοντας τα ευρήματά μας (Πίνακας 15) με μια μελέτη του 2020 στην Πολωνία [186], μια μελέτη του 2019 σε μια Περιφέρεια Υγείας της Δυτικής Φινλανδίας [187] και μια μελέτη του 2019 σε έναν Οργανισμό Υγείας στον Δυτικό Καναδά [208], υπογραμμίζεται το χαμηλό επίπεδο ευαισθητοποίησης και επίγνωσης για θέματα κυβερνοασφάλειας. Στα ιδρύματα Α, Β και Γ, το 22,7% αισθανόταν επαρκώς εκπαιδευμένο σε θέματα ασφάλειας και το 23,3% που αντιλαμβανόταν τη σπουδαιότητα των τερματικών σταθμών σε θέματα παραβιάσεων. Τα ποσοστά αυτά είναι σημαντικά χαμηλότερα σε σχέση με το 51,31% των 1200 Φινλανδών επαγγελματιών που ανέφεραν επαρκώς ενήμεροι σε τα θέματα κυβερνοασφάλειας που άπτονται τη δουλειά τους. Περίπου το ίδιο ποσοστό (55,7%) 586 επαγγελματιών μη ΤΠΕ στον καναδικό οργανισμό υγειονομικής περίθαλψης δήλωσαν ικανοποιημένοι από την ασφάλεια στις καθημερινές τους δραστηριότητες.

Το 73,2% των συμμετεχόντων μας, που δεν ανήκουν σε τμήματα ΤΠΕ, δήλωσαν άγνοια αναφορικά με τις επιθέσεις κοινωνικής δικτύωσης, γεγονός που τους καθιστά πιθανό κίνδυνο διαρροής ευαίσθητων πληροφοριών. Το 69,1% δεν μπορούσε να

συνειδητοποιήσει καν τις συνέπειες κοινής χρήσης τερματικών ή διαπιστευτηρίων με άλλους υπαλλήλους.

Η χαμηλή έως μέτρια γνώση και ευαισθητοποίηση στα ανωτέρω πεδία ενέχει υψηλό κίνδυνο κατά τις καθημερινές εργασιακές δραστηριότητες, όπως η επεξεργασία των δεδομένων του ασθενούς ή η επικοινωνία ιατρικών πληροφοριών σε άλλα μέρη. Ως εκ τούτου, συνάγεται ότι ο κίνδυνος περιστατικών ασφαλείας είναι υψηλός. Η απλούστευση της χρήσης των τερματικών σημείων και η διεξαγωγή συχνών εκπαιδεύσεων είναι απαραίτητες για την ευαισθητοποίηση του προσωπικού και επίκληση της προσοχής του σε απειλές στον κυβερνοχώρο και σε πολιτικές για τον περιορισμό των ανθρώπινων λαθών [209, 210, 211].

Πίνακας 15. Διακύμανση απαντήσεων σχετικών με θέματα επίγνωσης κυβερνοασφάλειας του υγειονομικού προσωπικού

Question	Institution A n = 449 (100%)	Institution B n = 124 (100%)	Institution C n = 126 (100%)
Do you have cyber-security policies at your hospital?			
Yes	11% ± 0.5	55% ± 4.9	60% ± 5.3
No	14% ± 0.7	2% ± 0.2	7% ± 0.6
Do not know	75% ± 3.5	43% ± 3.8	33% ± 2.9
Have you been informed or trained regarding General Data Protection Regulation (GDPR) in order to minimize private personal data breaches or cybersecurity incidents?			
Yes	31% ±2.5	31% ±0.2	31% ±0.1
No	69% ±0.08	69% ±0.2	69% ±0.1
How careful are you when you open an attachment in email?			
I always make sure it is from a person I know and I am expecting the email	32% ± 6.7	48% ± 15.9	50% ± 18.4
As long as I know the person or company that sent me the attachment, I open it	59% ± 7.7	42% ± 15.4	45% ± 18.4
There is nothing wrong with opening attachments	9% ± 6.3	10% ± 12.3	5% ± 7.4

Have you given your password to your colleagues or your manager, when you were asked for it?				
	Yes	33% ± 9.1	26% ± 14.2	30% ± 24.1
	No	67% ± 9.1	74% ± 14.2	70% ± 24.1
Is anti-virus currently installed on your computer?				
	Yes	60% ± 2.8	16% ± 1.4	79% ± 6.9
	No	11% ± 0.5	65% ± 5.8	5% ± 0.4
	Do not know	29% ± 1.3	19% ± 2.7	17% ± 1.5
I am confident that I could recognize a security issue or incident if I saw one.				
	Strongly agree	4% ± 2.4	4% ± 4.6	14% ± 12.3
	Agree	24% ± 8.1	39% ± 18.3	59% ± 15.3
	Neither agree nor disagree	42% ± 10	34% ± 18	8% ± 7.8
	Disagree	23% ± 8.3	20% ± 9.1	17% ± 10.3
	Strongly disagree	7% ± 4.5	3% ± 3	2% ± 1.9

Φάση Γ

Η ανάλυση του ερωτηματολογίου του διαδικτυακού σεμιναρίου έδειξε ότι τα τμήματα πληροφορικής κατανόησαν επαρκώς έννοιες όπως η εφαρμογή προτύπων στις πολιτικές τους και η ενσωμάτωση της επαναληπτικής αξιολόγησης κινδύνου των περιουσιακών τους στοιχείων στις δραστηριότητές τους. Επιπλέον, επέδειξαν υψηλή εξοικείωση με τις διάφορες τοπολογίες δικτύου και τα προηγμένα εργαλεία κυβερνοασφάλειας. Ωστόσο, θα πρέπει να δοθεί μεγαλύτερη έμφαση σε εστιασμένα προγράμματα κατάρτισης που στοχεύουν στην αξιολόγηση κινδύνου και στον προσδιορισμό των στοιχείων ενεργητικού.

Συνοψίζοντας τα αποτελέσματα της στοχευμένης εκστρατείας μετά την αξιολόγηση για το phishing, η πιο εμφανής και ταυτόχρονα απροσδόκητη παρατήρηση είναι ότι η χαμηλότερη μέση βαθμολογία αποδίδεται στους επαγγελματίες πληροφορικής. Αναμενόταν να είναι οι πιο ικανοί από τους ερωτηθέντες και εκείνοι που είναι ικανοί να καθοδηγούν και να συμβουλεύουν το προσωπικό των νοσοκομείων σχετικά με τις ενέργειές τους σε σχέση με ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου. Ωστόσο, αυτά τα αποτελέσματα προέκυψαν μετά από μια σειρά από καμπάνιες ανεπιθύμητης αλληλογραφίας Emotet που επηρέασαν τα νοσοκομεία τους. Αυτά τα γεγονότα μπορεί εύλογα να έχουν επηρεάσει την επίγνωσή τους και να έχουν σκληρύνει την κρίση τους.

Πράγματι, η χαμηλότερη βαθμολογία προκύπτει για το Email V όπου μόνο το 18% του προσωπικού πληροφορικής αναγνώρισε επιτυχώς ότι αυτό ήταν ένα νόμιμο μήνυμα ηλεκτρονικού ταχυδρομείου. Αν και ο παραπάνω συλλογισμός θα μπορούσε να δικαιολογήσει επαρκώς αυτό το αποτέλεσμα, δεν μπορεί να θεωρηθεί σημείο που δεν χρήζει περαιτέρω ενεργειών. Η επίδειξη ασφαλούς συμπεριφοράς στον κυβερνοχώρο απαιτεί σωστές αποφάσεις όπου τα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου θα φτάσουν στους παραλήπτες τους και θα απολαύσουν κατάλληλου χειρισμού, ενώ τα μηνύματα ηλεκτρονικού ψαρέματος θα εντοπιστούν αμέσως και θα απορριφθούν.

Ως εκ τούτου, τα αποτελέσματα υποδηλώνουν ότι υπάρχει ακόμη χώρος για ειδικά εκπαιδευτικά προγράμματα που θα πρέπει πρώτα – αλλά όχι αποκλειστικά – να στοχεύουν στα τμήματα πληροφορικής των νοσοκομείων ώστε να μπορούν να προσφέρουν ένα ισχυρό πρώτο επίπεδο ασφάλειας και να παρέχουν τις σωστές συμβουλές όταν τους ζητηθεί. Εξάλλου, η μεγάλη επιτυχία των μηνυμάτων ηλεκτρονικού ψαρέματος στην εξαπάτηση μπορεί να αποδοθεί στο γεγονός ότι οι phishers γίνονται ολοένα και πιο ευρηματικοί [212]. Ως εκ τούτου, ακόμη και οι γνώστες της τεχνολογίας μπορούν να εξαπατηθούν, ενώ η τακτική εκπαίδευση μπορεί σίγουρα να θωρακίσει έναν οργανισμό, όπως προτείνουν προηγούμενες εργασίες [213, 214].

Μια άλλη παρατήρηση είναι ότι δεν υπάρχει αξιοσημείωτη διαφορά μεταξύ των τριών ομάδων, προσωπικού πληροφορικής, τεχνικών και υπαλλήλων, όπως υποδεικνύεται τόσο από τη μέση βαθμολογία τους όσο και από την ατομική τους ανάλυση. Αυτό μπορεί να οφείλεται σε δύο λόγους. Πρώτον, γενικά, οι άνθρωποι τείνουν να δυσκολεύονται να συσχετιστούν με ένα θεωρητικό πρόβλημα, το οποίο πιστεύουν ότι δεν θα τους συμβεί [215]. Επομένως, όταν λαμβάνουν ένα νέο email, δεν επενδύουν χρόνο και προσπάθεια για να αμφισβητήσουν τις προθέσεις του. Δεύτερον, οι πιο έμπειροι χρήστες της τεχνολογίας τείνουν να έχουν υπερβολική αυτοπεποίθηση στην ικανότητά τους να εντοπίσουν την απάτη και την κακή πρόθεση, κάτι που συνήθως αποδεικνύεται ως αφελής πεποίθηση [215].

Τέλος, τα αποτελέσματα της ανάλυσης δεν έδωσαν αξιοσημείωτες διαφορές μεταξύ των τριών ελληνικών ιδρυμάτων υγείας που συμμετείχαν στην ανάλυση. Το ανησυχητικό εύρημα είναι ότι οι χαμηλότερες βαθμολογίες εμφανίζονται και για τα τρία νοσοκομεία για το Email V, το μόνο νόμιμο μήνυμα της δοκιμασίας phishing. Η εμπειρία έχει δείξει ότι δεν θα μπορεί να υπάρξει τέλειος μηχανισμός φιλτραρίσματος ηλεκτρονικού "ψαρέματος" και η ευαισθητοποίηση των παραληπτών σχετικά με την ασφάλεια στον κυβερνοχώρο είναι το κλειδί για την αποτυχία των phishers.

ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ

Στο πλαίσιο της παρούσας διατριβής σχεδιάστηκε και παρουσιάστηκε ένα πλαίσιο κουλτούρας κυβερνοασφάλειας για την αξιολόγηση της τρέχουσας ετοιμότητας κυβερνοασφάλειας του εργατικού δυναμικού ενός οργανισμού.

Ξεκινώντας από μια ενδελεχή ανασκόπηση των πιο συχνά χρησιμοποιούμενων πλαισίων ασφαλείας, προσδιορίστηκαν τα βασικά στοιχεία ασφάλειας που σχετίζονται με τον ανθρώπινο παράγοντα και ταξινομήθηκαν δομώντας ένα γενικευμένο μοντέλο κουλτούρας ασφάλειας. Έγινε διάκριση μεταξύ:

- της ερευνητικής προσέγγισης που κάνει χρήση διαφόρων επιστημονικών προσεγγίσεων (ανθρωπολογική, κοινωνική, κ.λπ.) με επίκεντρο τον ανθρώπινο παράγοντα και τα «εσωτερικά» χαρακτηριστικά του: τη συμπεριφορά, τη γνώση, την ικανότητα, την αντίληψη, και
- της προσέγγισης των επαγγελματιών του χώρου της κυβερνοασφάλειας που εστιάζουν στους «εξωτερικούς» παράγοντες: τις πολιτικές και αρχές ασφαλείας, τις υποδομές και εταιρικές λύσεις, που διαμορφώνουν το περιβάλλον στο οποίο καλείται να εργαστεί και να δράσει ο εργαζόμενος.

Το προτεινόμενο πλαίσιο, ακολουθώντας μια διεπιστημονική και πολυκριτηριακή προσέγγιση, αποπειράθηκε να γεφυρώσει το χάσμα μεταξύ των δύο αυτών ρευμάτων και να διαμορφώσει ένα υπερσύνολο παραγόντων ασφαλείας που εξετάζονται συνδυαστικά και συμπληρωματικά για την αξιολόγηση του επιπέδου ετοιμότητας και κουλτούρας κυβερνοασφάλειας ενός οργανισμού. Κάθε στοιχείο του μοντέλου αναλύθηκε και ορίστηκαν ποσοτικοί δείκτες με στόχο τον προσδιορισμό μιας διεξοδικής μεθοδολογίας αξιολόγησης.

Το προτεινόμενου μοντέλο συσχετίστηκε με δύο από τα πλέον διαδεδομένα και αναγνωρισμένα μοντέλα/πλαίσια ασφαλείας: το μοντέλο Εσωτερικής Απειλής (Insider Threat) και το μοντέλο MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Το αποτέλεσμα των προαναφερθέντων συσχετίσεων ήταν η ανάδειξη ενός πλαισίου κουλτούρας κυβερνοασφάλειας ικανού να αξιολογήσει την τρέχουσα κατάσταση ασφαλείας ενός οργανισμού, εντοπίζοντας τα κενά και τις αδυναμίες του και υποδεικνύοντας αντίμετρα, συστάσεις και εναλλακτικές προσεγγίσεις συμπεριλαμβανομένων προγραμμάτων κατάρτισης εργατικού δυναμικού.

Το προτεινόμενο πλαίσιο κουλτούρας κυβερνοασφάλειας, όντας απόλυτα δυναμικό, προσαρμόζεται εύκολα σε διάφορους επιχειρησιακούς τομείς με ιδιαίτερη έμφαση τις κρίσιμες υποδομές δεδομένων των αυστηρότερων κανονισμών στους οποίους αυτές υπόκεινται.

Προκειμένου το προτεινόμενο πλαίσιο να μην μείνει αποκλειστικά στο θεωρητικό επίπεδο και τόσο η καταλληλόλητα, όσο και η αξία του, να επικυρωθούν, πραγματοποιήθηκαν δύο πρακτικές εφαρμογές του. Στη λογική αυτή, το πρώτο βήμα ήταν η ανάπτυξη ενός λογισμικού (ανοικτού κώδικα) που εφαρμόζει ποικίλες τεχνικές και μεθοδολογίες αξιολόγησης με στόχο την προσμέτρηση τόσο των οργανωτικών όσο και των ατομικών δεικτών κυβερνοασφάλειας ενός οργανισμού.

Η **πρώτη εφαρμογή** (*ΚΕΦΑΛΑΙΟ 4: ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ ΣΕ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ ΚΑΤΑ ΤΗΝ ΠΕΡΙΟΔΟ ΤΟΥ ΚΟΡΟΝΟΪΟΥ (COVID-19)*) στόχευσε σε εκπροσώπους των τομέων της ενέργειας, των μεταφορών, της ύδρευσης, των τραπεζικών ιδρυμάτων, της

χρηματοπιστωτικής αγοράς, της υγειονομικής περίθαλψης και των ψηφιακών υποδομών από διάφορες ευρωπαϊκές χώρες (π.χ. Κύπρος, Γαλλία, Γερμανία, Ελλάδα, Ιταλία, Ρουμανία, Ισπανία) που επλήγησαν από την πανδημία. Μερικά αξιοσημείωτα συμπεράσματα στα οποία κατέληξε η εφαρμογή είναι:

- η ανάγκη ενίσχυσης των κατευθυντήριων γραμμών και της συνεχούς πληροφόρησης σχετικά με τους κινδύνους στον κυβερνοχώρο
- η αναγκαιότητα εκπαίδευσης και υποστήριξης για τη διασφάλιση υψηλού επιπέδου ασφάλειας και ευαισθητοποίησης εντός των οργανισμών
- η ανάγκη διαχείρισης και ασφάλειας απομακρυσμένων εταιρικών περιουσιακών στοιχείων με μεγαλύτερη σημασία και προτεραιότητα

Η **δεύτερη εφαρμογή** (*ΚΕΦΑΛΑΙΟ 5: ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ ΣΤΟΝ ΥΓΕΙΟΝΟΜΙΚΟ ΤΟΜΕΑ*) στόχευσε σε τρεις διαφορετικούς φορείς υγειονομικής περίθαλψης από τρεις Ευρωπαϊκές χώρες, την Ελλάδα, την Πορτογαλία και τη Ρουμανία, καθώς πληθώρα μελετών καταδείκνυε ότι το ιατρικό προσωπικό δεν διαθέτει επαρκή εκπαίδευση στον τομέα της κυβερνοασφάλειας. Τα σημαντικότερα συμπεράσματα που προέκυψαν από την εφαρμογή αυτή είναι:

- Ο κίνδυνος περιστατικών ασφαλείας στον τομέα αυτό είναι υψηλός.
- Η απλούστευση της χρήσης των τερματικών σημείων και η διεξαγωγή συχνών εκπαιδεύσεων είναι απαραίτητες για την ευαισθητοποίηση του προσωπικού.
- Η επίκληση της προσοχής του προσωπικού σε απειλές στον κυβερνοχώρο και σε πολιτικές για τον περιορισμό των ανθρώπινων λαθών.

Συμπερασματικά, τόσο η θεωρητική ανάλυση, όσο και οι πρακτικές εφαρμογές ανέδειξαν και υπογράμμισαν τη σπουδαιότητα υιοθέτησης ενός πολύπλευρου και πολυκριτηριακού μοντέλου κουλτούρας κυβερνοασφάλειας προσανατολισμένου στον ανθρώπινο παράγοντα με συνεξέταση εσωτερικών και εξωτερικών παραγόντων.

Οι ραγδαίες εξελίξεις του χώρου κυβερνοασφάλειας και των σχετιζόμενων μοντέλων και γνωσιακών βάσεων (π.χ. ISO 27001/2022) υπαγορεύουν την αδιάκοπη προσαρμογή και επέκταση του πλαισίου κουλτούρας κυβερνοασφάλειας έμμεσα διαμορφώνοντας, ενισχύοντας και επεκτείνοντας τις μελλοντικές προοπτικές του. Δεδομένης της αδιάλειπτης εξέλιξης της Τεχνολογίας και της Ασφάλειας Πληροφοριών είναι αναγκαία η συνεχής προσαρμογή, διεύρυνση, επικαιροποίηση και επέκταση του μοντέλου κουλτούρας κυβερνοασφάλειας προκειμένου να ακολουθεί την εξελικτική πορεία της σύγχρονης ψηφιακής πραγματικότητας και εργασιακού χώρο.

Ένας άλλος τομέας που προσφέρεται για τη διεύρυνση των προοπτικών τόσο του πλαισίου κουλτούρας κυβερνοασφάλειας όσο και του εργαλείου εφαρμογής του (SBA) είναι οι μέθοδοι αξιολόγησης των ελέγχων ασφάλειας οι οποίες δύναται να εμπλουτιστούν με επιπρόσθετα διαδραστικά εργαλεία και παίγνια ικανά να εκτιμήσουν τη συμπεριφορά, τη νοοτροπία, την αντίληψη και τη δυναμική των χρηστών σε θέματα κυβερνοασφάλειας σε ρεαλιστικά σενάρια εργασίας και δράσης.

Τέλος, η σημαντικότερη στόχευση των ερευνητικών μας προσπαθειών εστιάζει στην εφαρμογή του πλαισίου σε νέους επιχειρησιακούς τομείς. Ακολούθως συνοψίζονται έρευνες που βρίσκονταν σε σχεδιασμό, εξέλιξη ή ολοκληρώθηκαν κατά τη διάρκεια συγγραφής του παρόντος:

- Εφαρμογή στο χώρο της ενέργειας από εκπροσώπους του ερευνητικού προγράμματος EnergyShield:

- Μια πιλοτική εφαρμογή έλαβε ήδη χώρα για τους Βούλγαρους εκπρόσωπους του ενεργειακού χώρου (παραγωγούς, διανομείς, μεταφορείς, κτλ.) τα αποτελέσματα της οποίας παρουσιάστηκαν σε συνέδριο τον Αύγουστο του 2022 [216] ενώ μια εκτενής εφαρμογή του πλαισίου με αξιοποίηση του συνόλου των δομών του και του αξιολογητικού του περιεχομένου βρίσκεται ήδη σε εξέλιξη.
- Μια στοχευμένη εφαρμογή αξιολογητικής εκστρατείας για το διανομέα ηλεκτρικής ενέργειας της Ιταλίας (IREN) ολοκληρώθηκε τους προηγούμενους μήνες με ενδιαφέροντα αποτελέσματα που βρίσκονται υπό δημοσίευση σε επιστημονικό περιοδικό [217] ενώ μια εκτενέστερη με πολλαπλούς παράλληλους αξιολογητικούς κύκλους βρίσκεται σε εξέλιξη το τελευταίο εξάμηνο.

❖ Εφαρμογή στον ακαδημαϊκό χώρο: Μία στοχευμένη εκστρατεία αξιολόγησης πραγματοποιήθηκε από τις 28 Φεβρουαρίου 2022 έως τις 13 Μαρτίου 2022. Η καμπάνια αποτελούνταν από τέσσερα ερωτηματολόγια αυξημένης δυσκολίας και ένα phishing κουίζ, στοχεύοντας στην αξιολόγηση της κουλτούρα ασφάλειας των συμμετεχόντων εστιάζοντας σε τρεις διαστάσεις - τη στάση ασφαλείας τους, τις ικανότητές τους και την πραγματική τους συμπεριφορά. Τα αποτελέσματα της καμπάνιας έχουν αναλυθεί διεξοδικά και παρουσιαστεί μαζί με τα απρόσμενα ευρήματα τους σε άρθρο που παρουσιάστηκε τον Αύγουστο του 2022 [218]. Με βάση τα ευρήματα και τις αδυναμίες που εντοπίστηκαν, γίνεται σχεδιασμός εκπαιδευτικών δραστηριοτήτων σε θέματα κυβερνοασφάλειας καθώς και βελτιωτικών ενεργειών σε θέματα ασφάλειας πληροφοριών. Στόχος είναι ο επανέλεγχος της κουλτούρας μετά το πέρας των διορθωτικών ενεργειών και η εκ νέου αξιολόγηση με συνεκτίμηση της αποτελεσματικότητας των δράσεων.

Το πλαίσιο κουλτούρας κυβερνοασφάλειας, η μεθοδολογία του και το εργαλείο εφαρμογής του έχουν δυναμική εξέλιξης και περαιτέρω ερευνητικής αξιοποίησης σε πληθώρα τομέων με την ενδιαφέρουσα προοπτική της συνεξέτασης των ευρημάτων και αξιοποίησής τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] K. d. Leeuw και J. A. Bergstra, The history of information security : a comprehensive handbook, Amsterdam: Elsevier, 2007.

[2] J. M.Anderson, «Why we need a new definition of information security,» *Computers & Security,* τόμ. 22, αρ. 4, pp. 308-313, 203.

[3] B. v. Solms, «Information Security — The Third Wave?,» *Computers & Security,* τόμ. 19, pp. 615-620, 2000.

[4] A. Da Veiga και J. H. Eloff, «An Information Security Governance Framework,» *Information Systems Management,* τόμ. 24, αρ. 4, pp. 361-372, 2007.

[5] S. H. (. v. Solms, «The 5 Waves of Information Security – From Kristian Beckman to the Present,» σε *IFIP International Information Security Conference*, 2010.

[6] European Union Agency for Cybersecurity (ENISA), «BS 7799-3 - ENISA,» European Union Agency for Cybersecurity (ENISA), [Ηλεκτρονικό]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/bs-7799-3. [Πρόσβαση 14 03 2022].

[7] B. v. Solms, «Information Security – The Fourth Wave,» *Computers & Security,* τόμ. 25, αρ. 3, pp. 165-168, 2006.

[8] N. F. Doherty και H. Fulford, «Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis,» *Information Resources Management Journal,* τόμ. 18, αρ. 4, pp. 21-40, 2005.

[9] K. Rantos, K. Fysarakis και H. Manifavas, «How Effective Is Your Security Awareness Program? An Evaluation Methodology,» *Information Security Journal: A Global Perspective,* τόμ. 21, pp. 328-345, 01 2012.

[10] N. Hoffman και R. Klepper, «Assimilating New Technologies: The Role of Organizational Culture,» *Information Systems Management,* τόμ. 17, αρ. 3, pp. 1-7, 2000.

[11] P. Williams, «What Does Security Culture Look Like For Small Organizations?,» σε *7th Australian Information Security Management Conference*, Perth, Western Australia, 2009.

[12] Business and Advisory Committee to the OECD, Securing your business. An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems:Towards a culture of security, International Chamber of Commerce: OECD, 2004.

[13] L. Smircich, «Concepts of culture and organizational analysis,» *Administrative,* τόμ. 28, αρ. 3, pp. 339-358, 1983.

[14] W. G. Ouchi και A. L. Wilkins, «Organizational culture,» *Annual Review of Sociology,* τόμ. 11, pp. 457-483, 1985.

[15] K. S. Cameron και R. E. Quinn, Diagnosing and changing organizational culture: Based on the competing values framework, John Wiley & Sons, 2011.

[16] A. S. Tsui, Z.-X. Zhang, H. Wang, K. R. Xin και J. B. Wu, «Unpacking the relationship between CEO leadership behavior and organizational culture,» *The Leadership Quarterly,* τόμ. 17, αρ. 2, p. 113–137, 2006.

[17] K. Scarfone, M. Souppaya, A. Cody και A. Orebaugh, «Technical Guide to Information Security Testing and Assessment,» Computer Security Resource Center, 2008.

[18] M. Mora, O. Gelman, A. Steenkamp και M. Raisinghani, Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems, IGI Global, 2012.

[19] S. Aurigemma και R. Panko, «A Composite Framework for Behavioral Compliance with Information Security Policies,» σε *45th Hawaii International Conference on Systems Sciences*, 2012.

[20] B. Lebek, J. Uffen, M. Neumann, B. Hohler και M. H. Breitner, «Information security awareness and behavior: a theory-based literature review,» *Management Research Review,* τόμ. 37, αρ. 12, pp. 1049-1092, 2014.

[21] M. Siponen, S. Pahnila και A. Mahmood, «Employees' Adherence to Information Security Policies: An Empirical Study,» *Privacy and Trust in Complex Environments,* pp. 133-144, 2007.

[22] S. Pahnila, M. Siponen και A. Mahmood, «Employees' Behavior towards IS Security Policy Compliance,» σε *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, Waikoloa, 2007.

[23] M. Workman, W. H. Bommer και D. Straub, «Security lapses and the omission of information security measures: A threat control model and empirical test,» *Computers in Human Behavior,* τόμ. 24, αρ. 6, pp. 2799-2816, 2008.

[24] B.-Y. Ng, A. Kankanhalli και Y. (. Xu, «Studying users' computer security behavior: A health belief perspective,» *Decision Support Systems,* τόμ. 46, αρ. 4, pp. 815-825, 2009.

[25] H.-S. Rhee, C.-T. Kim και Y. U. Ryu, «Self-efficacy in information security: Its influence on end users' information security practice behavior,» *Computers & Security,* τόμ. 28, αρ. 8, pp. 816-826, 2009.

[26] M. Limayem και S. G. Hirt, «Force of habit and information systems usage: Theory and initial validation.,» *Journal of the Association for Information Systems,* τόμ. 4, pp. 65-97, 2003.

[27] K. F. McCrohan, K. Engel και J. W. Harvey, «Influence of Awareness and Training on Cyber Security,» *Journal of Internet Commerce,* τόμ. 9, αρ. 1, pp. 23-41, 2010.

[28] Q. Hu, T. Dinev, P. Hart και D. Cooke, «Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture,» *Decision Sciences,* τόμ. 43, αρ. 4, August 2012.

[29] R. E.Crossler, A. C.Johnston, P. B. Lowry, Q. Hu, M. Warkentin και R. Baskerville, «Future directions for behavioral information security research,» *Computers & Security,* τόμ. 32, pp. 90-101, 2013.

[30] Z. A. Soomro, M. H. Shah και J. Ahmed, «Information security management needs more holistic approach: A literature review,» *International Journal of Information Management,* τόμ. 36, αρ. 2, pp. 215-225, 2016.

[31] ISO/IEC, «ISO/IEC 27002:2013(E) Information technology — Security techniques — Code of practice for information security controls,» International Organization for Standardization (ISO), 2013.

[32] ISO/IEC, «ISO/IEC 27001. Information security management.,» International Organization for Standardization (ISO), 2015.

[33] Information Systems Audit and Control Association (ISACA), «COBIT5: A Business Framework for the Governance and Management of Enterprise IT,» 2012.

[34] J. H. Eloff και M. Eloff, «Information Security Architecture,» *Computer Fraud,* τόμ. 2005, αρ. 11, pp. 10-16, 2005.

[35] Joint Task Force Transformation Initiative, «SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations,» National Institute of Standards and Technology, 2013.

[36] European Union Agency for Cybersecurity (ENISA), «Cyber Security Culture in Organisations,» European Union Agency for Cybersecurity (ENISA), 2017.

[37] G. Petric και K. Roer, «To measure security culture: A scientific approach,» CLTRe North America, Inc., 2018.

[38] K. Bounas, A. Georgiadou, M. Kontoulis, S. Mouzakitis και D. Askounis, «Towards a CyberSecurity Culture Tool Though a Holistic, Multi-Dimensional Assessment Framework,» σε *13 th IADIS International Conference Information Systems 2020*, Sofia, 2020.

[39] S. Hacks, «Future of Cyber Security in Electrical Power and Energy Systems,» EnergyShield, 2020.

[40] «EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks,» CyberWatching, 2020.

[41] O. Bularca, «Trends, opportunities and choices in designing cyber resilient EPES infrastructure,» EnergyShield, 2021.

[42] «Energy Shield,» Energy Shield, 2019. [Ηλεκτρονικό]. Available: https://energy-shield.eu/. [Πρόσβαση 25 03 2020].

[43] A. Georgiadou, S. Mouzakitis, K. Bounas και D. Askounis, «A Cyber-Security Culture Framework for Assessing Organization Readiness,» *Journal of Computer Information Systems,* 2020.

[44] CIS, «CIS Controls,» Center for Internet Security, Inc., 2019.

[45] All Hazards Consortium (AHC), «Cyber Security Risk Mitigation Checklist,» [Ηλεκτρονικό]. Available: https://www.ahcusa.org/uploads/2/1/9/8/21985670/cybersecurityriskmitigationchecklist.pdf. [Πρόσβαση 7 10 2019].

[46] Utah Governement, «Cyber Security Controls Checklist».

[47] «Cybersecurity Checklist Series,» JMARK Business Solutions.

[48] ENISA, «The new users' guide: How to raise information security awareness,» 2010. [Ηλεκτρονικό]. Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide. [Πρόσβαση 24 10 2019].

[49] I. Bernik και K. Prislan, «Measuring information security performance with 10 by 10 model for holistic state evaluation,» 21 September 2016.

[50] j. Leach, «Improving user security behaviour,» *Computers & Security,* τόμ. 22, αρ. 8, pp. 685-692, 2003.

[51] S. Furnell και A. Rajendran, «Understanding the influences on information security behaviour,» *Computer Fraud & Security,* τόμ. 2012, αρ. 3, pp. 12-15, 2012.

[52] K. Padayachee, «Taxonomy of compliant information security behavior,» *Computers & Security,* τόμ. 31, αρ. 5, p. 673–680, 2012.

[53] S. M. S. C. A.B.Ruighaver, «Organisational security culture: Extending the end-user perspective,» *Computers & Security,* τόμ. 26, αρ. 1, pp. 56-62, 2007.

[54] M. Alshaikh, A. Ahmad, S. B. Maynard και S. Chang, «Towards a Taxonomy of Information Security Management Practices in Organisations,» σε *Proceedings of the 25th Australasian Conference on Information Systems*, Auckland, 2014.

[55] P. Chia, S. Maynard και A. Ruighaver, «Understanding Organizational Security Culture,» σε *Sixth Pacific Asia Conference on Information Systems*, Tokyo, 2002.

[56] L. Ngo, W. Zhou και M. Warren, «Understanding Transition towards Information Security Culture Change,» σε *Proceedings of the 3rd Australian Information Security Management Conference*, Perth, 2005.

[57] C. Vroom και R. Von Solms, «Towards information security behavioural compliance,» *Computers & Security,* τόμ. 23, αρ. 3, pp. 191-198, 2004.

[58] J. Andress και M. Leary, Building a Practical Information Security Program, Syngress, 2016.

[59] RiskWatch, «Cyber Security Assessment Checklist,» Risk Management Software Solutions.

[60] ITU, «Global Cybersecurity Index,» [Ηλεκτρονικό]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. [Πρόσβαση 2 October 2019].

[61] L. Hayden, People-Centric Security: Transforming Your Enterprise Security Culture, McGraw-Hill, 2015.

[62] A. Da Veiga και J. Eloff, «A framework and assessment instrument for information security culture,» *Computers & Security,* τόμ. 29, αρ. 2, pp. 196-207, 2010.

[63] A. Munteanu και D. Fotache, «Enablers of Information Security Culture,» *Procedia Economics & Finance,* τόμ. 20, pp. 414-422, 2015.

[64] K. M. R. M. T. B. T. Knapp, «Information security policy: an organisational-level process model,» *Computers & Security,* τόμ. 28, αρ. 7, pp. 493-508, 2009.

[65] K. v. S. R. L. L. Thomson, «Cultivating an organizational information security culture,» *Computer Fraud & Security,* τόμ. 2006, αρ. 10, pp. 7-11, 2006.

[66] R. Von Solms και B. Von Solms, «From policies to culture,» *Computers & Security,* τόμ. 23, αρ. 4, pp. 275-279, 2004.

[67] CISCO, «Measuring and Evaluating an Effective Security Culture,» Cisco Systems, Inc. , 2007.

[68] A. Da Veiga και N. Martins, «Improving the information security culture through monitoring and implementation actions illustrated through a case study,» *Computers & Security,* τόμ. 49, pp. 162-176, 2015.

[69] j. Lim, A. Ahmad, S. Chang και S. Maynard, «Embedding Information Security Culture Emerging Concerns and Challenges,» σε *Pacific Asia Conference on Information Systems*, Taipei, 2010.

[70] J. Lim, S. Chang, A. Ahmad και S. Maynard, «Towards an Organizational Culture Framework for Information Security Practices,» σε *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions*, M. Gupta, J. Walp και R. Sharman, Επιμ., IGI Global, 2012, pp. 296-315.

[71] N. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. Ghani και T. Herawan, «Information security conscious care behaviour formation in organizations,» *Computers & Security,* τόμ. 53, pp. 65-78, 2015.

[72] T. Herath και H. Rao, «Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,» *Decision Support Systems,* τόμ. 47, αρ. 2, pp. 154-165, 2009.

[73] A. Laycock, G. Petric και K. Roer, «The seven dimensions of security culture,» 2019.

[74] CPNI (Centre for the Protection of National Infrastructure), «Introduction to SeCuRE 4,» 2018.

[75] «Employee Survey Questions,» [Ηλεκτρονικό]. Available: https://hr-survey.com/EmployeeSurveyQuestions.htm. [Πρόσβαση 11 10 2019].

[76] S. Faily, S. Furnell και I. Flechais, «Designing and aligning e-Science security culture with design,» *Information Management & Computer Security,* τόμ. 18, αρ. 5, pp. 339-349, 2010.

[77] T. Halevi, N. Memon, J. Lewis, P. Kumaraguru, S. Arora, N. Dagar, F. Aloul και J. Chen, «Cultural and Psychological Factors in Cyber-Security,» σε *18th International Conference on Information Integration and Web-based Applications and Services*, 2016.

[78] A. Wiley, A. McCormac και D. Calic, «More than the individual: Examining the relationship between culture and Information Security Awareness,» *Computers & Security,* τόμ. 88, 2020.

[79] J. Van Niekerk και R. Von Solms, «A holistic framework for the fostering of an information security sub-culture in organizations,» σε *ISSA 2005 New Knowledge Today Conference*, Sandton, 2005.

[80] A. Da Veiga και N. Martins, «Defining and identifying dominant information security cultures and subcultures,» *Computers & Security,* τόμ. 2017, pp. 72-94, 2017.

[81] A. Da Veiga και N. Martins, «Information Security Culture: A Comparative Analysis of Four Assessments,» σε *Proceedings of the 8th European Conference on Information Management and Evaluation, ECIME 2014*, Ghent, 2014.

[82] A. Da Veiga, «Comparing the information security culture of employees who had read the information security policy and those who had not,» *Information and Computer Security,* τόμ. 24, αρ. 2, pp. 139-151, 2016.

[83] CPNI (Centre for the Protection of National Infrastructure), «Introduction to Security,» 2015.

[84] SANS, «Level-Up Test,» SANS, [Ηλεκτρονικό]. Available: https://www.sans.org/level-up/test.html.

[85] J. Abawajy, «User preference of cyber security awareness delivery methods,» *Behaviour & Information Technology,* τόμ. 33, αρ. 3, pp. 237-248, 2014.

[86] G. Bajaj, R. Agarwal, P. Singh, N. Georgantas και V. Issarny, «4W1H in IoT Semantics,» *IEEE Access,* τόμ. 6, pp. 65488-65506, 2018.

[87] R. S. Ronald , «Recommended Security Controls for Federal Information Systems and Organizations,» Special Publication (NIST SP) - 800-53 Rev 3, 2009.

[88] R. C. Brackney και R. H. Anderson, «Understanding the Insider Threat: Proceedings of a March 2004 Workshop,» RAND Corporation, Santa Monica, 2004.

[89] M. Bishop, «Position: "insider" is relative,» σε *Proceedings of the 2005 Workshop on New Security Paradigms*, Lake Arrowhead, California, 2005.

[90] F. L. Greitzer, A. P. Moore, D. M. Cappelli, D. H. Andrews, L. A. Carroll και T. D. Hull, «Combating the Insider Cyber Threat.,» *IEEE Security & Privacy,* τόμ. 6, αρ. 1, pp. 61-64, 2008.

[91] J. Hunker και C. W. Probst, «Insiders and Insider Threats - An Overview of Definitions and Mitigation Techniques,» *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* τόμ. 2, αρ. 1, pp. 4-27, 2011.

[92] M. Theis, R. F. Trzeciak, D. L. Costa, A. P. Moore, S. Miller, T. Cassidy και W. R. Claycomb, «Common Sense Guide to Mitigating Insider Threats, Sixth Edition,» Carnegie Mellon University, Pittsburgh, 2020.

[93] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici και M. Ochoa, «Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures.,» *ACM Computing Surveys,* τόμ. 52, αρ. 2, 2019.

[94] J. P. Anderson, Computer security threat monitoring and surveillance, Fort Washington: James P Anderson Company, 1980.

[95] M. B. Salem, S. Hershkop και S. J. Stolfo, «A Survey of Insider Attack Detection Research,» σε *Insider Attack and Cyber Security*, New York, Springer US, 2008, pp. 69-90.

[96] E. Cole και S. Ring, Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft., Syngress, 2005.

[97] G. Magklaras και S. Furnell, «Insider threat prediction tool: Evaluating the probability of IT misuse.,» *Computers & Security,* τόμ. 21, αρ. 1, pp. 62-73, 2002.

[98] A. H. Phyo και S. Furnell, «A detection-oriented classification of insider it misuse.,» σε *Third Security Conference*, 2004.

[99] D. Cappelli, A. Moore και R. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Boston: Addison-Wesley Professional, 2012.

[100] A. Kim, J. Oh, J. Ryu και K. Lee, «A Review of Insider Threat Detection Approaches With IoT Perspective,» *IEEE Access,* τόμ. 8, pp. 78847-78867, 2020.

[101] F. L. Greitzer, «Insider Threats: It's the HUMAN, Stupid!,» σε *Proceedings of the Northwest Cybersecurity Symposium*, Richland WA USA, 2019.

[102] M. Maasberg και N. L. Beebe, «The Enemy Within the Insider: Detecting the Insider Threat.,» *Journal of Information Privacy and Security,* τόμ. 10, αρ. 2, pp. 59-70, 2014.

[103] A. Kim, J. Oh, J. Ryu και K. Lee, «A Review of Insider Threat Detection Approaches.,» *IEEE Access,* τόμ. 8, pp. 78847-78867, 2020.

[104] F. L. Greitzer και D. A. Frincke, «Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation,» σε *Insider Threats in Cyber Security*, τόμ. 49, Boston, Springer, 2010, pp. 85-113.

[105] J. Ophoff, A. Jensen, J. Sanderson-Smith, M. Porter και K. Johnston, «A Descriptive Literature Review and Classification of Insider Threat Research,» σε *Proceedings of Informing Science & IT Education Conference (InSITE) 2014*, Wollongong, 2014.

[106] T. O. Oladimeji, C. K. Ayo και S. Adewumi, «Review on Insider Threat Detection Techniques,» *Journal of Physics: Conference Series,* τόμ. 1299, 2019.

[107] D. Cappelli, A. P. Moore, M. R. Randazzo, M. Keeney και E. Kowalski, «Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,» Software Engineering Institute, Pittsburgh, 2004.

[108] T. Conway, S. Keverline, M. Keeney, E. Kowalski, M. Williams, D. Cappelli, A. P. Moore, S. Rogers και T. J. Shimeall, «Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors,» Software Engineering Institute, Pittsburgh, 2005.

[109] A. Cummings, T. Lewellen, D. McIntire, A. P. Moore και R. F. Trzeciak, «Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,» Software Engineering Institute, Pittsburgh, 2012.

[110] D. M. Cappelli, A. G. Desai, A. P. Moore, T. J. Shimeall, E. A. Weaver και B. J. Willke, «Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage,» CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2008.

[111] M. A.P., C. D.M. και T. R.F., «The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures.,» σε *Insider Attack and Cyber Security.*, τόμ. 39, Boston, Springer, 2008.

[112] D. Andersen, D. Cappelli, J. Gonzalez, M. Mojtahedzadeh, A. Moore, E. Rich, J. Sarriegui, T. Shimeall, J. Stanton, E. Weaver και A. Zagonel, «Preliminary system dynamics maps of the insider cyber-threat problem.,» σε *Proceedings of the 22nd International Conference of the System dynamics Society*, 2004.

[113] W. R. Claycomb, C. L. Huth, L. Flynn, D. M. McIntire και T. B. Lewellen, «Chronological Examination of Insider Threat Sabotage: Preliminary Observations,» *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* τόμ. 3, αρ. 4, pp. 4-20, 2012.

[114] D. L. Costa, M. L. Collins, S. J. Perl, M. J. Albrethsen, G. J. Silowash και D. L. Spooner, «An Ontology for Insider Threat Indicators Development and Applications,» CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2014.

[115] F. L. Greitzer, J. Purl, Y. M. Leong και P. J. Sticha, «Positioning your organization to respond to insider threats.,» *IEEE Engineering Management Review,* τόμ. 47, αρ. 2, pp. 75-83, 2019.

[116] A. P. Moore, D. Cappelli, T. C. Caron, E. D. Shaw, D. Spooner και R. F. Trzeciak, «A Preliminary Model of Insider Theft of Intellectual Property.,» Software Engineering Institute, Pittsburgh, 2011.

[117] A. P. Moore, D. Cappelli, T. C. Caron, E. D. Shaw και R. F. Trzeciak, «Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model,» Software Engineering Institute, Pittsburgh, 2009.

[118] CERT Insider Threat Team, «Unintentional Insider Threats: A Foundational Study,» Software Engineering Insitute, Pittsburgh, 2013.

[119] D. Cappelli, A. Moore, R. Trzeciak και T. J. Shimeall, «Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1,» Software Engineering Institute, Pittsburgh, 2008.

[120] S. R. Band, D. Cappelli, L. F. Fischer, A. P. Moore, E. D. Shaw και R. F. Trzeciak, «Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis,» Software Engineering Institute, Pittsburgh, 2006.

[121] D. Cappelli, A. G. Desai, A. P. Moore, T. J. Shimeall, E. A. Weaver και B. J. Willke, «Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers Information, Systems, or Networks,» Software Engineering Institute, Pittsburgh, 2007.

[122] P. Legg, N. Moffat, J. R. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith και S. Creese, «Towards a conceptual model and reasoning structure for insider threat detection.,» *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* τόμ. 4, αρ. 4, pp. 20-37, 2013.

[123] M. Hanley, «Deriving Candidate Technical Controls and Indicators of Insider Attack from Socio-Technical Models and Data,» Software Engineering Institute, Pittsburgh, 2011.

[124] E. D. Shaw και H. V. Stock, «Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall,» Symantec, California.

[125] M. Hanley, T. Dean, W. Schroeder, M. Houy, R. F. Trzeciak και J. Montelibano, «An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases,» Software Engineering Institute, Pittsburgh, 2011.

[126] K. A. Kennedy, «Management and Mitigation of Insider Threats,» σε *Handbook of Behavioral Criminology*, Cham, Springer, 2017, pp. 485-499.

[127] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore και D. Mundie, «Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation,» σε *47th Hawaii International Conference on System Sciences*, Waikoloa, 2014.

[128] L. Hadlington, «The "Human Factor" in Cybersecurity: Exploring the Accidental Insider,» σε *Psychological and Behavioral Examinations in Cyber Security*, Pennsylvania, IGI Global, 2018, pp. 46-63.

[129] F. L. Greitzer, L. J. Kangas, C. Noonan και A. Dalton, «Identifying at-risk employees: A behavioral model for predicting potential insider threats,» Pacific Northwest National Lab, Richland, 2010.

[130] F. Greitzer, J. Purl, Y. M. Leong και D. S. Becker, «SOFIT: Sociotechnical and Organizational Factors for Insider Threat,» σε *2018 IEEE Security and Privacy Workshops (SPW)*, San Francisco, 2018.

[131] E. Shaw και L. F. Fischer, «Ten tales of betrayal: The threat to corporate infrastructure by information technology.,» Defense Personnel Security Research Center, Monterey, California, 2005.

[132] B. Marcus και H. Schuler, «Antecedents of Counterproductive Behavior at Work: A General Perspective.,» *Journal of Applied Psychology,* τόμ. 89, αρ. 4, p. 647–660, 2004.

[133] M. J. Martinko, M. J. Gundlach και S. C. Douglas, «Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective.,» *International Journal of Selection and Assessment,* τόμ. 10, αρ. 1-2, p. 36–50, 2002.

[134] A. Georgiadou, S. Mouzakitis και D. Askounis, «Detecting Insider Threat via a Cyber-Security Culture Framework,» *Journal of Computer Information Systems,* 2021.

[135] A.-R. Blais και E. U. Weber, «A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations,» *Judgment and Decision Making,* τόμ. 1, αρ. 1, p. 33–47, 2006.

[136] S. G. Scott και R. A. Bruce, «Decision-Making Style: The Development and Assessment of a New Measure,» *Educational and Psychological Measurement,* τόμ. 5, αρ. 5, pp. 818-831, 1995.

[137] A. Strathman, F. Gleicher, D. S. Boninger και S. Edwards, «The Consideration of Future Consequences: Weighing Immediate and Distant Outcomes of Behavior,» *Journal of Personality and Social Psychology,* τόμ. 66, αρ. 4, pp. 742-752, 1994.

[138] J. H. Patton, M. S. Stanford και E. S. B. PhD., «Factor structure of the Barratt impulsiveness scale,» *Journal of Clinical Psychology,* τόμ. 51, αρ. 6, pp. 768-774, 1995.

[139] J. T. Cacioppo και R. E. Petty, «The Need for Cognition,» *Journal of Personality and Social Psychology,* τόμ. 42, αρ. 1, pp. 116-131, 1982.

[140] S. Egelman και E. Peer, «Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS),» σε *33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul Republic of Korea, 2015.

[141] B. Strom, «ATT&CK 101,» Medium, 03 05 2018. [Ηλεκτρονικό]. Available: https://medium.com/mitre-attack/att-ck-101-17074d3bc62. [Πρόσβαση 03 01 2021].

[142] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington και C. B. Thomas, «MITRE ATT&CK®: Design and Philosophy,» The MITRE Corporation, 2018.

[143] B. E. Strom, J. A. Battaglia, M. S. Kemmerer, W. Kupersanin, D. P. Miller, C. Wampler, S. M. Whitley και R. D. Wolf, «Finding Cyber Threats with ATT&CK™ - Based Analytics,» The MITRE Corporation, 2017.

[144] The MITRE Corporation, «MITRE ATT&CK®,» The MITRE Corporation, 07 2016. [Ηλεκτρονικό]. Available: https://attack.mitre.org/. [Πρόσβαση 03 01 2021].

[145] R. Al-Shaer, J. M. Spring και E. Christou, «Learning the Associations of MITRE ATT&CK Adversarial Techniques,» σε *2020 IEEE Conference on Communications and Network Security (CNS)*, Avignon, 2020.

[146] S. Caimi, «MITRE ATT&CK: The Magic of Mitigations,» Cisco, 19 08 2020. [Ηλεκτρονικό]. Available: https://cscoblogs-prod-17bj.appspot.com/security/mitre-attck-the-magic-of-mitigations. [Πρόσβαση 03 01 2021].

[147] K. Esbeck και B. Strom, «Integrating PRE-ATT&CK Techniques into ATT&CK,» The MITRE Corporation, 13 04 2013. [Ηλεκτρονικό]. Available: https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/integrating-pre-attck-techniques-into-attck. [Πρόσβαση 03 01 2021].

[148] The MITRE Corporation, «ATT&CK® for Industrial Control Systems,» MediaWiki, 03 06 2020. [Ηλεκτρονικό]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page. [Πρόσβαση 03 01 2021].

[149] O. Alexander, M. Belisle και J. Steele, «MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy,» The MITRE Corporation, 2020.

[150] Claroty, «The Global State of Industrial Cybersecurity,» Claroty, 2020.

[151] D. K. Zafra, K. Lunden, O. Alexander, N. Brubaker και G. Agboruche, «In Pursuit of a Gestalt Visualization: Merging MITRE ATT&CK® for Enterprise and ICS to Communicate Adversary Behaviors,» FireEye, Inc., 29 09 2020. [Ηλεκτρονικό]. Available: https://www.fireeye.com/blog/executive-

perspective/2020/09/merging-mitre-attack-for-enterprise-and-ics-to-communicate-adversary-behaviors.html. [Πρόσβαση 04 01 2021].

[152] MITRE Corporation, «Mitigations - Enterprise | MITRE ATT&CK,» MITRE Corporation, [Ηλεκτρονικό]. Available: https://attack.mitre.org/mitigations/enterprise/. [Πρόσβαση 27 04 2021].

[153] MITRE Corporation, «Mitigations - attackics,» MITRE Corporation, 05 10 2020. [Ηλεκτρονικό]. Available: https://collaborate.mitre.org/attackics/index.php/Mitigations. [Πρόσβαση 27 04 2021].

[154] A. Georgiadou, S. Mouzakitis και D. Askounis, «Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework,» *Sensors,* τόμ. 21, αρ. 9, p. 3267, 2021.

[155] T. P. Velavan και C. G. Meyer, «The COVID-19 epidemic,» *Tropical Medicine and International Health,* τόμ. 25, αρ. 3, p. 278–280, 2020.

[156] D. S. Hui, E. I. Azhar, T. A. Madani, F. Ntoumi, R. Kock, O. Dar, G. Ippolito, T. D. Mchugh, Z. A. Memish, C. Drosten, A. Zumla και E. Petersen, «The continuing 2019-nCoV epidemic threat of novel coronaviruses to global health — The latest 2019 novel coronavirus outbreak in Wuhan, China,» *International Journal of Infectious Diseases,* τόμ. 91, pp. 264-266, 2020.

[157] «WHO Director-General's opening remarks at the media briefing on COVID-19,» World Health Organization (WHO), 2020.

[158] «ILO Monitor:COVID-19 and the world of work. Second edition,» International Labour Organization (ILO), 2020.

[159] Reason Cybersecurity, «COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report,» ReasonLabs, 09 03 2020. [Ηλεκτρονικό]. Available: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/. [Πρόσβαση 26 01 2022].

[160] «Coronavirus-related fraud reports increase by 400% in March,» ActionFraud - National Fraud and Cyber Crime Reporting Center, 20 03 2020. [Ηλεκτρονικό]. Available: https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march. [Πρόσβαση 16 04 2020].

[161] «Coronavirus scam costs victims over £800k in one month,» ActionFraud - National Fraud and Cyber Crime Reporting Center, 03 06 2020. [Ηλεκτρονικό]. Available: https://www.actionfraud.police.uk/alert/coronavirus-scam-costs-victims-over-800k-in-one-month. [Πρόσβαση 16 04 2020].

[162] «Pandemic profiteering: how criminals exploit the COVID-19 crisis,» Europol, 2020.

[163] Europol, «Internet Organised Crime Threat Assessment 2020,» European Union Agency for Law Enforcement Cooperation, 2020.

[164] Interpol, «INTERPOL warns of financial fraud linked to COVID-19,» Lyon, 2020.

[165] ENISA, «ENISA Threat Landscape 2020 - Phishing,» ENISA, 2020.

[166] A. Georgiadou, S. Mouzakitis και D. Askounis, «Towards Assessing Critical Infrastructures' Cyber-security Culture During COVID-19 Crisis: A Tailor-Made Survey,» *σε 4th International Conference on Networks and Security (NSEC 2020)*, Sydney, 2020.

[167] A. Georgiadou, S. Mouzakitis και D. Askounis, «Designing a Cyber-security Culture Assessment Survey Targeting Critical Infrastructures During Covid-19 Crisis,» *International Journal of Network Security & Its Applications (IJNSA),* τόμ. 13, αρ. 1, pp. 33-50, 2020.

[168] A. Georgiadou και S. Mouzakitis, «Working from home during COVID-19 crisis,» Athens, 2020.

[169] A. Georgiadou, S. Mouzakitis και D. Askounis, «Working from home during COVID-19 crisis – A Cyber-Security Culture Assessment Survey,» Mendeley Data, Athens, 2020.

[170] J. R. Draugalis, S. J. Coons και C. M. Plaza, «Best Practices for Survey Research Reports: A Synopsis for Authors and Reviewers,» *American Journal of Pharmaceutical Education,* τόμ. 72, αρ. 1, 2008.

[171] G. B. Willis, Cognitive interviewing: A tool for improving questionnaire design., Sage publications, 2004.

[172] F. J. Fowler Jr και F. J. Fowler., Improving survey questions: Design and evaluation., Sage, 1995.

[173] A. Georgiadou, S. Mouzakitis και D. Askounis, «Working from home during COVID-19 crisis: a cyber security culture assessment survey,» *Security Journal,* 2021.

[174] «COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report,» Reason Labs, 09 03 2020. [Ηλεκτρονικό]. Available: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/. [Πρόσβαση 16 04 2020].

[175] «Home working: preparing your organisation and staff,» National Cyber Security Centre, 17 03 2020. [Ηλεκτρονικό]. Available: https://www.ncsc.gov.uk/guidance/home-working. [Πρόσβαση 17 04 2020].

[176] «Working From Home - COVID19 - ENISA,» ENISA - European Union Agency for Cybersecurity, [Ηλεκτρονικό]. Available: https://www.enisa.europa.eu/topics/WFH-COVID19?tab=details. [Πρόσβαση 17 04 2020].

[177] A. Sfakianakis, C. Douligeris, L. M. (ENISA), M. L. (ENISA) και O. Raghimi, «ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends,» European Union Agency for Network and Information Security (ENISA), Athens, 2019.

[178] The European Parliament and the Council of the European Union, «EUR-Lex-32016L1148 - EN - EUR-Lex,» 6 7 2016. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. [Πρόσβαση 26 3 2020].

[179] S. Gyles, «Cyberattacks Hit Hospitals and Health Departments Amid COVID-19 Coronavirus Pandemic,» vpnoverview, 2020.

[180] ERN Newsroom, «Coronavirus: Hospitals face cyber attack that could "destroy systems",» ERN News, 2020.

[181] S. Porter, «Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak,» Healthcare IT News, 19 03 2020. [Ηλεκτρονικό]. Available: https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak. [Πρόσβαση 26 01 2022].

[182] P. H. O. page, «A patient has died after ransomware hackers hit a German hospital,» MIT Technology Review, 2020.

[183] W. J. Gordon, A. Wright, R. Aiyagari, L. Corbo, R. J. Glynn, J. Kadakia, J. Kufahl, C. Mazzone, J. Noga, M. Parkulo, B. Sanford, P. Scheib και A. B. Landman, «Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions,» *JAMA Netw Open,* τόμ. 2, αρ. 3, p. e190393, 2019.

[184] S. Landolt, J. Hirsche, T. Schlienger, W. Businger και A. M. Zbinden, «Assessing and Comparing Information Se-curity in Swiss Hospitals,» *Interactive Journal of Medical Research,* τόμ. 1, αρ. 2, p. e11, 2012.

[185] M. S. Jalali, M. Bruckes, D. Westmattelmann και G. Schewe, «Why Employees (Still) Click on Phishing Links: Investigation in Hospitals,» *Journal of Medical Internet Research,* τόμ. 22, αρ. 1, p. e16775, 2020.

[186] L. Fabisiak και T. Hyla, «Measuring Cyber Security Awareness within Groups of Medical Professionals in Poland,» σε *53rd Hawaii International Conference on System Sciences*, Hawaii, 2020.

[187] T. Haukilehto και J. Hautamäki, «Survey of Cyber Security Awareness in Health, Social Services and Regional Government in South Ostrobothnia, Finland,» σε *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, 2019.

[188] M. Evans, Y. He, C. Luo, I. Yevseyeva, H. Janicke και L. A. Maglaras, «Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form,» *IEEE Access,* τόμ. 7, pp. 102087-102101, 2019.

[189] A. B. Shahri, I. Z. και N. Z. A. Rahim, «Security effectiveness in health information system: Through improving the human factors by education and training,» *Australian Journal of Basic and Applied Sciences,* τόμ. 6, αρ. 12, pp. 226-233, 2012.

[190] Ponemon Institute LLC, «The Human Factor in Data Protection,» Ponemon Institute LLC, 2012.

[191] SPHINX Project EU, «SPHINX Project EU,» SPHINX, [Ηλεκτρονικό]. Available: https://sphinx-project.eu/. [Πρόσβαση 19 06 2021].

[192] HIMSS, «HIMSS Healthcare Cybersecurity Survey,» HIMSS, 16 11 2020. [Ηλεκτρονικό]. Available: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey. [Πρόσβαση 22 06 2021].

[193] W. J. Gordon, A. Wright, R. J. Glynn, J. Kadakia, C. Mazzone, E. Leinbach και A. Landman, «Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system,» *Journal of the American Medical Informatics Association,* τόμ. 26, αρ. 6, p. 547–552, 2019.

[194] N. Akbar, «Analysing persuasion principles in phishing emails,» University of Twente, Enschede, 2014.

[195] J. Walter, «Threat Intel | Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic,» SentinelLABS, 04 09 2020. [Ηλεκτρονικό]. Available: https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/. [Πρόσβαση 22 06 2021].

[196] TREND Micro, «Emotet Uses Coronavirus Scare in Latest Campaign, Targets Japan,» TREND Micro, 31 01 2020. [Ηλεκτρονικό]. Available: https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/emotet-uses-coronavirus-scare-in-latest-campaign-targets-japan. [Πρόσβαση 22 06 2021].

[197] J. Davis, «COVID-19 Impact on Ransomware, Threats, Healthcare Cybersecurity,» Health IT Security, 04 08 2020. [Ηλεκτρονικό]. Available: https://healthitsecurity.com/news/covid-19-impact-on-ransomware-threats-healthcare-cybersecurity. [Πρόσβαση 22 06 2021].

[198] N. Kumaran και S. Lugani, «Protecting businesses against cyber threats during COVID-19 and beyond,» Google Cloud, 16 04 2020. [Ηλεκτρονικό]. Available: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond. [Πρόσβαση 22 06 2021].

[199] M. S. Jalali, M. Bruckes, D. Westmattelmann και G. Schewe, «Why Employees (Still) Click on Phishing Links: Investigation in Hospitals,» *Journal of Medical Internet Research,* τόμ. 22, αρ. 1, 2020.

[200] «ICT specialists in employment,» eurostat, 2021.

[201] F. Gioulekas, E. Stamatiadis, A. Tzikas, K. Gounaris, A. Georgiadou, A. Michalitsi-Psarrou, D. G., K. M., N. Y., M. S., C. R. και C. Ntanos, «A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures,» *MDPI Healthcare,* τόμ. 10, αρ. 2, p. 327, 2022.

[202] «Panhellenic Scientific Association for Health Informatics,» [Ηλεκτρονικό]. Available: https://www.hsshi.gr/. [Πρόσβαση 29 07 2021].

[203] A. Georgiadou, A. Michalitsi-Psarrou, F. Gioulekas, E. Stamatiadis, A. Tzikas, K. Gounaris, D. G., N. C., L. R. L. και A. D., «Hospital's Cybersecurity Culture during the COVID-19 Crisis,» *MDPI Healthcare,* τόμ. 9, αρ. 10, p. 1335, 2021.

[204] U.S. Department of Health and Human Services, «Health Insurance Portability and Accountability Act of 1996 | ASPE,» ASPE - Office of the Assistant Secretary for Planning and Evaluation, 20 08 1996. [Ηλεκτρονικό]. Available: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996. [Πρόσβαση 25 08 2021].

[205] ISO/IEC, «ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002,» ISO, 2016.

[206] «2019 HIMSS Cybersecurity survey,» Healthcare Information and Management Systems Society, 2019.

[207] European Union Agency for Network and Information Security (ENISA), «Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures,» European Union Agency for Network and Information Security (ENISA), Athens, 2016.

[208] M. A. Arain, R. Tarraf και A. Ahmad, «Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization,» *Journal of Multidisciplinary Healthcare,* τόμ. 12, pp. 73-81, 2019.

[209] N. Waly, R. Tassabehji και M. Kamala, «Improving Organisational Information Security Management: The Impact of Training and Awareness,» σε *14th International Conference on High Performance Computing and Communication*, 2012.

[210] A. Ghazvini και Z. Shukur, «Awareness Training Transfer and Information Security Content Development for Healthcare Industry,» *International Journal of Advanced Computer Science and Applications,* τόμ. 7, αρ. 5, 2016.

[211] ISO/IEC, «ISO/IEC 27005. Information technology — Security techniques — Information security risk management,» International Organization for Standardization (ISO), 2018.

[212] T. N. Jagatic, N. Johnson, M. Jakobsson και F. Menczer, «Social phishing,» *Communications of the ACM,* τόμ. 50, αρ. 10, pp. 94-100, 2007.

[213] M. J. A. Miranda, «Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach,» *International Management Review ,* τόμ. 14, αρ. 2, pp. 5-10, 2018.

[214] D. Jampen, G. Gür, T. Sutter και B. Tellenbach , «Don’t click: towards an effective anti-phishing training. A comparative literature review,» *Human-centric Computing and Information Sciences,* τόμ. 10, αρ. 33, 2020.

[215] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong και E. Nunge, «Protecting people from phishing: the design and evaluation of an embedded training email system,» σε *CHI '07: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, San Jose California USA, 2007.

[216] A. Georgiadou, A. Michalitsi-Psarrou και D. Askounis, «Evaluating The Cyber-Security Culture of the EPES Sector: Applying a Cyber-Security Culture Framework to assess the EPES Sector's resilience and readiness,» σε *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna, 2022.

[217] American Hospital Association, «Hospitals Implementing Cybersecurity Measures,» American Hospital Association, 2017.

[218] M. S. Jalali και J. P. Kaiser, «Cybersecurity in Hospitals: A Systematic, Organizational Perspective,» *Journal of Medical Internet Research,* τόμ. 20, αρ. 5, 2018.

[219] S. S. Tirumala, M. R. Valluri και G. Babu, «A survey on cybersecurity awareness concerns, practices and conceptual measures,» σε *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 2019.

[220] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg και E. Almomani, «A Survey of Phishing Email Filtering Techniques,» *IEEE Communications Surveys & Tutorials,* τόμ. 15, αρ. 4, pp. 2070-2090, 2013.

ΠΑΡΑΡΤΗΜΑ Ι: ΕΓΧΕΙΡΙΔΙΟ ΧΡΗΣΗΣ ΕΡΓΑΛΕΙΟΥ ΚΟΥΛΤΟΥΡΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

1. Cyber-Security Culture Framework

The **Security Behaviour Analysis** (SBA) tool has its foundations on the **Cyber-Security Culture Framework** which was developed in the context of the EnergyShield project. It was officially introduced in 2020, presenting an evaluation and assessment methodology of both individuals' and organisations' security culture readiness.

The specific framework is based on a combination of organisational and individual security factors structured into **dimensions** and **domains**. Its main goal is to examine organisational security policies and procedures in conjunction with employees' individual characteristics, behaviour, attitude, and skills. Each security metric introduced by the framework is assessed using a variety of evaluation techniques, such as surveys, tests, simulations, and serious games.

The assessment results are exploited in identifying cyber-security threats the organisation is vulnerable against. The framework has been correlated both with the hybrid **MITRE ATT&CK** Model for an OT Environment, consisting of a combination of the Enterprise and the ICS threat model, and with an enriched version of the Management and Education of the Risk of Insider Threat (**MERIT**) model, developed by the Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University.

Based on the evaluation results and identified threats, a number of targeted recommendations, awareness training programs, seminars and free online games are introduced to both the decision-makers of the organisation as well as the individual employees and contractors.

2. Main Concepts

Based on the Cyber-Security Culture Framework, there is a firm distinction among three different business user roles:

- ***Administrator*** (superuser privileges): usually a system administrator or security officer with full privileges over the security culture assessment life-cycle of the organisation and, therefore, of the SBA tool. They are responsible for user management, global groups and campaigns creation and management.
- ***Manager***: any user who acts as a leader of an employee group and is responsible for their security assessment, evaluation and training. They are granted manager privileges within the SBA tool, allowing them to create new users (practically inviting them to access the tool), groups, campaigns (accessible only to themselves apart from the administrators), and monitor their status and progress by obtaining a number of graphical reports.
- ***User***: simple user able to participate in campaigns or perform a number of self-assessment iterations in order to evaluate their security culture status and sharpen their information security knowledge, familiarity and awareness.

The corresponding roles have been implemented in the SBA tool, offering customisation and personalisation of the security assessment experience. Other important security concepts used within the tool are the following:

- ***Campaign***: a security culture assessment iteration designed by a manager targeting specific security domains and user groups or individuals. It has a certain duration (start and end date) and results in a number of assignments to the participating employees with a determined expiration. It provides a snapshot of the security culture status of a part of the organisation giving useful insights and feedback to decision-makers.
- ***Self-assessment***: an interactive way of self-evaluating your security awareness, compliance and readiness while improving your security knowledge and culture. Via multiple repetitions, it can also be considered as a means of self-training both to the security policies and procedures of the organisation and on the various information security threats and current reality.
- ***Threat***: a cyber-security threat originating from either external adversaries or insiders, meaning employees or contractors, that could potentially harm the organisation, wittingly or unwittingly.
- ***Recommendation***: a suggestion meant to define in detail the awareness training programs and seminars, along with their main goals and objectives, needed for the organisation to enhance and elevate its defence against identified cyber-security threats.

3. Structure

The SBA Tool is a web-based application. To access the tool services, the users need to initially sign in (Fig 1).

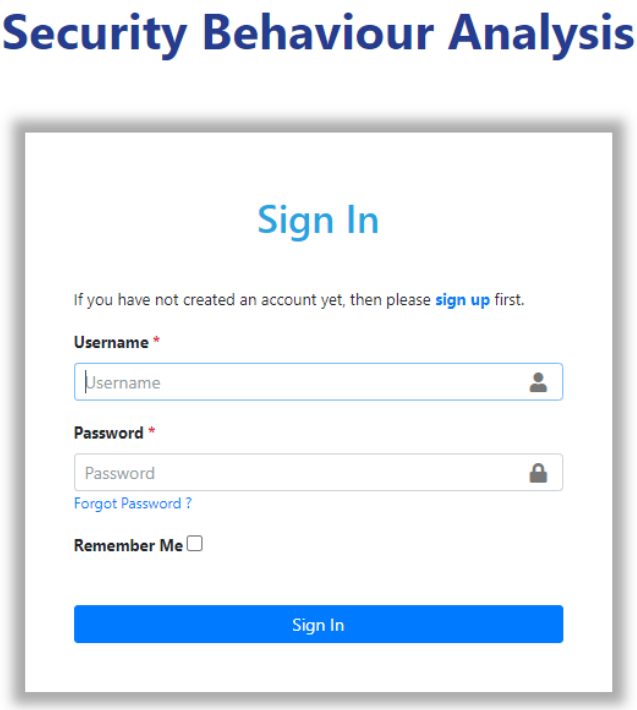


Fig 1. Sign-in view

Providing valid credentials leads the user to a personalised home page which differs depending on user role and privileges. The SBA tool console is divided into four (4) main parts (Fig 2):

- ***Header***: offers localisation possibilities via the "select language" menu, project contact information and a user submenu offering access to profile, change password and sign-out options.
- ***Sidebar***: offers access to different views of the tool (user role and privilege dependent).
- ***Footer***: contains project-related information and a connection to project's official website.
- ***Main panel***: is the main presentation part of the tool.

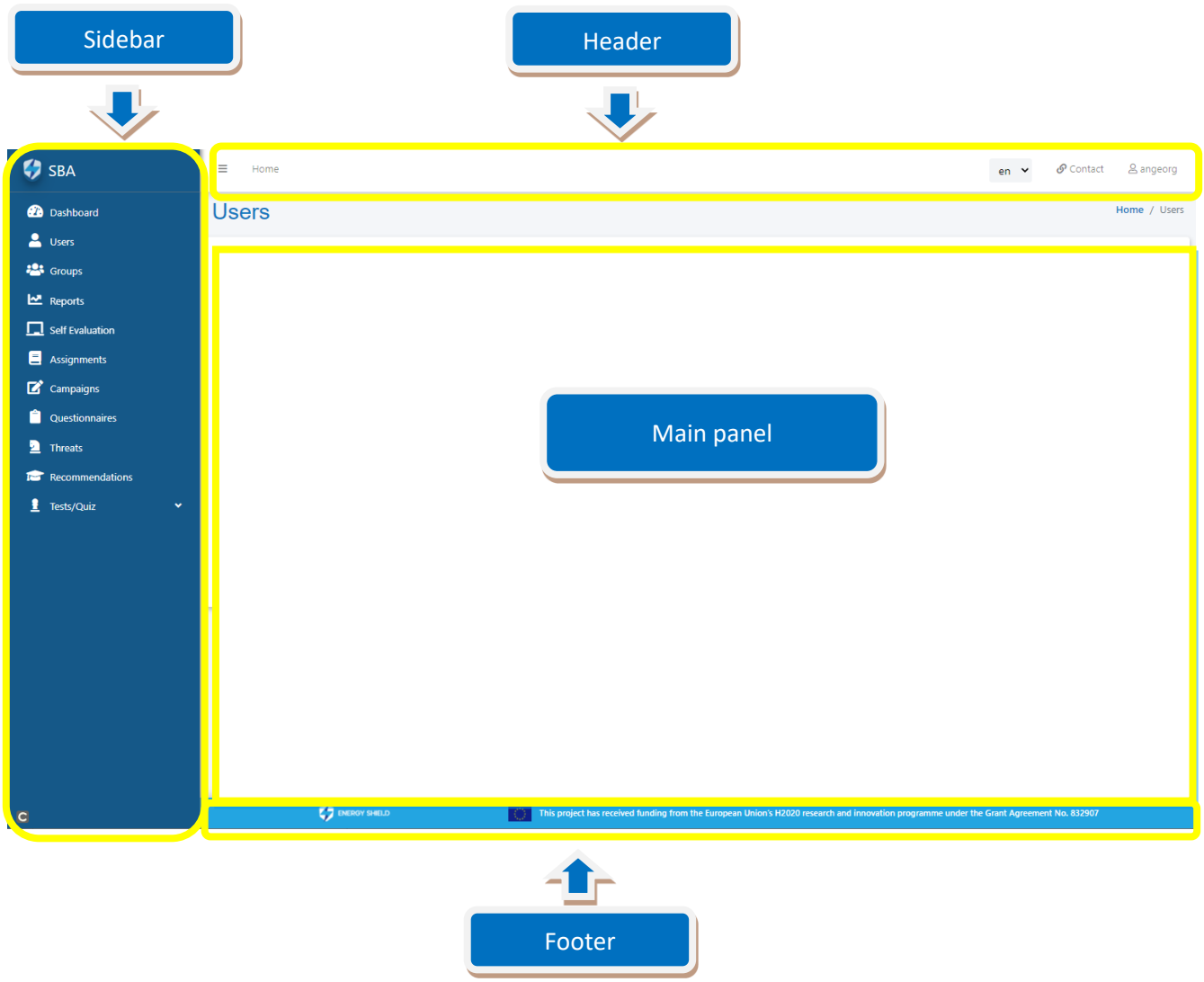


Fig 2. Console layout

Depending on user role and privileges, the sidebar offers a number of different options:

- ***Dashboard***: bears a different skeleton depending on user role, allowing an overall functionality view and control of the tool.

- ***Users*** (visible only to administrators and managers): listing the participating members of the tool along with a number of organisational info.
- ***Groups*** (visible only to administrators and managers): listing the groups of the tool serving different evaluation purposes.
- ***Reports***: visualisation of the security culture assessment results and status.
- ***Self Evaluation***: offering individuals the possibility to run a number of questionnaires and tests at their own pace.
- ***Assignments***: listing of all the assignments made to the logged-in user via the various campaigns addressed to them.
- ***Campaigns*** (visible only to administrators and managers): materialisation of a security culture evaluation iteration with direct assignments of specific questionnaires and tests to dedicated individuals or groups.
- ***Questionnaires*** (visible only to administrators and managers): listing of available questionnaires of the tool while correlating them to the security culture model.
- ***Threats*** (visible only to administrators and managers): displaying identified threats based on the organisation's current cyber-security culture assessment results.
- ***Recommendations***: this view differentiates based on the user roles and privileges. Simple users are presented with a listing of free online games for self-training, whereas administrators and managers are additionally presented with general and specific training recommendations targeting identified cyber-security weaknesses of the organisation.
- ***Tests/Quiz*** (visible only to administrators and managers): an interactive designing workspace, offering the possibility to create custom email phishing simulation and quiz templates, thus, making them available for customised evaluation tests.
- The following paragraphs present in detail each one of the above options of the tool while correlating it to its underlying cyber-security culture framework.

3.1. Dashboard

Having signed in, the user lands in the dashboard screen, which, depending on the user role and privileges, provides an overall preview of the SBA tool functionality (including pending assignments, cyber-security status graphs and tips, etc.) while offering quick access to targeted submenus, as exhibited in Fig 3.

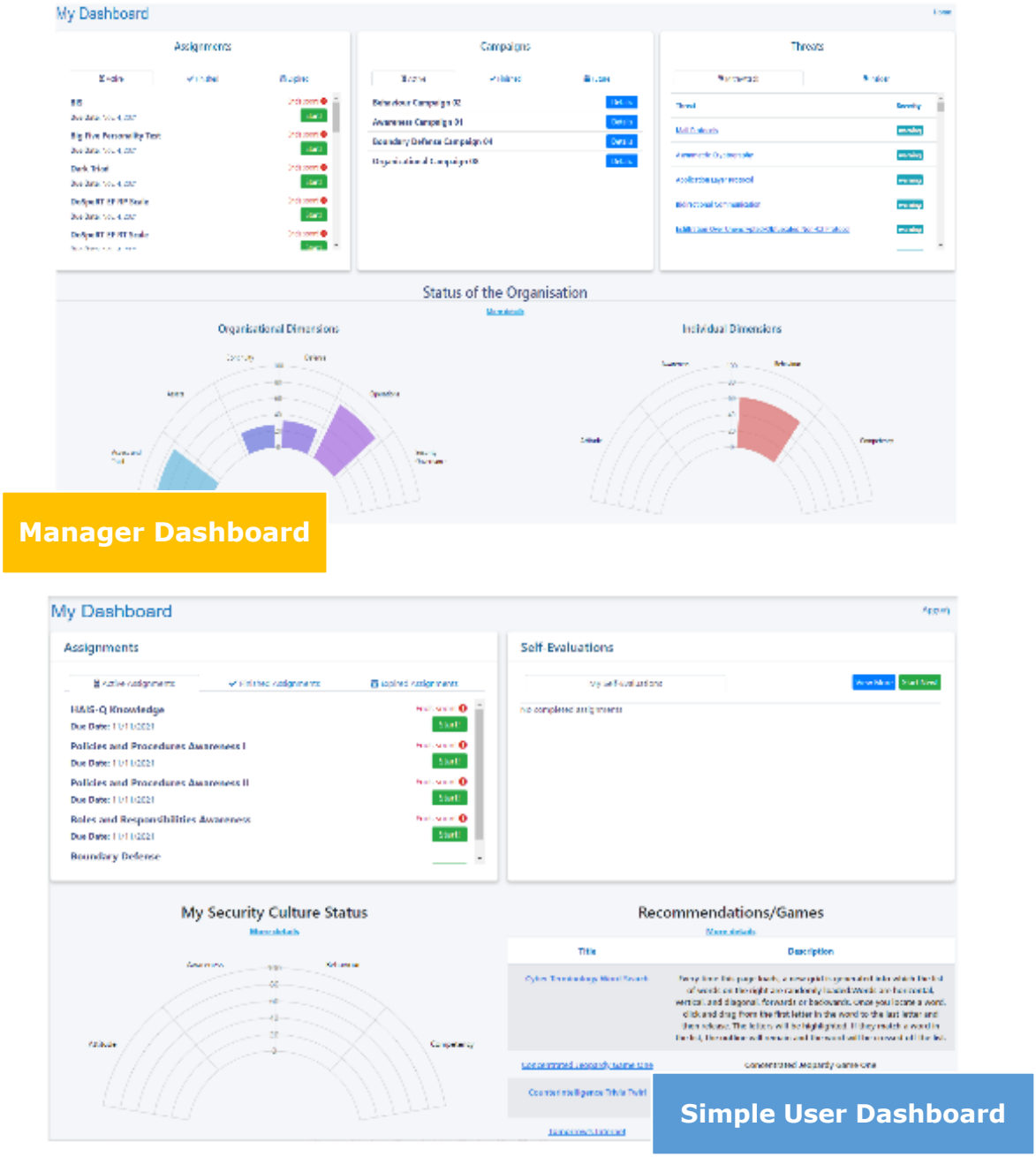


Fig 3. Dashboard view

3.2. Users

This view (visible only to administrators and managers) displays users' information in a responsive table offering searching and multiple column filtering capabilities, as presented in Fig 4. The toolbar present in the upper left part contains the following buttons:

- ***Add***: dropdown menu allowing creations of new user and group.
- ***Show/Hide columns***: control over column visibility.
- ***Copy***: copies selected table rows and columns to clipboard.

- ***Print***: prints selected table rows and columns while invoking the web browser print menu.
- ***Export to file***: dropdown menu allowing the export of the selected table rows and columns to different file formats (Excel, CSV and PDF).

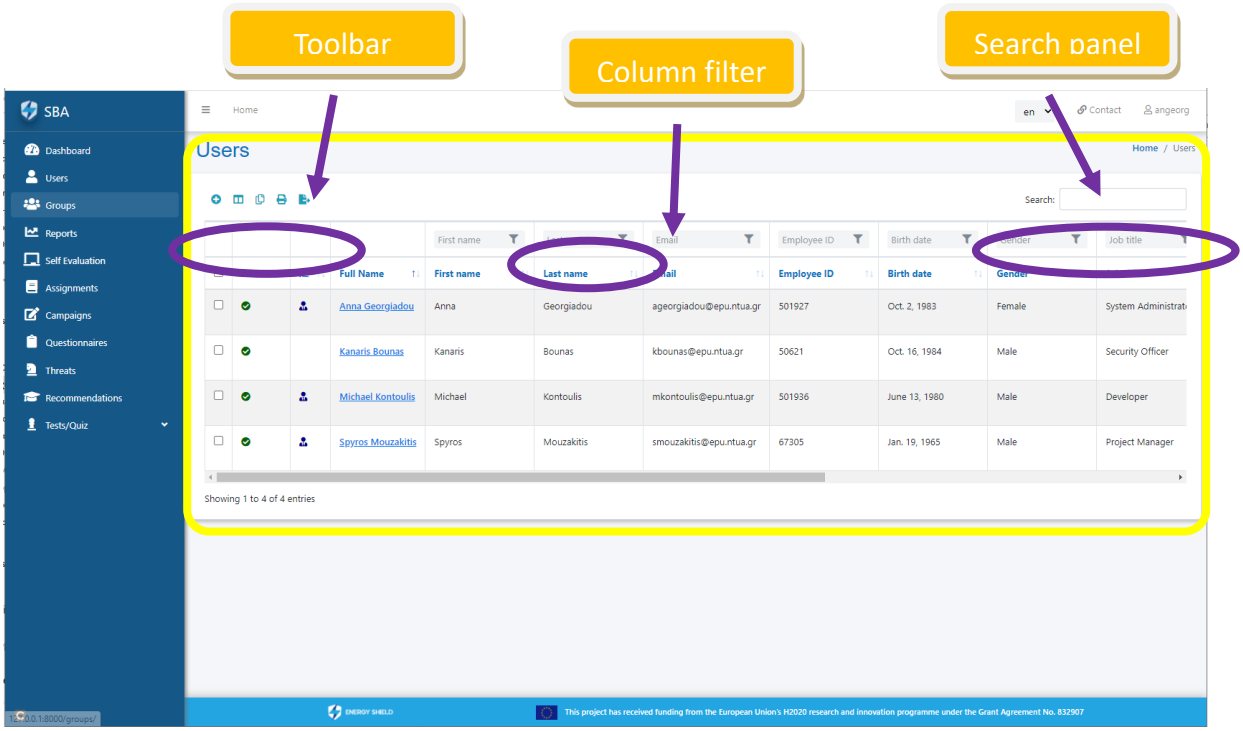


Fig 4. Users view

Selecting one of the displayed users (by clicking on their full name) redirects you to the user profile view, which, depending on access user role (administrator, manager or simple user) and privileges, presents user-specific information and offers a number of different control actions.

As presented in Fig 5, the user profile view contains:

- ***Summary panel***: generic user details (e.g. full name, job description)
- ***Personal Information Tab***: first and last name, contact details, organisation info, and so on.
- ***Account Tab*** (visible only to administrators): account privileges and group membership.
- ***Assignments*** (visible only to administrators or profile owners): table view of all user assignments (completed, expired, pending) with score achievement, completion and expiration date and redirection link to assignment execution.

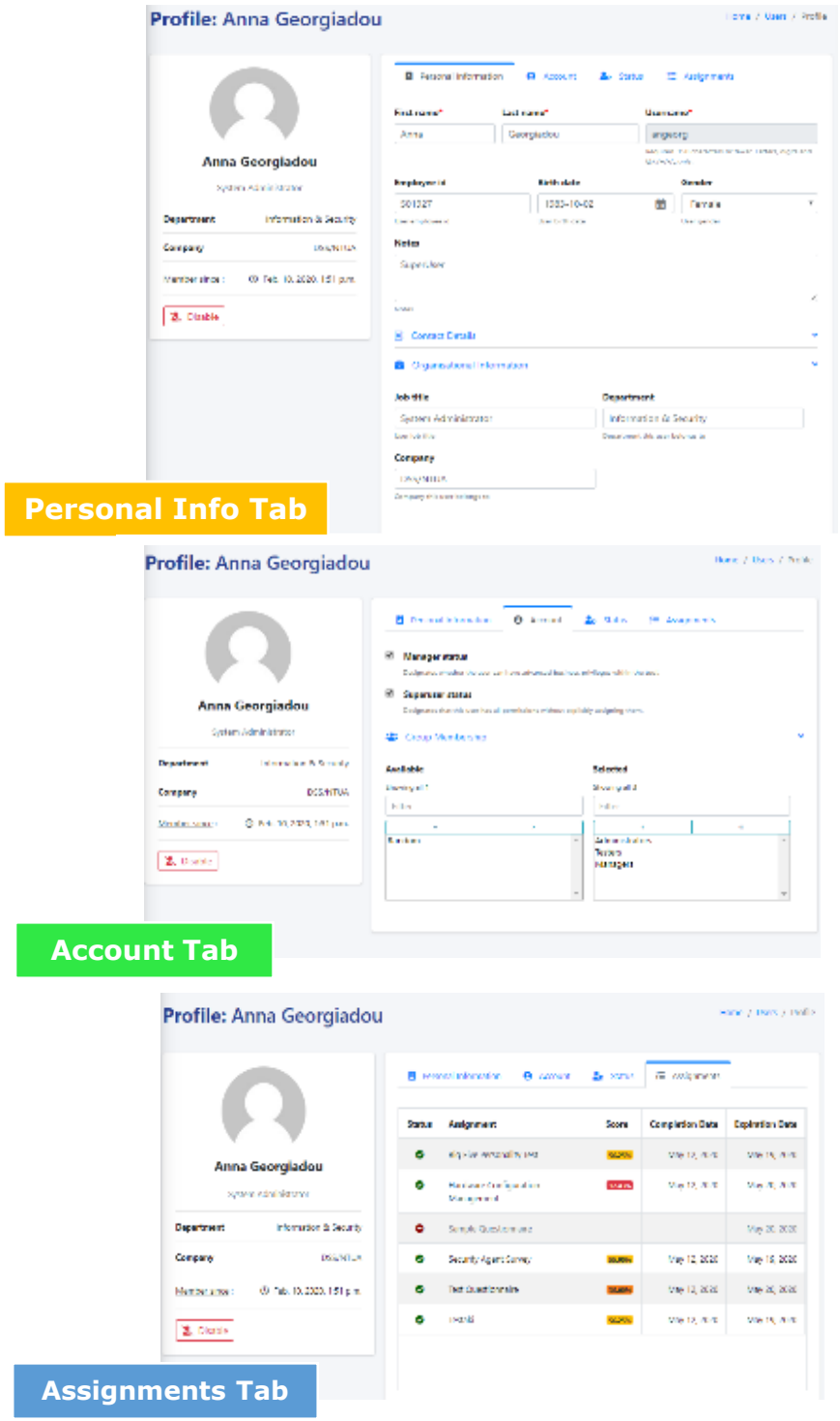


Fig 6. User profile view

For the creation of a new user, two options are available:

- ***Signup form*** (Fig 7): link to a specific form could be distributed via any corporate tool or simply via email. Users need to complete their first and last name,

username and password and an email, which shall be used as a security verification control, to sign up to the SBA tool and gain access as simple users.

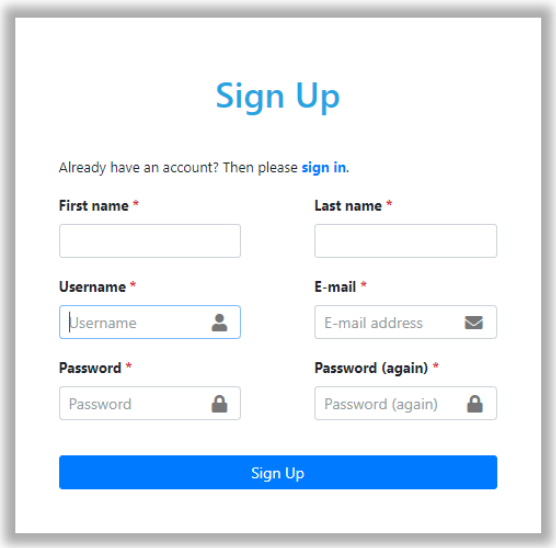


Fig 8. Sign-up view

- ***Create new user wizard*** (available only to administrators): accessible via the users and groups view toolbar (Fig 9). The wizard guides you through the creation procedure of a new user offering the possibility to complete both required and optional fields. Upon successful completion, a verification email is sent to the newly created user, and confirmation is expected for the account to be accessible.

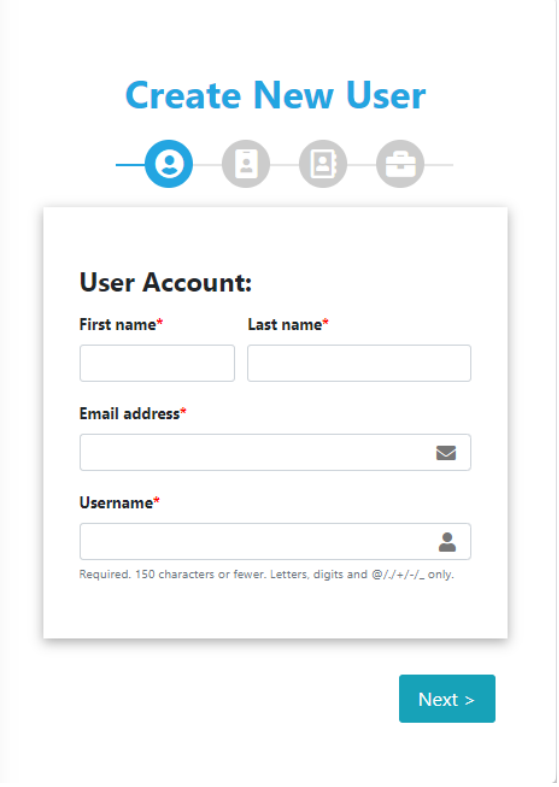


Fig 10. Create new user wizard

3.3. Groups

This view (visible only to administrators and managers) displays groups' information in a responsive table offering searching and multiple column filtering capabilities, as presented in Fig 11. The toolbar present in the upper left part contains the following buttons:

- ***Add***: dropdown menu allowing creations of new user and group.
- ***Show/Hide columns***: control over column visibility.
- ***Copy***: copies selected table rows and columns to clipboard.
- ***Print***: prints selected table rows and columns while invoking the web browser print menu.
- ***Export to file***: dropdown menu allowing the export of the selected table rows and columns to different file formats (Excel, CSV and PDF).

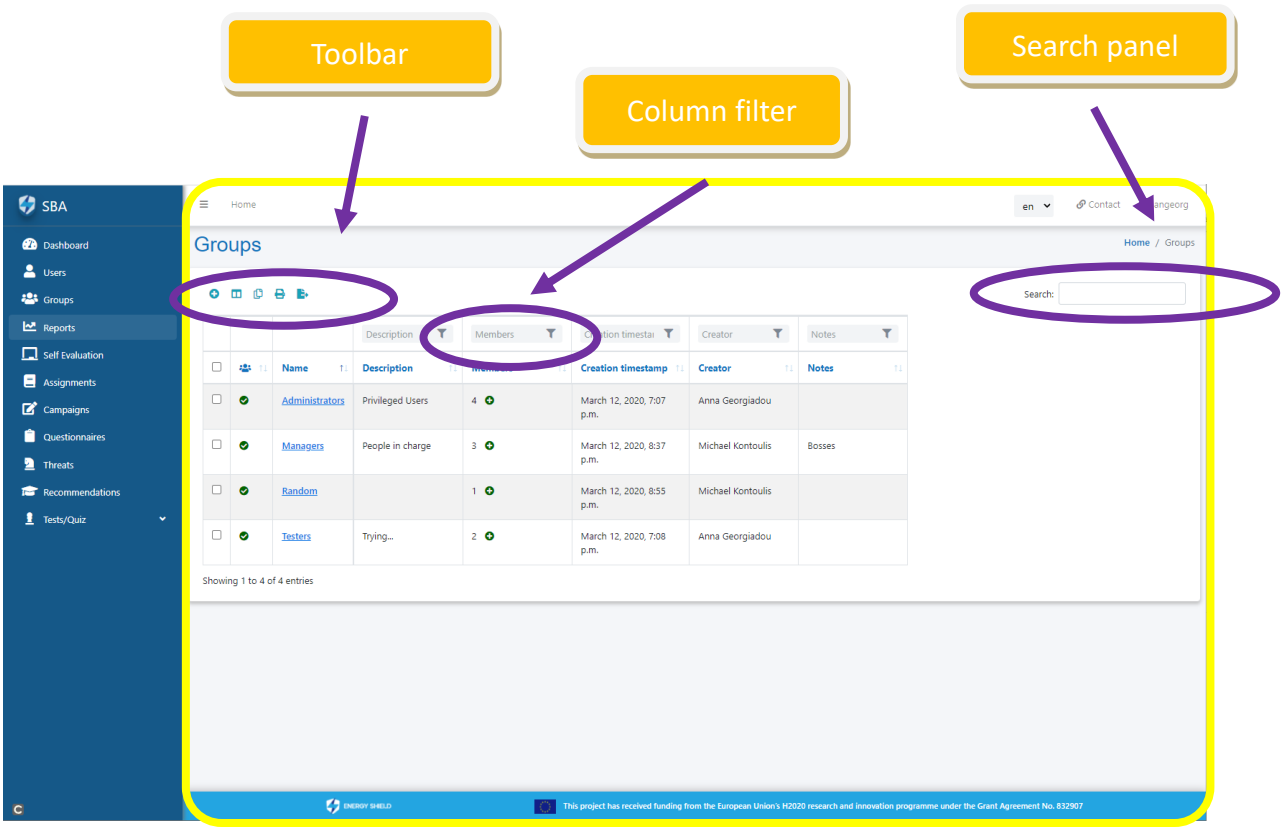


Fig 12. Groups view

Groups view exhibits ***global groups*** (description used for groups created by the administrators of the tool) to all users. If the signed-in user is a manager, along with global groups, the table also contains the groups created by the specific user. Administrators, as expected, have access and view to all groups available.

Selecting one of the displayed groups (by clicking on its name) redirects you to the group details view, which presents group-specific information and offers a number of different control actions.

As presented in Fig 13, the group details view contains:

- ***General Information Tab***: name, creation details, description, and so on.
- ***Members Tab***: members of the group.

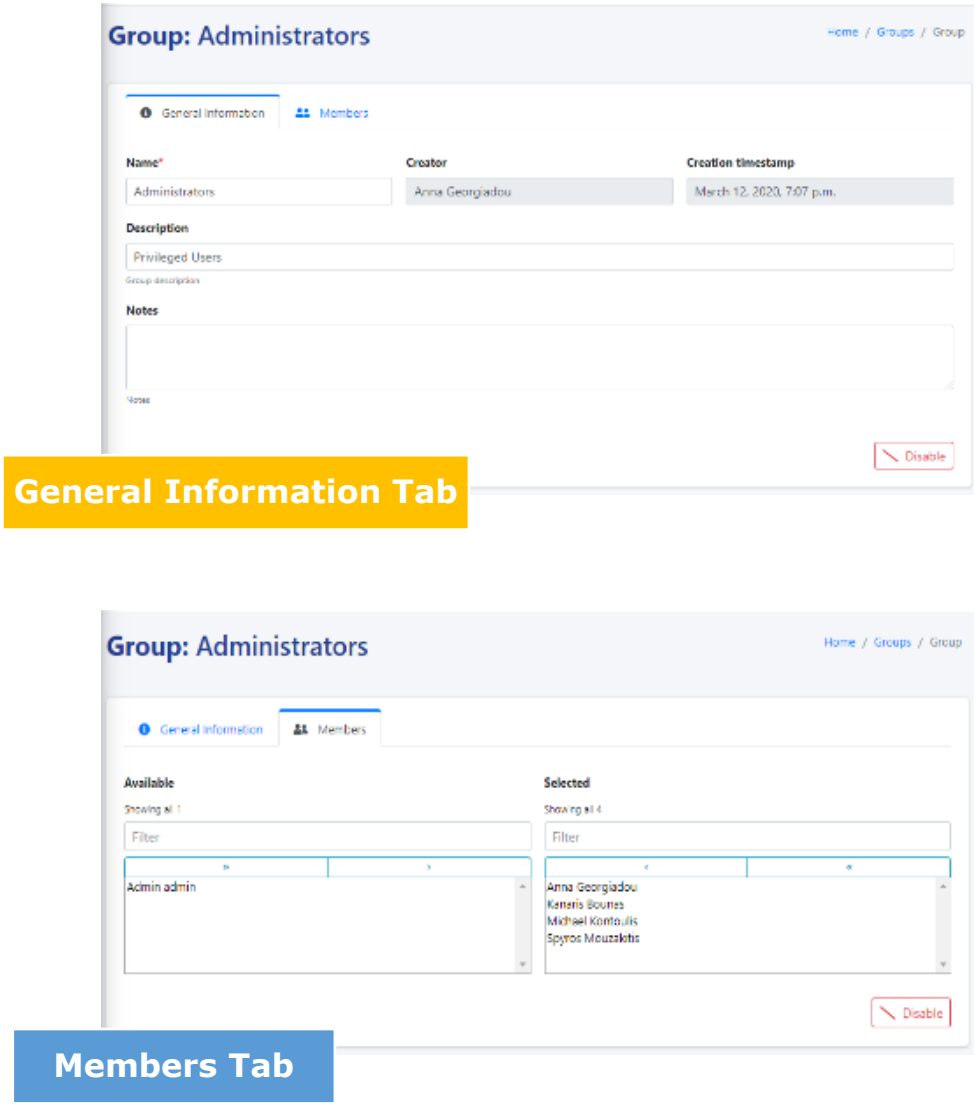


Fig 13. Group details view

The ***Create new group wizard*** is accessible via the users and groups view toolbar (Fig 14). The wizard guides you through the creation procedure of a new group offering the possibility to complete both required and optional fields.

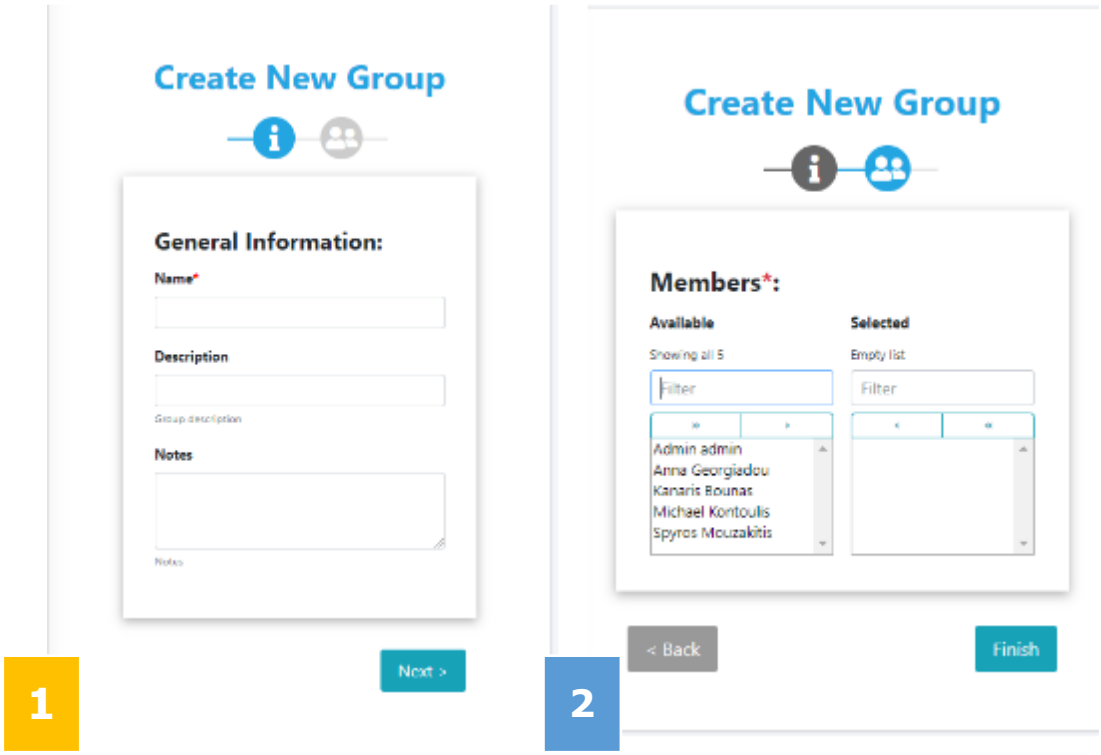


Fig 14. Create new group wizard

3.4. Reports

This view offers access to the reporting and visualisation mechanism of the SBA tool. The displayed information is properly filtered depending on user role and privileges guiding the user through the creation of a suitable security culture assessment analysis report.

As presented in

, this view consists of three main parts:

- ***Criteria panel (visible only to manager and administrators):*** user can select to create an organisation, campaign or group report by making the corresponding choice from the drop-down menu. Depending on the selection, the rest of the panel is updated to demonstrate available options. A level filter is also present in all cases to allow isolation of the different security culture levels (organisational and individual). At the bottom of the criteria panel, a time slide bar enables the user to further trim reported data adjusting time window (starting from a 24-months period). Having inserted desired reporting criteria, the user may preview security dimensions status by simply clicking on the "*Update Charts*" button. "*Calculation info*" button pops up a new window offering a detailed preview of the survey responses that were used for the calculation of the metrics displayed on the charts. More specifically, calculation info is divided into the cyber-security culture model dimensions and domains and reach down to a questionnaire level.
- ***Security Dimensions board:*** contains a responsive vertical bar chart of the cyber-security dimensions. In the case of a simple user, it is limited down to security culture individual-level dimensions demonstrating data for the specific user while, for managers and administrators, charts are formulated based on the

criteria panel. Hovering over any element of the chart gives an overview of its details, while clicking on it updates the ***Domains board*** accordingly. At the upper right corner of the board, an export button is available, offering a variety of formatting options (image, data, print).

- ***Domains board:*** contains a horizontal bar chart of the cyber-security domains related to the selected dimension. At the upper right corner of the board, an export button is available, offering a variety of formatting options (image, data, print).

Fig 15. Reports view

3.5. Self Evaluation

This view offers access to the self-evaluation mechanism of the SBA tool. It displays a self-evaluation history log containing all surveys completed by the sign-in user along with

an achievement score and the affected security culture dimensions and domains as presented in Fig 16.

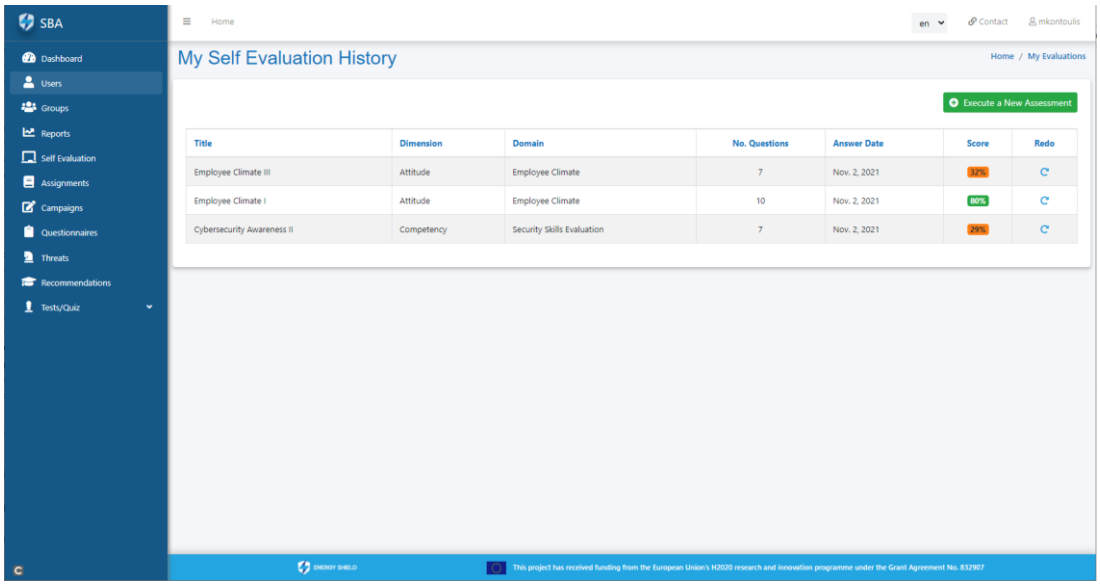


Fig 16. Self-evaluations view

On the upper right part, an "Execute a New Assessment" button is available, redirecting the user to the self-evaluation view presented in Fig 17, which displays all available individual level questionnaires along with a number of security culture model correlation details and the highest related achievement score. The users can preview their cyber-security performance status and exercise via triggering the execution of any of the available assessment questionnaires by simply clicking on the questionnaire of interest.

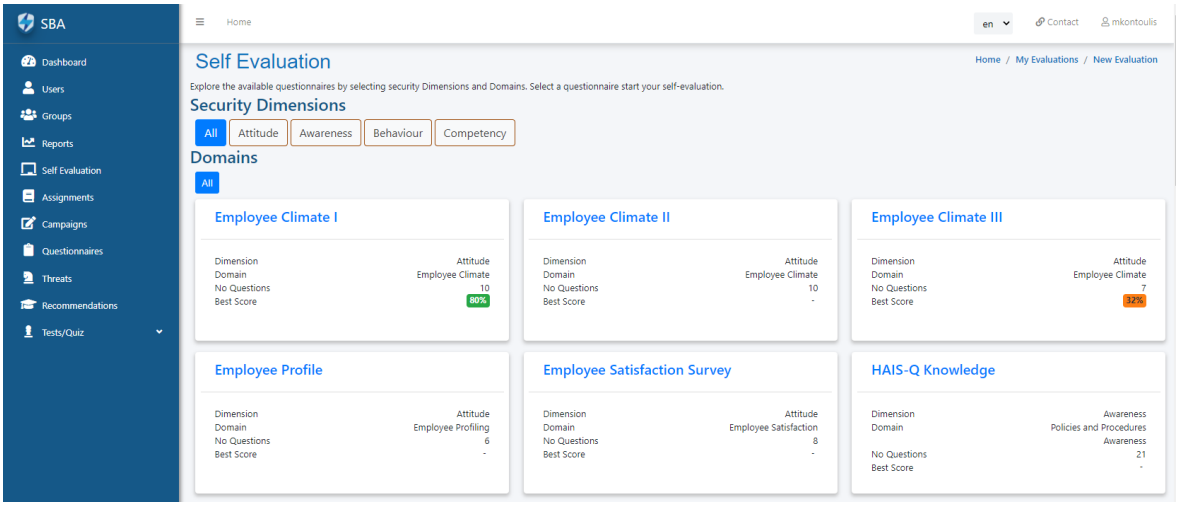


Fig 17. Execute new assessment view

3.6. Campaigns

This view (available only to administrators and managers) displays campaigns' information in a table as presented in Fig 18.

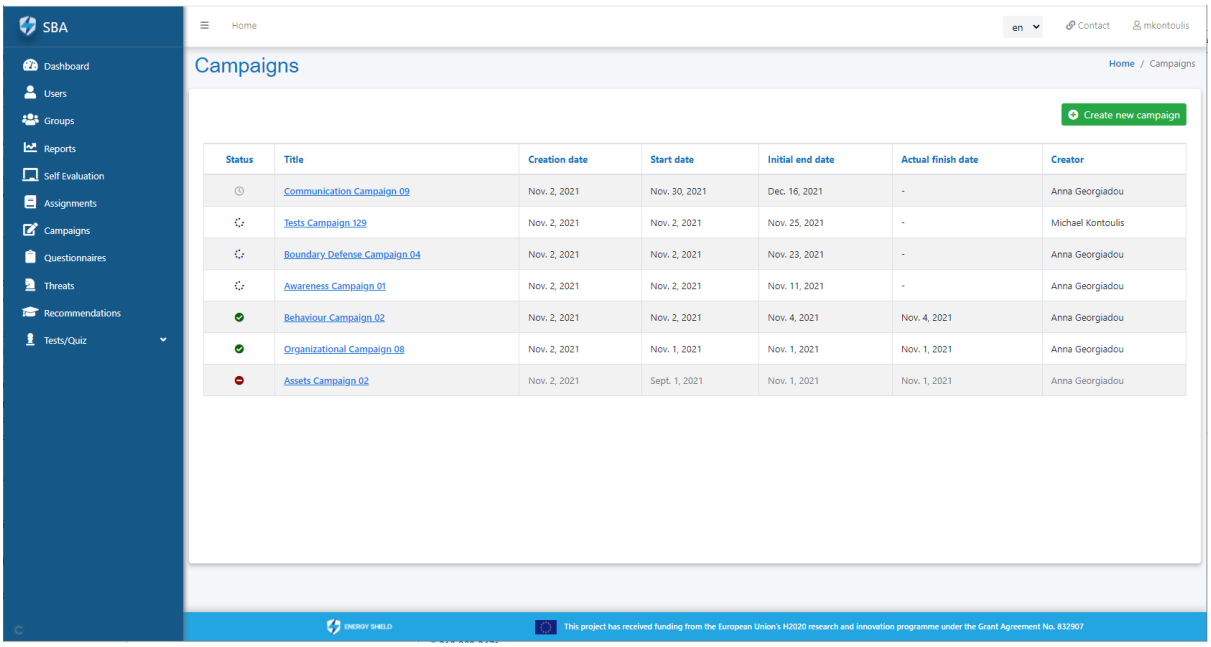


Fig 18. Campaigns view

The campaigns' view exhibits ***global campaigns*** (description used for campaigns created by the administrators of the tool) to all users. If the signed-in user is a manager, along with global campaigns, the table also contains the campaigns created by the specific user. Administrators, as expected, have access and view to all campaigns available.

Selecting one of the displayed campaigns (by clicking on its title) redirects you to the campaign details view, which presents campaign-specific information and offers a number of different control actions.

As presented in Fig 19, the campaign details view contains:

- ***General Information Tab***: title, creation details, start and end date, questionnaires and tests assigned and participants.
- ***Results Tab***: summary of the results per user along with progress status.
- ***Threats Tab***: summary of the identified cyber-security threats based on the evaluation results of the campaign.

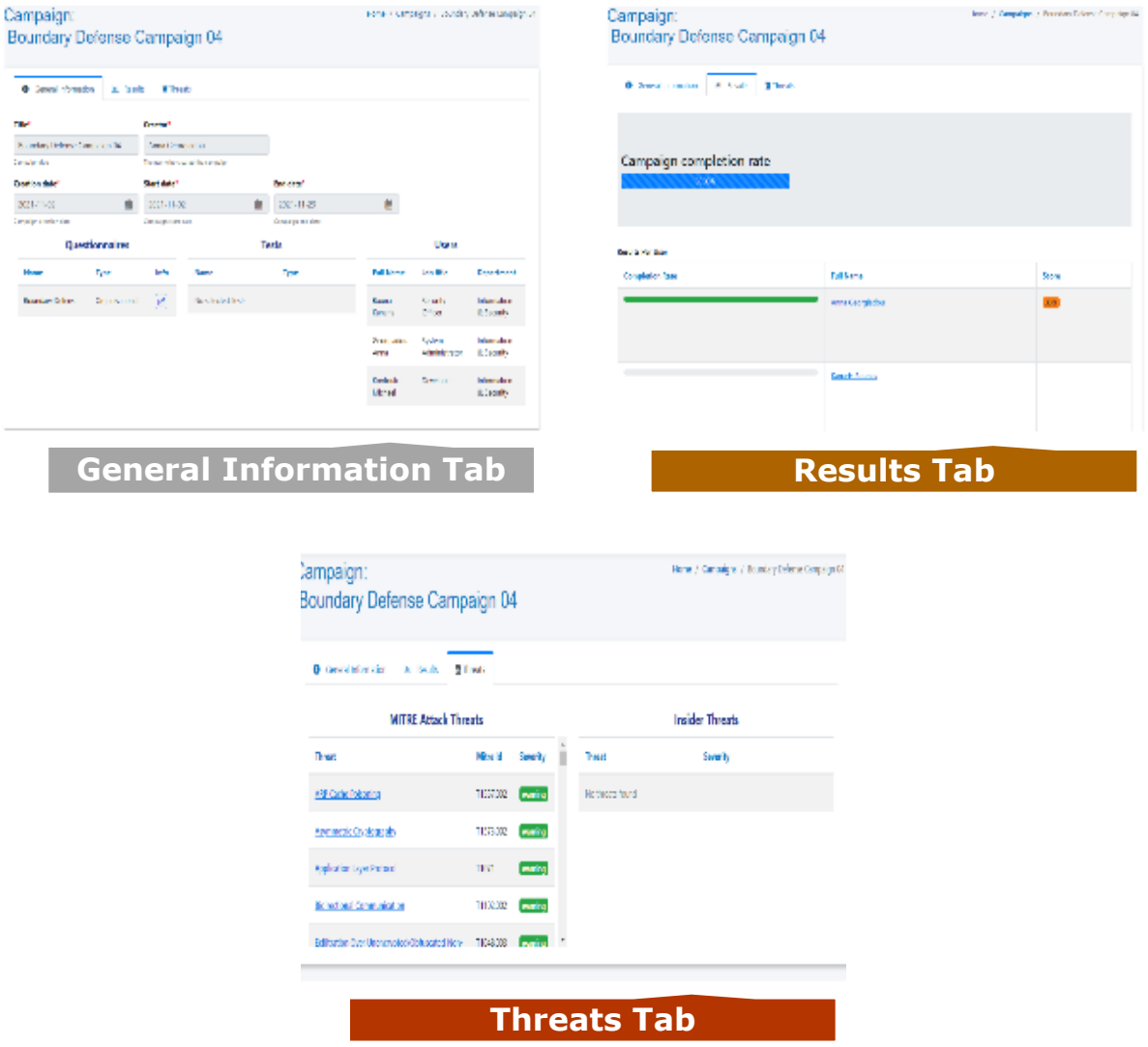


Fig 19. Campaign details' view

On the upper right part of the campaigns view, a "Create New Campaign" button is available, redirecting the user to the creation view presented in

. This view consists of:

- ***Assignment card***: presents, in a tree view, the available questionnaires, tests, users and groups. Selecting any of these results in listing them on the lower part of the card while making correlated assignments between security culture controls and the corresponding campaign participants.
- ***Campaign details card***: holds the campaign title along with the start and end date of the assessment period.

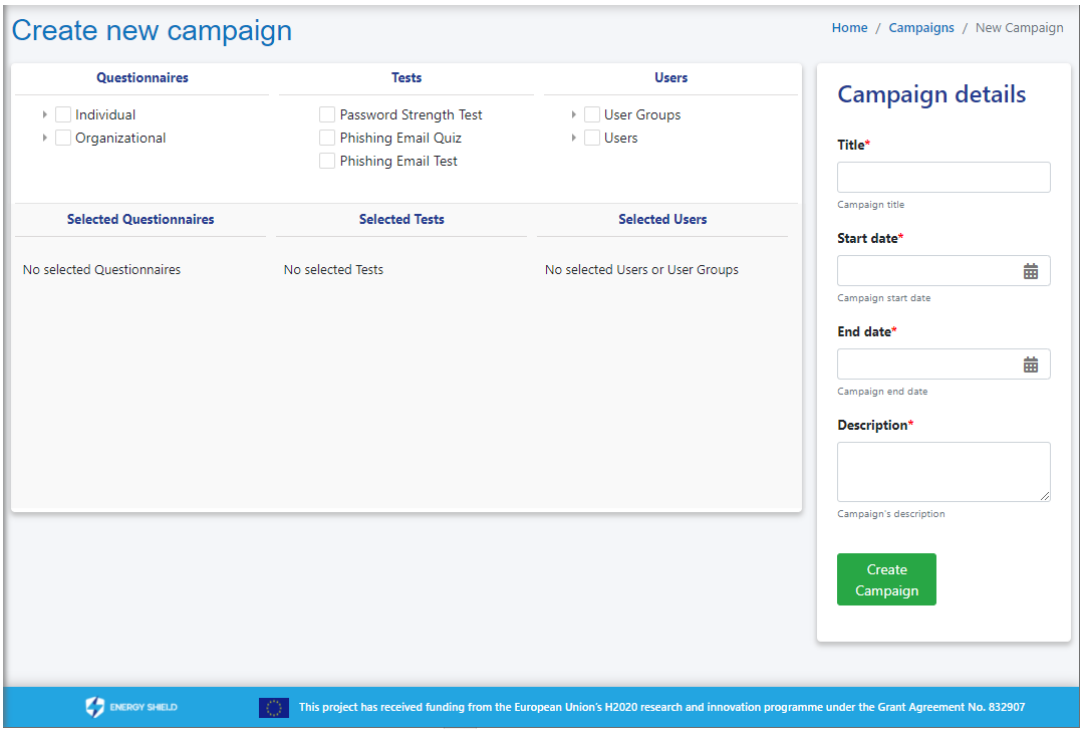


Fig 20. Create new campaign view

Upon creation of a campaign, a number of assignments are created and presented to the corresponding assignees through alternative paths, as follows:

- ***Dashboard –> Assignments Card***: presents and offers access to active assignments. Additionally, it lists the completed and expired ones in different tabs.
- ***User profile -> Assignment Tab***: presents user assignments along with a number of details offering access to the pending ones.
- ***Assignments***: presents all users assignments along with a number of details, such as status, due date, etc. (paragraph 3.7 presents in detail the specific view).

When an active assignment is selected by its assignee, if it refers to a questionnaire, the survey execution mechanism is triggered, and an evaluation iteration is initiated, guiding the user through its completion. Upon submission, an achievement score is presented to the end-user.

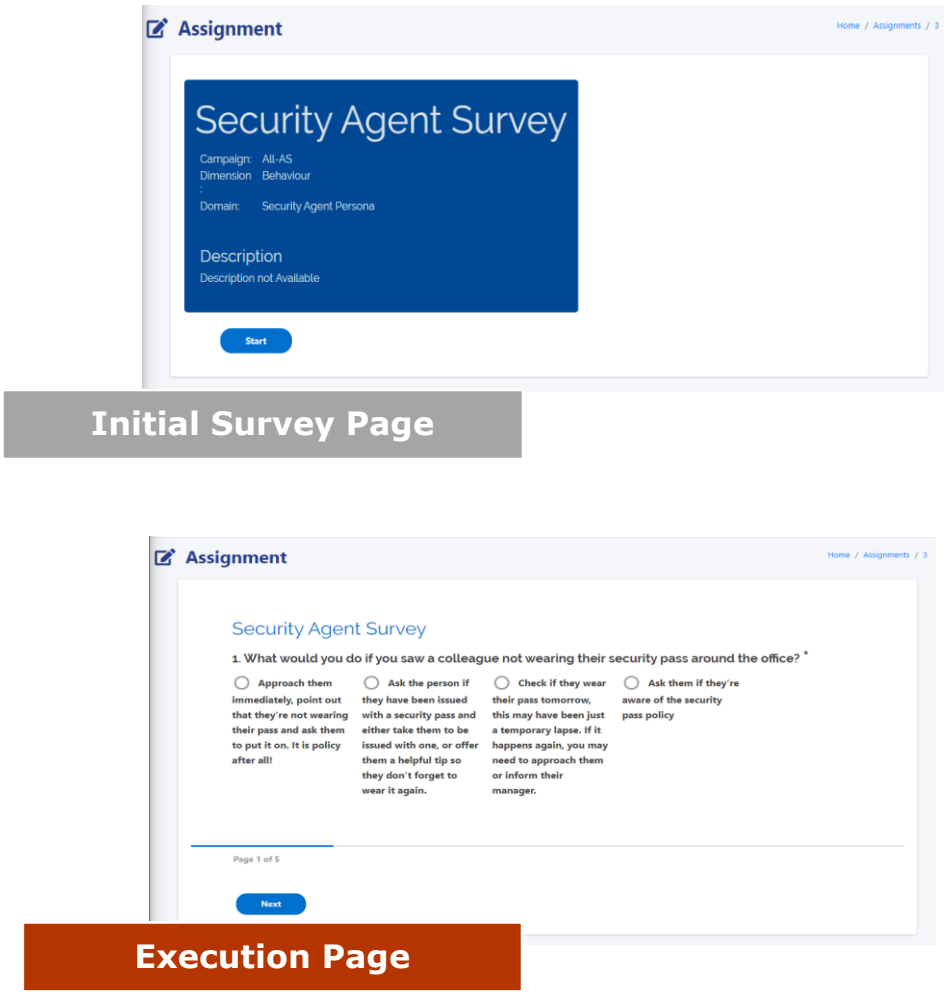


Fig 21. Questionnaire assignment execution

If the assignment refers to a test, then the corresponding test is initiated, guiding the user through its completion. Upon submission, an achievement score is presented to the end-user.

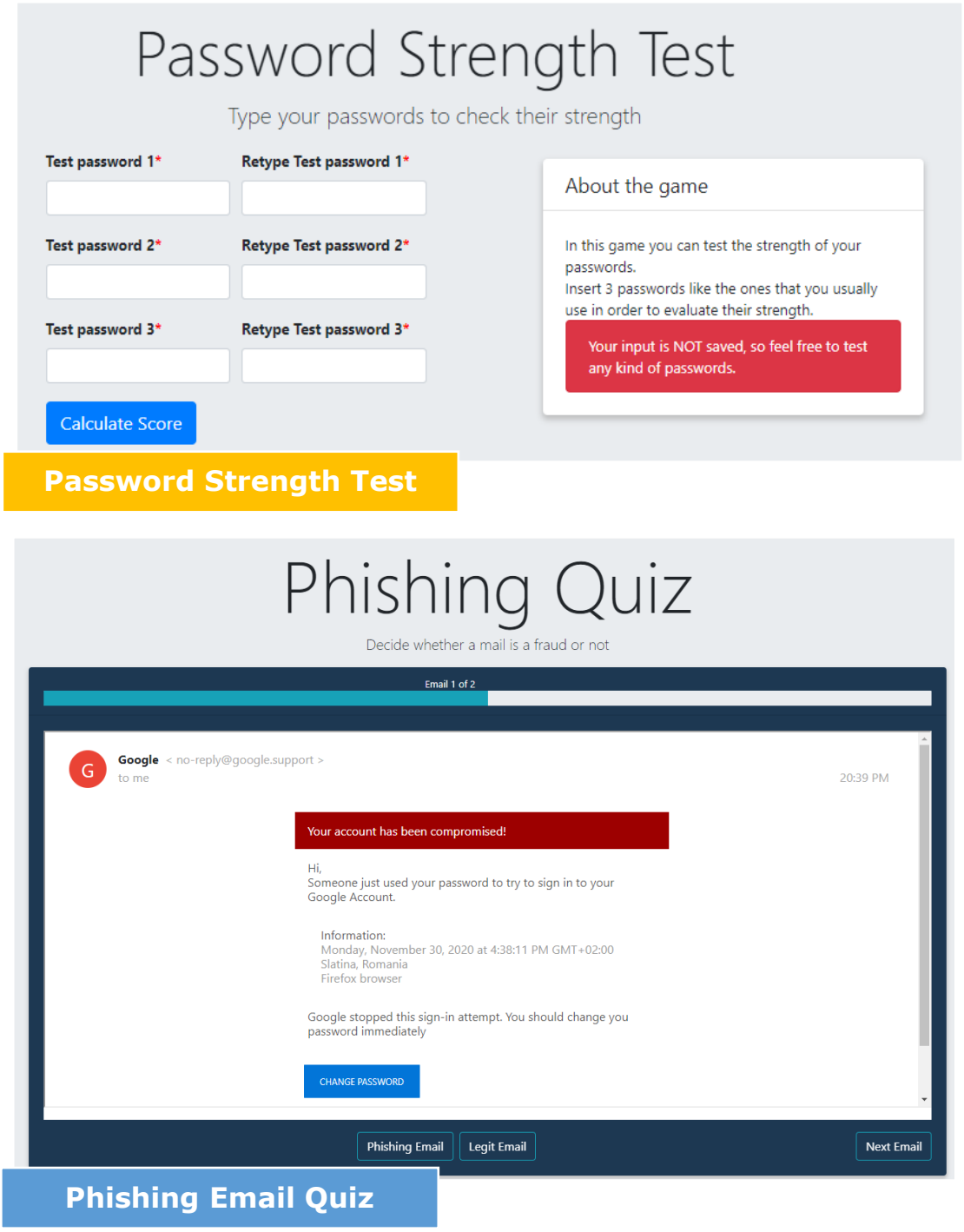


Fig 22. Test assignment execution

3.7. Assignments

This view displays all assignments, questionnaires and tests (apart from the phishing simulation test) made to the signed-in user via the different campaigns they are participating in. In case the same questionnaire or test is assigned to them via different campaigns more than once during the same period, the tool ensures the user completes only once the assignment and the corresponding score is used in all related metrics.

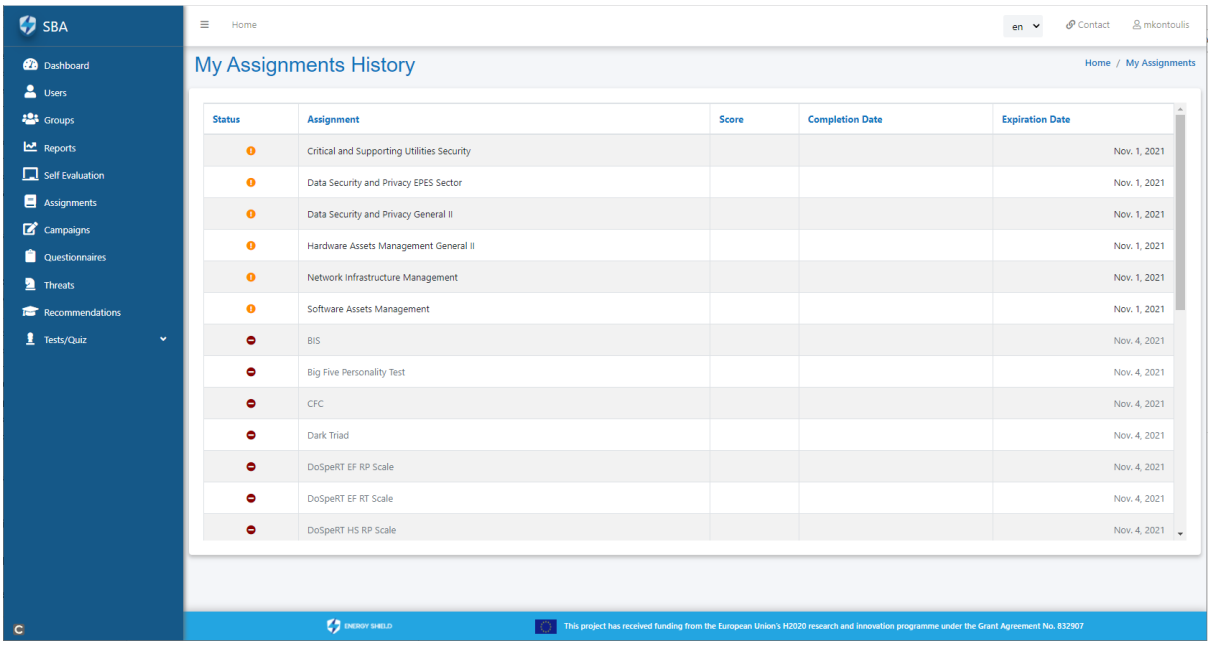


Fig 23. Assignments view

If an active assignment is selected, by clicking on its hyperlinked title, the survey or the test execution mechanism is triggered, depending on the nature of the assignment, and an evaluation iteration is initiated guiding the user through its completion.

3.8. Questionnaires

This view (available only to administrators and managers) displays the available cyber-security culture questionnaires while correlating them with the suggested model (levels, dimensions and domains) as presented in Fig 24.

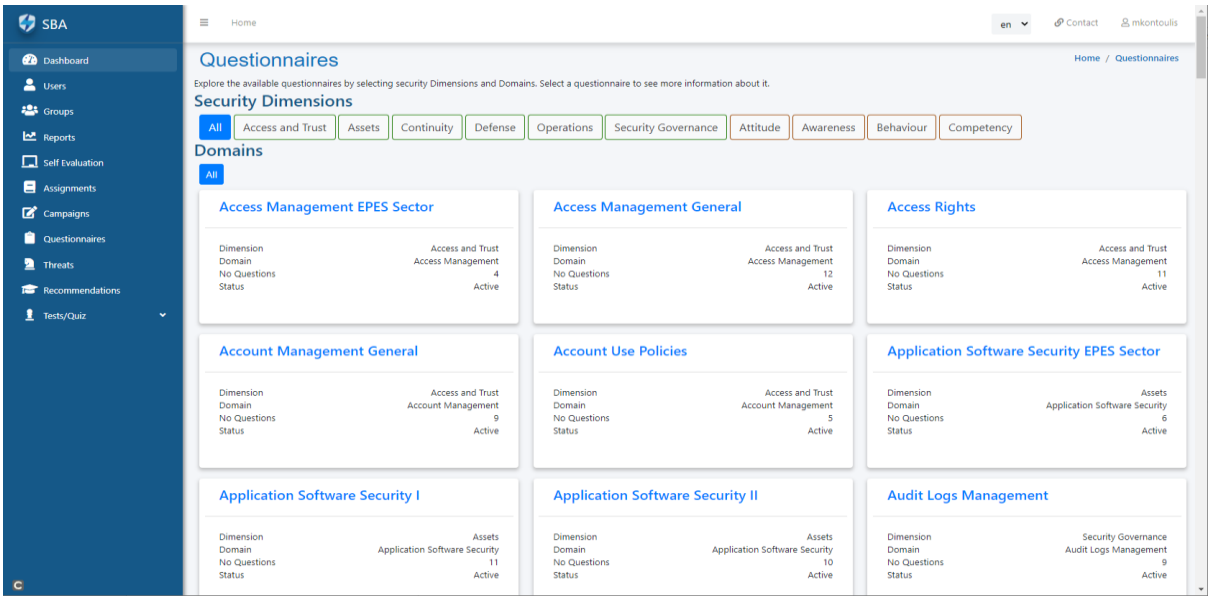


Fig 24. Questionnaires view

Selecting one of the displayed questionnaires (by clicking on its title) redirects you to the questionnaire details view, which presents questionnaire-specific information offering control over its activity status.

As presented in Fig 25, the questionnaire details view presents:

- Information correlating the questionnaire with the underlying cyber-security culture model.
- Questions along with their available options and control over their activity status.

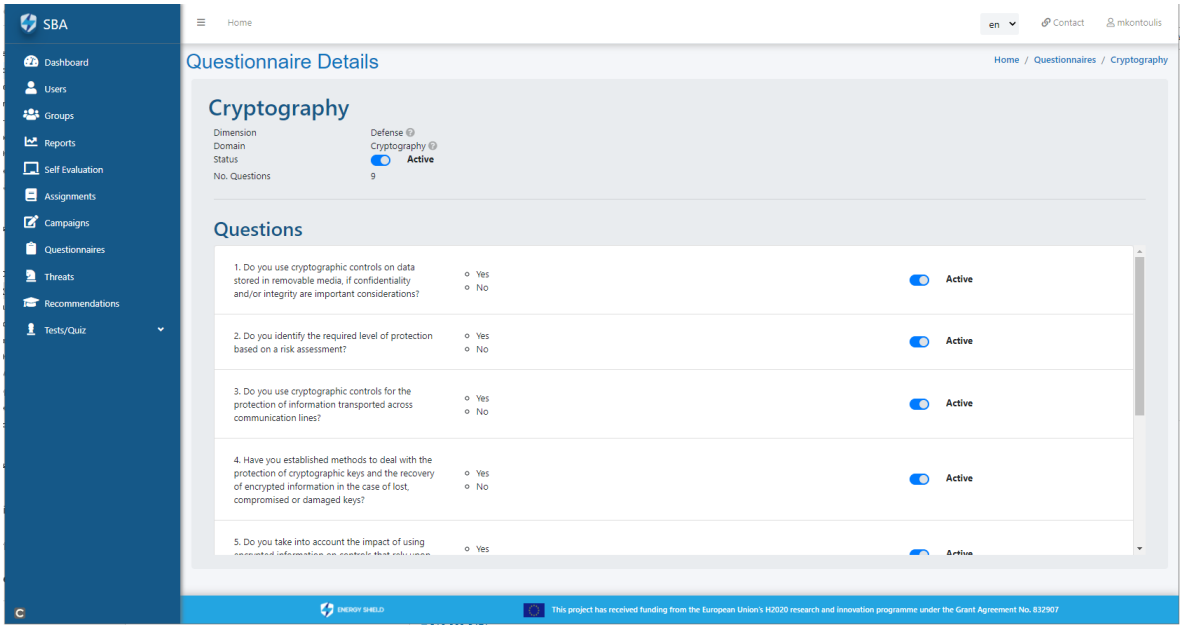


Fig 25. Questionnaire details view

3.9. Threats

This view (available only to administrators and managers) displays the identified cyber-security threats the organisation is vulnerable against based on the evaluation campaigns held.

As presented in Fig 27, the recommendations view contains:

- ***MITRE ATT&CK Tab***: listing all identified threats based on the hybrid MITRE ATT&CK Model for an OT Environment, consisting of a combination of the Enterprise and the ICS threat model. The specific tab enables the user to further investigate the attack patterns by offering an interconnection with the MITRE ATT&CK official website.
- ***Insider Tab***: listing all identified insider threats based on the MERIT model developed by the Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University.

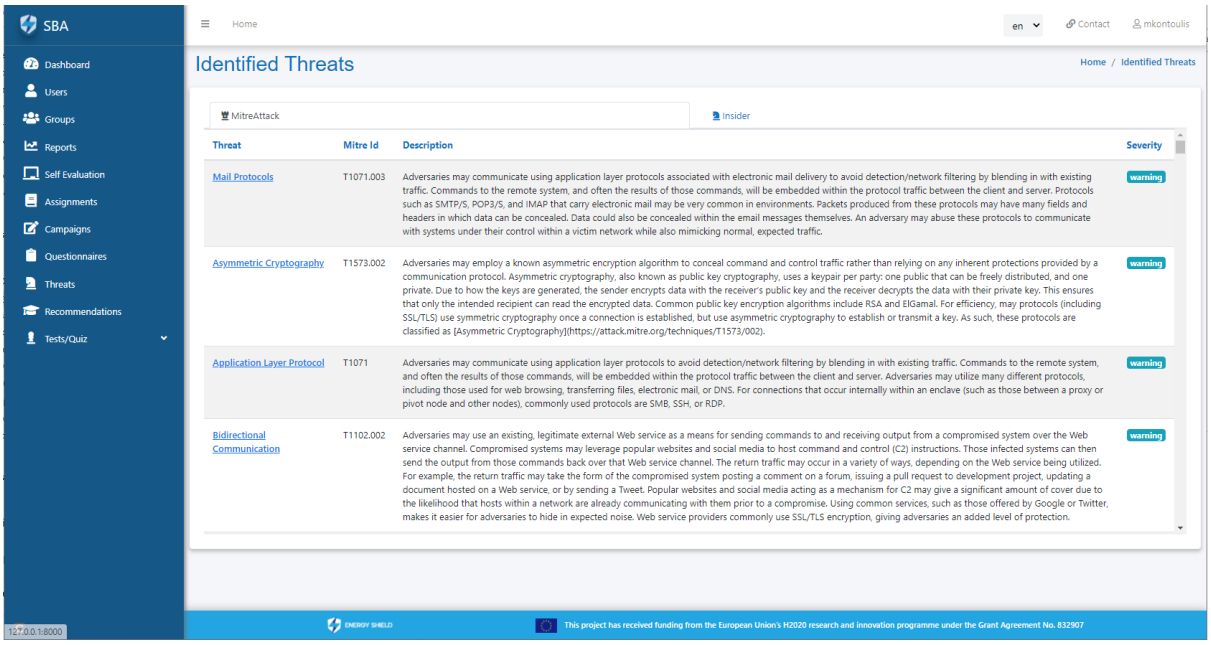


Fig 26. Threats view

3.10. Recommendations

This view (available only to administrators and managers) displays a number of training recommendations aiming to assist the organisation in enhancing its cyber defence against the identified threats.

As presented in
, the recommendations view contains:

- ***General Recommendations Tab***: listing training recommendations encompassing three aspects of the organisation:
  - Insider Threat Awareness Training for all organisational personnel (employees, contractors, consultants)
  - Training for Insider Threat Program personnel
  - Role-based training for mission specialists that are likely to observe certain aspects of insider threat events, e.g.:
    - Human Resources
    - Information Assurance
    - Compliance Inspection
    - Legal Counsel
    - Behavioural Sciences
    - Information Governance
    - Finance
- ***Insider Recommendations Tab:*** listing training recommendations targeting the cyber-security threats the organisation is prone against based on the evaluation campaigns results.

- ***Games:*** listing a number of free online games where users can cultivate their cyber-security culture while playing and enjoying themselves. The specific games have been developed by security experts, agencies and educational institutions targeting individuals of different ages, nationalities, cultures and professional backgrounds.

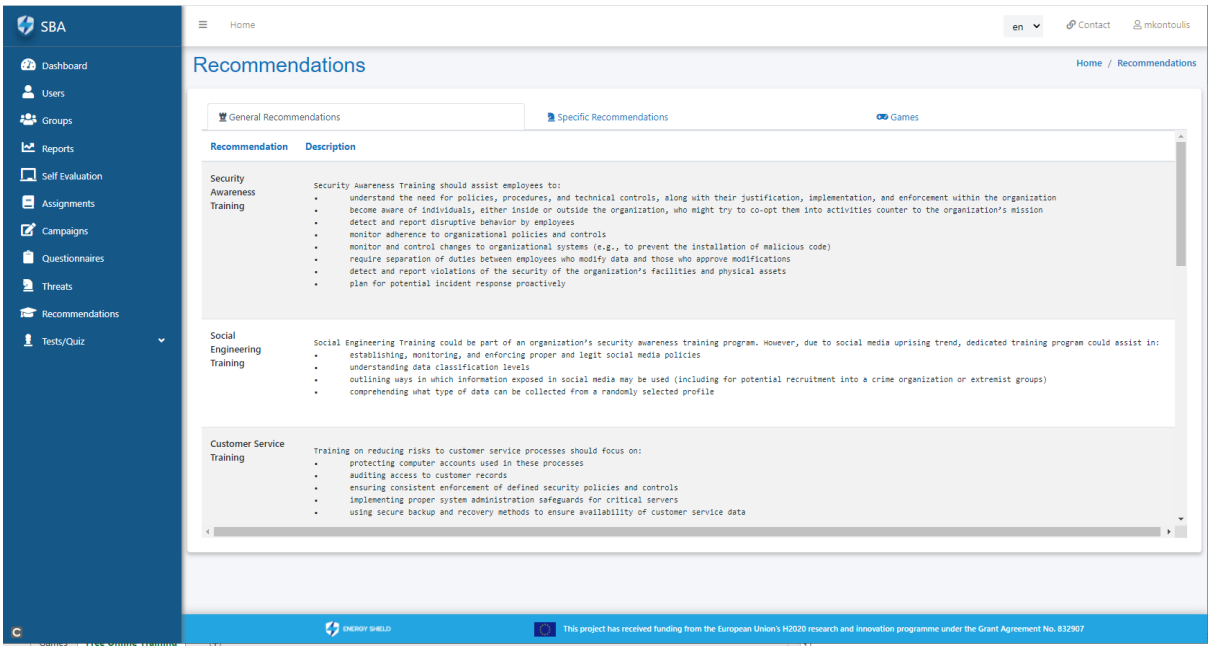


Fig 27. Recommendations view

3.11.Tests/Quiz

This view (available only to administrators and managers) offers a workspace where a user can customise the available tests to better address the organisational needs. This menu offers the following options:

- ***Phishing Quiz Creation Form***: this form allows the user to create a new email entry which shall later on become available for usage to the Email Phishing Quiz. Information required includes the sender email and display name, the email title, a phishing flag indicating whether the email is legit or not and an email file (UTF-8 encoded HTML file). When all information is filled in, an email preview offers the possibility to the user to overview the result prior to uploading it to the SBA tool.
- ***Phishing Simulation Creation Form***: this form allows the user to create a new email entry which shall later on become available for usage to the Email Phishing Simulation. Information required includes the email title, the email subject and an email file (UTF-8 encoded HTML file). The email file needs to be properly edited prior to uploading so as to include the encrypted link provided within the form. If not, an error message shall inform the user that the email file does not meet the required specifications. When all information is provided appropriately, an email preview offers the possibility to the user to overview the result prior to uploading it to the SBA tool.

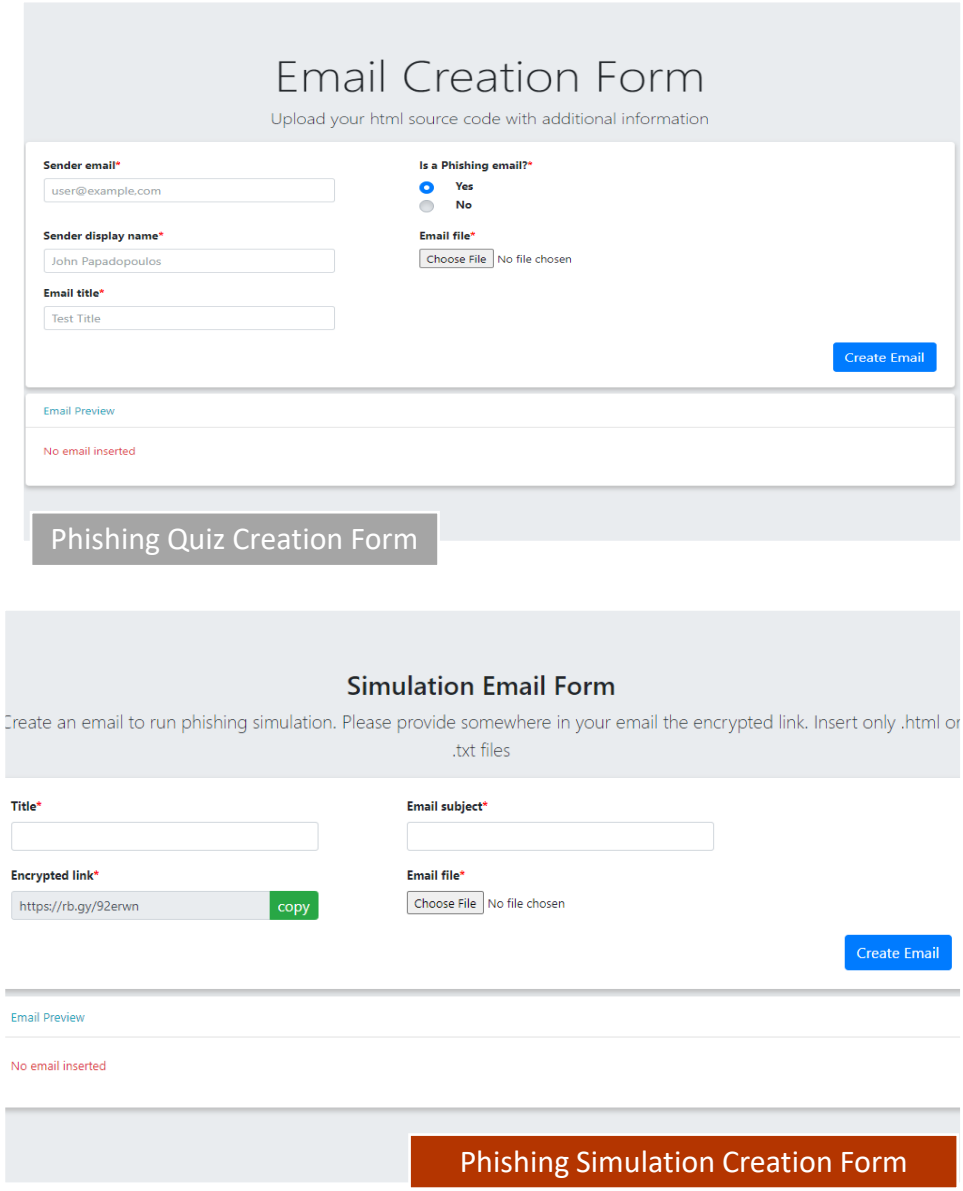


Fig 28. Test/Quiz views

The uploaded emails, in both cases, become instantly available for selection to the campaign creation form (tests submenu).

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΔΗΜΟΣΙΕΥΜΕΝΟ ΕΡΓΟ

Δημοσιεύσεις σε Επιστημονικά Περιοδικά

- Georgiadou, A., Mouzakitis, S., Bounas, K. & Askounis, D. (2020) A Cyber-Security Culture Framework for Assessing Organization Readiness, Journal of Computer Information Systems, 62:3, 452-462. DOI: 10.1080/08874417.2020.1845583, Impact Factor (2021): 3.317
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Designing a cyber-security culture assessment survey targeting critical infrastructures during COVID-19 crisis. International Journal of Network Security & Its Applications (IJNSA) Vol, 13 (1). DOI: 10.5121/ijnsa.2021.13103
- Georgiadou, A., Mouzakitis, S. & Askounis, D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal (2021). DOI: 10.1057/s41284-021-00286-21845583, Impact Factor (2021): 1.701
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Detecting Insider Threat via a Cyber-Security Culture Framework. Journal of Computer Information Systems, 1-11. DOI: 10.1080/08874417.2021.1903367, Impact Factor (2021): 3.317
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a Cyber-Security Culture Framework. Sensors, 21(9), 3267. DOI: 10.3390/s21093267, Impact Factor (2021): 3.847
- Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Doukas G., Ntanos C., Landeiro Ribeiro L. & Askounis D. (2021, October). Hospitals' Cybersecurity Culture during the COVID-19 Crisis. In Healthcare (Vol. 9, No. 10, p. 1335). Multidisciplinary Digital Publishing Institute. DOI: 10.3390/healthcare9101335, Impact Factor (2021): 3.160
- Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas G., Kontoulis M., Nikoloudakis Y., Marin S., Cabecinha R. & Ntanos, C. (2022, February). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. In Healthcare (Vol. 10, No. 2, p. 327). MDPI. DOI: 10.3390/healthcare10020327, Impact Factor (2021): 3.160
- Georgiadou, A., Michalitsi-Psarrou, A., & Askounis D. 2022. A Security Awareness and Competency Evaluation in the Energy Sector (accepted for publication)

Δημοσιεύσεις σε Βιβλία

- Georgiadou A., Kokkinakos P., Panopoulos D., Koussouris S., Askounis D. (2013) A Multicriteria Methodology for the Selection and Prioritisation of Public Services. In: Douligeris C., Polemi N., Karantjias A., Lamersdorf W. (eds) Collaborative, Trusted and Privacy-Aware e/m-Services. I3E 2013. IFIP Advances in Information and Communication Technology, vol 399. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-37437-1_27

Δημοσιεύσεις σε Πρακτικά Συνεδρίων

- K. Bounas, A. Georgiadou, M. Kontoulis, S. Mouzakitis, D. Askounis (2020), Towards a CyberSecurity Culture Tool Though a Holistic, Multi-Dimensional Assessment Framework, 13th IADIS International Conference Information Systems 2020, p.135-139, Sofia, 2020. ISBN: 978-989-8704-15-3
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2020). Towards Assessing Critical Infrastructures Cyber-Security Culture During Covid-19 Crisis: A Tailor-Made Survey. arXiv preprint arXiv:2012.13718
- Hacks, S., Butun, I., Lagerström, R., Buhaiu, A., Georgiadou, A., & Michalitsi Psarrou, A. (2021, August). Integrating Security Behaviour into Attack Simulations. In The 16th International Conference on Availability, Reliability and Security (pp. 1-13). DOI: 10.1145/3465481.3470475
- Touloumis, K., Michalitsi-Psarrou, A., Kapsalis, P., Georgiadou, A., & Askounis, D. (2021, December). Vulnerabilities Manager, a platform for linking vulnerability data sources. In 2021 IEEE International Conference on Big Data (Big Data) (pp. 2178-2184). IEEE. DOI: 10.1109/BigData52589.2021.9672026
- Georgiadou, A., Michalitsi-Psarrou, A., & Askounis D. 2022. Evaluating The Cyber-Security Culture of the EPES Sector: Applying a Cyber-Security Culture Framework to assess the EPES Sector's resilience and readiness. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery, New York, NY, USA, Article 77, 1–10. DOI: 10.1145/3538969.3543813
- Georgiadou, A., Michalitsi-Psarrou, A., & Askounis D. 2022. Cyber-Security Culture Assessment in Academia: A COVID-19 Study: Applying a Cyber-Security Culture Framework to assess the Academia's resilience and readiness. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery, New York, NY, USA, Article 126, 1–8. DOI: 10.1145/3538969.3544467
- K. Touloumis, A. Michalitsi-Psarrou, A. Georgiadou and D. Askounis, "A tool for assisting in the forensic investigation of cyber-security incidents," 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 2022, pp. 2630-2636, doi: 10.1109/BigData55660.2022.10020208
- Pelekis, S., Sarmas, E., Georgiadou, A., Karakolis, V., Ntanos, C., Dimitropoulos, N., Korbakis, G. & Doukas, C. 2022. TWINP2G: A digital twin architecture for optimal pOWER-TO-GAS planning. In e-Society 2023 (accepted for publication)